Muster

AWS Prescriptive Guidance

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Prescriptive Guidance: Muster

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

AWS Präskriptive Beratungsmuster 1
Cloud-Grundlagen 3
Automatisieren Sie die Kontoerstellung mit dem Landing Zone Accelerator auf AWS 4
Übersicht 4
Voraussetzungen und Einschränkungen 4
Architektur 5
Tools 6
Bewährte Methoden 9
Epen 10
Zugehörige Ressourcen 37
Zusätzliche Informationen 37
Automatische Inventarisierung von AWS Ressourcen 39
Übersicht 39
Voraussetzungen und Einschränkungen 40
Architektur 41
Tools 42
Bewährte Methoden 43
Epen 43
Fehlerbehebung 50
Zugehörige Ressourcen 51
VPC-Flow-Logs kontenübergreifend konfigurieren 52
Übersicht 52
Voraussetzungen und Einschränkungen 52
Architektur 53
Tools 54
Bewährte Methoden 54
Epen 56
Zugehörige Ressourcen 58
Zusätzliche Informationen 59
Automatisches Markieren von Transit Gateway Gateway-Anhängen 61
Übersicht 61
Voraussetzungen und Einschränkungen 61
Architektur 61
Tools 63

Epen 65
Zugehörige Ressourcen 72
Mehr Muster 73
KI und maschinelles Lernen 74
Aggregieren Sie DynamoDB-Daten für ML-Prognosen in Athena 76
Übersicht 76
Voraussetzungen und Einschränkungen 76
Architektur 76
Tools 77
Epen 78
Zugehörige Ressourcen 91
Kontenübergreifend ein AWS CodeCommit Repository mit Amazon SageMaker AI Studio Classic verknüpfen 92
Übersicht 92
Voraussetzungen und Einschränkungen 92
Architektur 93
Tools 93
Epen 94
Zusätzliche Informationen 100
Automatisches Extrahieren von Inhalten aus PDF-Dateien 103
Übersicht 103
Voraussetzungen und Einschränkungen 103
Architektur 104
Tools 105
Epen 106
Zugehörige Ressourcen 112
Anlagen 112
Erstellen Sie mit SageMaker AI DeepAR ein Kaltstart-Prognosemodell 113
Übersicht 113
Voraussetzungen und Einschränkungen 113
Architektur 114
Tools 115
Bewährte Methoden 116
Epen 116
Zugehörige Ressourcen 118
Erstellen Sie einen MLOps Workflow mit SageMaker KI und Azure DevOps 119

Übersicht 119
Voraussetzungen und Einschränkungen 119
Architektur 120
Tools 122
Bewährte Methoden 123
Epen 124
Fehlerbehebung 134
Zugehörige Ressourcen 135
Konfigurieren Sie die Protokollierung in Amazon Bedrock mit CloudFormation 137
Übersicht 137
Voraussetzungen und Einschränkungen 137
Architektur 138
Tools 139
Epen 140
Zugehörige Ressourcen 143
Erstellen Sie Docker-Container SageMaker für das Modelltraining in Step Functions 145
Übersicht 145
Voraussetzungen und Einschränkungen 145
Architektur 146
Tools 146
Epen 147
Zugehörige Ressourcen 162
Erstellen Sie Zugriffskontrollen in Amazon EKS mit Amazon Bedrock-Agenten 163
Übersicht 163
Voraussetzungen und Einschränkungen 163
Architektur 164
Tools 165
Bewährte Methoden 166
Epen 166
Fehlerbehebung 187
Zugehörige Ressourcen 188
Stellen Sie einen RAG-Anwendungsfall bereit auf AWS 189
Übersicht 189
Voraussetzungen und Einschränkungen 189
Architektur 191
Tools 192

Bewährte Methoden 193
Epen 194
Zugehörige Ressourcen 197
Zusätzliche Informationen 198
Stellen Sie mehrere Pipeline-Modellobjekte auf einem einzigen Endpunkt bereit SageMaker ... 200
Übersicht 200
Voraussetzungen und Einschränkungen 200
Architektur 201
Tools 201
Epen 202
Zugehörige Ressourcen 212
Entwickeln Sie Chat-basierte KI-Assistenten mithilfe von RAG und Eingabeaufforderungen ReAct 213
Übersicht 213
Voraussetzungen und Einschränkungen 214
Architektur 215
Tools 216
Bewährte Methoden 218
Epen 219
Fehlerbehebung 226
Zugehörige Ressourcen 226
Zusätzliche Informationen 227
Entwickeln Sie mit Amazon Bedrock einen Chat-basierten Assistenten 228
Übersicht 228
Voraussetzungen und Einschränkungen 229
Architektur 229
Tools 230
Bewährte Methoden 232
Epen 233
Zugehörige Ressourcen 237
Zusätzliche Informationen 238
Dokumentieren Sie institutionelles Wissen anhand von Spracheingaben 240
Übersicht 240
Voraussetzungen und Einschränkungen 240
Architektur 241
Tools 242

Bewährte Methoden 244
Epen 244
Zugehörige Ressourcen 251
Generieren Sie personalisierte Empfehlungen mit Amazon Personalize 253
Übersicht 253
Voraussetzungen und Einschränkungen 253
Architektur 253
Tools 255
Epen 256
Zugehörige Ressourcen 259
Zusätzliche Informationen 259
Optimieren Sie ML-Workflows mithilfe SageMaker von KI und Hydra 263
Übersicht 263
Voraussetzungen und Einschränkungen 263
Architektur 264
Tools 265
Bewährte Methoden 266
Epen 267
Fehlerbehebung 274
Zugehörige Ressourcen 274
Zusätzliche Informationen 274
Trainieren und implementieren Sie ein benutzerdefiniertes GPU-unterstütztes ML-Modell 276
Übersicht 276
Voraussetzungen und Einschränkungen 276
Architektur 277
Tools 277
Epen 278
Zugehörige Ressourcen 295
Zusätzliche Informationen 295
..... 298
Übersicht 298
Voraussetzungen und Einschränkungen 299
Architektur 302
Tools 304
Bewährte Methoden 305
Epen 306

Zugehörige Ressourcen 314
Zusätzliche Informationen 314
Verwenden Sie Amazon Q Developer als Programmierassistenten 319
Übersicht 319
Voraussetzungen und Einschränkungen 320
Tools 320
Bewährte Methoden 320
Epen 321
Fehlerbehebung 330
Zugehörige Ressourcen 330
Verwenden Sie SageMaker Processing für das verteilte Feature-Engineering von ML-Datensätzen im Terabyte-Bereich 331
Übersicht 331
Voraussetzungen und Einschränkungen 331
Architektur 332
Tools 335
Epen 335
Zugehörige Ressourcen 348
Anlagen 349
Visualisieren Sie KI/ML-Modellergebnisse mit Flask und Elastic Beanstalk 350
Übersicht 350
Voraussetzungen und Einschränkungen 350
Architektur 351
Tools 353
Epen 354
Zugehörige Ressourcen 365
Zusätzliche Informationen 365
Mehr Muster 369
Analysen 370
Analysieren Sie Amazon Redshift Redshift-Daten in Microsoft SQL Server Analysis Services .. 372
Übersicht 372
Voraussetzungen und Einschränkungen 372
Architektur 372
Tools 373
Epen 373
Zugehörige Ressourcen 375

..... 376
Übersicht 376
Voraussetzungen und Einschränkungen 376
Architektur 377
Tools 377
Epen 378
Zugehörige Ressourcen 383
Automatisieren Sie die Datenaufnahme aus Amazon AWS Data Exchange S3 385
Übersicht 385
Voraussetzungen und Einschränkungen 385
Architektur 385
Tools 386
Epen 387
Zugehörige Ressourcen 389
Anlagen 389
Automatisieren Sie die Durchsetzung von Verschlüsselungen in AWS Glue 390
Übersicht 390
Voraussetzungen und Einschränkungen 390
Architektur 390
Tools 391
Bewährte Methoden 392
Epen 393
Zugehörige Ressourcen 395
Erstellen Sie mit dem AWS DataOps Development Kit eine Datenpipeline zur Verarbeitung von Google Analytics-Daten 397
Übersicht 397
Voraussetzungen und Einschränkungen 397
Architektur 398
Tools 398
Epen 400
Fehlerbehebung 402
Zugehörige Ressourcen 402
Zusätzliche Informationen 402
Bauen Sie eine Pipeline zur Videoverarbeitung auf 405
Übersicht 405
Voraussetzungen und Einschränkungen 405

Architektur 406
Tools 406
Epen 407
Zugehörige Ressourcen 416
Zusätzliche Informationen 417
Anlagen 417
Erstellen Sie mit AWS Glue eine ETL-Pipeline von Amazon S3 zu Amazon Redshift 418
Übersicht 418
Voraussetzungen und Einschränkungen 418
Architektur 419
Tools 419
Epen 420
Zugehörige Ressourcen 429
Zusätzliche Informationen 429
Bauen Sie mit Amazon ein Datennetz für Unternehmen auf DataZone 431
Übersicht 431
Voraussetzungen und Einschränkungen 431
Architektur 432
Tools 433
Epen 434
Zugehörige Ressourcen 450
Zusätzliche Informationen 450
Value at Risk (VaR) mithilfe von AWS-Services berechnen 452
Übersicht 452
Voraussetzungen und Einschränkungen 453
Architektur 453
Tools 454
Bewährte Methoden 455
Epen 456
Zugehörige Ressourcen 459
Konfigurieren Sie den kontoübergreifenden Zugriff auf einen gemeinsamen AWS Glue Glue-Datenkatalog mit Athena 460
Übersicht 460
Voraussetzungen und Einschränkungen 460
Architektur 461
Tools 462

Epen 462
Zugehörige Ressourcen 475
Zusätzliche Informationen 475
NORMALIZE nach Amazon Redshift SQL konvertieren 476
Übersicht 476
Voraussetzungen und Einschränkungen 476
Architektur 476
Tools 477
Epen 482
Zugehörige Ressourcen 482
RESET WHEN nach Amazon Redshift SQL konvertieren 484
Übersicht 484
Voraussetzungen und Einschränkungen 484
Architektur 484
Tools 485
Epen 489
Zugehörige Ressourcen 489
Bereitstellen und verwalten Sie einen serverlosen Data Lake auf AWS 491
Übersicht 491
Voraussetzungen und Einschränkungen 491
Architektur 492
Tools 493
Epen 494
Zugehörige Ressourcen 497
..... 498
Übersicht 498
Voraussetzungen und Einschränkungen 498
Architektur 499
Tools 499
Epen 500
Zugehörige Ressourcen 504
Anlagen 504
Stellen Sie sicher, dass Amazon EMR bei Amazon S3 protokolliert wird 505
Übersicht 505
Voraussetzungen und Einschränkungen 506
Architektur 506

Tools 507
Epen 507
Zugehörige Ressourcen 510
Anlagen 510
Generieren Sie Testdaten mit AWS Glue 511
Übersicht 511
Voraussetzungen und Einschränkungen 511
Architektur 512
Tools 512
Bewährte Methoden 513
Epen 513
Zugehörige Ressourcen 525
Zusätzliche Informationen 526
IoT-Daten direkt in Amazon S3 aufnehmen 531
Übersicht 531
Voraussetzungen und Einschränkungen 531
Architektur 532
Tools 533
Bewährte Methoden 533
Epen 534
Fehlerbehebung 542
Zugehörige Ressourcen 543
Zusätzliche Informationen 543
Starten Sie einen Spark-Job in Amazon EMR mithilfe einer Lambda-Funktion 548
Übersicht 548
Voraussetzungen und Einschränkungen 548
Architektur 549
Tools 549
Epen 550
Zugehörige Ressourcen 554
Zusätzliche Informationen 554
Anlagen 556
Migrieren Sie Apache Cassandra-Workloads zu Amazon Keyspaces 557
Übersicht 557
Voraussetzungen und Einschränkungen 557
Architektur 557

Tools 558
Bewährte Methoden 559
Epen 559
Fehlerbehebung 573
Zugehörige Ressourcen 573
Zusätzliche Informationen 574
Migrieren Sie Hadoop-Daten mithilfe WANdisco LiveData von Migrator zu Amazon S3 575
Übersicht 575
Voraussetzungen und Einschränkungen 575
Architektur 576
Epen 577
Zugehörige Ressourcen 583
Zusätzliche Informationen 583
Migrieren Sie Oracle Business Intelligence 12C zur AWS-Cloud 585
Übersicht 585
Voraussetzungen und Einschränkungen 585
Architektur 586
Tools 587
Epen 588
Zugehörige Ressourcen 603
Zusätzliche Informationen 604
Migrieren Sie einen Kafka-Cluster zu Amazon MSK mit MirrorMaker 609
Übersicht 609
Voraussetzungen und Einschränkungen 609
Architektur 610
Tools 610
Bewährte Methoden 611
Epen 611
Zugehörige Ressourcen 616
Zusätzliche Informationen 616
Migrieren Sie einen ELK-Stack in die AWS-Cloud 617
Übersicht 617
Voraussetzungen und Einschränkungen 617
Architektur 619
Tools 621
Epen 622

Zugehörige Ressourcen 631
Zusätzliche Informationen 633
Migrieren Sie Daten zur AWS Verwendung von Starburst 634
Übersicht 634
Voraussetzungen und Einschränkungen 634
Architektur 634
Tools 636
Epen 637
Zugehörige Ressourcen 640
Optimieren Sie die ETL-Erfassung der Größe der Eingabedatei 641
Übersicht 641
Voraussetzungen und Einschränkungen 641
Architektur 641
Tools 642
Epen 642
Zugehörige Ressourcen 646
Zusätzliche Informationen 647
Orchestrieren Sie eine ETL-Pipeline mit AWS Step Functions 648
Übersicht 648
Voraussetzungen und Einschränkungen 648
Architektur 649
Tools 650
Epen 651
Fehlerbehebung 659
Zugehörige Ressourcen 659
Zusätzliche Informationen 659
Führen Sie ML-Analysen mit Amazon Redshift ML durch 660
Übersicht 660
Voraussetzungen und Einschränkungen 660
Architektur 661
Tools 662
Epen 663
Zugehörige Ressourcen 667
Fragen Sie Amazon DynamoDB mithilfe von Amazon Athena ab 669
Übersicht 669
Voraussetzungen und Einschränkungen 669

Architektur 670
Tools 670
Epen 671
Fehlerbehebung 674
Zugehörige Ressourcen 675
DynamoDB-Tabellen mit Athena abfragen 676
Übersicht 676
Voraussetzungen und Einschränkungen 676
Architektur 677
Tools 677
Epen 678
Zugehörige Ressourcen 687
Zusätzliche Informationen 688
Richten Sie einen nutzbaren Mindestdatenraum ein 690
Übersicht 690
Voraussetzungen und Einschränkungen 691
Architektur 693
Tools 693
Bewährte Methoden 694
Epen 695
Fehlerbehebung 750
Zugehörige Ressourcen 750
Zusätzliche Informationen 750
Sprachspezifische Sortierung für Amazon Redshift Redshift-Abfrageergebnisse einrichten 756
Übersicht 756
Voraussetzungen und Einschränkungen 756
Architektur 757
Tools 757
Epen 757
Zugehörige Ressourcen 763
Zusätzliche Informationen 763
Abonnieren Sie eine Lambda-Funktion für Ereignisbenachrichtigungen aus regionsübergreifenden S3-Buckets 767
Übersicht 767
Voraussetzungen und Einschränkungen 767
Architektur 768

Tools 768
Epen 769
Zugehörige Ressourcen 774
Drei AWS Glue Glue-Auftragstypen für die Konvertierung von Daten 775
Übersicht 775
Voraussetzungen und Einschränkungen 775
Architektur 775
Tools 776
Epen 777
Zugehörige Ressourcen 780
Zusätzliche Informationen 780
Anlagen 786
Visualisieren Sie Amazon Redshift Redshift-Prüfprotokolle mit Athena und QuickSight 787
Übersicht 787
Voraussetzungen und Einschränkungen 787
Architektur 787
Tools 788
Epen 788
Zugehörige Ressourcen 794
Anlagen 794
Visualisieren Sie Berichte über IAM-Anmeldeinformationen mit Amazon QuickSight 795
Übersicht 795
Voraussetzungen und Einschränkungen 796
Architektur 796
Tools 797
Epen 798
Zusätzliche Informationen 805
Mehr Muster 807
Datenverarbeitung 809
Container und Microservices 810
Greifen Sie von Amazon EKS aus auf Amazon Neptune zu 812
Greifen Sie auf Container-Anwendungen auf Amazon ECS zu 825
Greifen Sie mit einem AWS Fargate-Starttyp auf Container-Anwendungen auf Amazon ECS zu 843
Greifen Sie privat auf Container-Anwendungen auf Amazon EKS zu 859
Aktivieren Sie mTLS in App Mesh auf Amazon EKS 868

Automatisieren Sie Backups für Amazon RDS for PostgreSQL PostgreSQL-DB-Instances .. 876
Automatisieren Sie die Bereitstellung von Node Termination Handler 891
Automatisches Erstellen und Bereitstellen einer Java-Anwendung für Amazon EKS 907
Erstellen Sie eine Amazon ECS-Aufgabendefinition für EC2 Instances, die Amazon EFS verwenden 934
Stellen Sie Lambda-Funktionen mit Container-Images bereit 941
Bereitstellen von Java-Microservices auf Amazon ECS mithilfe von AWS Fargate 951
Bereitstellen von Kubernetes-Paketen mit Amazon EKS und Helm 958
Stellen Sie einen Java-Microservice auf Amazon EKS bereit und stellen Sie ihn mit einem Application Load Balancer bereit 970
Stellen Sie mithilfe von AWS Copilot eine geclusterte Anwendung in Amazon ECS bereit 984
Stellen Sie eine GRPC-basierte Anwendung auf Amazon EKS bereit 996
Bereitstellen und Debuggen von Amazon EKS-Clustern 1010
Container mithilfe von Elastic Beanstalk bereitstellen 1042
Generieren Sie eine statische ausgehende IP-Adresse mit Lambda und Amazon VPC 1048
Identifizieren Sie doppelte Container-Images automatisch 1063
SSM Agent auf Amazon EKS-Worker-Knoten installieren 1094
Installieren Sie den SSM-Agent und den CloudWatch Agenten auf Amazon EKS-Worker-Knoten mit preBootstrapCommands 1100
Migrieren Sie NGINX-Ingress-Controller für den automatischen EKS-Modus 1107
Migrieren Sie Container-Workloads von ARO zu ROSA 1128
Optimieren Sie generierte Docker-Images 1146
Platzieren Sie Kubernetes-Pods auf kompatiblen Knoten in Amazon EKS 1157
Replizieren Sie gefilterte Amazon ECR-Container-Images über Konten oder Regionen hinweg 1177
Rotieren Sie die Anmeldeinformationen, ohne Container neu zu starten 1196
Amazon ECS-Aufgaben auf Amazon ausführen WorkSpaces 1203
Führen Sie einen ASP.NET-Web-API-Docker-Container auf AWS aus 1214
Führen Sie nachrichtengesteuerte Workloads mit AWS Fargate aus 1228
Führen Sie statusbehaftete Workloads mit persistentem Datenspeicher aus 1238
auto Skalierung mit Amazon EKS Pod Identity und KEDA einrichten 1265
..... 1289
Verwenden Sie Mutual TLS in Amazon ECS mit ALB 1313
Mehr Muster 1345
Serverless 1347
Erstellen Sie eine React Native-App mit AWS Amplify 1348

Zentrale Verwaltung von Mandanten über mehrere SaaS-Produkte hinweg 1370
Erstellen Sie eine kontoübergreifende Amazon-Verbindung EventBridge 1384
Bereitstellung von DynamoDB-Datensätzen an Amazon S3 mithilfe von Kinesis Data Streams und Firehose 1399
Implementieren Sie die pfadbasierte API-Versionierung mithilfe von API Gateway 1406
Importieren Sie die psycopg2-Bibliothek in AWS Lambda 1418
Integrieren Sie API Gateway mit Amazon SQS 1429
APIs Asynchrone Verarbeitung mit AWS Lambda 1446
APIs Asynchrone Verarbeitung mit Amazon DynamoDB Streams 1456
APIs Asynchrone Verarbeitung mit Amazon SQS 1468
Führen Sie Systems Manager Automation-Aufgaben synchron über Step Functions aus ... 1479
parallel Lesevorgänge von S3-Objekten ausführen mit AWS Lambda 1494
Senden Sie Telemetriedaten von Lambda an OpenSearch 1508
Richten Sie einen serverlosen Mobilfunkrouter ein 1526
Richten Sie den privaten Zugriff auf einen Amazon S3 S3-Bucket ein 1546
Fehlerbehebung bei Step Functions Functions-Status 1554
Verwenden Sie einen serverlosen Ansatz, um AWS-Services miteinander zu verketten 1565
Mehr Muster 1571
Netzwerk 1574
Automatisieren Sie das Peering für AWS Transit Gateway 1575
Zentralisieren Sie die Netzwerkkonnektivität mit AWS Transit Gateway 1583
Konfigurieren Sie die HTTPS-Verschlüsselung für Oracle JD Edwards EnterpriseOne mithilfe eines Application Load Balancer 1590
Stellen Sie über ein privates Netzwerk eine Connect zu Daten- und Steuerungsebenen des Application Migration Service her 1603
Erstellen Sie Infoblox-Objekte mithilfe von benutzerdefinierten AWS-Ressourcen CloudFormation 1619
Passen Sie die CloudWatch Benachrichtigungen für die Network Firewall an 1633
Stellen Sie mithilfe von Terraform Ressourcen in einer Wellenlängenzone bereit 1652
Massenmigrieren von DNS-Einträgen in eine private gehostete Route 53 53-Zone 1661
Ändern Sie HTTP-Header, wenn Sie von F5 zu einem Application Load Balancer auf AWS migrieren 1671
Greifen Sie privat von mehreren aus auf einen AWS-Serviceendpunkt zu VPCs 1677
Melden Sie die Ergebnisse von Network Access Analyzer in mehreren AWS-Konten 1688
Richten Sie die DNS-Auflösung für Hybridnetzwerke in einer Umgebung mit mehreren AWS Konten ein 1723

..... 1739
AWS-Netzwerk-Firewall-Protokolle und -Metriken mit Splunk anzeigen 1745
Mehr Muster 1757
Bereitstellung von Inhalten 1759
AWS WAF Logs mit Firehose an Splunk senden 1760
Stellen Sie statische Inhalte in einem S3-Bucket über eine VPC bereit, indem Sie CloudFront 1770
Mehr Muster 1779
Datenbanken und Speicher 1780
Datenbanken 1781
Greifen Sie mithilfe von Verbindungsservern auf lokale SQL Server-Daten zu 1784
HA zu Oracle PeopleSoft auf AWS hinzufügen 1790
Beurteilen Sie die Abfrageleistung für die Migration von SQL Server-Datenbanken zu MongoDB Atlas auf AWS 1815
Automatisieren Sie blaue/grüne Bereitstellungen globaler Aurora-Datenbanken mit IaC 1826
Automatisieren Sie Datenbankaufgaben mit einem AWS Lambda Taskplaner 1862
Automatisieren Sie Failover und Failback mit DR Orchestrator Framework 1876
Automatisieren Sie die Replikation von Amazon RDS-Instances auf AWS-Konten 1904
Automatisches Backup von SAP HANA-Datenbanken 1920
Automatisches Generieren von PynamoDB-Modellen und CRUD-Funktionen für DynamoDB 1929
Sperren Sie den öffentlichen Zugriff auf Amazon RDS 1937
Kontoübergreifenden Amazon DynamoDB DynamoDB-Zugriff konfigurieren 1945
Konfigurieren Sie schreibgeschütztes Routing in einer Always-On-Verfügbarkeitsgruppe .. 1961
Stellen Sie eine Connect über einen SSH-Tunnel in pgAdmin her 1970
JSON-Oracle-Abfragen in PostgreSQL-Datenbank-SQL konvertieren 1975
Amazon DynamoDB-Tabellen zwischen Konten kopieren 2007
Amazon DynamoDB-Tabellen zwischen Konten kopieren 2014
Kosten- und Nutzungsberichte für Amazon RDS und Amazon Aurora erstellen 2027
Stellen Sie SQL Server FCIs auf Amazon EC2 und Amazon bereit FSx 2035
Emulieren Sie Oracle RAC-Workloads mit Aurora PostgreSQL 2052
Verschlüsselte Verbindungen für PostgreSQL-DB-Instances aktivieren 2059
Verschlüsseln Sie eine bestehende Amazon RDS for PostgreSQL PostgreSQL-DB-Instance 2069
Automatisches Tagging von Amazon RDS-Datenbanken beim Start erzwingen 2078
Schätzung der DynamoDB-Kosten 2084

Schätzung der Speicherkosten für eine Amazon DynamoDB-Tabelle ... 2097
Schätzen Sie die Größe der Amazon RDS-Engine für eine Oracle-Datenbank mithilfe von AWR-Berichten ... 2102
Exportieren Sie Amazon RDS for SQL Server-Tabellen in einen S3-Bucket ... 2137
Behandeln Sie anonyme Blöcke in dynamischen SQL-Anweisungen ... 2150
Behandeln Sie überladene Oracle-Funktionen in Aurora PostgreSQL-kompatibel ... 2158
Helfen Sie mit, DynamoDB-Tagging durchzusetzen ... 2165
Implementieren Sie regionsübergreifende DR ... 2171
Migrieren Sie Oracle-Funktionen mit mehr als 100 Argumenten nach PostgreSQL ... 2189
Migrieren Sie Amazon RDS for Oracle Oracle-DB-Instances zu AMS-Konten ... 2195
Migrieren Sie Oracle OUT-Bind-Variablen nach PostgreSQL ... 2206
Migrieren Sie SAP HANA mit HSR zu AWS ... 2215
Migrieren Sie SQL Server mithilfe verteilter Verfügbarkeitsgruppen zu AWS ... 2230
Migrieren Sie mithilfe von AWS DMS von Oracle 8i oder 9i zu Amazon RDS for Oracle SharePlex ... 2242
Überwachen Sie Amazon Aurora auf Verschlüsselung ... 2251
Überwachen Sie GoldenGate Protokolle mithilfe von Amazon CloudWatch ... 2257
Replattform von Oracle Database EE auf Amazon RDS for Oracle SE2 ... 2272
Replizieren Sie Mainframe-Datenbanken mithilfe von Precisely Connect nach AWS ... 2284
Jobs für Amazon RDS und Aurora PostgreSQL planen ... 2305
Senden Sie Benachrichtigungen für RDS for SQL Server über einen lokalen SMTP-Server 2311
DR für SAP auf IBM Db2 auf AWS einrichten ... 2326
Richten Sie mithilfe von Terraform eine CI/CD-Pipeline für die Datenbankmigration ein ... 2351
Richten Sie eine HA/DR-Architektur für Oracle E-Business Suite auf Amazon RDS Custom ein ... 2361
Richten Sie die Datenreplikation zwischen RDS for MySQL und MySQL auf Amazon EC2 ... 2370
Rollen für eine PeopleSoft Oracle-Anwendung wechseln ... 2376
Kontenübergreifend Daten aus Amazon Redshift entladen ... 2412
Datenbankmigrationsmuster nach Workload ... 2443
Mehr Muster ... 2454
Speicher und Backup ... 2460
Erlauben Sie EC2 Instanzen den Schreibzugriff auf S3-Buckets in AMS ... 2461
Automatisieren Sie die Aufnahme von Datenströmen in eine Snowflake-Datenbank ... 2467
Automatisches Verschlüsseln Sie EBS-Volumes ... 2480
Sun SPARC-Server im Charon-SSP-Emulator auf AWS sichern ... 2494

Daten mit Veeam auf Amazon S3 sichern und archivieren 2521
NetBackup Für VMware Cloud on AWS konfigurieren 2550
Kopieren Sie S3-Objekte mithilfe der AWS-CLI zwischen Konten und Regionen 2558
Kopieren Sie S3-Objekte mithilfe von S3 Batch Replication zwischen Konten und Regionen 2573
Migrieren Sie Hadoop-Daten mithilfe von DistCp AWS PrivateLink für Amazon S3 zu Amazon S3 2587
Mehr Muster 2604
Entwickler-Tools 2606
DevOps 2607
Automatisieren Sie den AWS Infrastrukturbetrieb 2611
Automatisieren Sie CloudFront Updates für Änderungen an Load Balancer-Endpunkten ... 2621
Automatisieren Sie CodeGuru Bewertungen für AWS CDK Python-Anwendungen 2630
Automatisieren Sie die AWS-Ressourcenbewertung 2642
Automatisieren Sie die Installation von SAP-Systemen 2657
Automatisieren Sie das Service Catalog-Portfolio und die Produktbereitstellung mit AWS CDK 2671
Automatisieren Sie Backups von AWS CodeCommit nach Amazon S3 2691
Automatisieren Sie das Löschen von Stacks CloudFormation 2699
Automatisieren Sie das dynamische Pipeline-Management zur Bereitstellung von Hotfix-Lösungen 2711
Automatisieren Sie die Erfassung von benutzerdefinierten Amazon MWAA-Metriken 2741
Automatisieren Sie die Verwaltung von Amazon Lex-Ressourcen mit dem AWS CDK und CloudFormation 2760
Automatisieren Sie die Stackset-Bereitstellung mithilfe von AWS CodePipeline und AWS CodeBuild 2781
Automatisches Anhängen einer verwalteten Richtlinie für Systems Manager an EC2 Instanzprofile 2813
Automatisches Erstellen von CI/CD-Pipelines und Amazon ECS-Clustern für Microservices 2830
Bauen Sie eine lose gekoppelte Architektur mit Microservices auf 2844
Docker-Images erstellen und auf Amazon ECR übertragen 2857
iOS-Apps mit AWS-Services erstellen und testen 2864
In AWS CDK-Anwendungen oder CloudFormation -Vorlagen finden Sie bewährte Methoden mithilfe von Regelpaketen 2870
Gegenseitiges TLS für Anwendungen auf Amazon EKS konfigurieren 2875

Erstellen Sie AppStream 2.0-Ressourcen mit AWS CloudFormation 2888
Erstellen Sie mit Firelens einen benutzerdefinierten Log-Parser für Amazon ECS 2894
Erstellen Sie eine Pipeline und ein AMI mit CodePipeline und HashiCorp Packer 2904
Erstellen Sie eine Pipeline und stellen Sie Updates für lokale EC2 Instanzen bereit mit CodePipeline 2912
Erstellen Sie dynamische CI-Pipelines für Java- und Python-Projekte 2922
Setzen Sie CloudWatch Synthetics Canaries ein 2940
Stellen Sie eine CI/CD-Pipeline für Java-Microservices auf Amazon ECS bereit 2948
Stellen Sie eine ChatOps Lösung zur Verwaltung von SAST-Scanergebnissen bereit 2958
Stellen Sie eine Firewall mit AWS Network Firewall und AWS Transit Gateway bereit 2977
..... 2993
Stellen Sie mithilfe eines EC2 Instanzprofils einen Amazon EKS-Cluster aus AWS Cloud9 bereit 2998
Code in mehreren AWS-Regionen bereitstellen 3011
Amazon Redshift SQL-Abfragen ausführen 3025
Exportieren Sie AWS Backup Backup-Berichte als CSV-Datei 3038
EC2 Amazon-Instanz-Tags in eine CSV-Datei exportieren 3048
Generieren Sie eine CloudFormation AWS-Vorlage mit verwalteten AWS Config-Regeln .. 3055
Gewähren Sie SageMaker Notebook-Instances kontoübergreifenden Zugriff auf ein Repository CodeCommit 3062
Implementieren Sie eine GitHub Flow-Branching-Strategie 3074
Implementieren Sie eine Gitflow-Branching-Strategie 3085
Implementieren Sie eine Trunk-Branching-Strategie 3097
Implementieren Sie ein zentrales benutzerdefiniertes Checkov-Scanning 3103
Initiieren Sie verschiedene CI/CD-Pipelines, nachdem Sie Änderungen in einem Monorepo erkannt haben 3115
Integrieren Sie ein Bitbucket-Repository mit AWS Amplify 3134
Starten Sie mit CodeBuild Lambda ein Projekt für alle AWS-Konten 3143
Multi-AZ-Failover für EMR-Cluster mithilfe von Application Recovery Controller verwalten . 3158
Verwalten Sie blaue/grüne Bereitstellungen von Microservices für mehrere Konten und Regionen 3175
Überwachen Sie Amazon ECR-Repositorys auf Platzhalterberechtigungen 3209
Optimieren Sie serverlose Bereitstellungen mit mehreren Konten 3214
Führen Sie benutzerdefinierte Aktionen aus CodeCommit AWS-Ereignissen durch 3235
Stellen Sie AWS Service Catalog Produkte mithilfe von GitHub Aktionen bereit 3240
Stellen Sie IAM-Rollen mit den geringsten Rechten bereit 3252

Veröffentlichen Sie CloudWatch Amazon-Metriken in einer CSV-Datei 3267
Entfernen Sie EC2 Amazon-Einträge auf der anderen Seite AWS-Konten von AWS Managed Microsoft AD 3273
Entfernen Sie EC2 Amazon-Einträge in demselben AWS-Konto Formular AWS Managed Microsoft AD 3292
Führen Sie Komponententests für Python-ETL-Jobs aus in AWS Glue 3304
Helm v3-Diagramme in Amazon S3 einrichten 3315
Richten Sie eine CI/CD-Pipeline ein mit CodePipeline 3325
Richten Sie mit Terraform eine zentrale Protokollierung in großem Maßstab ein 3341
end-to-endVerschlüsselung für Anwendungen auf Amazon EKS einrichten 3369
Vereinfachen Sie die Bereitstellung von Amazon EKS-Anwendungen für mehrere Mandanten 3383
Abonnieren Sie ein SNS-Thema für mehrere E-Mail-Endpunkte 3402
Verwenden Sie das AWS Fargate WaitCondition Hook-Konstrukt 3407
Verwenden Sie Git-Repos von Drittanbietern in AWS CodePipeline 3419
Validieren Sie Terraform-Konfigurationen mithilfe von AWS CodePipeline 3430
Mehr Muster 3449
Infrastruktur 3453
Greifen Sie mit Session Manager und Amazon EC2 Instance Connect auf einen Bastion-Host zu 3455
Zentralisieren Sie die DNS-Auflösung mithilfe von AWS Managed Microsoft AD 3474
Zentralisieren Sie die Überwachung mithilfe von Observability Access Manager 3486
Prüfen Sie die EC2 Instances beim Start auf obligatorische Tags 3502
Bereinigen Sie AFT-Ressourcen nach dem Verlust von Statusdateien sicher 3508
Stellen Sie mithilfe von Session Manager eine Connect zu einer EC2 Instanz her 3522
Erstellen Sie eine Pipeline in AWS-Regionen, die AWS nicht unterstützen CodePipeline ... 3529
Passen Sie Standardrollennamen mithilfe von AWS CDK Aspekten und Escape-Schraffuren an 3538
Stellen Sie einen Cassandra-Cluster auf Amazon EC2 mit Private Static bereit IPs 3547
Mit Transit Gateway Connect auf AWS erweitern VRFs 3555
Erhalten Sie Amazon SNS SNS-Benachrichtigungen für Statusänderungen von AWS-KMS-Schlüsseln 3573
Beibehaltung von routingfähigem IP-Speicherplatz in VPC-Designs mit mehreren Konten für Subnetze ohne Arbeitslast 3581
Stellen Sie ein Terraform-Produkt in Service Catalog aus einem Code-Repository bereit ... 3587
Registrieren Sie mehrere AWS-Konten mit einer einzigen E-Mail-Adresse 3609

Richten Sie die DNS-Auflösung für Hybridnetzwerke in einer AWS-Umgebung mit einem Konto ein ... 3627
UiPath RPA-Bots automatisch auf Amazon einrichten EC2 ... 3633
Richten Sie eine hochverfügbare PeopleSoft Architektur auf AWS ein ... 3652
Richten Sie die Notfallwiederherstellung für Oracle JD Edwards ein EnterpriseOne ... 3684
Richten Sie die Erkennung und Berichterstattung von Abweichungen ein ... 3718
Importiert erfolgreich einen S3-Bucket als CloudFormation Stack ... 3724
Synchronisieren Sie Amazon EFS-Dateisysteme in verschiedenen Regionen ... 3737
Testen Sie die AWS Infrastruktur mithilfe von LocalStack Terraform-Tests ... 3747
Aktualisieren Sie SAP Pacemaker-Cluster von auf ENSA1 ENSA2 ... 3756
Verwenden Sie konsistente Availability Zones VPCs für verschiedene Konten ... 3780
Verwenden Sie den Benutzer IDs in IAM-Richtlinien ... 3786
Validieren Sie den Account Factory for Terraform-Code lokal ... 3798
Mehr Muster ... 3819
Web- und mobile Apps ... 3824
Authentifizieren Sie Benutzer von React-Webanwendungen ... 3825
Stellen Sie kontinuierlich eine Amplify-Webanwendung bereit ... 3836
Erstellen Sie eine React-App mithilfe von AWS Amplify und Amazon Cognito ... 3845
Erstellen Sie ein Portal für Mikro-Frontends ... 3863
Stellen Sie ein React-basiertes SPA auf Amazon S3 bereit und CloudFront ... 3896
Stellen Sie eine Amazon API Gateway Gateway-API mithilfe von privaten Endpunkten und einem Application Load Balancer bereit ... 3904
Betten Sie ein QuickSight Amazon-Dashboard in eine lokale Angular-Anwendung ein ... 3912
Erkunden Sie die Entwicklung von Web-Apps mit Green Boost ... 3934
Führen Sie Komponententests mithilfe von AWS aus CodeBuild ... 3965
Strukturieren Sie ein Python-Projekt in hexagonaler Architektur ... 3975
Mehr Muster ... 4002
IoT ... 4004
Konfigurieren Sie die Protokollierung und Überwachung von Sicherheitsereignissen in Ihrer IoT-Umgebung ... 4005
Übersicht ... 4005
Voraussetzungen und Einschränkungen ... 4005
Architektur ... 4006
Tools ... 4008
Epen ... 4009
Zugehörige Ressourcen ... 4014

Extrahieren und Abfragen von AWS IoT SiteWise Metadatenattributen 4015
Übersicht 4015
Voraussetzungen und Einschränkungen 4015
Architektur 4016
Tools 4016
Epen 4017
Zugehörige Ressourcen 4020
Zusätzliche Informationen 4021
..... 4023
Übersicht 4023
Voraussetzungen und Einschränkungen 4024
Architektur 4024
Tools 4025
Bewährte Methoden 4025
Epen 4026
Fehlerbehebung 4042
Zugehörige Ressourcen 4044
Zusätzliche Informationen 4044
Mehr Muster 4046
Migration und Modernisierung 4047
Migration 4048
CloudFormation AWS-Vorlagen für AWS DMS erstellen 4049
Beginnen Sie mit der automatisierten Portfolioerkennung 4053
Migrieren Sie lokale Cloudera-Workloads zu AWS 4062
Verbindungsfehler nach der Migration von SQL Server zu AWS beheben 4080
Starten Sie den AWS Replication Agent automatisch neu, ohne ihn zu deaktivieren SELinux 4083
Re-Architekt 4091
Erneut hosten 4515
Umziehen 4810
Plattformwechsel 4869
Migrationsmuster nach Arbeitslast 5541
Mehr Muster 5550
Modernisierung 5552
Analysieren und visualisieren Sie die Softwarearchitektur in CAST Imaging 5553

Beurteilen Sie die Anwendungsbereitschaft vor der Migration zu AWS mithilfe von CAST Highlight 5564
Automatisches Archivieren abgelaufener DynamoDB-Daten in Amazon S3 5591
Erstellen Sie eine serverlose Architektur mit mehreren Mandanten in Amazon Service OpenSearch 5608
Stellen Sie Anwendungen mit mehreren Stacks bereit 5660
Stellen Sie verschachtelte Anwendungen mit AWS SAM bereit 5670
Implementieren Sie die SaaS-Mandantenisolierung für Amazon S3 mithilfe eines AWS Lambda TVM 5679
Implementieren Sie das serverlose Saga-Muster mithilfe von AWS Step Functions 5706
Verwalten Sie lokale Containeranwendungen mit Amazon ECS Anywhere 5721
Modernisieren Sie ASP.NET Web Forms-Anwendungen auf AWS 5731
Führen Sie ereignisgesteuerte Workloads mit AWS Fargate aus 5747
Mandanten-Onboarding in der SaaS-Architektur 5758
Verwenden Sie CQRS und Event Sourcing 5785
Mehr Muster 5812
Großrechner 5815
Zugriff AWS-Services von IBM z/OS aus durch Installation des AWS CLI 5817
Mainframe-Daten auf Amazon S3 sichern und archivieren 5839
Erstellen Sie COBOL Db2-Programme mit und AWS Mainframe Modernization AWS CodeBuild 5870
Erstellen Sie ein Micro Focus Enterprise Server PAC 5897
Erstellen Sie einen Mainframe-Dateiviewer in der AWS-Cloud 5919
Containerisieren Sie modernisierte Blu Age-Anwendungen 5936
EBCDIC-Daten in ASCII auf AWS konvertieren 5947
Mainframe-EBCDIC-Dateien mit AWS Lambda in ASCII-Dateien konvertieren 5966
Konvertieren Sie Mainframe-Datendateien mit komplexen Datensatzlayouts 5989
Stellen Sie eine Umgebung für containerisierte Apps bereit 6009
Generieren Sie Einblicke in Db2 z/OS-Daten 6020
Generieren Sie Einblicke mithilfe von AWS Mainframe Modernization und Amazon Q in QuickSight 6075
Integrieren Sie Stonebranch Universal Controller in AWS 6094
Migrieren und replizieren Sie VSAM-Dateien mit Precisely in die AWS-Cloud 6133
Modernisieren Sie das Mainframe-Output-Management auf AWS 6152
Modernisieren Sie die Mainframe-Anwendung mit CardDemo AWS Transform 6206
Modernisieren Sie Ihre Mainframe-Batchdruck-Workloads auf AWS 6227

Modernisieren Sie Ihre Mainframe-Umgebung mit der Rocket Software Enterprise Suite ... 6258
Modernisieren Sie Ihre Mainframe-Online-Druck-Workloads auf AWS ... 6276
Verschieben Sie Mainframe-Dateien mit Transfer Family nach Amazon S3 ... 6311
Sicherer Benutzerzugriff in einer Db2-Verbunddatenbank ... 6327
Übertragung von Db2 z/OS-Daten nach AWS ... 6337
Mehr Muster ... 6366
Verwaltung ... 6367
Kostenmanagement ... 6368
Erstellen Sie detaillierte Kosten- und Nutzungsberichte für AWS Glue Glue-Jobs ... 6369
Erstellen Sie detaillierte Kosten- und Nutzungsberichte für Amazon EMR-Cluster ... 6375
Mehr Muster ... 6380
Datenverarbeitung in Hochleistung ... 6381
Stellen Sie ein Lustre-Dateisystem mithilfe von Terraform und DRA bereit ... 6382
Richten Sie ein Grafana-Monitoring-Dashboard für AWS ein ParallelCluster ... 6391
Richten Sie einen Auto Scaling-VDI mit NICE DCV ein ... 6406
Hybride Cloud ... 6421
Konfiguration einer Rechenzentrumserweiterung für VMware Cloud on AWS ... 6422
Konfigurieren Sie vRealize Automation für die Bereitstellung VMs in der VMware Cloud auf AWS ... 6427
Integrieren Sie VMware vRealize Network Insight mit VMware Cloud on AWS ... 6440
Migrieren VMs Sie mithilfe von HCX OSAM zur VMware Cloud auf AWS ... 6445
Senden Sie Logs von VMware Cloud on an Splunk AWS ... 6451
Richten Sie eine CI/CD-Pipeline für Hybrid-Workloads auf Amazon ECS Anywhere ein ... 6458
Mehr Muster ... 6481
Management & Governance ... 6482
Warnung, wenn Amazon Data Firehose-Ressourcen nicht verschlüsselt sind ... 6484
Automatisieren Sie das Hinzufügen oder Aktualisieren von Windows-Registrierungseinträgen ... 6489
Automatisch einen RFC mit Python erstellen ... 6494
Automatisches Stoppen und Starten einer Amazon RDS-DB-Instance ... 6502
Zentralisieren Sie die Verteilung von Softwarepaketen in AWS Organizations mithilfe von Terraform ... 6518
Konfigurieren Sie die Protokollierung für .NET-Anwendungen in CloudWatch Logs ... 6532
AWS Service Catalog-Produkte zwischen AWS-Konten und Regionen kopieren ... 6542
Erstellen Sie eine RACI-Matrix für Cloud-Operationen ... 6552
Erstellen Sie Alarme für benutzerdefinierte Metriken mit CloudWatch ... 6559

Erstellen Sie eine AWS Cloud9 Cloud9-IDE mit standardmäßigen verschlüsselten EBS-Volumes ... 6567
Automatisches Erstellen von Tag-basierten Dashboards CloudWatch ... 6574
Dokumentieren Sie Ihr Landezonendesign ... 6584
Aktivieren Sie Amazon DevOps Guru unternehmensweit mit dem AWS CDK ... 6588
Implementieren Sie AFT mithilfe einer Bootstrap-Pipeline ... 6616
AWS Service Catalog-Produkte in mehreren AWS-Konten und Regionen verwalten ... 6643
Migrieren Sie ein AWS-Konto von AWS Organizations zu AWS Control Tower ... 6651
Überwachen Sie SAP RHEL Pacemaker-Cluster ... 6668
Überwachen Sie die Anwendungsaktivität mithilfe von CloudWatch Logs Insights ... 6691
Überwachen Sie die Nutzung eines AMI überall AWS-Konten ... 6704
Benachrichtigungen für programmatische Kontoschließungen in AWS Organizations einrichten ... 6721
EBS-Snapshot-Details für Ihr AWS-Konto oder Ihre Organisation anzeigen ... 6731
Mehr Muster ... 6738
Nachrichtenübermittlung und Kommunikation ... 6741
Automatisieren Sie die RabbitMQ-Konfiguration in Amazon MQ ... 6742
Verbessern Sie die Anrufqualität auf den Agenten-Workstations in Amazon Connect ... 6750
Mehr Muster ... 6769
Sicherheit, Identität und Compliance ... 6770
Zugriff AWS-Services von ASP.NET mit Amazon Cognito ... 6773
Übersicht ... 6773
Voraussetzungen und Einschränkungen ... 6774
Architektur ... 6774
Tools ... 6774
Epen ... 6775
Fehlerbehebung ... 6780
Zugehörige Ressourcen ... 6780
Anlagen ... 6781
Authentifizieren Sie SQL Server mithilfe von AWS Directory Service ... 6782
Übersicht ... 6782
Voraussetzungen und Einschränkungen ... 6782
Architektur ... 6782
Tools ... 6783
Epen ... 6783
Zugehörige Ressourcen ... 6787

Automatisieren Sie die Reaktion auf Vorfälle und die Forensik 6789
Übersicht 6789
Voraussetzungen und Einschränkungen 6789
Architektur 6790
Tools 6793
Epen 6794
Zugehörige Ressourcen 6798
Zusätzliche Informationen 6798
Anlagen 6799
Automatisieren Sie die Behebung von Security Hub Hub-Standardergebnissen 6800
Übersicht 6800
Voraussetzungen und Einschränkungen 6801
Architektur 6801
Tools 6802
Bewährte Methoden 6802
Epen 6803
Zugehörige Ressourcen 6806
Anlagen 6806
Automatisieren Sie Sicherheitsscans für kontoübergreifende Workloads mit Amazon Inspector 6807
Übersicht 6807
Voraussetzungen und Einschränkungen 6807
Architektur 6808
Tools 6809
Epen 6810
Zugehörige Ressourcen 6814
Anlagen 6815
Überwachen Sie automatisch den Zugriff von öffentlichen IP-Adressen 6816
Übersicht 6816
Voraussetzungen und Einschränkungen 6816
Architektur 6817
Tools 6819
Bewährte Methoden 6820
Epen 6820
Fehlerbehebung 6826
Zugehörige Ressourcen 6826

Automatische Reaktivierung CloudTrail von AWS mithilfe bewährter Sicherheitsmethoden 6827
Übersicht 6827
Voraussetzungen und Einschränkungen 6827
Architektur 6828
Tools 6828
Epen 6829
Zugehörige Ressourcen 6835
Anlagen 6836
Automatically remediate unencrypted Amazon RDS DB instances and clusters 6837
Übersicht 6837
Voraussetzungen und Einschränkungen 6837
Architektur 6839
Tools 6839
Bewährte Methoden 6841
Epen 6841
Zugehörige Ressourcen 6848
Zusätzliche Informationen 6849
Automatische Rotation der IAM-Benutzerzugriffsschlüssel 6850
Übersicht 6850
Voraussetzungen und Einschränkungen 6851
Architektur 6852
Tools 6854
Epen 6856
Zugehörige Ressourcen 6866
Automatische Validierung und Bereitstellung von IAM-Richtlinien und -Rollen in einem AWS-Konto 6868
Übersicht 6868
Voraussetzungen und Einschränkungen 6869
Architektur 6870
Tools 6870
Epen 6871
Zugehörige Ressourcen 6876
Integrieren Sie Security Hub und Jira bidirektional 6877
Übersicht 6877
Voraussetzungen und Einschränkungen 6878
Architektur 6879

Tools 6880
Epen 6881
Zugehörige Ressourcen 6893
Zusätzliche Informationen 6893
Erstellen Sie eine Pipeline für gehärtete Container-Images 6895
Übersicht 6895
Voraussetzungen und Einschränkungen 6895
Architektur 6896
Tools 6899
Epen 6900
Fehlerbehebung 6908
Zugehörige Ressourcen 6909
Zentralisieren Sie die Verwaltung von IAM-Zugriffsschlüsseln in AWS Organizations mithilfe von Terraform 6910
Übersicht 6910
Voraussetzungen und Einschränkungen 6911
Architektur 6911
Tools 6913
Bewährte Methoden 6914
Epen 6914
Fehlerbehebung 6924
Zugehörige Ressourcen 6924
Suchen Sie in einer CloudFront Amazon-Distribution nach Zugriffsprotokollierung, HTTPS- und TLS-Version 6925
Übersicht 6925
Voraussetzungen und Einschränkungen 6926
Architektur 6926
Tools 6927
Epen 6927
Zugehörige Ressourcen 6931
Anlagen 6931
Suchen Sie in den Eingangsregeln für Sicherheitsgruppen nach Einträgen für einzelne Hosts nach Netzwerkeinträgen für einzelne Hosts IPv4 IPv6 6932
Übersicht 6932
Voraussetzungen und Einschränkungen 6932
Architektur 6932

Tools 6933
Epen 6934
Zugehörige Ressourcen 6938
Anlagen 6938
Wählen Sie einen Amazon Cognito Cognito-Authentifizierungsablauf 6939
Übersicht 6939
Voraussetzungen und Einschränkungen 6939
Architektur 6940
Tools 6944
Epen 6945
Zugehörige Ressourcen 6948
Zusätzliche Informationen 6949
Erstellen Sie AWS Config benutzerdefinierte Regeln mit Guard 6951
Übersicht 6951
Voraussetzungen und Einschränkungen 6952
Architektur 6952
Tools 6957
Epen 6957
Fehlerbehebung 6960
Zugehörige Ressourcen 6961
Erstellen Sie einen Bericht mit den Ergebnissen von Prowler aus mehreren AWS-Konten 6963
Übersicht 6963
Voraussetzungen und Einschränkungen 6964
Architektur 6965
Tools 6966
Epen 6968
Fehlerbehebung 6995
Zugehörige Ressourcen 6996
Zusätzliche Informationen 6996
Löschen Sie ungenutzte Amazon EBS-Volumes mit AWS Config 6998
Übersicht 6998
Voraussetzungen und Einschränkungen 6998
Architektur 6999
Tools 6999
Epen 7000
Fehlerbehebung 7003

Zugehörige Ressourcen 7004
Stellen Sie AWS Control Tower Kontrollen bereit mit AWS CDK 7005
Übersicht 7005
Voraussetzungen und Einschränkungen 7006
Architektur 7007
Tools 7008
Bewährte Methoden 7009
Epen 7009
Zugehörige Ressourcen 7017
Zusätzliche Informationen 7017
Stellen Sie AWS Control Tower Steuerelemente mit Terraform bereit 7021
Übersicht 7021
Voraussetzungen und Einschränkungen 7022
Architektur 7023
Tools 7024
Bewährte Methoden 7024
Epen 7025
Fehlerbehebung 7031
Zugehörige Ressourcen 7033
Zusätzliche Informationen 7033
Stellen Sie eine Pipeline bereit, die Sicherheitsprobleme im Code erkennt 7037
Übersicht 7037
Voraussetzungen und Einschränkungen 7037
Architektur 7038
Tools 7039
Epen 7039
Fehlerbehebung 7042
Zugehörige Ressourcen 7043
Zusätzliche Informationen 7043
Stellen Sie detektivische Kontrollen für öffentliche Subnetze bereit 7046
Übersicht 7046
Voraussetzungen und Einschränkungen 7047
Architektur 7047
Tools 7049
Bewährte Methoden 7049
Epen 7049

Zugehörige Ressourcen 7060
Zusätzliche Informationen 7061
Implementieren Sie präventive Kontrollen für öffentliche Subnetze 7063
Übersicht 7063
Voraussetzungen und Einschränkungen 7063
Architektur 7064
Tools 7065
Epen 7066
Zugehörige Ressourcen 7072
Zusätzliche Informationen 7073
Stellen Sie die Sicherheitsautomatisierungslösung mithilfe von Terraform bereit AWS WAF ... 7075
Übersicht 7075
Voraussetzungen und Einschränkungen 7075
Architektur 7076
Tools 7076
Bewährte Methoden 7077
Epen 7077
Fehlerbehebung 7081
Zugehörige Ressourcen 7081
Erkennen Sie Amazon RDS-Instances mit ablaufenden CA-Zertifikaten 7083
Übersicht 7083
Voraussetzungen und Einschränkungen 7083
Architektur 7084
Tools 7086
Bewährte Methoden 7087
Epen 7087
Fehlerbehebung 7092
Zugehörige Ressourcen 7092
Generieren Sie dynamisch eine IAM-Richtlinie mit IAM Access Analyzer 7094
Übersicht 7094
Voraussetzungen und Einschränkungen 7094
Architektur 7095
Tools 7096
Epen 7098
Zugehörige Ressourcen 7104
Aktivieren Sie die GuardDuty Verwendung von Vorlagen CloudFormation 7106

Übersicht 7106
Voraussetzungen und Einschränkungen 7106
Architektur 7106
Tools 7107
Epen 7108
Zugehörige Ressourcen 7110
Zusätzliche Informationen 7110
Aktivieren Sie die transparente Datenverschlüsselung in Amazon RDS for SQL Server 7114
Übersicht 7114
Voraussetzungen und Einschränkungen 7114
Architektur 7114
Tools 7115
Epen 7115
Zugehörige Ressourcen 7118
Stellen Sie sicher, dass AWS-Load Balancer sichere Listener-Protokolle verwenden 7119
Übersicht 7119
Voraussetzungen und Einschränkungen 7119
Architektur 7120
Tools 7120
Bewährte Methoden 7121
Epen 7121
Fehlerbehebung 7125
Zugehörige Ressourcen 7125
Anlagen 7125
Stellen Sie die Verschlüsselung für Amazon EMR-Daten im Ruhezustand sicher 7126
Übersicht 7126
Voraussetzungen und Einschränkungen 7127
Architektur 7127
Tools 7128
Epen 7128
Zugehörige Ressourcen 7131
Anlagen 7131
Stellen Sie sicher, dass ein IAM-Profil einer Instanz zugeordnet ist EC2 7132
Übersicht 7132
Voraussetzungen und Einschränkungen 7132
Architektur 7133

Tools 7133
Epen 7134
Zugehörige Ressourcen 7137
Anlagen 7137
Stellen Sie sicher, dass neue Amazon Redshift Redshift-Cluster verschlüsselt sind 7138
Übersicht 7138
Voraussetzungen und Einschränkungen 7138
Architektur 7138
Tools 7139
Epen 7140
Zugehörige Ressourcen 7142
Anlagen 7142
Exportieren Sie einen Bericht über IAM Identity Center-Identitäten und deren Zuweisungen ... 7143
Übersicht 7143
Voraussetzungen und Einschränkungen 7144
Architektur 7145
Tools 7145
Epen 7146
Fehlerbehebung 7148
Zugehörige Ressourcen 7149
Zusätzliche Informationen 7150
Helfen Sie, das geplante Löschen von KMS-Schlüsseln zu verhindern 7152
Übersicht 7152
Voraussetzungen und Einschränkungen 7152
Architektur 7153
Tools 7154
Epen 7155
Zugehörige Ressourcen 7158
Zusätzliche Informationen 7159
Anlagen 7159
Identifizieren Sie öffentliche Amazon S3 S3-Buckets in AWS Organizations 7160
Übersicht 7160
Voraussetzungen und Einschränkungen 7160
Architektur 7161
Tools 7162
Epen 7163

Fehlerbehebung 7167
Zugehörige Ressourcen 7168
Zusätzliche Informationen 7168
AWS-Sicherheitsprotokolle in Microsoft Sentinel aufnehmen 7170
Übersicht 7170
Voraussetzungen und Einschränkungen 7170
Architektur 7172
Tools 7173
Bewährte Methoden 7174
Epen 7174
Zugehörige Ressourcen 7186
AWS Organizations Richtlinien als Code verwalten 7187
Übersicht 7187
Voraussetzungen und Einschränkungen 7188
Architektur 7188
Tools 7190
Bewährte Methoden 7191
Epen 7191
Fehlerbehebung 7212
Zugehörige Ressourcen 7213
Zusätzliche Informationen 7214
Verwalten Sie IAM Identity Center-Berechtigungssätze mit CodePipeline 7216
Übersicht 7216
Voraussetzungen und Einschränkungen 7216
Architektur 7218
Tools 7219
Bewährte Methoden 7220
Epen 7220
Fehlerbehebung 7232
Zugehörige Ressourcen 7233
Anmeldeinformationen mit AWS Secrets Manager verwalten 7234
Übersicht 7234
Voraussetzungen und Einschränkungen 7234
Architektur 7234
Tools 7235
Epen 7235

Zugehörige Ressourcen 7237
Zusätzliche Informationen 7237
..... 7240
Übersicht 7240
Voraussetzungen und Einschränkungen 7240
Architektur 7241
Tools 7241
Epen 7242
Zugehörige Ressourcen 7245
Anlagen 7245
Überwachen Sie Amazon EMR-Cluster beim Start auf Verschlüsselung während der Übertragung 7246
Übersicht 7246
Voraussetzungen und Einschränkungen 7247
Architektur 7247
Tools 7248
Epen 7249
Zugehörige Ressourcen 7251
Anlagen 7252
ElastiCache Amazon-Cluster auf Verschlüsselung im Ruhezustand überwachen 7253
Übersicht 7253
Voraussetzungen und Einschränkungen 7254
Architektur 7255
Tools 7255
Epen 7256
Zugehörige Ressourcen 7259
Anlagen 7259
Überwachen Sie EC2 Instanz-Schlüsselpaare 7260
Übersicht 7260
Voraussetzungen und Einschränkungen 7260
Architektur 7261
Tools 7261
Epen 7262
Zugehörige Ressourcen 7266
Anlagen 7266
IAM-Root-Benutzeraktivitäten überwachen 7267

Übersicht 7267
Voraussetzungen und Einschränkungen 7267
Architektur 7268
Tools 7268
Epen 7270
Zugehörige Ressourcen 7275
Zusätzliche Informationen 7275
Benachrichtigen, wenn ein IAM-Benutzer erstellt wird 7276
Übersicht 7276
Voraussetzungen und Einschränkungen 7276
Architektur 7276
Tools 7277
Epen 7278
Zugehörige Ressourcen 7281
Anlagen 7281
Verhindern Sie den Internetzugang mithilfe eines SCP 7282
Übersicht 7282
Voraussetzungen und Einschränkungen 7282
Tools 7283
Bewährte Methoden 7283
Epen 7284
Zugehörige Ressourcen 7286
Beschränken Sie den Zugriff anhand der IP-Adresse oder des Standorts 7287
Übersicht 7287
Voraussetzungen und Einschränkungen 7287
Tools 7288
Epen 7289
Zugehörige Ressourcen 7295
Git-Repositorys nach vertraulichen Informationen scannen 7296
Übersicht 7296
Voraussetzungen und Einschränkungen 7296
Architektur 7296
Tools 7297
Bewährte Methoden 7297
Epen 7297
Zugehörige Ressourcen 7301

Benachrichtigungen von der AWS-Netzwerk-Firewall an einen Slack-Channel senden 7302
Übersicht 7302
Voraussetzungen und Einschränkungen 7302
Architektur 7303
Tools 7304
Epen 7305
Zugehörige Ressourcen 7311
Zusätzliche Informationen 7311
Vereinfachen Sie die Verwaltung privater Zertifikate mithilfe von AWS Private CA und AWS RAM 7316
Übersicht 7316
Voraussetzungen und Einschränkungen 7317
Architektur 7317
Tools 7318
Epen 7319
Zugehörige Ressourcen 7328
Zusätzliche Informationen 7329
Deaktivieren Sie die Sicherheitsstandardkontrollen für alle Security Hub Hub-Mitgliedskonten 7330
Übersicht 7330
Voraussetzungen und Einschränkungen 7330
Architektur 7331
Tools 7332
Epen 7333
Zugehörige Ressourcen 7337
Aktualisieren Sie die AWS-CLI-Anmeldeinformationen aus dem IAM Identity Center mit PowerShell 7338
Übersicht 7338
Voraussetzungen und Einschränkungen 7338
Architektur 7339
Tools 7339
Bewährte Methoden 7340
Epen 7340
Fehlerbehebung 7343
Zugehörige Ressourcen 7343
Zusätzliche Informationen 7344
Verwenden Sie AWS Config zur Überwachung von Amazon Redshift 7346

Übersicht 7346
Voraussetzungen und Einschränkungen 7346
Architektur 7347
Tools 7347
Epen 7348
Zugehörige Ressourcen 7352
Zusätzliche Informationen 7352
Verwenden Sie die Network Firewall, um DNS-Domainnamen aus ausgehendem Netzwerkverkehr zu erfassen 7353
Übersicht 7353
Voraussetzungen und Einschränkungen 7353
Architektur 7354
Tools 7355
Epen 7355
Verwenden Sie Terraform, um es automatisch zu aktivieren GuardDuty 7372
Übersicht 7372
Voraussetzungen und Einschränkungen 7373
Architektur 7375
Tools 7376
Epen 7377
Zugehörige Ressourcen 7388
Zusätzliche Informationen 7388
Überprüfen Sie die bewährten Verfahren für PCI DSS 4.0 7390
Übersicht 7390
Voraussetzungen und Einschränkungen 7391
Tools 7392
Epen 7392
Zugehörige Ressourcen 7395
Zusätzliche Informationen 7395
Anlagen 7396
..... 7397
Übersicht 7397
Voraussetzungen und Einschränkungen 7397
Architektur 7398
Tools 7398
Epen 7399

Zugehörige Ressourcen 7402
Anlagen 7403
..... 7404
Übersicht 7404
Voraussetzungen und Einschränkungen 7404
Architektur 7405
Tools 7405
Epen 7406
Zugehörige Ressourcen 7409
Anlagen 7409
Mehr Muster 7410
..... 7413

AWS Präskriptive Beratungsmuster

Die Prescriptive Guidance-Muster von Amazon Web Services (AWS) bieten step-by-step Anweisungen, Architektur, Tools und Code für die Implementierung bestimmter Cloud-Migrations-, Modernisierungs- und Bereitstellungsszenarien. Diese Muster, die von Fachexperten unter geprüft werden AWS, richten sich an Entwickler und praktische Anwender, die eine Migration zu planen oder gerade dabei sind, eine Migration zu vorzunehmen. AWS Sie unterstützen auch Benutzer, die bereits im Einsatz sind AWS und nach Möglichkeiten suchen, ihren Cloud-Betrieb zu optimieren oder zu modernisieren.

Sie können diese Muster verwenden, um Ihre lokalen oder Cloud-Workloads unterschiedlicher Komplexität in die Cloud zu verlagern AWS und Ihre Bemühungen um die Einführung, Optimierung und Modernisierung der Cloud zu beschleunigen, unabhängig davon, ob Sie sich in der Machbarkeitsnachweisphase, Planungs- oder Implementierungsphase Ihres Projekts befinden. Zum Beispiel für ein Cloud-Migrationsprojekt:

- In der Planungsphase können Sie die verschiedenen Optionen bewerten, zu denen Sie migrieren können AWS. Sie können das richtige Muster wählen, das Ihren Bedürfnissen entspricht, je nachdem, ob Sie umziehen, rehosten, eine neue Plattform oder eine neue Architektur einrichten möchten. Sie können sich auch mit den verschiedenen Tools vertraut machen, die für die Migration verfügbar sind, und mit der Planung der Lizenzbeschaffung beginnen oder erste Gespräche mit Anbietern aufnehmen.
- In der Machbarkeitsstudie und in der Implementierungsphase können Sie den step-by-step Anweisungen folgen, die in dem Muster für die Migration Ihres Workloads enthalten sind. AWS Jedes Muster enthält Details wie Voraussetzungen, Zielreferenzarchitekturen, Tools, step-by-step Aufgaben, bewährte Methoden, Problembehandlung und Code.
- Wenn Sie das bereits verwenden AWS Cloud, können Sie Muster finden, die Ihnen helfen, Ihre Nutzung von Cloud-Ressourcen zu modernisieren, zu optimieren, zu skalieren und zu sichern.

Verwenden Sie die folgenden Links oder die Filter- und Suchoptionen auf der AWS Prescriptive Guidance-Startseite, um nach technischen Bereichen aufgeschlüsselte Musterlisten aufzurufen.

- Grundlagen der Cloud
- KI und maschinelles Lernen
- Analysen
- Datenverarbeitung

- Datenbanken und Speicher
- Tools für Entwickler
- IoT
- Migration und Modernisierung
- Verwaltung
- Sicherheit, Identität und Compliance

Alle Veröffentlichungen, einschließlich Leitfäden, Strategien und Mustern, finden Sie auf der AWS Prescriptive Guidance-Startseite.

Cloud-Grundlagen

Themen

- Automatisieren Sie die Kontoerstellung mit dem Landing Zone Accelerator auf AWS
- Automatische Inventarisierung von AWS Ressourcen für mehrere Konten und Regionen
- Konfiguration von VPC Flow Logs für die Zentralisierung über AWS-Konten hinweg
- Automatisches Taggen Transit Gateway Gateway-Anhängen mithilfe von AWS Organizations
- Mehr Muster

Automatisieren Sie die Kontoerstellung mit dem Landing Zone Accelerator auf AWS

Erstellt von Justin Kuskowski (AWS), Joe Behrens (AWS) und Nathan Scott (AWS)

Übersicht

Dieses Muster erklärt, wie Sie die Landing Zone Accelerator-Lösung verwenden, um automatisch eine neue AWS Lösung bereitzustellen, AWS-Konto wenn ein autorisierter Benutzer eine Anfrage einreicht. Es dient AWS Step Functions zur Orchestrierung einer Reihe von AWS Lambda Funktionen. Die Lambda-Funktionen fügen die Kontoinformationen einem Git-Repository hinzu, initiieren eine AWS CodePipeline Pipeline und überprüfen, ob die erforderlichen AWS Ressourcen bereitgestellt wurden. Wenn der Vorgang abgeschlossen ist, erhält der Benutzer eine Benachrichtigung, dass das Konto erstellt wurde.

Optional können Sie Microsoft Entra ID-Gruppen integrieren und während der Kontoerstellung AWS IAM Identity Center Berechtigungssätze zuweisen. Wenn Ihre Organisation Microsoft Entra ID als Identitätsquelle verwendet, hilft Ihnen diese optionale Funktion dabei, den Zugriff auf das neue Konto automatisch zu verwalten und zu konfigurieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zugriff auf das Verwaltungskonto in AWS Organizations
- AWS Cloud Development Kit (AWS CDK) Version 2.118.0 oder höher, installiert und konfiguriert
- Python Version 3.9 oder höher, installiert
- AWS Command Line Interface (AWS CLI) Version 2.13.19 oder höher, installiert
- Docker Version 24.0.6 oder höher, installiert
- Landing Zone Accelerator auf AWS Lösung, bereitgestellt im Verwaltungskonto
- (Optional) Microsoft Entra ID und IAM Identity Center, integriert

Einschränkungen

Der Workflow zur Kontoerstellung unterstützt sequentielle Ausführungen zur Bereitstellung eines einzelnen Kontos. AWS-Konto Diese Einschränkung stellt sicher, dass der Workflow zur

Kontoerstellung erfolgreich abgeschlossen wurde, ohne dass während eines parallel Laufs um Ressourcen konkurriert werden muss.

Architektur

Zielarchitektur

Die folgende Abbildung zeigt die allgemeine Architektur der Automatisierung der Erstellung einer neuen Datei AWS-Konto mithilfe des Landing Zone Accelerators. AWS AWS Step Functions orchestriert die Automatisierung. Jede Aufgabe im Step Functions Functions-Workflow wird von einer oder mehreren AWS Lambda Funktionen ausgeführt.

Das Diagramm zeigt den folgenden Workflow:

1. Der Benutzer fordert ein Konto an, indem er entweder ein Python-Skript ausführt oder Amazon API Gateway verwendet.
2. Der Orchestrator-Workflow zur Kontoerstellung beginnt in AWS Step Functions.
3. Der Workflow aktualisiert die `account-config.yaml` Datei im Quellcode-Repository. Außerdem wird der Landing Zone Accelerator in der AWS Pipeline gestartet und der Status der Pipeline überprüft. Diese Pipeline erstellt und richtet das neue Konto ein. Weitere Informationen dazu, wie das funktioniert, finden Sie in der Architekturübersicht für den Landing Zone Accelerator unter AWS.
4. (Optional) Wenn die Pipeline abgeschlossen ist, überprüft der Workflow, ob die Gruppe in Microsoft Entra ID vorhanden ist. Wenn die Gruppe nicht in Microsoft Entra ID vorhanden ist, fügt der Workflow die Gruppe zu Microsoft Entra ID hinzu.
5. Der Workflow führt zusätzliche Schritte durch, die der Landing Zone Accelerator auf der AWS Lösung nicht ausführen kann. Zu den Standardschritten gehören:
   - Erstellen eines Kontoalias in AWS Identity and Access Management (IAM)
   - Hinzufügen von Tags an das Konto in AWS Organizations
   - Erstellen von Parametern im AWS Systems Manager Parameter Store auf der Grundlage der dem Konto zugewiesenen Tags
6. (Optional) Der Workflow weist der Microsoft Entra ID-Gruppe, die Sie zuvor angegeben haben, einen oder mehrere Berechtigungssätze zu. Die Berechtigungssätze ermöglichen es Benutzern in der Gruppe, auf das neue Konto zuzugreifen und die von Ihnen konfigurierten Aktionen auszuführen.

7. Eine AWS Lambda Funktion führt QA- und Validierungstests durch. Sie validiert die Erstellung von Ressourcen, prüft, ob Tags erstellt wurden, und überprüft, ob Sicherheitsressourcen bereitgestellt wurden.
8. Der Workflow gibt das Konto frei und verwendet Amazon Simple Email Service (Amazon SES), um den Benutzer darüber zu informieren, dass der Vorgang erfolgreich abgeschlossen wurde.

Weitere Informationen zum Step Functions-Workflow finden Sie unter Step Functions Functions-Workflow-Diagramm im Abschnitt Zusätzliche Informationen dieses Musters.

Microsoft Entra ID-Anwendungen

Wenn Sie sich für die Integration mit Microsoft Entra ID entscheiden, erstellen Sie bei der Bereitstellung dieses Musters die folgenden beiden Anwendungen:

- Eine Anwendung, die mit IAM Identity Center verknüpft ist und sicherstellt, dass Microsoft Entra ID-Gruppen in IAM Identity Center verfügbar sind. In diesem Beispiel wird diese Microsoft Entra ID-Anwendung benanntLZA2.
- Eine Anwendung, die es einer Lambda-Funktion ermöglicht, mit Microsoft Entra ID zu kommunizieren und Microsoft Graph aufzurufen. APIs In diesem Muster wird diese Anwendung benannt. `create_aws_account`

Diese Anwendungen sammeln Daten, die zum Synchronisieren der Microsoft Entra ID-Gruppe und zum Zuweisen von Berechtigungssätzen verwendet werden.

Tools

AWS-Services

- Amazon API Gateway unterstützt Sie bei der Erstellung, Veröffentlichung, Wartung, Überwachung und Sicherung von REST, HTTP und WebSocket APIs in jeder Größenordnung. In diesem Muster verwenden Sie API Gateway, um die Verfügbarkeit von AWS-Konto Namen zu überprüfen, den AWS Step Functions Workflow zu initiieren und den Status der Ausführung von Step Functions zu überprüfen.
- AWS Cloud Development Kit (AWS CDK)ist ein Softwareentwicklungs-Framework, das Ihnen hilft, AWS Cloud Infrastruktur im Code zu definieren und bereitzustellen.
- AWS Control Towerhilft Ihnen bei der Einrichtung und Verwaltung einer Umgebung AWS mit mehreren Konten und folgt dabei den vorgeschriebenen Best Practices.

- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS Lambda Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen. AWS-Konten Diese Lösung verwendet eine EventBridge Regel, die eine Lambda-Funktion startet, wenn sich der Status des Step Functions Functions-Workflows auf `FailedTimed-out`, oder `Aborted` ändert.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS IAM Identity Centerhilft Ihnen dabei, den Single Sign-On (SSO) -Zugriff auf all Ihre Anwendungen AWS-Konten und Cloud-Anwendungen zentral zu verwalten.
- AWS Key Management Service (AWS KMS) hilft Ihnen dabei, kryptografische Schlüssel zu erstellen und zu kontrollieren, um Ihre Daten zu schützen. In diesem Muster werden AWS KMS Schlüssel verwendet, um Daten zu verschlüsseln, z. B. Daten, die in Amazon Simple Storage Service (Amazon S3) gespeichert sind, Lambda-Umgebungsvariablen und Daten in Step Functions.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Organizationsist ein Kontoverwaltungsservice, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie erstellen und zentral verwalten.
- Amazon Simple Email Service (Amazon SES) unterstützt Sie beim Senden und Empfangen von E-Mails mithilfe Ihrer eigenen E-Mail-Adressen und Domains. Nachdem ein neues Konto erfolgreich erstellt wurde, erhalten Sie eine Benachrichtigung über Amazon SES.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen. Wenn bei der Kontoerstellung ein Fehler auftritt, sendet Amazon SNS eine Benachrichtigung an die von Ihnen konfigurierten E-Mail-Adressen.
- AWS Step Functionsist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Funktionen und andere Funktionen kombinieren können, um geschäftskritische Anwendungen AWS-Services zu erstellen.
- AWS Systems Manager Parameter Store bietet sicheren, hierarchischen Speicher für die Verwaltung von Konfigurationsdaten und Geheimnissen.

Andere Tools

- awscurl automatisiert den Prozess des Signierens von AWS API-Anfragen und hilft Ihnen, Anfragen als Standard-Curl-Befehl zu stellen.
- Microsoft Entra ID, früher bekannt als Azure Active Directory, ist ein cloudbasierter Identitäts- und Zugriffsverwaltungsdienst.
- Microsoft Graph APIs hilft Ihnen beim Zugriff auf Daten und Informationen in Microsoft-Cloud-Diensten wie Microsoft Entra und Microsoft 365.

Code-Repository

Der Code für dieses Muster ist im GitHub lza-account-creation-workflowRepository verfügbar.

Das Verzeichnis lambda_layer enthält die folgenden Ebenen, auf die in mehr als einer Lambda-Funktion verwiesen wird:

- account_creation_helper — Diese Ebene enthält die Module zur Übernahme von Rollen und zur Überprüfung des Fortschritts. AWS Service Catalog
- boto3 — Diese Ebene enthält das AWS SDK für Python (Boto3)Modul, um sicherzustellen, dass die neueste Version installiert ist. AWS Lambda
- identity_center_helper — Diese Ebene unterstützt Aufrufe von IAM Identity Center.

Das Verzeichnis lambda_src enthält die folgenden Lambda-Funktionen:

- AccountTagToSsmParameter— Diese Funktion verwendet die an das Konto angehängten Tags, um Parameter AWS Organizations im Parameter Store zu erstellen. Jeder Parameter beginnt mit einem `/account/tags/` Präfix.
- AttachPermissionSet— Diese Funktion fügt einer IAM Identity Center-Gruppe einen Berechtigungssatz hinzu.
- Azure ADGroup Sync — Diese Funktion synchronisiert die Microsoft Entra ID-Zielgruppe mit dem IAM Identity Center.
- CheckForRunningProcesses— Diese Funktion prüft, ob die `AWSAccelerator-Pipeline` Pipeline derzeit läuft. Wenn die Pipeline läuft, verzögert die Funktion den AWS Step Functions Workflow.
- CreateAccount— Diese Funktion verwendet AWS Service Catalog und AWS Control Tower , um das Neue zu erstellen AWS-Konto.

- CreateAdditionalResources— Diese Funktion erstellt die AWS Ressourcen, die nicht von Landing Zone Accelerator oder verwaltet werden AWS CloudFormation, wie z. B. der Alias und die AWS Service Catalog Tags des Kontos.
- GetAccountStatus— Diese Funktion sucht nach dem bereitgestellten Produkt, AWS Service Catalog um festzustellen, ob der Kontoerstellungsprozess abgeschlossen ist.
- GetExecutionStatus— Diese Funktion ruft den Status einer laufenden oder abgeschlossenen AWS Step Functions Ausführung ab.
- NameAvailability— Diese Funktion prüft, ob ein AWS-Konto Name bereits in AWS Organizations existiert.
- ReturnResponse— Wenn die Kontoerstellung erfolgreich war, gibt diese Funktion die ID des neuen Kontos zurück. Wenn die Kontoerstellung nicht erfolgreich war, wird eine Fehlermeldung zurückgegeben.
- RunStepFunction— Diese Funktion führt den AWS Step Functions Workflow aus, der das Konto erstellt.
- SendEmailWithSES — Diese Funktion sendet E-Mails an die Benutzer, die darauf warten, dass die Kontoerstellung abgeschlossen ist.
- ADGroupSyncToSSO validieren — Diese Funktion überprüft, ob die angegebenen Microsoft Entra ID-Gruppen mit IAM Identity Center synchronisiert sind.
- ValidateResources— Diese Funktion überprüft, ob alle AWS Control Tower Anpassungen erfolgreich ausgeführt wurden.

Bewährte Methoden

Wir empfehlen die folgenden Benennungskonventionen für: AWS CDK

- Starten Sie alle Parameter mit einem `p` Präfix.
- Starten Sie alle Bedingungen mit einem `c` Präfix.
- Starten Sie alle Ressourcen mit einem `r` Präfix.
- Startet alle Ausgaben mit einem o Präfix.

Epen

Stellen Sie die IAM-Rollen für Validierung und Tagging bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereite den Landing Zone Accelerator auf AWS die Anpassung vor.	1. Erstellen Sie im AWS Code-Repository von Landing Zone Accelerator eine Datei mit dem Namen `customizations-config.yaml` . Sie verwenden diese Datei, um Anpassungen für die Kernlösung zu definieren. Weitere Informationen finden Sie unter Anpassen der Lösung. 2. Erstellen Sie in der `customizations-config.yaml` Datei einen Abschnitt mit dem Namen `cloudFormationStacks` .	AWS DevOps
Bereiten Sie sich auf die Bereitstellung der `lza-account-creation-validation` Rolle vor.	Jetzt passen Sie die Lösung so an, dass die `lza-account-creation-validation` IAM-Rolle in allen Konten außer dem Verwaltungskonto bereitgestellt wird. Diese Rolle bietet der `ValidateResources` Lambda-Funktion schreibgeschützten Zugriff auf die neuen Konten.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Laden Sie die account-creation-validation-role.yaml-Datei von herunter. GitHub 2. Speichern Sie die Datei an dem Speicherort, der im Abschnitt „Vorlagen“ der `customizations-config.yaml` Datei angegeben ist. 3. Öffnen Sie die `customizations-config.yaml` Datei. 4. Fügen Sie in dem `cloudFormationStacks` Abschnitt den folgenden Code hinzu. Aktualisiere das Ziel nach AWS-Region Bedarf für deine landing zone: `- deploymentTargets: organizationalUnits: - Root excludedAccounts: - Management description: IAM Role to allow Account Validation name: lza-account-creation-validation regions:`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>- us-
	east-1
	template:
	cloudformation/acc
	ount-creation-vali
	dation-role.yaml
	runOrder: 1
	terminati
	onProtection: true
	parameters:
	- name:
	pManagementAccount
	Id
	value:
	"{{ account Managemen
	t }}"</pre> 5. Speichern und schließen Sie die Datei `customiza tions-config.yaml` .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie sich auf die Bereitstellung der `account-tagging-to-ssm-parameter-role` Rolle vor.	Jetzt passen Sie die Lösung so an, dass die `account-tagging-to-ssm-parameter-role` IAM-Rolle in allen Konten außer dem Verwaltungskonto bereitgestellt wird. Diese Rolle wird verwendet, um die Parameter im AWS Systems Manager Parameter Store zu erstellen. 1. Laden Sie die Datei account-tagging-to-ssm-parameter-role.yaml von herunter. GitHub 2. Speichern Sie die Datei an dem Speicherort, der im Abschnitt „Vorlagen“ der Datei angegeben ist. `customizations-config.yaml` 3. Öffnen Sie die `customizations-config.yaml` Datei. 4. Fügen Sie in dem `cloudFormationStacks` Abschnitt den folgenden Code hinzu. Aktualisiere das Ziel nach AWS-Region Bedarf für deine landing zone: `- deploymentTargets:`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>organizationalUnits:
	- Root
	excludedAccounts:
	- Management
	description: IAM Role to create SSM Parameters based on Account Tagging
	name: lza-account-tagging-to-ssm-parameter
	regions:
	- us-east-1
	template: cloudformation/account-tagging-to-ssm-parameter-role.yaml
	runOrder: 1
	terminationProtection: true
	
	parameters:
	- name: pManagementAccountId
	value: "{{ account Management }}"</pre> 5. Speichern und schließen Sie die Datei `customizations-config.yaml` .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie sich auf die Bereitstellung der `config-log-validation-role` Rolle vor.	Jetzt passen Sie die Lösung an, um die `config-log-validation-role` IAM-Rolle im Protokollarchivkonto bereitzustellen. Diese Rolle ermöglicht der `ValidateResources` Lambda-Funktion den Zugriff auf den Amazon S3 S3-Bucket für Protokollierung und AWS Config Zugriffsregeln. 1. Laden Sie die config-log-validation-role.yaml-Datei von herunter. GitHub 2. Speichern Sie die Datei an dem Speicherort, der im Abschnitt „Vorlagen“ der `customizations-config.yaml` Datei angegeben ist. 3. Öffnen Sie die `customizations-config.yaml` Datei. 4. Fügen Sie in dem `cloudFormationStacks` Abschnitt den folgenden Code hinzu. Aktualisiere das Ziel nach AWS-Region Bedarf für deine landing zone: `- deploymentTargets: accounts:`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>- LogArchive
	descripti
	on: IAM Role to
	validate Config and
	Logs
	name:
	lza-config-log-val
	idation-role
	regions:
	- us-
	east-1
	template:
	cloudformation/con
	fig-log-validation-
	role.yaml
	runOrder: 1
	terminati
	onProtection: true
	
	parameters:
	- name:
	pManagementAccount
	Id
	value:
	"{{ account Managemen
	t }}"</pre>
	5. Speichern, schließen und übernehmen Sie die an der `customiza tions-config.yaml` Datei vorgenommenen Änderungen.	

(Optional) Daten von Microsoft Entra ID abrufen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Anwendung, die es einer Lambda-Funktion ermöglicht, mit Microsoft Entra ID zu kommunizieren.	1. Registrieren Sie die `create_aws_account` Anwendung im Microsoft Entra ID Admin Center. Anweisungen finden Sie in der Microsoft-Dokumentation unter Registrieren einer Anwendung.
	2. Folgen Sie den Anweisungen unter Aktualisieren der angeforderten Berechtigungen einer App in der Microsoft-Dokumentation, um die folgenden Microsoft Graph-Berechtigungen für die `create_aws_account` Anwendung zu konfigurieren:
	• Anwendung.Lesen.Alles
	  • Typ: Anwendung
	  • Zustimmung des Administrators erforderlich: Ja
	• AppRoleAssignment. ReadWrite. Alle
	  • Typ: Anwendung
	  • Zustimmung des Administrators erforderlich: Ja
	• Gruppe. ReadWrite. Alle
	  • Typ: Anwendung
		Microsoft Entra ID

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	• Zustimmung des Administrators erforderlich: Ja
	• ServicePrincipalEndpoint.Lesen.Alle
	  • Typ: Anwendung
	  • Zustimmung des Administrators erforderlich: Ja
	• Synchronisation. ReadWrite. Alle
	  • Typ: Anwendung
	  • Zustimmung des Administrators erforderlich: Ja
	• Benutzer.Lesen
	  • Typ: Delegiert
	  • Zustimmung des Administrators erforderlich: Nein	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ruft Werte für die `create_aws_account` Anwendung ab.	Jetzt rufen Sie die Werte ab, die Sie für die `create_aws_account` Anwendung benötigen. 1. Navigieren Sie im Microsoft Entra ID Admin Center zu App-Registrierungen und wählen Sie `create_aws_account` dann. 2. Wählen Sie im linken Bereich „Übersicht“ aus. 3. Notieren Sie sich auf der Übersichtsseite die folgenden Werte: • Anwendungs-ID (Client) • Verzeichnis-ID (Mandanten-ID) 4. Wählen Sie im linken Bereich unter Verwalten die Option Certificates & Secrets aus. 5. Wählen Sie auf der Seite Certificates & Secrets den Tab Client Secrets aus und notieren Sie sich dann die folgenden Werte: • Wert für den geheimen Clientschlüssel • Geheime Kunden-ID	Microsoft Entra ID

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Anwendung, die Microsoft Entra ID mit IAM Identity Center integriert.	Registrieren Sie die `LZA2` Anwendung im Microsoft Entra ID Admin Center. Anweisungen finden Sie in der Microsoft-Dokumentation unter Registrieren einer Anwendung.	Microsoft Entra ID
Ruft Werte für die `LZA2` Anwendung ab.	Jetzt rufen Sie die Werte ab, die Sie für die `LZA2` Anwendung benötigen. 1. Navigieren Sie im Microsoft Entra ID Admin Center zu Unternehmensanwendungen und wählen Sie `LZA2` dann. 2. Wählen Sie im linken Bereich „Übersicht“ aus. 3. Notieren Sie sich auf der Übersichtsseite die folgenden Werte: • Name • Objekt-ID 4. Wählen Sie im linken Bereich unter Verwalten die Option Manifest aus. 5. Suchen Sie in der JSON-Datei im `appRoles` Abschnitt nach der benannten App-Rolle`User`. 6. Notieren Sie sich den `id` Wert für diese App-Rolle.	Microsoft Entra ID

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie ein Geheimnis.	1. Geben Sie in der AWS CLI den folgenden Befehl ein, um die Variablen zu erstellen. Verwenden Sie die Werte, die Sie für die LZA2 Anwendungen `create_aws_account` und abgerufen haben:
	`# Variables for create_aws_account app TENANT_ID='<Directory ID>' CLIENT_ID='<Application ID>' SECRET_ID='<Client secret ID>' SECRET_VALUE='<Client secret value>'`
	`# Variables for LZA2 app OBJECT_ID='<Object ID>' APP_ROLE_ID='<App role ID>' ENTERPRISE_APP_NAME='<Name>'`
	2. Geben Sie den folgenden Befehl ein, um ein Geheimnis mit dem Namen `GraphApiSecret` in zu erstellen AWS Secrets Manager:
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`aws secretsmanager create-secret \ --name GraphApiSecret \ --secret-string "{\"client_id\": \"${CLIENT_ID}\", \"tenant_id\": \"${TENANT_ID}\", \"object_id\": \"${OBJECT_ID}\", \"app_role_id\": \"${APP_ROLE_ID}\", \"secret_value\": \"${SECRET_VALUE}\", \"secret_id\": \"${SECRET_ID}\"}"`
	
	Wenn Sie das Geheimnis in future aktualisieren müssen, können Sie die Variablen aktualisieren und den folgenden Befehl ausführen:
	
	`aws secretsmanager update-secret \ --secret-id GraphApiSecret \ --secret-string "{\"client_id\": \"${CLIENT_ID}\", \"tenant_id\": \"${TENANT_ID}\", \"object_id\": \"${OBJECT_ID}\", \"app_role_id\": \"${APP_ROLE_ID}\", \"secret_value\": \"${SECRET_VALUE}\`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`", \"secret_id\": \"${SECRET_ID}\"}"`	

Stellen Sie die Lösung bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Klonen Sie den Quellcode.	1. Geben Sie den folgenden Befehl ein, um das lza-account-creation-workflowRepository zu klonen:
	`git clone https://github.com/aws-samples/lza-account-creation-workflow`
	2. Geben Sie den folgenden Befehl ein, um in das `config` Verzeichnis des geklonten Repositorys zu navigieren:
	`cd lza-account-creation-workflow/config`
		DevOps Ingenieur

Aktualisieren Sie die `deploy-config.yaml` Datei.	1. Öffnen Sie die `deploy-config.yaml` Datei. 2. Überprüfen Sie die Vorlage und aktualisieren Sie die Werte nach Bedarf für die Bereitstellung in Ihrer AWS Umgebung. Aktualisieren Sie beispielsweise Werte für Folgendes:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `accountCreationFailure` • `accountCompletionFromEmail` • `ssoLoginUrl` • `rootEmailPrefix` • `rootEmailDomain` 3. Wenn Sie mit Microsoft Entra ID integrieren, gehen Sie wie folgt vor: • Setzen Sie `enableAzureADIntegration` auf `true`. • Geben Sie als `graphApiSecretName` Wert das Geheimnis ein, das Sie zuvor erstellt haben (`GraphApiSecret`). 4. Speichern und schließen Sie die Datei `deploy-config.yaml` .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die Lösung in Ihrer AWS Umgebung bereit.	1. Geben Sie den folgenden Befehl ein:
	`cdk bootstrap <account-number>/<Region>`
	Weitere Informationen finden Sie in der Dokumentation unter Bootstrapping. AWS CDK
	2. Geben Sie den folgenden Befehl ein, um die Vorlage zu synthetisieren: CloudFormation
	`cdk synth`
	Weitere Informationen finden Sie in der AWS CDK Dokumentation unter Konfiguration und Durchführung der AWS CDK Stack-Synthese.
	3. Geben Sie den folgenden Befehl ein, um die Lösung bereitzustellen.
	`cdk deploy`
	Weitere Informationen finden Sie in der AWS CDK Dokumentation unter
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bereitstellen von AWS CDK Anwendungen. **Note** Diese Lösung verwendet einen Amazon S3 S3-Bucket , um den Quellcode für diese Lösung zu speichern. Sie können das Skript upload_to_source_bucket.py verwenden, um ein Archiv des Quellcode s zu erstellen und eine aktualisierte Version hochzuladen.	

Option 1 — Erstellen Sie ein Konto mit Python

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie, welche Argumente verwendet werden sollen.	Wählen Sie aus, welche Argumente verwendet werden sollen, wenn Sie das Python-Skript ausführen, das den Step Functions-Workflow initiiert. Eine vollständige Liste der Argumente finden Sie im Abschnitt Zusätzliche Informationen dieses Musters.	AWS DevOps, Python

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Starten Sie das Python-Skript.	1. Geben Sie den folgenden Befehl ein, um zum geklonten Repository zu navigieren:
	`cd lza-account-creation-workflow`
	2. Führen Sie das Python-Skript aus, das den Step Functions Functions -Workflow initiiert. Im Folgenden finden Sie einen Beispielbefehl, der Beispielargumente und Werte enthält:
	`python ./run-stepfunction.py \ --account-name "lza-test-01" \ --support-dl "johnsmith@example.com" \ --managed-org-unit "Workloads/Workload-1" \ --purpose "Testing new micro service" \ --force-update true \ --ad-integration "{\"CustomerAccountAdmin\": \"platform-admin\", \"CustomerAccountDev\": \"workload1-app1\" }" \`
		DevOps Ingenieur, Python

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--bypass-creation true \ --tags APPLICATION=TestingMicroService` 3. Warten Sie, bis Sie eine Benachrichtigung erhalten, dass das Konto erfolgreich erstellt wurde. **Note** Wenn die Kontoerstellung fehlschlägt, sendet Amazon SNS eine Benachrichtigung an die E-Mail-Adressen, die Sie `accountCreationFailure` in der `deploy-config.yaml` Datei definiert haben. Der Kontoanforderer wird nicht benachrichtigt.	

Option 2 — Erstellen Sie ein Konto mit API Gateway und awscurl

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Variablen für awscurl ein.	1. Geben Sie den folgenden Befehl ein, um in das	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Quellcodeverzeichnis zu navigieren:
	
	`cd lza-account-creation-workflow`
	
	2. Geben Sie den folgenden Befehl ein, um die AWS Zugriffsschlüsselvariablen festzulegen. Sie können die Variablen aus dem AWS Access Portal kopieren und sie dann in eine Shell einfügen. Im Folgenden wird ein Beispiel gezeigt:
	
	`export AWS_ACCESS_KEY_ID="<id>"`
	`export AWS_SECRET_ACCESS_KEY="<key>"`
	`export AWS_SESSION_TOKEN="<token>"`
	
	3. Geben Sie den folgenden Befehl ein, um die AWS-Region für API-Aufrufe festzulegen:
	
	`export AWS_REGION=$(aws configure get region)`
	
	4. Geben Sie den folgenden Befehl ein, um den API-Gateway-Endpunkt aus der `lza-account-creation-workflow-applic`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`ation` CloudFormation Ausgabe abzurufen: `export API_GATEWAY_ENDPOINT=$(aws cloudformation describe-stacks --stack-name "lza-account-creation-workflow-application" --query 'Stacks[*].Outputs[?OutputKey==`oApiGatewayCreateAccountEndpoint`].OutputValue' --output text)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Verfügbarkeit von Namen.	Geben Sie den folgenden Befehl ein, um zu überprüfen, ob der Name für verfügbar ist AWS-Konto. Durch <AWS_ACCOUNT_NAME> den Namen des Zielkontos ersetzen: `awscurl --service execute-api \ --region ${AWS_REGION} \ --access_key ${AWS_ACCESS_KEY_ID} \ --secret_key ${AWS_SECRET_ACCESS_KEY} \ --security_token ${AWS_SESSION_TOKEN} \ -X POST ${API_GATEWAY_ENDPOINT}check_name?account_name=<AWS_ACCOUNT_NAME>`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den Workflow zur Kontoerstellung aus.	1. Öffnen Sie die `api_example.json` Datei im Stammordner des geklonten Repositorys. 2. Aktualisieren Sie die Parameter mit Ihren Konfigurationswerten: `{ "account_name": "lza-test-01", "account_email": "johnsmith+lzatest01@example.com", "support_dl": "johnsmith@example.com", "managed_org_unit": "Workloads/Workload-1", "ad_integration": [{ "PermissionSetName": "CustomerAccountAdmin", "ActiveDirectoryGroupName": "platform-admin" }, { "PermissionSetName": "CustomerAccountDev", "ActiveDirectoryGroupName": "workload1-app1" }`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>],
	    "force_update":
	 "true",
	    "bypass_c
	reation": "false",
	    "account_tags": [
	        {
	            "Key":
	 "Environment",
	            "Value":
	 "Dev"
	        }, {
	            "Key":
	 "DeploymentMethod",
	            "Value":
	 "ApiGateway"
	        }
	    ]
	}</pre>	

	3. Speichern und schließen Sie die Datei `api_examp le.json` .	

	4. Geben Sie den folgenden Befehl ein, um den Step Functions Functions-Workflow zu starten:
	<pre>awscurl --service
	 execute-api \
	    --data @api-exam
	ple.json \
	    --region ${AWS_REG
	ION} \
	    --access_key
	 ${AWS_ACCESS_KEY_I
	D} \
	    --secret_key
	 ${AWS_SECRET_ACCES
	S_KEY} \</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>--security_token
	${AWS_SESSION_TOKEN} \
	-X POST ${API_GATEWAY_ENDPOINT}execute</pre>
	5. Notieren Sie sich in der Ausgabe des vorherigen Befehls den Amazon Resource Name (ARN) für die Ausführung von Step Functions.
	6. Wenn Sie den Status des Step Functions Functions-Workflows überprüfen möchten, geben Sie den folgenden Befehl ein. `<STEP_FUNCTION_EXECUTION_NAME>` Ersetzen Sie durch den Ausführungs-ARN oder den Namen der Step Functions Functions-Ausführung:
	<pre>awscurl --service execute-api \
	--region ${AWS_REGION} \
	--access_key ${AWS_ACCESS_KEY_ID} \
	--secret_key ${AWS_SECRET_ACCESS_KEY} \
	--security_token ${AWS_SESSION_TOKEN} \</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
  -X GET ${API_GAT
EWAY_ENDPOINT}get_
execution_status?e
xecution=<STEP_FUN
CTION_EXECUTION_NA
ME>
```

7. Warten Sie, bis Sie eine Benachrichtigung erhalten, dass das Konto erfolgreich erstellt wurde.

> **Note**
>
> Wenn die Kontoerstellung fehlschlägt, sendet Amazon SNS eine Benachrichtigung an die E-Mail-Adressen, die Sie `accountCreationFailure` in der `deploy-config.yaml` Datei definiert haben. Der Kontoanforderer wird nicht benachrichtigt.

(Optional) Bereinigen Sie die Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Objekte aus den Amazon S3 S3-Buckets entfernen.	Entfernen Sie alle Objekte in den folgenden Amazon S3 S3-Buckets: • `lza-account-creation-work-<CDK_UNIQUE_ID>` • `lza-account-creation-workflow-src-<AWS_REGION>-<AWS_ACCOUNT>` • `lza-account-creation-workflow-<AWS_REGION>-<AWS_ACCOUNT>`	AWS DevOps

Löschen Sie den CloudFormation Stack.	Geben Sie den folgenden Befehl ein, um den CloudFormation Stack zu löschen:
	`aws cloudformation delete-stack \ --stack-name lza-account-creation-workflow-application`
	`aws cloudformation wait stack-delete-complete \ --stack-name lza-account-creation-workflow-application`
		AWS DevOps

Löschen der Pipeline.	Geben Sie den folgenden Befehl ein, um die `lza-accou`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`nt-creation-workfl ow-pipeline` Pipeline zu löschen: `cdk destroy lza-accou nt-creation-workflow- pipeline --force`	

Zugehörige Ressourcen

- Landing Zone Accelerator aktiviert AWS (AWS Lösungsbibliothek)
- Behebung häufig AWS CDK auftretender Probleme (AWS CDK Dokumentation)

Zusätzliche Informationen

Workflow-Diagramm von Step Functions

Die folgende Abbildung zeigt die Status im Step Functions Functions-Workflow.

Argumente

Die folgenden Argumente können Sie verwenden, wenn Sie das Python-Skript ausführen, das den Step Functions Functions-Workflow initiiert.

Die folgenden Argumente sind erforderlich:

- `account-name (-a)`(string) — Der Name des neuen AWS-Konto.
- `support-dl (-s)`(string) — Die E-Mail-Adresse, an die eine Benachrichtigung gesendet wird, wenn der Kontoerstellungsvorgang abgeschlossen ist.
- `managed-org-unit (-m)`(string) — Die verwaltete Organisationseinheit (OU), die das neue Konto enthalten wird.

Die folgenden Argumente sind optional:

- `ad-integration (-ad)`(Zeichenkettenwörterbuch) — Die Microsoft Entra ID-Gruppe und der zugewiesene Berechtigungssatz. Im Folgenden finden Sie ein Beispiel für die Verwendung dieses Arguments:

```
--ad-integration "{\"<PermissionSetName>\": \"<EntraIdGroupName>\"}"
```

- `account-email (-e)`(string) — Die E-Mail-Adresse für den Root-Benutzer des neuen AWS-Konto.

> **Note**
>
> Wenn dieses Argument nicht verwendet wird, wird anhand der Werte `rootEmailPrefix` und `rootEmailDomain` aus der `configs/deploy-config.yaml` Datei eine E-Mail-Adresse generiert. Wenn keine E-Mail-Adresse angegeben wird, wird eine E-Mail-Adresse im folgenden Format generiert:`rootEmailPrefix+accountName@rootEmailDomain`.

- `region (-r)`(string) — Der AWS-Region Ort, an dem der Step Functions Functions-Workflow bereitgestellt wurde. Der Standardwert ist `us-east-1`.
- `force-update (-f)`(string Boolean) — Geben Sie die Eingabetaste ein`true`, um die Aktualisierung des bereitgestellten Produkts AWS Service Catalog zu erzwingen.
- `bypass-creation (-b)`(string Boolean) — Geben Sie `true` diese Option ein, um das Hinzufügen des Kontos zur `accounts-config.yaml` Datei und die Ausführung der Pipeline zu umgehen. `AWSAccelerator-Pipeline` Dieses Argument wird normalerweise verwendet, um den Workflow-Prozess zur Kontoerstellung zu testen oder um die restlichen Step Functions-Schritte auszuführen, falls in der `Landing Zone Accelerator` Pipeline ein Fehler auftritt.
- `tags (-t)`(string) — Zusätzliche Tags, die Sie dem hinzufügen möchten AWS-Konto. Standardmäßig werden die folgenden Tags hinzugefügt: `account-namesupport-dl`, und`purpose`. Im Folgenden finden Sie ein Beispiel für die Verwendung dieses Arguments:

```
--tags TEST1=VALUE1 TEST2=VALUE2
```

Automatische Inventarisierung von AWS Ressourcen für mehrere Konten und Regionen

Erstellt von Matej Macek (AWS)

Übersicht

Dieses Muster beschreibt einen automatisierten Ansatz zur Verwaltung eines umfassenden AWS Ressourcenbestands für mehrere Konten und. AWS-Regionen Es soll Infrastruktur- und Sicherheitsingenieuren dabei helfen, ihre Ressourcenmanagementpraktiken zu verbessern. Es verwendet, AWS Config um Ressourcenänderungen zu verfolgen, Amazon Athena für Abfragen und Amazon QuickSight für interaktive Dashboards. Sie implementieren diese Lösung, indem Sie einen Stack bereitstellen. AWS CloudFormation

Diese Lösung ähnelt der in Visualisieren von AWS Config Daten mithilfe von Amazon Athena und Amazon QuickSight (AWS Blogbeitrag) vorgestellten Lösung. Dieses Muster erweitert diese Lösung, um die folgenden allgemeinen Anforderungen zu erfüllen und die folgenden Hauptvorteile zu bieten:

- Compliance-orientiert — Dieser Ansatz kann Ihnen helfen, regulatorische Anforderungen wie PCI DSS, NIST SP 800-53, ISO/IEC 27001, HIPAA, GDPR und andere zu erfüllen, die genaue Inventarisierungen vorschreiben.
- Anpassungsframework — Es bietet eine Grundlage für die Erstellung von QuickSight Dashboards für verschiedene AWS Ressourcen, sodass Sie die Lösung an Ihre spezifischen Anforderungen anpassen können.
- Benutzerorientierte Verbesserungen — Dieser Ansatz berücksichtigt Feedback aus realen Anwendungsfällen und geht auf Anfragen nach einer umfassenderen Lösung ein.

Infrastruktur-, Sicherheits- und Finanzteams stehen in dynamischen Umgebungen mit mehreren Konten oder Regionen häufig vor Herausforderungen in Bezug auf Transparenz und Zusammenarbeit. Diese Lösung wurde entwickelt, um diesen Herausforderungen zu begegnen und den Zeit- und Arbeitsaufwand für die Erstellung und Pflege eines Ressourceninventars erheblich zu reduzieren. Das Ergebnis ist eine zentrale Ansicht der Ressourcen, die Ihnen hilft, Entscheidungen zur Ressourcenzuweisung zu treffen, Risiken zu identifizieren und zu mindern, Kosten zu optimieren und die allgemeine Transparenz und Zusammenarbeit zu verbessern. Dieser Ansatz schließt die Lücke zwischen konzeptionellen Lösungen und realen Implementierungsanforderungen für Sicherheits-, Compliance- und Betriebszwecke.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Folgendes ist aktiv AWS-Konten:
  - Verwaltungskonto — Ein zentrales Konto für die Abrechnung, die Erstellung von Konten und die Steuerung des Zugriffs im gesamten Unternehmen
  - Auditkonto — Ein zentraler Knotenpunkt für Sicherheitsüberwachung, Compliance-Prüfungen und Drift-Benachrichtigungen
  - Protokollarchivkonto — Ein zentrales Konto zum Speichern und Analysieren der gesammelten Daten
- Im Auditkonto ein AWS Config Aggregator, der Konfigurationsdaten aus Ihren Zielkonten und Regionen sammelt und aggregiert
- Richten Sie im Protokollarchivkonto Folgendes ein:
  - Ein Amazon Simple Storage Service (Amazon S3) -Bucket, in dem Sie die Daten aus dem AWS Config Aggregator speichern
  - Ein QuickSight Amazon-Abonnement
  - Eine autorisierte Verbindung zwischen QuickSight und Amazon Athena
  - Berechtigungen für den Zugriff auf den Amazon S3 S3-Bucket über eine Athena-Abfrage
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert
- Berechtigungen zur Bereitstellung eines CloudFormation Stacks, der die folgenden Ressourcen bereitstellt:
  - Eine AWS Lambda Funktion
  - Eine Amazon S3 S3-Benachrichtigungskonfiguration
  - Athena-Datenbank, Tabellen und Ansichten
  - QuickSight Datensätze und Datenquellen
- Berechtigungen zum Ausführen von Automatisierungen in AWS Systems Manager
- Zugriffsberechtigungen QuickSight

Einschränkungen

- Die Lösung stützt sich auf AWS Config. AWS Config In der Regel werden Konfigurationsänderungen an Ihren Ressourcen unmittelbar nach dem Erkennen einer Änderung

oder in der von Ihnen angegebenen Häufigkeit aufgezeichnet. Dies erfolgt jedoch nach bestem Wissen und kann manchmal länger dauern.

- Diese Lösung verfolgt nur Ressourcentypen, die AWS Config unterstützt werden.
- Die Lösung verfolgt nicht den Ressourcenbestand anderer Cloud-Anbieter oder lokaler Umgebungen.
- Einige AWS-Services sind nicht in allen AWS-Regionen verfügbar. Informationen zur regionalen Verfügbarkeit finden Sie auf der Seite Dienstendpunkte und Kontingente in der AWS Dokumentation. Wählen Sie dort den Link für den Dienst.

Architektur

Das folgende Diagramm zeigt einen optimierten Prozess zum Sammeln, Organisieren, Analysieren und Visualisieren von Konfigurations- und Compliance-Daten für mehrere Konten in einer Organisation. AWS

Das Diagramm zeigt den folgenden Workflow:

1. In regelmäßigen Abständen sammelt der AWS Config Aggregator Konfigurations- und Compliance-Daten zu den Ressourcen in den Zielkonten und Regionen und übermittelt die Daten dann an den Amazon S3 S3-Bucket im Protokollarchivkonto.
2. Das Hinzufügen neuer AWS Config Daten zum Amazon S3 S3-Bucket ruft eine AWS Lambda Funktion auf.
3. Die Lambda-Funktion partitioniert die Daten, indem Schlüssel mit Werten konfiguriert werden, die der Region und dem Datum jeder Snapshot-Datei entsprechen. Dies hilft dabei, die Konfigurations- und Compliance-Daten AWS Glue effizient abzufragen und zu verarbeiten.
4. Amazon Athena verwendet ein AWS Glue Schema, um SQL-Abfragen für die im Amazon S3 S3-Bucket gespeicherten Daten auszuführen. Es verwendet die Schema-Metadaten von AWS Glue , um die Struktur der Daten zu verstehen.
5. Ansichten in Athena definieren und extrahieren die Zieldatensätze.
6. Dashboards in Amazon QuickSight helfen Ihnen dabei, die Datensätze zu visualisieren und zu analysieren.

Tools

AWS-Services

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon S3 analysieren können.
- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und AWS-Regionen zu verwalten.
- AWS Configbietet einen detaillierten Überblick über die Ressourcen in Ihrem System AWS-Konto und darüber, wie sie konfiguriert sind. Es hilft Ihnen zu erkennen, wie Ressourcen miteinander zusammenhängen und wie sich ihre Konfigurationen im Laufe der Zeit geändert haben. Ein AWS Config Aggregator sammelt AWS Config Konfigurations- und Compliance-Daten aus mehreren AWS-Konten Regionen.
- AWS Glueist ein vollständig verwalteter ETL-Service (Extrahieren, Transformieren und Laden). Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben. Dieses Muster verwendet einen AWS Glue Datenkatalog und eine Schemaregistrierung.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Organizationsist ein Kontoverwaltungsservice, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie erstellen und zentral verwalten.
- Amazon QuickSight ist ein Business Intelligence (BI) -Service auf Cloud-Ebene, mit dem Sie Ihre Daten in einem einzigen Dashboard visualisieren, analysieren und melden können.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Systems Managerhilft Ihnen bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der AWS Cloud ausgeführt werden. Es vereinfacht das Anwendungs- und Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme und hilft Ihnen, Ihre AWS Ressourcen sicher und in großem Umfang zu verwalten.AWS Systems Manager Die Automatisierung vereinfacht häufig auftretende Wartungs-, Bereitstellungs- und Problembehebungsaufgaben für viele. AWS-Services

Code-Repository

Die AWS CloudFormation Vorlage für dieses Muster ist im AWS Config GitHub Visualisierungs-Repository verfügbar. Diese CloudFormation Vorlage stellt ein AWS Systems Manager Automatisierungs-Runbook bereit, das AWS Config für die Verwendung mit Amazon Athena eingerichtet ist. Diese Automatisierung bereitet die AWS Glue Verbindung mit dem angegebenen Amazon S3 S3-Bucket vor, erstellt Ansichten in Amazon Athena und konfiguriert Amazon QuickSight für die Dashboard-Visualisierung.

Bewährte Methoden

- Wir empfehlen Ihnen, die bewährten Methoden unter Einrichtung und Verwaltung einer sicheren AWS Umgebung mit mehreren Konten ohne vorgeschriebene Anleitung AWS Control Tower zu AWS befolgen.
- Wir empfehlen Ihnen, einen AWS Config Aggregator zu erstellen, der Konfigurations- und Compliance-Daten für das gesamte Unternehmen sammelt. AWS Weitere Informationen finden Sie in der Dokumentation unter Datenaggregation für mehrere Konten und Regionen. AWS Config
- Bevor Sie diese Lösung einsetzen, empfehlen wir Ihnen, die aktuellen Preisinformationen für Amazon S3 AWS Config, Athena und QuickSightzu lesen.

Epen

Stellen Sie den Stack CloudFormation bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die CloudFormation Vorlage herunter.	Laden Sie die Vorlage Config-QuickSight CloudFormation - Visualization-SSM-Automation.yaml herunter.	AWS-Administrator, Cloud-Administrator, DevOps Ingenieur
Ändern Sie die CloudFormation Vorlage.	Führen Sie diesen Schritt nur aus, wenn Sie ihn verwenden AWS Control Towerund AWS Config von verwaltet werden AWS Control Tower. Sie müssen die CloudFormation Vorlage ändern.	DevOps Ingenieur, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	1. Melden Sie sich beim -Verwaltungskonto an.
	2. Öffnen Sie die AWS Organizations -Konsole.
	3. Navigieren Sie zur Seite Einstellungen. Auf dieser Seite werden Details zur Organisation angezeigt, einschließlich der Organisations-ID.
	4. Kopieren Sie die Organisations-ID.
	5. Öffnen Sie in Ihrem bevorzugten Texteditor die Datei Config- QuickSight -Visualization-SSM-Automation.yaml.
	6. Suchen Sie die folgende Zeile:
	`return re.match( '^AWSLogs/(\d+)/Config/([\w-]+)/(\d+)/(\d+)/(\d+)/ConfigSnapshot/[^\\\]+$', object_key)`
	7. Ersetzen Sie diese Zeile durch die folgende, wobei sich die ID `<ORGANIZATION_ID>` befindet, die Sie zuvor kopiert haben:
	`return re.match( '^<ORGANIZATION_ID`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`>/AWSLogs/(\d+)/Config/([\w-]+)/(\d+)/(\d+)/(\d+)/ConfigSnapshot/[^\\\]+$', object_key)` 8. Speichern und schließen Sie die Datei Config-QuickSight -Visualization-SSM-Automation.yaml.	
Erstellen Sie einen CloudFormation Stack.	Folgen Sie den Anweisungen unter Einen Stack von der CloudFormation Konsole aus erstellen. Beachten Sie Folgendes: 1. Wählen Sie Eine Vorlagendatei hochladen und wählen Sie dann die YAML-Datei aus, die Sie heruntergeladen haben. 2. Geben Sie unter Stack name (Stack-Name) `Config-QuickSight-Visualization-SSM-Automation` ein. 3. Wählen Sie Absenden aus.	AWS-Administrator, Cloud-Administrator, DevOps Ingenieur

Führen Sie die Automatisierung im Systems Manager aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Finden Sie Ihren QuickSight Benutzernamen.	1. Öffnen Sie die QuickSight - Konsole. 2. Öffne das Profilmenü. 3. Notieren Sie sich den Benutzernamen. Sie benötigen diesen Wert später.	AWS-Administrator, Cloud-Administrator, DevOps Ingenieur
Suchen Sie den Namen des Lieferkanals und den Namen des Amazon S3 S3-Buckets.	1. Geben Sie im AWS CLI den folgenden Befehl ein: `aws configservice describe-delivery-channels` 2. Notieren Sie sich den Namen des Amazon S3 S3-Buckets und den Namen Ihres AWS Config Lieferkanals. Sie benötigen diese Werte später.	AWS-Administrator, Cloud-Administrator, DevOps Ingenieur
Führen Sie die Automatisierung im Systems Manager aus.	1. Öffnen Sie die AWS Systems Manager - Konsole. 2. Wählen Sie im Navigationsbereich die Option Dokumente aus. 3. Wählen Sie Owned by me (In meinem Besitz) aus. 4. Wählen Sie Config-QuickSight -Visualization.	AWS-Administrator, Cloud-Administrator, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Wählen Sie Automatisierung ausführen. 6. Geben Sie im Abschnitt Eingabeparameter Ihre Werte für die folgenden Parameter ein: • `ConfigDeliveryChannelName` — Geben Sie den Namen Ihres AWS Config Lieferkanals ein. Dieser Parameter muss angegeben werden. • `ConfigS3BucketLocation` — Geben Sie den Namen des Amazon S3 S3-Buckets ein, in dem Sie die AWS Config Konfigurationsdaten speichern. Dieser Parameter muss angegeben werden. • `QuickSightUserName` — Geben Sie einen Benutzernamen ein, auf den Sie Administratorzugriff haben QuickSight. Dieser Parameter muss angegeben werden. • `AutomationAssumeRole` — Der Amazon-Ressourcenname (ARN) der Rolle AWS Identity and Access	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Management (IAM), der es Systems Manager Automation ermöglich t, die Aktionen in Ihrem Namen durchzuführen. Dieser Parameter ist optional. Lassen Sie diesen Parameter leer. • `DeleteConfigVisual ization` — Wählen Sie`false`. 7. Wählen Sie Ausführen.	

Daten in Amazon visualisieren QuickSight

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Daten aktualisieren.	Um Datensatzaktualisierungen gemäß Ihren spezifischen Anforderungen zu planen, folgen Sie den Anweisungen unter SPICE-Daten aktualisi eren.	AWS-Administrator, DevOps Ingenieur, Cloud-Administrator
Erstellen Sie eine -Analyse.	Um ein Dashboard zu erstellen QuickSight , mit dem Sie die Ressourcen visualisi eren können, folgen Sie den Anweisungen unter Eine Analyse in Amazon starten QuickSight.	QuickSight Administrator
Erstellen Sie ein Dashboard.	1. Wenn Sie mit der Bearbeitu ng Ihrer QuickSight Analyse	QuickSight Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	fertig sind, folgen Sie den Anweisungen unter Dashboards veröffentlichen, um ein Dashboard zu erstellen. Ein Dashboard ist eine Analyse, die Sie mit anderen QuickSight Benutzern teilen können. 2. Folgen Sie den Anweisungen unter Zugriff auf ein Dashboard gewähren, um das Dashboard mit Ihren QuickSight Zielbenutzern zu teilen.	

(Optional) Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die Ressourcen, die durch die Systems Manager Manager-Automatisierung erstellt wurden.	1. Öffnen Sie die AWS Systems Manager -Konsole. 2. Wählen Sie im Navigationsbereich die Option Dokumente aus. 3. Wählen Sie Owned by me (In meinem Besitz) aus. 4. Wählen Sie Config-QuickSight -Visualization. 5. Wählen Sie Automatisierung ausführen. 6. Geben Sie im Abschnitt Eingabeparameter für den	AWS-Administrator, Cloud-Administrator, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`DeleteConfigVisualization` Parameter Folgendes ein`true`. 7. Wählen Sie Ausführen.	
Löschen Sie den CloudFormation Stack.	Folgen Sie den Anweisungen unter Löschen eines `Config-QuickSight-Visualization-SSM-Automation` Stacks aus der CloudFormation Konsole, um die Ressourcen im Stack zu löschen.	AWS-Administrator, Cloud-Administrator, DevOps Ingenieur

Fehlerbehebung

Problem	Lösung

Amazon QuickSight versucht, eine Verbindung zu der herzustellen `us-east-1` AWS-Region, aber die Erstellung von Ressourcen in dieser Region ist nicht zulässig.	Eine Servicekontrollrichtlinie schränkt Ihr Abonnement für Amazon QuickSight in dieser Region ein. Geben Sie in der Servicesteuerungsrichtlinie das Ziel AWS-Region manuell an. `<REGION_ID>` Ersetzen Sie es durch die entsprechende Regionskennung:
	`https://<REGION_ID>.quicksight.aws.amazon.com/sn/start/dashboards`
	Im Folgenden wird ein Beispiel gezeigt:
	`https://eu-central-1.quicksight.aws.amazon.com/sn/start/dashboards`

Problem	Lösung
In Amazon Athena wird die folgende Meldung angezeigt: `Before you run your first query, you need to set up a query result location in Amazon S3.`	Stellen Sie sicher, dass Sie einen Amazon S3 S3-Bucket vorbereitet haben, in dem Sie die Abfrageergebnisse von Amazon Athena speichern werden. Folgen Sie dann den Anweisungen unter Geben Sie einen Speicherort für Abfrageergebnisse mithilfe der Amazon Athena Athena-Konsole an.

Zugehörige Ressourcen

AWS Dokumentation

- AWS Config Dokumentation
- QuickSight Amazon-Dokumentation

AWS Blogbeitrag

- Automatisieren Sie AWS Config die Datenvisualisierung mit AWS Systems Manager
- Wie zeichnet man regelmäßig Änderungen der Ressourcenkonfiguration auf mit AWS Config

Sonstige Ressourcen

- Amazon QuickSight Community-Lernzentrum
- QuickSight Amazon-Community-Galerie

Konfiguration von VPC Flow Logs für die Zentralisierung über AWS-Konten hinweg

Erstellt von Benjamin Morris (AWS) und Aman Kaur Gandhi (AWS)

Übersicht

In einer virtuellen privaten Cloud (VPC) von Amazon Web Services (AWS) kann die VPC Flow Logs-Funktion nützliche Daten für betriebliche und sicherheitstechnische Problembehebungen bereitstellen. Es gibt jedoch Einschränkungen bei der Verwendung von VPC Flow Logs in einer Umgebung mit mehreren Konten. Insbesondere kontenübergreifende Datenflussprotokolle von Amazon CloudWatch Logs werden nicht unterstützt. Stattdessen können Sie die Protokolle zentralisieren, indem Sie einen Amazon Simple Storage Service (Amazon S3) -Bucket mit der entsprechenden Bucket-Richtlinie konfigurieren.

> **Note**
>
> In diesem Muster werden die Anforderungen für das Senden von Flow-Protokollen an einen zentralen Ort beschrieben. Wenn Sie jedoch möchten, dass Protokolle auch lokal in Mitgliedskonten verfügbar sind, können Sie für jede VPC mehrere Flow-Logs erstellen. Benutzer ohne Zugriff auf das Log Archive-Konto können Datenverkehrsprotokolle zur Fehlerbehebung einsehen. Alternativ können Sie ein einzelnes Flow-Protokoll für jede VPC konfigurieren, die CloudWatch Protokolle an Logs sendet. Anschließend können Sie einen Amazon Data Firehose-Abonnementfilter verwenden, um die Protokolle an einen S3-Bucket weiterzuleiten. Weitere Informationen finden Sie im Abschnitt Verwandte Ressourcen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Organisation von AWS Organizations mit einem Konto, das zur Zentralisierung von Protokollen verwendet wird (z. B. Log Archive)

Einschränkungen

Wenn Sie den verwalteten Schlüssel des AWS Key Management Service (AWS KMS) verwenden, `aws/s3` um Ihren zentralen Bucket zu verschlüsseln, empfängt er keine Protokolle von einem anderen Konto. Stattdessen wird Ihnen der `Unsuccessful` Fehlercode 400 mit einer Meldung wie `"LogDestination: <bucketName> is undeliverable"` der von Ihnen angegebenen `ResourceId` angezeigt.

Dies liegt daran, dass die von AWS verwalteten Schlüssel eines Kontos nicht von mehreren Konten gemeinsam genutzt werden können.

Die Lösung besteht darin, entweder die von Amazon S3 verwaltete Verschlüsselung (SSE-S3) oder einen vom Kunden verwalteten AWS KMS-Schlüssel zu verwenden, den Sie mit Mitgliedskonten teilen können.

Architektur

Zieltechnologie-Stack

In der folgenden Abbildung werden zwei Flow-Logs für jede VPC bereitgestellt. Einer sendet Protokolle an eine lokale CloudWatch Protokollgruppe. Die andere sendet Protokolle an einen S3-Bucket in einem zentralen Protokollierungskonto. Die Bucket-Richtlinie ermöglicht es dem Log-Lieferdienst, Logs in den Bucket zu schreiben.

> **Note**
>
> Seit November 2023 unterstützt es AWS jetzt den Bedingungsschlüssel aws: SourceOrg ID. Diese Bedingung ermöglicht es Ihnen, Konten außerhalb Ihrer AWS Organizations Organisation das Schreiben in den zentralen Bucket zu verweigern.

Zielarchitektur

Automatisierung und Skalierung

Jede VPC ist so konfiguriert, dass sie Protokolle an den S3-Bucket im zentralen Protokollierungskonto sendet. Verwenden Sie eine der folgenden Automatisierungslösungen, um sicherzustellen, dass die Flow-Logs ordnungsgemäß konfiguriert sind:

- AWS CloudFormation StackSets

- AWS Control Tower Account Factory für Terraform (AFT)
- Eine AWS Config-Regel mit Problembehebung

Tools

Tools

- Amazon CloudWatch Logs hilft Ihnen dabei, die Protokolle all Ihrer Systeme, Anwendungen und AWS-Services zu zentralisieren, sodass Sie sie überwachen und sicher archivieren können.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS. Dieses Muster verwendet die Funktion VPC Flow Logs, um Informationen über den IP-Verkehr zu und von Netzwerkschnittstellen in Ihrer VPC zu erfassen.

Bewährte Methoden

Die Verwendung von Infrastructure as Code (IaC) kann den Bereitstellungsprozess von VPC Flow Logs erheblich vereinfachen. Wenn Sie Ihre VPC-Bereitstellungsdefinitionen so abstrahieren, dass sie ein Flow-Log-Ressourcenkonstrukt enthalten, werden Ihre VPCs With-Flow-Logs automatisch bereitgestellt. Dies wird im nächsten Abschnitt demonstriert.

Zentralisierte Flussprotokolle

Beispielsyntax für das Hinzufügen zentraler Flow-Logs zu einem VPC-Modul in Terraform HashiCorp

Dieser Code erstellt ein Flow-Protokoll, das Protokolle von einer VPC an einen zentralen S3-Bucket sendet. Beachten Sie, dass dieses Muster nicht die Erstellung des S3-Buckets abdeckt.

Empfohlene Bucket-Richtlinien finden Sie im Abschnitt Zusätzliche Informationen.

```
variable "vpc_id" { type = string }
locals { custom_log_format_v5 = "$${version} $${account-id} $${interface-id} $
${srcaddr} $${dstaddr} $${srcport} $${dstport} $${protocol} $${packets} $${bytes}
 $${start} $${end} $${action} $${log-status} $${vpc-id} $${subnet-id} $${instance-
```

```
id} $${tcp-flags} $${type} $${pkt-srcaddr} $${pkt-dstaddr} $${region} $${az-id} $
${sublocation-type} $${sublocation-id} $${pkt-src-aws-service} $${pkt-dst-aws-service}
 $${flow-direction} $${traffic-path}" }
resource "aws_flow_log" "centralized_flow_log" {
  log_destination      = "arn:aws:s3:::centralized-vpc-flow-logs-
<log_archive_account_id>" # Optionally, a prefix can be added after the ARN.
  log_destination_type = "s3"
  traffic_type         = "ALL"
  vpc_id               = var.vpc_id
  log_format           = local.custom_log_format_v5 # If you want fields from VPC Flow
 Logs v3+, you will need to create a custom log format.
}
```

Weitere Informationen zum benutzerdefinierten Protokollformat finden Sie in der AWS-Dokumentation.

Lokale Datenflussprotokolle

Beispielsyntax für das Hinzufügen von lokalen Flow-Logs zu einem VPC-Modul in Terraform mit den erforderlichen Berechtigungen

Dieser Code erstellt ein Flow-Protokoll, das Protokolle von einer VPC an eine lokale CloudWatch Logs-Gruppe sendet.

```
data "aws_region" "current" {}
variable "vpc_id" { type = string }
resource "aws_iam_role" "local_flow_log_role" {
  name = "flow-logs-policy-${var.vpc_id}"
  assume_role_policy = <<EOF
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Principal": {"Service": "vpc-flow-logs.amazonaws.com"},
      "Action": "sts:AssumeRole"
  }]
}
EOF
}
resource "aws_iam_role_policy" "logs_permissions" {
  name = "flow-logs-policy-${var.vpc_id}"
  role = aws_iam_role.local_flow_log_role.id
  policy = <<EOF
```

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Action": ["logs:CreateLog*", "logs:PutLogEvents", "logs:DescribeLog*",
 "logs:DeleteLogDelivery"],
      "Effect": "Allow",
      "Resource": "arn:aws:logs:${data.aws_region.current.name}:*:log-group:vpc-flow-
logs*"
  }]
}
EOF
}
resource "aws_cloudwatch_log_group" "local_flow_logs" {
  name              = "vpc-flow-logs/${var.vpc_id}"
  retention_in_days = 30
}
resource "aws_flow_log" "local_flow_log" {
  iam_role_arn    = aws_iam_role.local_flow_log_role.arn
  log_destination = aws_cloudwatch_log_group.local_flow_logs.arn
  traffic_type    = "ALL"
  vpc_id          = var.vpc_id
}
```

Epen

Stellen Sie die VPC Flow Logs-Infrastruktur bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie die Verschlüsselungsstrategie und erstellen Sie die Richtlinie für den zentralen S3-Bucket.	Der zentrale Bucket unterstützt den `aws/s3` AWS-KMS-Schlüssel nicht, daher müssen Sie entweder SSE-S3 oder einen vom Kunden verwalteten AWS KMS-Schlüssel verwenden. Wenn Sie einen AWS-KMS-Schlüssel verwenden, muss die Schlüsselrichtlinie den Mitgliedskonten die	Compliance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Verwendung des Schlüssels ermöglichen.	
Erstellen Sie den zentralen Flow-Log-Bucket.	Erstellen Sie den zentralen Bucket, an den die Flow-Logs gesendet werden, und wenden Sie die Verschlüs selungsstrategie an, die Sie im vorherigen Schritt ausgewähl t haben. Dies sollte sich in einem Log-Archiv oder einem Konto mit ähnlichem Zweck befinden. Rufen Sie die Bucket-Ri chtlinie im Abschnitt Zusätzlic he Informationen ab und wenden Sie sie auf Ihren zentralen Bucket an, nachdem Sie die Platzhalter mit Ihren umgebungsspezifischen Werten aktualisiert haben.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie VPC Flow Logs so, dass Protokolle an den zentralen Flow-Log-Bucket gesendet werden.	Fügen Sie jeder VPC, von der Sie Daten sammeln möchten, Flow-Logs hinzu. Der skalierbarste Weg, dies zu tun, ist die Verwendung von IaC-Tools wie AFT oder AWS Cloud Development Kit (AWS CDK). Sie können beispielsweise ein Terraform -Modul erstellen, das eine VPC zusammen mit einem Flow-Log bereitstellt. Bei Bedarf fügen Sie die Flow-Logs manuell hinzu.	Netzwerkadministrator
Konfigurieren Sie VPC Flow Logs so, dass sie an lokale CloudWatch Logs gesendet werden.	(Optional) Wenn Sie möchten, dass Flow-Protokolle in den Konten sichtbar sind, in denen die Protokolle generiert werden, erstellen Sie ein weiteres Flow-Protokoll, um Daten an CloudWatch Logs im lokalen Konto zu senden. Alternativ können Sie die Daten an einen kontospez ifischen S3-Bucket im lokalen Konto senden.	Allgemeines AWS

Zugehörige Ressourcen

- So erleichtern Sie die Datenanalyse und erfüllen Sicherheitsanforderungen mithilfe zentralisierter Flow-Protokolldaten (Blogbeitrag)
- So aktivieren Sie VPC Flow Logs automatisch mithilfe von AWS Config-Regeln (Blogbeitrag)

Zusätzliche Informationen

Bucket-Richtlinie

Dieses Beispiel für eine Bucket-Richtlinie kann auf Ihren zentralen S3-Bucket für Flow-Logs angewendet werden, nachdem Sie Werte für Platzhalternamen hinzugefügt haben.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceOrgID": "<ORG_ID>"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>",
            "Condition": {
                "StringEquals": {
                    "aws:SourceOrgID": "<ORG_ID>"
                }
            }
        },
        {
            "Sid": "DenyUnencryptedTraffic",
            "Effect": "Deny",
            "Principal": {
```

```
                "AWS": "*"
            },
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::<BUCKET_NAME>/*",
                "arn:aws:s3:::<BUCKET_NAME>"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

Automatisches Taggen Transit Gateway Gateway-Anhängen mithilfe von AWS Organizations

Erstellt von Richard Milner-Watts (AWS), Haris Bin Ayub (AWS) und John Capps (AWS)

Übersicht

Auf Amazon Web Services (AWS) können Sie verwenden, AWS Resource Access Managerum AWS Transit Gateway AWS-Konto grenzübergreifend zu teilen. Wenn Sie Transit Gateway Gateway-Anlagen über Kontogrenzen hinweg erstellen, werden die Anlagen jedoch ohne Namensschild erstellt. Das kann die Identifizierung von Anhängen zeitaufwändig machen.

Diese Lösung bietet einen automatisierten Mechanismus zum Sammeln von Informationen über jeden Transit Gateway Gateway-Anhang für Konten innerhalb einer Organisation, die von verwaltet wird AWS Organizations. Der Prozess umfasst die Suche nach dem CIDR-Bereich (Classless Inter-Domain Routing) aus der Transit Gateway Gateway-Routentabelle. Die Lösung wendet dann ein Namensschild in der Form von `<CIDR-range>-<AccountName>` auf den Anhang innerhalb des Kontos an, das das Transit-Gateway enthält.

Diese Lösung kann zusammen mit einer Lösung wie dem Serverless Transit Network Orchestrator aus der AWS Solutions Library verwendet werden. Serverless Transit Network Orchestrator ermöglicht die automatisierte Erstellung von Transit Gateway Gateway-Anhängen in großem Umfang.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Eine AWS Organizations Organisation, die alle zugehörigen Konten enthält
- Zugriff auf das Organisationsverwaltungskonto unter dem Stammkonto der Organisation, um die erforderliche Rolle AWS Identity and Access Management (IAM) zu erstellen
- Ein Shared Networking-Mitgliedskonto, das ein oder mehrere Transit-Gateways enthält, die mit der Organisation gemeinsam genutzt werden und Anlagen haben

Architektur

Der folgende Screenshot AWS Management Console zeigt Beispiele für Transit Gateway Gateway-Anhänge ohne zugeordnetes Namensschild und zwei Transit Gateway Gateway-Anlagen mit

Namensschildern, die von dieser Lösung generiert wurden. Die Struktur des generierten Namenstags ist`<CIDR-range>-<AccountName>`.

Diese Lösung verwendet AWS CloudFormation, um einen AWS Step FunctionsWorkflow bereitzustellen, der die Erstellung von Transit Gateway-Namens-Tags für alle konfigurierten Daten verwaltet AWS-Regionen. Der Workflow ruft AWS LambdaFunktionen auf, die die zugrunde liegenden Aufgaben ausführen.

Nachdem die Lösung die Kontonamen von abgerufen hat AWS Organizations, erhält die Step Functions Functions-Zustandsmaschine alle Transit Gateway Gateway-Anlagen IDs. Diese werden parallel nach Regionen verarbeitet. Diese Verarbeitung beinhaltet das Nachschlagen des CIDR-Bereichs für jeden Anhang. Der CIDR-Bereich wird ermittelt, indem die Transit Gateway Gateway-Routentabellen innerhalb der Region nach einer passenden Transit Gateway Gateway-Anhangs-ID durchsucht werden. Wenn alle erforderlichen Informationen verfügbar sind, fügt die Lösung dem Anhang ein Namensschild hinzu. Die Lösung überschreibt keine vorhandenen Name-Tags.

Die Lösung läuft nach einem Zeitplan, der durch ein EventBridgeAmazon-Ereignis gesteuert wird. Die Veranstaltung initiiert die Lösung täglich um 6:00 Uhr UTC.

Zieltechnologie-Stack

- Amazon EventBridge
- AWS Lambda
- AWS Organizations
- AWS Transit Gateway
- Amazon Virtual Private Cloud (Amazon VPC)
- AWS X-Ray

Zielarchitektur

Die Lösungsarchitektur und der Arbeitsablauf sind in der folgenden Abbildung dargestellt.

1. Das geplante Ereignis initiiert die Regel.
2. Die EventBridge Regel startet die Step Functions Functions-Zustandsmaschine.

3. Die Zustandsmaschine ruft die `tgw-tagger-organizations-account-query` Lambda-Funktion auf.
4. Die `tgw-tagger-organizations-account-query` Lambda-Funktion übernimmt die Rolle im Organisationsverwaltungskonto.
5. Die `tgw-tagger-organizations-account-query` Lambda-Funktion ruft die Organizations-API auf, um AWS-Konto Metadaten zurückzugeben.
6. Die Zustandsmaschine ruft die `tgw-tagger-attachment-query` Lambda-Funktion auf.
7. Für jede Region ruft die Zustandsmaschine parallel die `tgw-tagger-rtb-query` Lambda-Funktion auf, um den CIDR-Bereich für jeden Anhang zu lesen.
8. Für jede Region ruft die Zustandsmaschine parallel die `tgw-tagger-attachment-tagger` Lambda-Funktion auf.
9. Namensschilder werden für Transit Gateway Gateway-Anlagen im Shared Networking-Konto erstellt.

Automatisierung und Skalierung

Die Lösung verarbeitet jede Region parallel, um die Gesamtdauer des Laufs zu reduzieren.

Tools

AWS-Services

- AWS CloudFormationbietet die Möglichkeit, eine Sammlung verwandter Ressourcen AWS und Ressourcen von Drittanbietern zu modellieren, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus zu verwalten, indem Infrastruktur als Code behandelt wird.
- Amazon CloudWatch hilft Ihnen dabei, die Metriken Ihrer AWS-Ressourcen und der Anwendungen, auf denen Sie laufen, AWS in Echtzeit zu überwachen.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen verbinden können. EventBridge empfängt ein Ereignis, ein Indikator für eine Änderung der Umgebung, und wendet eine Regel an, um das Ereignis an ein Ziel weiterzuleiten. Regeln ordnen Ereignisse Zielen entweder auf der Grundlage der Struktur des Ereignisses, eines so genannten Ereignismusters, oder anhand eines Zeitplans zu.
- AWS Lambdaist ein Rechendienst, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch, von wenigen Anfragen pro Tag bis hin zu Tausenden pro Sekunde. Sie zahlen nur

für die tatsächlich konsumierte Zeit. Es werden keine Gebühren berechnet, solange Ihr Code nicht ausgeführt wird.

- AWS Organizationshilft Ihnen dabei, Ihre Umgebung zentral zu verwalten und zu steuern, während Sie Ihre AWS Ressourcen erweitern und skalieren. Mithilfe von Organizations können Sie programmgesteuert neue Ressourcen erstellen AWS-Konten und zuweisen, Konten gruppieren, um Ihre Workflows zu organisieren, Richtlinien auf Konten oder Gruppen zur Verwaltung anwenden und die Abrechnung vereinfachen, indem Sie eine einzige Zahlungsmethode für alle Ihre Konten verwenden.
- AWS Step Functionsist ein visueller Workflow-Dienst mit geringem Programmieraufwand AWS-Services, der zur Orchestrierung und Automatisierung von Geschäftsprozessen und zur Entwicklung serverloser Anwendungen verwendet wird. Workflows verwalten Fehler, Wiederholungen, Parallelisierung, Serviceintegrationen und Beobachtbarkeit, sodass sich Entwickler auf die wertvollere Geschäftslogik konzentrieren können.
- AWS Transit Gatewayverbindet VPCs und lokale Netzwerke über einen zentralen Hub. Dies vereinfacht Ihr Netzwerk und macht Schluss mit komplexen Peering-Beziehungen. Es fungiert als Cloud-Router, sodass jede neue Verbindung nur einmal hergestellt wird.
- Amazon Virtual Private Cloud (Amazon VPC) ist ein Service zum Starten von AWS Ressourcen in einem logisch isolierten virtuellen Netzwerk, das Sie definieren.
- AWS X-Raysammelt Daten über Anfragen, die Ihre Anwendung bedient, und stellt Tools bereit, mit denen Sie diese Daten anzeigen, filtern und Einblicke in sie gewinnen können, um Probleme und Optimierungsmöglichkeiten zu identifizieren.

Code

Der Quellcode für diese Lösung ist im Transit Gateway Attachment GitHub Tagger-Repository verfügbar. Das Repository enthält die folgenden Dateien:

- `tgw-attachment-tagger-main-stack.yaml`erstellt alle Ressourcen zur Unterstützung dieser Lösung innerhalb des Shared Networking-Kontos.
- `tgw-attachment-tagger-organizations-stack.yaml`erstellt eine Rolle im Verwaltungskonto der Organisation.

Epen

Stellen Sie das Hauptlösungspaket bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sammeln Sie die erforderlichen Informationen zu den Voraussetzungen.	Um den kontoübergreifenden Zugriff von der Lambda-Funktion auf die AWS Organizations API zu konfigurieren, benötigen Sie die Konto-ID für das Verwaltungskonto der Organisation. **Note** Die Reihenfolge, in der die beiden AWS CloudFormation Stapel erstellt werden, ist wichtig. Sie müssen zuerst Ressourcen für das Shared Networking-Konto bereitstellen. Die Rolle im Shared Networking-Konto muss bereits vorhanden sein, bevor Ressourcen für das Verwaltungskonto der Organisation bereitgestellt werden können. Weitere Informationen finden Sie in der AWS-Dokumentation.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die AWS CloudFormation Vorlage für den Hauptlösungsstapel.	Die Vorlage für den Hauptlösungsstapel stellt die IAM-Rollen, den Step Functions Functions-Workflow, die Lambda-Funktionen und das CloudWatch Amazon-Event bereit. Öffnen Sie das Konto AWS Management Console für das Shared Networking und dann die: &CFN-Konsole. Erstellen Sie den Stack mithilfe der `tgw-attachment-tagger-main-stack.yaml` Vorlage und der folgenden Werte: • Stackname — tgw-attachment-tagger-main-stack • awsOrganizationsRootAccountId— Konto-ID für das Verwaltungskonto der Organisation • TGWRegionsParameter — AWS-Regionen für die Lösung, eingegeben als kommagetrennte Zeichenfolge • TGWListParameter — Transit-Gateway IDs , das von der Lösung ausgeschlossen werden soll, eingegeben in einer	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	durch Kommas getrennten Zeichenfolge Weitere Informationen zum Starten eines AWS CloudFormation Stacks finden Sie in der Dokumentation.AWS	
Stellen Sie sicher, dass die Lösung erfolgreich gestartet wurde.	Warten Sie, bis der CloudFormation Stack den Status CREATE_COMPLETE erreicht hat. Dies sollte weniger als eine Minute dauern. Öffnen Sie die Step Functions Functions-Konsole und stellen Sie sicher, dass eine neue Zustandsmaschine mit dem Namen tgw-attachment-tagger-state-machine erstellt wurde.	DevOps Ingenieur

Stellen Sie den AWS Organizations Stack bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sammeln Sie die erforderlichen Informationen zu den Voraussetzungen.	Um den kontoübergreifenden Zugriff von der Lambda-Funktion auf die AWS Organizations API zu konfigurieren, benötigen Sie die Konto-ID für das Shared Networking-Konto.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die CloudFormation Vorlage für den Organisations-Stack	Die Vorlage für den AWS Organizations Stack stellt die IAM-Rolle im Verwaltungskonto der Organisation bereit. Greifen Sie auf die AWS-Konsole für das Verwaltungskonto der Organisation zu und öffnen Sie dann die CloudFormation Konsole. Erstellen Sie den Stack mithilfe der `tgw-attachment-tagger-organizations-stack.yaml` Vorlage und der folgenden Werte: • Stackname — tgw-attachment-tagger-organizations-stack • NetworkingAccountIdParameter — Konto-ID für das Shared Networking-Konto Verwenden Sie für die anderen Optionen zur Stapelerstellung die Standardeinstellungen.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die Lösung erfolgreich gestartet wurde.	Warten Sie, bis der AWS CloudFormation Stack den Status CREATE_COMPLETE erreicht hat. Dies sollte weniger als eine Minute dauern. Öffnen Sie die AWS Identity and Access Management (IAM-) Konsole und vergewissern Sie sich, dass eine neue Rolle mit dem Namen tgw-attachment-tagger-organization-query-role erstellt wurde.	DevOps Ingenieur

Überprüfen Sie die Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Zustandsmaschine aus.	Öffnen Sie die Step Functions Functions-Konsole für das Shared Networking-Konto und wählen Sie im Navigationsbereich State Machines aus. Wählen Sie die Zustandsmaschine tgw-attachment-tagger-state-Maschine und dann Ausführung starten aus. Da die Eingabe für diesen Zustandsmaschine nicht von der Lösung verwendet wird,	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	können Sie den Standardwert verwenden. `{ "Comment": "Insert your JSON here" }` Wählen Sie Start Execution aus.	
Beobachten Sie die Zustandsmaschine bis zur Fertigstellung.	Auf der neuen Seite, die geöffnet wird, können Sie zusehen, wie die Zustandsmaschine läuft. Die Dauer hängt von der Anzahl der zu verarbeitenden Transit Gateway Gateway-Anlagen ab. Auf dieser Seite können Sie jeden Schritt der Zustandsmaschine untersuchen. Sie können die verschiedenen Aufgaben innerhalb der Zustandsmaschine anzeigen und den Links zu den CloudWatch Protokollen für die Lambda-Funktionen folgen. Für die Aufgaben, die innerhalb der Map parallel ausgeführt werden, können Sie die Dropdownliste Index verwenden, um die spezifischen Implementierungen für jede Region anzuzeigen.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Transit Gateway Gateway-Anhangs-Tags.	Öffnen Sie die VPC-Konsole für das Shared Networking-Konto und wählen Sie Transit Gateway Attachments aus. Auf der Konsole wird ein Namen-Tag für Anlagen bereitgestellt, die die Kriterien erfüllen (der Anhang wird an eine Transit Gateway Gateway-Routentabelle weitergegeben, und der Ressourcenbesitzer ist Mitglied der Organisation).	DevOps Ingenieur
Überprüfen Sie die Initiierung des CloudWatch Ereignisses.	Warten Sie, bis das CloudWatch Ereignis ausgelöst wird. Dies ist für 06:00 Uhr UTC geplant. Öffnen Sie dann die Step Functions Functions-Konsole für das Shared Networking-Konto und wählen Sie im Navigationsbereich State Machines aus. Wählen Sie den Zustandsmaschine tgw-attachment-tagger-state-machine aus. Stellen Sie sicher, dass die Lösung um 06:00 Uhr UTC ausgeführt wurde.	DevOps Ingenieur

Zugehörige Ressourcen

- AWS Organizations
- AWS Resource Access Manager
- Serverloser Transit Network Orchestrator
- IAM-Rollen erstellen
- Einen Stack auf der AWS CloudFormation Konsole erstellen

Mehr Muster

- Bereitstellen von AWS Service Catalog Produkten auf der Grundlage von AWS CloudFormation Vorlagen mithilfe von GitHub Aktionen
- Stellen Sie IAM-Rollen mit den geringsten Rechten bereit, indem Sie eine Rollenautomatenlösung bereitstellen

KI und maschinelles Lernen

Themen

- Aggregieren Sie Daten in Amazon DynamoDB für ML-Prognosen in Athena
- Verknüpfen Sie ein AWS CodeCommit Repository in einem AWS-Konto mit Amazon SageMaker AI Studio Classic in einem anderen Konto
- Automatisches Extrahieren von Inhalten aus PDF-Dateien mit Amazon Textract
- Erstellen Sie ein Kaltstart-Prognosemodell, indem Sie DeepAR für Zeitreihen in Amazon SageMaker AI Studio Lab verwenden
- Erstellen Sie einen MLOps Workflow mithilfe von Amazon SageMaker AI und Azure DevOps
- Konfigurieren Sie die Protokollierung von Modellaufrufen in Amazon Bedrock mithilfe von AWS CloudFormation
- Erstellen Sie ein benutzerdefiniertes Docker-Container-Image für SageMaker und verwenden Sie es für Modelltrainings in AWS Step Functions
- Verwenden Sie Amazon Bedrock-Agenten, um die Erstellung von Zugriffskontrollen in Amazon EKS durch textbasierte Eingabeaufforderungen zu automatisieren
- Stellen Sie mithilfe AWS von Terraform und Amazon Bedrock einen RAG-Anwendungsfall bereit
- Stellen Sie mithilfe einer Inferenz-Pipeline in Amazon Vorverarbeitungslogik in einem ML-Modell an einem einzigen Endpunkt bereit SageMaker
- Entwickeln Sie mithilfe von RAG und Prompting fortschrittliche, auf KI basierende Chat-Assistenten ReAct
- Entwickeln Sie mithilfe von Amazon Bedrock-Agenten und Wissensdatenbanken einen vollautomatischen Chat-basierten Assistenten
- Dokumentieren Sie institutionelles Wissen anhand von Spracheingaben mithilfe von Amazon Bedrock und Amazon Transcribe
- Generieren Sie mit Amazon Personalize personalisierte und neu eingestufte Empfehlungen
- Optimieren Sie mithilfe von SageMaker KI und Hydra Workflows für maschinelles Lernen — von der lokalen Entwicklung bis hin zu skalierbaren Experimenten
- Trainieren und implementieren Sie ein benutzerdefiniertes GPU-unterstütztes ML-Modell auf Amazon SageMaker
- Translate natürliche Sprache in Abfragen, DSL für OpenSearch und Elasticsearch-Abfragen

- Verwenden Sie Amazon Q Developer als Programmierassistenten, um Ihre Produktivität zu steigern
- Verwenden Sie SageMaker Processing für verteiltes Feature-Engineering von ML-Datensätzen im Terabyte-Bereich
- Visualisieren Sie KI/ML-Modellergebnisse mit Flask und AWS Elastic Beanstalk
- Mehr Muster

Aggregieren Sie Daten in Amazon DynamoDB für ML-Prognosen in Athena

Erstellt von Sachin Doshi (AWS) und Peter Molnar (AWS)

Übersicht

Dieses Muster zeigt Ihnen, wie Sie mithilfe von Amazon Athena komplexe Aggregationen von Internet of Things (IoT) -Daten in einer Amazon DynamoDB-Tabelle erstellen. Sie lernen auch, wie Sie die Daten mithilfe von Amazon SageMaker AI mit Inferenz für maschinelles Lernen (ML) anreichern und wie Sie mithilfe von Athena Geodaten abfragen. Sie können dieses Muster als Grundlage für die Erstellung einer ML-Prognoselösung verwenden, die den Anforderungen Ihres Unternehmens entspricht.

Zu Demonstrationszwecken verwendet dieses Muster ein Beispielszenario eines Unternehmens, das eine Mitfahrgelegenheit für Roller betreibt und die optimale Anzahl von Rollern vorhersagen möchte, die für Kunden in verschiedenen Stadtvierteln eingesetzt werden müssen. Das Unternehmen verwendet ein vorab trainiertes ML-Modell, das die Kundennachfrage für die nächste Stunde auf der Grundlage der letzten vier Stunden prognostiziert. Das Szenario verwendet einen öffentlichen Datensatz des Office of Civic Innovation & Technology für die Regierung der Metropolregion Louisville. Die Ressourcen für dieses Szenario sind in einem GitHub Repository verfügbar.

Voraussetzungen und Einschränkungen

- Ein aktiver AWS-Konto
- Berechtigungen zum Erstellen eines AWS CloudFormation Stacks mit AWS Identity and Access Management (IAM-) Rollen für Folgendes:
  - Amazon Simple Storage Service (Amazon S3)-Bucket
  - Athena
  - DynamoDB
  - SageMaker KI
  - AWS Lambda

Architektur

Technologie-Stack

- Amazon QuickSight
- Amazon S3
- Athena
- DynamoDB
- Lambda
- SageMaker KI

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur für die Erstellung komplexer Datenaggregationen in DynamoDB mithilfe der Abfragefunktionen von Athena, einer Lambda-Funktion, Amazon S3 S3-Speicher, eines SageMaker KI-Endpunkts und eines Dashboards. QuickSight

Das Diagramm zeigt den folgenden Workflow:

1. Eine DynamoDB-Tabelle nimmt IoT-Daten auf, die von einer Flotte von Rollern übertragen werden.
2. Eine Lambda-Funktion lädt die DynamoDB-Tabelle mit den aufgenommenen Daten.
3. Eine Athena-Abfrage erstellt eine neue DynamoDB-Tabelle für die Geodaten, die die Stadtviertel repräsentieren.
4. Der Abfragespeicherort wird in einem S3-Bucket gespeichert.
5. Eine Athena-Funktion fragt die ML-Inferenz vom SageMaker KI-Endpunkt ab, der das vortrainierte ML-Modell hostet.
6. Athena fragt Daten direkt aus den DynamoDB-Tabellen ab und aggregiert die Daten für die Analyse.
7. Ein Benutzer sieht sich die Ausgabe der analysierten Daten in einem Dashboard an. QuickSight

Tools

AWS-Services

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon S3 analysieren können.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.

- Amazon SageMaker AI ist ein verwalteter ML-Service, der Ihnen hilft, ML-Modelle zu erstellen und zu trainieren und sie dann in einer produktionsbereiten gehosteten Umgebung bereitzustellen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon QuickSight ist ein Business Intelligence (BI) -Service auf Cloud-Ebene, mit dem Sie Ihre Daten in einem einzigen Dashboard visualisieren, analysieren und melden können.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub Use ML-Predictions over Amazon DynamoDB data with Amazon Athena ML verfügbar. Sie können die CloudFormation Vorlage aus dem Repository verwenden, um die folgenden Ressourcen zu erstellen, die im Beispielszenario verwendet werden:

- Eine DynamoDB-Tabelle
- Eine Lambda-Funktion zum Laden der Tabelle mit relevanten Daten
- Ein SageMaker KI-Endpunkt für Inferenzanfragen mit dem vortrainierten XGBoost Modell, das in Amazon S3 gespeichert ist
- Eine Athena-Arbeitsgruppe namens `V2EngineWorkGroup`
- Named Athena fragt nach Geodaten-Shapefiles und prognostiziert die Nachfrage nach Rollern
- Ein vordefinierter Amazon Athena DynamoDB-Connector, der Athena die Kommunikation mit DynamoDB ermöglicht und AWS Serverless Application Model(AWS SAM) verwendet, um die Anwendung in Bezug auf den DynamoDB-Konnektor zu erstellen

Epen

Holen Sie sich den Beispieldatensatz

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Datensatz und die Ressourcen herunter.	1. Laden Sie einen öffentlichen Datensatz mit Autovermietungen ohne	App-Entwickler, Datenwissenschaftler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anlegestelle herunter. Zu Demonstrationszwecken werden diese Daten in DynamoDB als Teil des Anwendungsfalls vorab ausgefüllt. In einer Produktionsumgebung senden Sie diese Daten jedoch über verschiedene Mechanismen wie IoT-Geräte oder Amazon Kinesis Kinesis-Verbraucher an DynamoDB. Diese Mechanismen verwenden Lambda, um Daten in DynamoDB einzufügen. 2. Laden Sie die GIS-Shapefiles herunter, die die Grenzen der historischen und kulturellen Viertel in der Stadt Louisville, KY, darstellen. Der öffentliche Datensatz wird vom Louisville and Jefferson County, KY Information Consortium, bereitgestellt. Die ursprünglichen Shapefiles sind bereits in eine Textdatei konvertiert, die Sie mit Athena abfragen können. Den Python-Code für die Transformation von Shapefiles finden Sie jedoch im Jupyter-Notizbuch unter Geo-Spatial	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	processing of GIS shapefile s with Amazon Athena in. GitHub 3. Laden Sie den vortraini erten Python-Code herunter, der das ML-Modell mithilfe von SageMaker KI und Athena für stündliche Prognosen trainiert. 4. Holen Sie sich die SQL-Abfrage in Athena, die alles für Live-Vorhersagen aus den in DynamoDB gespeicherten Daten zusammenführt. 5. (Optional) Wird verwendet QuickSight , um Geodaten auf einer Karte von Louisville, Kentucky, zu visualisieren.	

Verwenden Sie eine CloudFormation Vorlage, um die erforderlichen Ressourcen bereitzustellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen CloudFormation Stapel.	1. Laden Sie die CloudFormation Vorlage aus dem GitHub Repository herunter. 2. **Note** Melden Sie sich bei der AWS	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Managemen t Console an und wählen Sie dann`us-east-1` . : Das ML-Modell ist in der Amazon Elastic Container Registry (Amazon ECR) für gespeiche rt `us-east-1` AWS-Region, aber das Muster ist regionsunabhängig. Sie können das Muster in jeder Region replizieren, in der die in diesem Muster AWS-Servi ces verwendeten Muster unterstützt werden. 3. Öffnen Sie die CloudForm ation Konsole und wählen Sie dann im Navigatio nsbereich Stacks aus. 4. Wählen Sie Stapel erstellen und dann Mit vorhandenen Ressourcen (Ressourcen importieren) aus. 5. Wählen Sie auf der Seite Ressourcen identifizieren die Option Weiter aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Wählen Sie im Abschnitt Vorlage angeben für Vorlagenquelle die Option Vorlagendatei hochladen aus. 7. Wählen Sie Datei und dann die CloudFormation Vorlage aus, die Sie zuvor heruntergeladen haben. 8. Wählen Sie Weiter, akzeptieren Sie die Standardparameterwerte und klicken Sie auf Weiter, um den Rest des Setup-Assistenten durchzugehen. 9. Aktivieren Sie das Kontrollkästchen Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen mit benutzerdefinierten Namen erstellt werden. 10. Wählen Sie Stack erstellen aus. **Note** Es kann 15 bis 20 Minuten dauern, bis der CloudFormation Stack diese Ressourcen erstellt hat.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die CloudFormation Bereitstellung.	Gehen Sie wie folgt vor, um zu überprüfen, ob die Beispieldaten aus der CloudFormation Vorlage in DynamoDB geladen wurden: 1. Öffnen Sie die DynamoDB-Konsole, und wählen Sie dann im Navigationsbereich Tabellen aus. 2. Suchen Sie im Abschnitt Tabellen nach der `DynamoDBTableDocklessVehicles` Tabelle. 3. Nachdem die Ressourcenerstellung abgeschlossen ist, öffnen Sie die Athena-Konsole und wählen Sie dann im Navigationsbereich Workgroups aus. 4. Wählen Sie die **`V2EngineWorkGroup`** Arbeitsgruppe und dann Arbeitsgruppe wechseln aus. 5. Wenn Sie aufgefordert werden, den Speicherort der Abfrageergebnisse zu speichern, wählen Sie einen Amazon S3 S3-Speicherort aus, für den Sie Schreibberechtigungen haben. 6. Wählen Sie Speichern. 7. Wählen Sie im Navigationsbereich den Abfrage-E	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ditor und dann die `athena-ml-db-<your-AWS-account-number>` Datenbank aus.	

Laden Sie Geolocation-Dateien in Athena

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Athena-Tabelle mit Geodaten.	Gehen Sie wie folgt vor, um die Geolocation-Dateien in Athena zu laden: 1. Öffnen Sie die Athena-Konsole und wählen Sie dann im Navigationsbereich den Abfrage-Editor aus. 2. Wählen Sie die Registerkarte Gespeicherte Abfragen. 3. Suchen Sie nach Q1: Nachbarschaften und wählen Sie es aus. 4. Um zum Abfrage-Editor zurückzukehren, wählen Sie die Registerkarte Editor. 5. Wählen Sie Ausführen aus. Dadurch wird eine Tabelle mit dem Namen `louisville_ky_neighborhoods` in Ihrer Datenbank erstellt. Stellen Sie sicher, dass die Tabelle in der `athena-ml-db-`	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`<your-AWS-account-number>` Datenbank erstellt wurde. Die Abfrage erstellt eine neue Tabelle für die Geodaten, die die Stadtviertel repräsentieren. Die Datentabelle wird aus GIS-Shapefiles erstellt. Die `CREATE EXTERNAL TABLE` Anweisung definiert das Schema der Tabelle sowie den Speicherort und das Format der zugrunde liegenden Datendatei. Den Python-Code zur Verarbeitung von Shapefiles und zur Erstellung dieser Tabelle finden Sie unter Geospatiale Verarbeitung von GIS-Shapefiles mit Amazon Athena in Beispielen. AWS Ausführlichen SQL-Code finden Sie unter create_neighborhood_table.sql. GitHub	

Prognostizieren Sie anhand der aggregierten DynamoDB-Daten die Nachfrage nach Rollern nach Stadtvierteln

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Deklarieren Sie eine Funktion in Athena, um SageMaker KI abzufragen.	1. Öffnen Sie die Athena-Konsole, wählen Sie im Navigationsbereich Query-Editor und dann die Registerkarte Editor aus. 2. Kopieren Sie die folgende SQL-Anweisung und fügen Sie sie in den Abfrage-Editor ein. `USING EXTERNAL FUNCTION predict_demand ( location_id BIGINT, hr BIGINT , dow BIGINT, n_pickup_1 BIGINT, n_pickup_2 BIGINT, n_pickup_3 BIGINT, n_pickup_4 BIGINT, n_dropoff_1 BIGINT, n_dropoff_2 BIGINT, n_dropoff_3 BIGINT, n_dropoff_4 BIGINT ) RETURNS DOUBLE SAGEMAKER '<Your SageMaker endpoint>'` Der erste Teil der SQL-Anweisung deklariert die externe Funktion zur Abfrage von ML-Inferenzen vom SageMaker KI-Endpun	Datenwissenschaftler, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	kt, der das vortrainierte Modell hostet. 3. Definieren Sie die Reihenfolge und den Typ der Eingabeparameter sowie den Typ der Rückgabewerte. 4. Wählen Sie Ausführen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Prognostizieren Sie anhand der aggregierten DynamoDB-Daten die Nachfrage nach Rollern nach Stadtvierteln.	Jetzt können Sie Athena verwenden, um Transakti onsdaten direkt aus DynamoDB abzufragen und die Daten anschließend für Analysen und Prognosen zu aggregieren. Dies ist nicht einfach zu erreichen, indem eine DynamoDB-NoSQL-Dat enbank direkt abgefragt wird. 1. Öffnen Sie die Athena-Ko nsole und wählen Sie dann im Navigationsbereich den Abfrage-Editor aus. 2. Wählen Sie die Registerk arte Gespeicherte Abfragen. 3. Suchen Sie nach Q2: Dynamo DBAthena MLScooter Predict und wählen Sie es aus. 4. Um zum Abfrage-Editor zurückzukehren, wählen Sie die Registerkarte Editor. 5. Wählen Sie Ausführen aus. Die SQL-Anweisung macht Folgendes: • Verwendet eine Athena Federated Query, um die DynamoDB-Tabelle mit den Reise-Rohdaten abzufragen	App-Entwickler, Datenwiss enschaftler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Platziert geografische Koordinaten mithilfe der Geodatenfunktionen von Athena in Nachbarschaften • Reichert Daten mithilfe von KI mit ML-Inferenz an SageMaker Informationen zur Verwendung von SQL zum Aggregieren von DynamoDB-Daten und SageMaker AI-Inferenzdaten in Athena finden Sie unter athena_long.sql unter. GitHub	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Ausgabe.	Die Ausgabetabelle enthält die Nachbarschaft, den Längengrad und den Breitengrad des Schwerpunkts der Nachbarschaft. Sie enthält auch die Anzahl der Fahrzeuge, die für die nächste Stunde prognostiziert werden. Die Abfrage generiert die Vorhersagen für einen ausgewählten Zeitpunkt. Sie können Vorhersagen für jeden anderen Zeitpunkt treffen, indem Sie den Ausdruck an einer beliebigen `TIMESTAMP '2019-09-07 15:00'` Stelle in der Anweisung ändern. Wenn Ihre DynamoDB-Tabelle einen Echtzeit-Datenfeed enthält, ändern Sie den Zeitstempel auf. `NOW()`	App-Entwickler, Datenwissenschaftler

Säubere die Umwelt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ressourcen löschen.	1. Öffnen Sie die Athena-Konsole und leeren Sie den Bucket, den Sie als Teil des CloudFormation Stacks erstellt haben.	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Öffnen Sie die CloudFormation Konsole und löschen Sie dann den genannten `bdb-1462-athena-dynamodb-ml-stack` Stack. 3. Öffnen Sie die CloudWatch Amazon-Konsole und löschen Sie dann die Protokollgruppe mit dem Namen `/aws/sagemaker/Endpoints/Sg-athena-ml-dynamodb-model-endpoint` .	

Zugehörige Ressourcen

- Amazon Athena Query Federation SDK () GitHub
- Abfragen von Geodaten (Dokumentation)AWS
- Verwenden Sie ML-Vorhersagen für Amazon DynamoDB DynamoDB-Daten mit Amazon Athena ML (AWS Big Data Blog)
- Amazon ElastiCache (Redis OSS) (AWS Dokumentation)
- Amazon Neptune (Dokumentation)AWS

Verknüpfen Sie ein AWS CodeCommit Repository in einem AWS-Konto mit Amazon SageMaker AI Studio Classic in einem anderen Konto

Erstellt von Laurens van der Maas (AWS) und Aubrey Oosthuizen (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Dieses Muster enthält Anweisungen und Code zur Verknüpfung eines AWS CodeCommit Repositorys in einem AWS-Konto (Konto A) mit Amazon SageMaker AI Studio Classic in einem anderen AWS-Konto (Konto B). Um die Zuordnung einzurichten, müssen Sie eine AWS Identity and Access Management (IAM-) Richtlinie und Rolle in Konto A und eine IAM-Inline-Richtlinie in Konto B erstellen. Anschließend verwenden Sie ein Shell-Skript, um das CodeCommit Repository von Konto A nach Amazon SageMaker AI Classic in Konto B zu klonen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zwei AWS-Konten, eine enthält das CodeCommit Repository und die andere enthält eine SageMaker AI-Domäne mit einem Benutzer
- Bereitgestellte SageMaker KI-Domäne und Benutzer mit Internetzugang oder Zugriff auf CodeCommit und AWS Security Token Service (AWS STS) über virtuelle private Netzwerke (VPC) -Endpunkte
- Ein grundlegendes Verständnis von IAM
- Ein grundlegendes Verständnis von SageMaker AI Studio Classic
- Ein grundlegendes Verständnis von Git und CodeCommit

Einschränkungen

Dieses Muster gilt nur für SageMaker AI Studio Classic, nicht für RStudio Amazon SageMaker AI.

Architektur

Technologie-Stack

- Amazon SageMaker KI
- Amazon SageMaker AI Studio Klassisch
- AWS CodeCommit
- AWS Identity and Access Management (ICH BIN)
- Git

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur, die ein CodeCommit Repository von Konto A mit SageMaker AI Studio Classic in Konto B verknüpft.

Das Diagramm zeigt den folgenden Workflow:

1. Ein Benutzer übernimmt die `MyCrossAccountRepositoryContributorRole` Rolle in Konto A über die `sts:AssumeRole` Rolle, während er die AI-Ausführungsrolle in SageMaker SageMaker AI Studio Classic in Konto B verwendet. Die übernommene Rolle beinhaltet die CodeCommit Berechtigungen zum Klonen und Interagieren mit dem angegebenen Repository.
2. Der Benutzer führt Git-Befehle vom Systemterminal in SageMaker AI Studio Classic aus.

Automatisierung und Skalierung

Dieses Muster besteht aus manuellen Schritten, die mithilfe von AWS Cloud Development Kit (AWS CDK)AWS CloudFormation, oder Terraform automatisiert werden können.

Tools

AWS-Tools

- Amazon SageMaker AI ist ein verwalteter Service für maschinelles Lernen (ML), mit dem Sie ML-Modelle erstellen und trainieren und sie dann in einer produktionsbereiten, gehosteten Umgebung bereitstellen können.

- Amazon SageMaker AI Studio Classic ist eine webbasierte, integrierte Entwicklungsumgebung (IDE) für maschinelles Lernen, mit der Sie Ihre Machine-Learning-Modelle erstellen, trainieren, debuggen, bereitstellen und überwachen können.
- AWS CodeCommitist ein Versionskontrolldienst, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.

  Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.

Andere Tools

- Git ist ein verteiltes Versionskontrollsystem zur Nachverfolgung von Änderungen im Quellcode während der Softwareentwicklung.

Epen

Erstellen Sie eine IAM-Richtlinie und eine IAM-Rolle in Konto A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Richtlinie für den Repository-Zugriff in Konto A.	1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole. 2. Wählen Sie im Navigationsbereich Richtlinien und dann Richtlinie erstellen. 3. Wählen Sie den Tab JSON. 4. Kopieren Sie die Richtlinienanweisung aus der Beispiel-IAM-Richtlinie im Abschnitt Zusätzliche Informationen dieses	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Musters und fügen Sie die Anweisung dann in den JSON-Editor ein. Achten Sie darauf, alle Platzhalt erwerte in der Richtlinie zu ersetzen. 5. Wählen Sie Weiter: Schlagworte und dann Weiter: Überprüfen. 6. Geben Sie unter Name einen Namen für die Richtlinie ein. Hinweis: In diesem Muster wird die IAM-Richtlinie als bezeichnet`CrossAcco untAccessForMyShar edDemoRepo` , aber Sie können einen beliebigen Richtliniennamen wählen. 7. Wählen Sie Richtlinie erstellen aus. **Tip** Es hat sich bewährt, den Geltungsbereich Ihrer IAM-Richt linien auf die für Ihren Anwendung sfall erforderlichen Mindestberechtigun gen zu beschränken.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle für den Repository-Zugriff in Konto A.	1. Klicken Sie im Navigationsbereich der IAM-Konsole auf Rollen und wählen Sie dann Rolle erstellen aus. 2. Wählen Sie unter Vertrauenswürdiger Entitätstyp die Option AWS-Konto aus. 3. Wählen Sie im Abschnitt AWS-Konto die Option Anderes AWS-Konto aus. 4. Geben Sie als Konto-ID die Konto-ID für Konto B ein. 5. Suchen Sie auf der Seite „Berechtigungen hinzufügen“ nach der `CrossAccountAccessForMySharedDemoRepo` Richtlinie, die Sie zuvor erstellt haben, und wählen Sie sie aus. 6. Wählen Sie Weiter aus. 7. Geben Sie in Role name (Name der Rolle) einen Namen ein. Hinweis: In diesem Muster wird der IAM-Rollenname als bezeichnet`MyCrossAccountRepositoryContributorRole` , aber Sie können einen beliebigen Rollennamen wählen. 8. Wählen Sie Rolle erstellen und kopieren Sie dann den	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon-Ressourcennamen (ARN) der neuen Rolle.	

Erstellen Sie eine IAM-Inline-Richtlinie in Konto B

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie der Ausführungsrolle, die Ihrem SageMaker Domain-Benutzer in Konto B zugewiesen ist, eine Inline-Richtlinie hinzu.	1. Wählen Sie im Navigationsbereich der IAM-Konsole Rollen aus. 2. Suchen Sie nach der Ausführungsrolle, die Ihrem SageMaker AI-Domänenbenutzer in Konto B zugewiesen ist, und wählen Sie sie aus. 3. Wählen Sie Add permissions (Berechtigungen hinzufügen) und dann Create inline policy (Inline-Richtlinie erstellen) aus. 4. Wählen Sie den Tab JSON. 5. Kopieren Sie die folgende Richtlinienerklärung und fügen Sie sie dann in den JSON-Editor ein. `{ "Version": "2012-10-17", "Statement": [ { "Sid": "VisualEditor0",`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "arn:aws:iam::<Account_A_ID>:role/<Account_A_Role_Name>" }] }</pre> 6. `<Account_A_ID>` Ersetzen Sie es durch die Konto-ID für Konto A. `<Account_A_Role_Name>` Ersetzen Sie es durch den Namen der IAM-Rolle, die Sie zuvor erstellt haben. 7. Wählen Sie Richtlinie prüfen. 8. Geben Sie unter Name einen Namen für Ihre Inline-Richtlinie ein. 9. Wählen Sie Richtlinie erstellen aus.	

Klonen Sie das Repository in SageMaker AI Studio Classic für Konto B

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Shell-Skript in SageMaker AI Studio Classic in Konto B.	1. Wählen Sie im Navigationsbereich der SageMaker Konsole Studio aus.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie Ihr Benutzerprofil und dann Open Studio aus. 3. Wählen Sie im Home-Bereich die Option Launcher öffnen. 4. Wählen Sie im Bereich Dienstprogramme und Dateien die Option Textdatei aus. 5. Kopieren Sie das Skript aus dem SageMaker Beispiel-Shell-Skript im Abschnitt Zusätzliche Informationen dieses Musters und fügen Sie die Anweisung dann in die neue Datei ein. Achten Sie darauf, alle Platzhalterwerte im Skript zu ersetzen. 6. Klicken Sie mit der rechten Maustaste auf die Registerkarte untitled.txt Ihrer neuen Datei und wählen Sie dann Text umbenennen. Geben Sie für „Neuer Name“ cross_account_git_clone.sh ein, und wählen Sie dann „Umbenennen“.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie das Shell-Skript vom Systemterminal aus auf.	1. Wählen Sie im Home-Bereich der SageMaker Konsole die Option Launcher öffnen. 2. Wählen Sie im Bereich „Dienstprogramme und Dateien“ die Option „Systemterminal“. 3. Führen Sie im Terminal den folgenden Befehl aus: `chmod u+x ./cross_account_git_clone.sh && ./cross_account_git_clone.sh` Sie haben Ihr CodeCommit Repository in ein SageMaker AI Studio-Cross-Konto geklont. Sie können jetzt alle Git-Befehle vom Systemterminal aus ausführen.	AWS DevOps

Zusätzliche Informationen

Beispiel für eine IAM-Richtlinie

Wenn Sie diese Beispielrichtlinie verwenden, gehen Sie wie folgt vor:

- `<CodeCommit_Repository_Region>`Ersetzen Sie es durch das AWS-Region für das Repository.
- `<Account_A_ID>`Ersetzen Sie es durch die Konto-ID für Konto A.
- `<CodeCommit_Repository_Name>`Ersetzen Sie es durch den Namen Ihres CodeCommit Repositorys in Konto A.

```
{
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "codecommit:BatchGet*",
            "codecommit:Create*",
            "codecommit:DeleteBranch",
            "codecommit:Get*",
            "codecommit:List*",
            "codecommit:Describe*",
            "codecommit:Put*",
            "codecommit:Post*",
            "codecommit:Merge*",
            "codecommit:Test*",
            "codecommit:Update*",
            "codecommit:GitPull",
            "codecommit:GitPush"
        ],
        "Resource": [

 "arn:aws:codecommit:<CodeCommit_Repository_Region>:<Account_A_ID>:<CodeCommit_Repository_Name>
        ]
    }
]
}
```

Beispiel für ein SageMaker AI-Shell-Skript

Wenn Sie dieses Beispielskript verwenden, gehen Sie wie folgt vor:

- <Account_A_ID>Ersetzen Sie es durch die Konto-ID für Konto A.
- <Account_A_Role_Name>Ersetzen Sie durch den Namen der IAM-Rolle, die Sie zuvor erstellt haben.
- Ersetzen Sie <CodeCommit_Repository_Region> durch den AWS-Region für das Repository.
- <CodeCommit_Repository_Name>Ersetzen Sie es durch den Namen Ihres CodeCommit Repositorys in Konto A.

```
#!/usr/bin/env bash
```

```
#Launch from system terminal
pip install --quiet git-remote-codecommit

mkdir -p ~/.aws
touch ~/.aws/config

echo "[profile CrossAccountAccessProfile]
region = <CodeCommit_Repository_Region>
credential_source=EcsContainer
role_arn = arn:aws:iam::<Account_A_ID>:role/<Account_A_Role_Name>
output = json" > ~/.aws/config

echo '[credential "https://git-
codecommit.<CodeCommit_Repository_Region>.amazonaws.com"]
        helper = !aws codecommit credential-helper $@ --profile
 CrossAccountAccessProfile
        UseHttpPath = true' > ~/.gitconfig

git clone codecommit::<CodeCommit_Repository_Region>://
CrossAccountAccessProfile@<CodeCommit_Repository_Name>
```

Automatisches Extrahieren von Inhalten aus PDF-Dateien mit Amazon Textract

Erstellt von Tianxia Jia (AWS)

Übersicht

Viele Unternehmen müssen Informationen aus PDF-Dateien extrahieren, die in ihre Geschäftsanwendungen hochgeladen werden. Beispielsweise könnte eine Organisation Informationen aus steuerlichen oder medizinischen PDF-Dateien für die Steueranalyse oder die Bearbeitung von medizinischen Ansprüchen präzise extrahieren müssen.

In der Amazon Web Services (AWS) Cloud extrahiert Amazon Textract automatisch Informationen (z. B. gedruckten Text, Formulare und Tabellen) aus PDF-Dateien und erstellt eine Datei im JSON-Format, die Informationen aus der ursprünglichen PDF-Datei enthält. Sie können Amazon Textract in der AWS-Managementkonsole oder durch Implementierung von API-Aufrufen verwenden. Wir empfehlen, programmatische API-Aufrufe zu verwenden, um eine große Anzahl von PDF-Dateien zu skalieren und automatisch zu verarbeiten.

Wenn Amazon Textract eine Datei verarbeitet, erstellt es die folgende `Block` Objektliste: Seiten, Textzeilen und Wörter, Formulare (Schlüssel-Wert-Paare), Tabellen und Zellen sowie Auswahlelemente. Andere Objektinformationen sind ebenfalls enthalten, z. B. Begrenzungsrahmen, Konfidenzintervalle und Beziehungen. IDs Amazon Textract extrahiert die Inhaltsinformationen als Zeichenketten. Korrekt identifizierte und transformierte Datenwerte sind erforderlich, da sie von Ihren nachgelagerten Anwendungen einfacher verwendet werden können.

Dieses Muster beschreibt einen step-by-step Workflow für die Verwendung von Amazon Textract, um automatisch Inhalte aus PDF-Dateien zu extrahieren und zu einer sauberen Ausgabe zu verarbeiten. Das Muster verwendet ein Verfahren zum Abgleich von Vorlagen, um das erforderliche Feld, den Schlüsselnamen und die Tabellen korrekt zu identifizieren, und wendet dann die Nachbearbeitungskorrekturen auf jeden Datentyp an. Sie können dieses Muster verwenden, um verschiedene Arten von PDF-Dateien zu verarbeiten. Anschließend können Sie diesen Workflow skalieren und automatisieren, um PDF-Dateien mit identischem Format zu verarbeiten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.

- Ein vorhandener Amazon Simple Storage Service (Amazon S3) -Bucket zum Speichern der PDF-Dateien, nachdem sie zur Verarbeitung durch Amazon Textract in das JPEG-Format konvertiert wurden. Weitere Informationen zu S3-Buckets finden Sie unter Buckets-Übersicht in der Amazon S3 S3-Dokumentation.
- Das `Textract_PostProcessing.ipynb` Jupyter-Notebook (angeschlossen), installiert und konfiguriert. Weitere Informationen zu Jupyter-Notebooks finden Sie unter Erstellen eines Jupyter-Notizbuchs in der Amazon-Dokumentation. SageMaker
- Bestehende PDF-Dateien, die ein identisches Format haben.
- Ein Verständnis von Python.

Einschränkungen

- Ihre PDF-Dateien müssen von guter Qualität und gut lesbar sein. Systemeigene PDF-Dateien werden empfohlen, aber Sie können gescannte Dokumente verwenden, die in ein PDF-Format konvertiert wurden, wenn alle einzelnen Wörter klar sind. Weitere Informationen dazu finden Sie unter Vorverarbeitung von PDF-Dokumenten mit Amazon Textract: Erkennung und Entfernung von Grafiken im AWS Machine Learning Learning-Blog.
- Für mehrseitige Dateien können Sie einen asynchronen Vorgang verwenden oder die PDF-Dateien in eine einzelne Seite aufteilen und einen synchronen Vorgang verwenden. Weitere Informationen zu diesen beiden Optionen finden Sie unter Erkennen und Analysieren von Text in mehrseitigen Dokumenten und Erkennen und Analysieren von Text in einseitigen Dokumenten in der Amazon Textract Textract-Dokumentation.

Architektur

Der Workflow dieses Musters führt Amazon Textract zunächst für eine Beispiel-PDF-Datei aus (Erstausführung) und führt ihn dann für PDF-Dateien aus, die ein identisches Format wie das erste PDF haben (Wiederholungslauf). Das folgende Diagramm zeigt den kombinierten Arbeitsablauf beim ersten Ausführen und beim wiederholten Ausführen, der automatisch und wiederholt Inhalte aus PDF-Dateien mit identischen Formaten extrahiert.

Das Diagramm zeigt den folgenden Arbeitsablauf für dieses Muster:

1. Konvertiert eine PDF-Datei in das JPEG-Format und speichert sie in einem S3-Bucket.

2. Rufen Sie die Amazon Textract Textract-API auf und analysieren Sie die Amazon Textract Textract-Antwort-JSON-Datei.
3. Bearbeiten Sie die JSON-Datei, indem Sie das richtige `KeyName:DataType` Paar für jedes erforderliche Feld hinzufügen. Erstellen Sie eine `TemplateJSON` Datei für die Phase „Ausführung wiederholen“.
4. Definieren Sie die Korrekturfunktionen für die Nachbearbeitung für jeden Datentyp (z. B. Float, Integer und Date).
5. Bereiten Sie die PDF-Dateien vor, die ein identisches Format wie Ihre erste PDF-Datei haben.
6. Rufen Sie die Amazon Textract Textract-API auf und analysieren Sie die Amazon Textract Textract-Antwort-JSON.
7. Ordnen Sie die geparste JSON-Datei der Datei zu. `TemplateJSON`
8. Implementieren Sie Korrekturen nach der Bearbeitung.

Die endgültige JSON-Ausgabedatei enthält das richtige `KeyName` und `Value` für jedes erforderliche Feld.

Zieltechnologie-Stack

- Amazon SageMaker
- Amazon S3
- Amazon Textract

Automatisierung und Skalierung

Sie können den Repeat Run-Workflow automatisieren, indem Sie eine AWS Lambda Lambda-Funktion verwenden, die Amazon Textract initiiert, wenn eine neue PDF-Datei zu Amazon S3 hinzugefügt wird. Amazon Textract führt dann die Verarbeitungsskripten aus und die endgültige Ausgabe kann an einem Speicherort gespeichert werden. Weitere Informationen dazu finden Sie in der Lambda-Dokumentation unter Verwenden eines Amazon S3 S3-Triggers zum Aufrufen einer Lambda-Funktion.

Tools

- Amazon SageMaker ist ein vollständig verwalteter ML-Service, mit dem Sie schnell und einfach ML-Modelle erstellen und trainieren und sie dann direkt in einer produktionsbereiten gehosteten Umgebung bereitstellen können.

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Textract macht es einfach, Ihren Anwendungen die Erkennung und Analyse von Dokumententext hinzuzufügen.

Epen

Erster Lauf

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konvertiert die PDF-Datei.	Bereiten Sie die PDF-Datei für Ihre erste Ausführung vor, indem Sie sie in eine einzelne Seite aufteilen und sie für den synchronen Vorgang von Amazon Textract in das JPEG-Format konvertieren (`Syn API`). **Note** Sie können die asynchrone Amazon Textract Textract-Operation (`Asyn API`) auch für mehrseitige PDF-Dateien verwenden.	Datenwissenschaftler, Entwickler
Analysieren Sie die JSON der Amazon Textract Textract-Antwort.	Öffnen Sie das `Textract_PostProcessing.ipynb` Jupyter-Notizbuch (angehängt) und rufen Sie die Amazon Textract Textract-API mit dem folgenden Code auf:	Datenwissenschaftler, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`response = textract.analyze_document( Document={ 'S3Object': { 'Bucket': BUCKET, 'Name': '{}'.format(filename) } }, FeatureTypes=["TABLES", "FORMS"])`
	
	Analysieren Sie den Antwort-JSON mithilfe des folgenden Codes in ein Formular und eine Tabelle:
	
	`parseformKV=form_kv_from_JSON(response) parseformTables=get_tables_fromJSON(response)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bearbeiten Sie die TemplateJSON-Datei.	Bearbeiten Sie den analysierten JSON-Code für jeden `KeyName` und die entsprechenden `DataType` (z. B. Zeichenfolge, Fließkommazahl, Ganzzahl oder Datum) und Tabellenüberschriften (z. B. und). `ColumnNames` `RowNames` Diese Vorlage wird für jeden einzelnen PDF-Dateityp verwendet, was bedeutet, dass die Vorlage für PDF-Dateien mit identischem Format wiederverwendet werden kann.	Datenwissenschaftler, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie die Korrektur funktionen für die Nachbearb eitung.	Die Werte in der Antwort von Amazon Textract für die `TemplateJSON` Datei sind Zeichenketten. Es gibt keine Unterscheidung nach Datum, Fließkommazahl, Ganzzahl oder Währung. Diese Werte müssen in den richtigen Datentyp für Ihren Downstrea m-Anwendungsfall konvertiert werden. Korrigieren Sie jeden Datentyp entsprechend der `TemplateJ SON` Datei, indem Sie den folgenden Code verwenden: `finalJSON=postproc essingCorrection(p arsedJSON,template JSON)`	Datenwissenschaftler, Entwickler

Lauf wiederholen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die PDF-Dateien vor.	Bereiten Sie die PDF-Datei en vor, indem Sie sie auf eine einzelne Seite aufteilen und sie für den synchronen Vorgang von Amazon Textract in das JPEG-Format konvertie ren (). `Syn API`	Datenwissenschaftler, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Sie können die asynchrone Amazon Textract Textract-Operation (`Asyn API`) auch für mehrseitige PDF-Dateien verwenden.	
Rufen Sie die Amazon Textract Textract-API auf.	Rufen Sie die Amazon Textract Textract-API mit dem folgenden Code auf: `response = textract.analyze_document( Document={ 'S3Object': { 'Bucket': BUCKET, 'Name': '{}'.format(filename) } }, FeatureTypes=["TABLES", "FORMS"])`	Datenwissenschaftler, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Analysieren Sie die JSON der Amazon Textract Textract-Antwort.	Analysieren Sie die Antwort-JSON mithilfe des folgenden Codes in ein Formular und eine Tabelle:
	`parseformKV=form_kv_from_JSON(response)`
	`parseformTables=get_tables_fromJSON(response)`
		Datenwissenschaftler, Entwickler

Laden Sie die TemplateJSON-Datei und ordnen Sie sie der analysierten JSON-Datei zu.	Verwenden Sie die `TemplateJSON` Datei, um mithilfe der folgenden Befehle die richtigen Schlüssel-Wert-Paare und die richtige Tabelle zu extrahieren:
	`form_kv_corrected=form_kv_correction(parseformKV,templateJSON)`
	`form_table_corrected=form_Table_correction(parseformTables, templateJSON)`
	`form_kv_table_corrected_final={**form_kv_corrected , **form_table_corrected}`
		Datenwissenschaftler, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Korrekturen nach der Bearbeitung.	Verwenden Sie `DataType` in der `TemplateJSON` Datei und in der Nachbearbeitung Funktionen, um Daten mithilfe des folgenden Codes zu korrigieren: `finalJSON=postprocessingCorrection(form_kv_table_corrected_final,templateJSON)`	Datenwissenschaftler, Entwickler

Zugehörige Ressourcen

- Extrahieren Sie mit Amazon Textract automatisch Text und strukturierte Daten aus Dokumenten
- Extrahieren Sie Text und strukturierte Daten mit Amazon Textract
- Amazon Textract Textract-Ressourcen

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Erstellen Sie ein Kaltstart-Prognosemodell, indem Sie DeepAR für Zeitreihen in Amazon SageMaker AI Studio Lab verwenden

Erstellt von Ivan Cui (AWS) und Eyal Shacham (AWS)

Übersicht

Ganz gleich, ob Sie Ressourcen effizienter für den Web-Traffic einsetzen, die Nachfrage von Patienten aufgrund des Personalbedarfs prognostizieren oder den Verkauf von Produkten eines Unternehmens vorhersehen möchten, Prognosen sind ein unverzichtbares Instrument. Bei Kaltstartprognosen werden Prognosen für eine Zeitreihe erstellt, die nur wenige historische Daten enthält, z. B. für ein neues Produkt, das gerade auf den Einzelhandelsmarkt gekommen ist. Dieses Muster verwendet den Amazon SageMaker AI DeepAR-Prognosealgorithmus, um ein Kaltstart-Prognosemodell zu trainieren, und zeigt, wie Prognosen für Kaltstartartikel durchgeführt werden.

DeepAR ist ein überwachter Lernalgorithmus zur Prognose skalarer (eindimensionaler) Zeitreihen unter Verwendung rekurrenter neuronaler Netze (RNN). DeepAR verfolgt den Ansatz, ein einziges Modell gemeinsam über alle Zeitreihen verwandter Produkte hinweg zu trainieren.

Herkömmliche Methoden zur Vorhersage von Zeitreihen wie der autoregressive integrierte gleitende Durchschnitt (ARIMA) oder die exponentielle Glättung (ETS) stützen sich stark auf historische Zeitreihen jedes einzelnen Produkts. Daher sind diese Methoden für Kaltstartprognosen nicht wirksam. Sobald der Datensatz Hunderte verwandter Zeitreihen enthält, liefert die DeepAR-Methode bessere Ergebnisse als die Standardmethoden ARIMA und ETS. Sie können das trainierte Modell auch verwenden, um Prognosen für neue Zeitreihen zu generieren, die den Zeitreihen ähneln, für die es trainiert wurde.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto.
- Eine Amazon SageMaker AI-Domain.
- Eine Amazon SageMaker AI Studio Lab - oder Jupiter Lab-Anwendung.
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket mit Lese- und Schreibberechtigungen.
- Programmierkenntnisse in Python.
- Kenntnisse in der Verwendung eines Jupyter-Notebooks.

Einschränkungen

- Beim Aufrufen des Prognosemodells ohne historische Datenpunkte wird ein Fehler zurückgegeben. Wenn das Modell mit einer minimalen Anzahl historischer Datenpunkte aufgerufen wird, werden ungenaue Vorhersagen mit hoher Zuverlässigkeit zurückgegeben. Dieses Muster deutet auf einen Ansatz zur Lösung dieser bekannten Einschränkungen der Kaltstartprognose hin.
- Einige AWS-Services sind nicht in allen verfügbar. AWS-Regionen Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie unter AWS-Services nach Regionen. Informationen zu bestimmten Endpunkten finden Sie unter Service-Endpunkte und Kontingente. Wählen Sie dort den Link für den Service aus.

Produktversionen

- Python-Version 3.10 oder höher.
- Das Notizbuch des Musters wurde in Amazon SageMaker AI Studio auf einer ml.t3.medium-Instance mit dem Python 3-Kernel (Data Science) getestet.

Architektur

Das folgende Diagramm zeigt den Workflow und die Architekturkomponenten für dieses Muster.

Der Workflow führt die folgenden Aufgaben aus:

1. Eingabedateien mit Trainings- und Testdaten werden synthetisiert und dann in einen Amazon S3 S3-Bucket hochgeladen. Diese Daten umfassen mehrere Zeitreihen mit kategorialen und dynamischen Merkmalen sowie Zielwerte (die vorhergesagt werden müssen). Das Jupyter-Notebook visualisiert die Daten, um die Anforderungen der Trainingsdaten und die erwarteten vorhergesagten Werte besser zu verstehen.
2. Ein Hyperparameter-Tuner-Job wird erstellt, um das Modell zu trainieren und anhand vordefinierter Metriken das beste Modell zu finden.
3. Die Eingabedateien werden aus dem Amazon S3 S3-Bucket in jede Instanz der Hyperparameter-Tuning-Jobs heruntergeladen.
4. Nachdem der Tuner-Job auf der Grundlage des vordefinierten Schwellenwerts des Tuners das beste Modell ausgewählt hat, wird das Modell als SageMaker KI-Endpunkt bereitgestellt.

5. Das bereitgestellte Modell kann dann aufgerufen werden, wo seine Vorhersagen anhand der Testdaten validiert werden.

Das Notizbuch zeigt, wie gut das Modell die Zielwerte vorhersagt, wenn eine ausreichende Anzahl historischer Datenpunkte verfügbar ist. Wenn wir das Modell jedoch mit weniger historischen Datenpunkten aufrufen (die ein kaltes Produkt darstellen), stimmen die Vorhersagen des Modells nicht mit den ursprünglichen Testdaten überein, auch nicht innerhalb der Konfidenzniveaus des Modells. In diesem Muster wird ein neues Modell für kalte Produkte erstellt, dessen anfängliche Kontextlänge (vorhergesagte Punkte) als die Menge der verfügbaren historischen Punkte definiert ist, und ein neues Modell wird iterativ trainiert, sobald neue Datenpunkte erfasst werden. Aus dem Notizbuch geht hervor, dass das Modell genaue Vorhersagen liefern kann, solange die Menge der historischen Datenpunkte der Kontextlänge nahe kommt.

Tools

AWS-Services

- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Amazon SageMaker AI ist ein verwalteter Service für maschinelles Lernen (ML), mit dem Sie ML-Modelle erstellen und trainieren und diese dann in einer produktionsbereiten, gehosteten Umgebung bereitstellen können.
- Amazon SageMaker AI Studio ist eine webbasierte, integrierte Entwicklungsumgebung (IDE) für ML, mit der Sie Ihre ML-Modelle erstellen, trainieren, debuggen, bereitstellen und überwachen können.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere Tools

- Python ist eine Allzweck-Computerprogrammiersprache.

Code-Repository

Der Code für dieses Muster ist im GitHub DeepAR- ColdProduct -Pattern-Repository verfügbar.

Bewährte Methoden

- Trainieren Sie Ihr Modell in einer virtuellen Umgebung und verwenden Sie stets die Versionskontrolle, um ein Höchstmaß an Reproduzierbarkeit zu erzielen.
- Fügen Sie so viele hochwertige kategoriale Merkmale wie möglich hinzu, um das prädiktivste Modell zu erhalten.
- Stellen Sie sicher, dass die Metadaten ähnliche kategoriale Elemente enthalten, damit das Modell die Prognosen für Kaltstartprodukte angemessen ableiten kann.
- Führen Sie einen Hyperparameter-Tuning-Job aus, um das beste Vorhersagemodell zu erhalten.
- In diesem Muster hat das Modell, das Sie erstellen, eine Kontextlänge von 24 Stunden, was bedeutet, dass es die nächsten 24 Stunden vorhersagt. Wenn Sie versuchen, die nächsten 24 Stunden vorherzusagen, obwohl Sie historisch gesehen weniger als 24 Stunden an Daten haben, verschlechtert sich die Prognosegenauigkeit des Modells linear, basierend auf der Menge der historischen Datenpunkte. Um dieses Problem zu beheben, erstellen Sie für jeden Satz historischer Datenpunkte ein neues Modell, bis diese Zahl die gewünschte Länge der Vorhersage (des Kontextes) erreicht hat. Beginnen Sie beispielsweise mit einem Kontextlängenmodell von 2 Stunden und erhöhen Sie das Modell dann schrittweise auf 4 Stunden, 8 Stunden, 16 Stunden und 24 Stunden.

Epen

Starten Sie Ihre SageMaker AI Studio Classic-Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie Ihre Notebook-Umgebung.	1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die SageMaker AI Studio-St artseite. Wählen Sie dann Open Studio. 2. Wählen Sie im linken Navigationsbereich unter Anwendungen das Studio Classic-Symbol aus.	Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wählen Sie dann in der Anwendungsliste die Schaltfläche Öffnen aus. Weitere Informationen finden Sie in der SageMaker KI-Dokumentation unter Amazon SageMaker AI Studio starten.	

Erstellen und aktivieren Sie das Notizbuch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Ihre virtuelle Umgebung für das Modelltraining ein.	Gehen Sie wie folgt vor, um Ihre virtuelle Umgebung für das Modelltraining einzurichten: 1. Laden Sie das `deepar_synthetic.ipynb` Notizbuch aus dem GitHub Repository dieses Patterns auf Ihren lokalen Computer herunter. 2. Wählen Sie in Amazon SageMaker AI Studio Classic das Symbol Dateien hochladen in der Studio Classic-Menüleiste und wählen Sie das heruntergeladene Notizbuch aus. 3. Wählen Sie das Notizbuch im Dateibrowser im linken Navigationsbereich aus.	Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Folgen Sie den Anweisungen, um eine Notebook-Umgebung einzurichten. Wählen Sie das Data Science 3.0-Image und den Python 3-Kernel aus. Weitere Informationen finden Sie in der AI-Dokumentation unter Dateien auf SageMaker SageMaker AI Studio Classic hochladen.	
Erstellen und validieren Sie ein Prognosemodell.	• Folgen Sie den Anweisungen im Notizbuch, um die Trainings- und Testdaten zu erstellen, das Modell zu trainieren und dann das Modell aufzurufen. • Beobachten Sie, wie genau die Vorhersagen des Modells sind, wenn es über angemessene historische Datenpunkte verfügt.	Data Scientist

Zugehörige Ressourcen

- DeepAR Hyperparameter
- Prognose der Nachfrage nach neuen Produkteinführungen mithilfe von Diensten für maschinelles Lernen AWS
- Starten Sie Amazon SageMaker AI Studio Classic
- Verwenden Sie den SageMaker AI DeepAR-Prognosealgorithmus

Erstellen Sie einen MLOps Workflow mithilfe von Amazon SageMaker AI und Azure DevOps

Erstellt von Deepika Kumar (AWS), Philips Kokoh Prasetyo (AWS) und Sara van de Moosdijk (AWS)

Übersicht

Bei Machine Learning Operations (MLOps) handelt es sich um eine Reihe von Praktiken, mit denen Workflows und Bereitstellungen für maschinelles Lernen (ML) automatisiert und vereinfacht werden. MLOps konzentriert sich auf die Automatisierung des ML-Lebenszyklus. Es trägt dazu bei, dass Modelle nicht nur entwickelt, sondern auch systematisch und wiederholt eingesetzt, überwacht und neu trainiert werden. Es bringt DevOps Prinzipien in das maschinelle Lernen. MLOps führt zu einer schnelleren Bereitstellung von ML-Modellen, einer höheren Genauigkeit im Laufe der Zeit und einer stärkeren Gewissheit, dass sie einen echten Geschäftswert bieten.

Organizations verfügen häufig über vorhandene DevOps Tools und Datenspeicherlösungen, bevor sie ihre MLOps Reise beginnen. Dieses Muster zeigt, wie Sie die Stärken von Microsoft Azure und AWS nutzen können. Es hilft Ihnen, Azure DevOps in Amazon SageMaker AI zu integrieren, um einen MLOps Workflow zu erstellen.

Die Lösung vereinfacht die Arbeit zwischen Azure und AWS. Sie können Azure für die Entwicklung und AWS für maschinelles Lernen verwenden. Es fördert einen effektiven Prozess zur Erstellung von Modellen für maschinelles Lernen von Anfang bis Ende, einschließlich Datenverarbeitung, Schulung und Bereitstellung auf AWS. Aus Effizienzgründen verwalten Sie diese Prozesse über DevOps Azure-Pipelines. Die Lösung eignet sich für grundlegende Modelloperationen (FMOps) und umfangreiche Sprachmodelloperationen (LLMOps) in generativer KI, was Feinabstimmung, Vektordatenbanken und schnelle Verwaltung umfasst.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Azure-Abonnement — Zugriff auf Azure-Dienste wie Azure DevOps für die Einrichtung der CI/CD-Pipelines (Continuous Integration and Continuous Deployment).
- Aktives AWS-Konto — Berechtigungen zur Verwendung der in diesem Muster AWS-Services verwendeten.
- Daten — Zugriff auf historische Daten zum Trainieren des Modells für maschinelles Lernen.

- Vertrautheit mit ML-Konzepten — Verständnis von Python, Jupyter Notebooks und Modellentwicklung für maschinelles Lernen.
- Sicherheitskonfiguration — Richtige Konfiguration von Rollen, Richtlinien und Berechtigungen in Azure und AWS, um eine sichere Datenübertragung und einen sicheren Datenzugriff zu gewährleisten.
- (Optional) Vektordatenbank — Wenn Sie einen RAG-Ansatz (Retrieval Augmented Generation) und einen Drittanbieter-Service für die Vektordatenbank verwenden, benötigen Sie Zugriff auf die externe Vektordatenbank.

Einschränkungen

- In dieser Anleitung wird nicht auf sichere cloudübergreifende Datenübertragungen eingegangen. Weitere Informationen zu cloudübergreifenden Datenübertragungen finden Sie unter AWS Lösungen für Hybrid- und Multicloud.
- Multicloud-Lösungen können die Latenz für Datenverarbeitung und Modellinferenz in Echtzeit erhöhen.
- Diese Anleitung bietet ein Beispiel für eine Architektur mit mehreren MLOps Konten. Je nach Ihrem maschinellen Lernen und Ihrer AWS Strategie sind Anpassungen erforderlich.
- Diese Anleitung beschreibt nicht die Nutzung anderer KI/ML-Dienste als Amazon SageMaker AI.
- Einige AWS-Services sind nicht in allen verfügbar. AWS-Regionen Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie auf der Seite Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Architektur

Zielarchitektur

Die Zielarchitektur integriert Azure DevOps mit Amazon SageMaker AI und schafft so einen cloudübergreifenden ML-Workflow. Es verwendet Azure für CI/CD processes and SageMaker AI for ML model training and deployment. It outlines the process of obtaining data (from sources such as Amazon S3, Snowflake, and Azure Data Lake) through model building and deployment. Key components include CI/CD Pipelines für Modellerstellung und -bereitstellung, Datenvorbereitung, Infrastrukturmanagement und Amazon SageMaker AI für das Training und die Feinabstimmung, Evaluierung und Bereitstellung von ML-Modellen. Diese Architektur wurde entwickelt, um effiziente, automatisierte und skalierbare ML-Workflows auf Cloud-Plattformen bereitzustellen.

Die Architektur besteht aus den folgenden Komponenten:

1. Datenwissenschaftler führen im Entwicklungskonto ML-Experimente durch, um mithilfe verschiedener Datenquellen verschiedene Ansätze für ML-Anwendungsfälle zu untersuchen. Datenwissenschaftler führen Unit-Tests und Versuche durch und können Amazon SageMaker AI verwenden, um ihre Experimente nachzuverfolgen MLflow. Bei der generativen KI-Modellentwicklung optimieren Datenwissenschaftler grundlegende Modelle vom Amazon SageMaker AI JumpStart Model Hub aus. Nach der Modellevaluierung übertragen Datenwissenschaftler den Code und führen ihn in das Model Build-Repository ein, das auf Azure DevOps gehostet wird. Dieses Repository enthält Code für eine mehrstufige Modellerstellungspipeline.
2. In Azure DevOps kann die Model Build-Pipeline, die kontinuierliche Integration (CI) ermöglicht, bei der Codezusammenführung mit dem Hauptzweig automatisch oder manuell aktiviert werden. Im Automation-Konto aktiviert dies die SageMaker KI-Pipeline für die Datenvorverarbeitung, das Training und die Feinabstimmung von Modellen, die Modellevaluierung und die bedingte Modellregistrierung auf der Grundlage der Genauigkeit.
3. Das Automation-Konto ist ein zentrales Konto für alle ML-Plattformen, das ML-Umgebungen (Amazon ECR), Modelle (Amazon S3), Modellmetadaten (SageMaker AI Model Registry), Funktionen (SageMaker AI Feature Store), automatisierte Pipelines (SageMaker AI Pipelines) und ML-Log-Insights () hostet. CloudWatch Für einen generativen KI-Workload benötigen Sie möglicherweise zusätzliche Evaluierungen für Eingabeaufforderungen in den nachgelagerten Anwendungen. Eine Anwendung zur Verwaltung von Eingabeaufforderungen hilft dabei, den Prozess zu rationalisieren und zu automatisieren. Dieses Konto ermöglicht die Wiederverwendbarkeit von ML-Assets und setzt bewährte Verfahren durch und beschleunigt die Bereitstellung von ML-Anwendungsfällen.
4. Die neueste Modellversion wird zur Überprüfung in das SageMaker AI Model Registry aufgenommen. Es verfolgt Modellversionen und entsprechende Artefakte (Herkunft und Metadaten). Es verwaltet auch den Status des Modells (genehmigt, abgelehnt oder ausstehend) und verwaltet die Version für die nachgelagerte Bereitstellung.
5. Nachdem ein in Model Registry trainiertes Modell über die Studio-Oberfläche oder einen API-Aufruf genehmigt wurde, kann eine Veranstaltung an Amazon gesendet werden EventBridge. EventBridge startet die Model Deploy-Pipeline auf Azure DevOps.
6. Die Model Deploy-Pipeline, die eine kontinuierliche Bereitstellung (CD) ermöglicht, checkt die Quelle aus dem Model Deploy-Repository aus. Der Quellcode enthält Code, die Konfiguration für

die Modellbereitstellung und Testskripte für Qualitätsbenchmarks. Die Model Deploy-Pipeline kann auf Ihren Inferenztyp zugeschnitten werden.

7. Nach den Qualitätskontrollen stellt die Model Deploy-Pipeline das Modell für das Staging-Konto bereit. Das Staging-Konto ist eine Kopie des Produktionskontos und wird für Integrationstests und Evaluierungen verwendet. Bei einer Batch-Transformation kann die Model Deploy-Pipeline den Batch-Inferenzprozess automatisch aktualisieren, sodass die neueste genehmigte Modellversion verwendet wird. Für eine serverlose oder asynchrone Inferenz in Echtzeit richtet sie den jeweiligen Modellendpunkt ein oder aktualisiert ihn.
8. Nach erfolgreichen Tests im Staging-Konto kann ein Modell durch manuelle Genehmigung über die Model Deploy-Pipeline für das Produktionskonto bereitgestellt werden. Diese Pipeline stellt einen Produktionsendpunkt im Schritt „Bereitstellen bis zur Produktion“ bereit, einschließlich der Modellüberwachung und eines Mechanismus zur Datenrückkopplung.
9. Sobald das Modell in Produktion ist, können Sie Tools wie SageMaker AI Model Monitor und SageMaker AI Clarify verwenden, um Abweichungen zu erkennen, Abweichungen zu erkennen und die Leistung des Modells kontinuierlich zu überwachen.

Automatisierung und Skalierung

Verwenden Sie Infrastructure as Code (IaC) für die automatische Bereitstellung auf mehreren Konten und Umgebungen. Durch die Automatisierung des Prozesses der Einrichtung eines MLOps Workflows ist es möglich, die Umgebungen zu trennen, die von ML-Teams verwendet werden, die an verschiedenen Projekten arbeiten. AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen zu modellieren, bereitzustellen und zu verwalten, indem Infrastruktur als Code behandelt wird.

Tools

AWS-Services

- Amazon SageMaker AI ist ein verwalteter ML-Service, der Ihnen hilft, ML-Modelle zu erstellen und zu trainieren und sie dann in einer produktionsbereiten gehosteten Umgebung bereitzustellen.
- AWS Glueist ein vollständig verwalteter Service zum Extrahieren, Transformieren und Laden (ETL). Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt. In diesem Muster wird Amazon S3 für die Datenspeicherung verwendet und in SageMaker KI für Modelltraining und Modellobjekte integriert.

- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen. In diesem Muster wird Lambda für Datenvorverarbeitungs- und Nachverarbeitungsaufgaben verwendet.
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist. In diesem Muster werden Docker-Container gespeichert, die SageMaker KI als Schulungs- und Bereitstellungsumgebungen verwendet.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. In diesem Muster EventBridge orchestriert er ereignisgesteuerte oder zeitbasierte Workflows, die eine automatische Neuschulung oder Bereitstellung des Modells einleiten.
- Amazon API Gateway unterstützt Sie bei der Erstellung, Veröffentlichung, Wartung, Überwachung und Sicherung von REST, HTTP und WebSocket APIs in jeder Größenordnung. In diesem Muster wird es verwendet, um einen nach außen gerichteten, zentralen Einstiegspunkt für SageMaker KI-Endpunkte zu schaffen.
- Für RAG-Anwendungen können Sie z. AWS-Services B. Amazon OpenSearch Service und Amazon RDS for PostgreSQL verwenden, um die Vektor-Einbettungen zu speichern, die das LLM mit Ihren internen Daten versorgen.

Andere Tools

- Azure DevOps unterstützt Sie bei der Verwaltung von CI/CD-Pipelines und erleichtert das Erstellen, Testen und Bereitstellen von Code.
- Azure Data Lake Storage oder Snowflake sind mögliche Quellen von Drittanbietern für Trainingsdaten für ML-Modelle.
- Pinecone, Milvus oder ChromaDB sind mögliche Vektordatenbanken von Drittanbietern zum Speichern von Vektoreinbettungen.

Bewährte Methoden

Bevor Sie eine Komponente dieses Multicloud-Workflows implementieren, führen Sie die folgenden Aktivitäten durch: MLOps

- Definieren und verstehen Sie den Workflow für maschinelles Lernen und die Tools, die zu seiner Unterstützung erforderlich sind. Verschiedene Anwendungsfälle erfordern unterschiedliche

Workflows und Komponenten. Beispielsweise kann ein feature store für die Wiederverwendung von Funktionen und die Inferenz mit niedriger Latenz in einem Personalisierungs-Anwendungsfall erforderlich sein, für andere Anwendungsfälle jedoch möglicherweise nicht. Um die Architektur erfolgreich anpassen zu können, ist es erforderlich, den Ziel-Workflow, die Anforderungen an den Anwendungsfall und die bevorzugten Methoden der Zusammenarbeit des Data-Science-Teams zu verstehen.

- Sorgen Sie für eine klare Trennung der Zuständigkeiten für die einzelnen Komponenten der Architektur. Die Verteilung des Datenspeichers auf Azure Data Lake Storage, Snowflake und Amazon S3 kann die Komplexität und die Kosten erhöhen. Wählen Sie nach Möglichkeit einen konsistenten Speichermechanismus. Vermeiden Sie auch die Verwendung einer Kombination aus Azure- und DevOps AWS-Diensten oder einer Kombination aus Azure- und AWS ML-Diensten.
- Wählen Sie ein oder mehrere vorhandene Modelle und Datensätze aus, um den MLOps Workflow zu end-to-end testen. Die Testartefakte sollten reale Anwendungsfälle widerspiegeln, die die Data-Science-Teams entwickeln, wenn die Plattform in Produktion geht.

Epen

Entwerfen Sie Ihre Architektur MLOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Datenquellen.	Dokumentieren Sie auf der Grundlage aktueller und future Anwendungsfälle, verfügbarer Datenquellen und Datentypen (z. B. vertrauli cher Daten) die Datenquellen, die in die MLOps Plattform integriert werden müssen. Daten können in Amazon S3, Azure Data Lake Storage, Snowflake oder anderen Quellen gespeichert werden. Bei generativen KI-Worklo ads können die Daten auch eine Wissensdatenbank	Dateningenieur, Datenwiss enschaftler, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	enthalten, die die generiert e Antwort begründet. Diese Daten werden als Vektorein bettungen in Vektordat enbanken gespeichert. Erstellen Sie einen Plan zur Integration dieser Quellen in Ihre Plattform und zur Sicherung des Zugriffs auf die richtigen Ressourcen.	
Wählen Sie die entsprech enden Dienste aus.	Passen Sie die Architektur an, indem Sie Dienste auf der Grundlage des gewünscht en Workflows des Data-Scie nce-Teams, der entsprech enden Datenquellen und der vorhandenen Cloud-Architektur hinzufügen oder entfernen. Beispielsweise können Dateningenieure und Datenwissenschaftl er Datenvorverarbeitung und Feature-Engineering in SageMaker KI oder Amazon EMR durchführen. AWS Glue Es ist unwahrscheinlich, dass alle drei Dienste erforderlich wären.	AWS-Administrator, Dateninge nieur, Datenwissenschaftler, ML-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie die Sicherheitsanforderungen.	Sammeln und dokumentieren Sie die Sicherheitsanforderungen. Dies beinhaltet die Festlegung von: • Welche Teams oder Ingenieure können auf bestimmte Datenquellen zugreifen • Welche Teams oder Ingenieure können auf vortrainierte Basismodelle zugreifen • Ob Teams auf den Code und die Modelle anderer Teams zugreifen dürfen • Welche Berechtigungen (falls vorhanden) sollten Teammitglieder für Konten haben, die keine Entwickler sind • Welche Sicherheitsmaßnahmen müssen für die cloudübergreifende Datenübertragung implementiert werden Weitere Informationen zur Sicherung generativer KI-Workloads finden Sie unter Absicherung generativer KI: Eine Einführung in die Generative AI	AWS-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Security Scoping Matrix (AWS Blogbeitrag).	

Einrichten AWS Organizations

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Einrichten AWS Organizations.	AWS Organizations Auf der Wurzel einrichten AWS-Konto . Auf diese Weise können Sie die nachfolgenden Konten verwalten, die Sie im Rahmen einer MLOps Strategie für mehrere Konten erstellen. Weitere Informationen finden Sie in der AWS Organizations -Dokumentation.	AWS-Administrator

Richten Sie die Entwicklungsumgebung und die Versionierung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein AWS Entwicklungskonto.	Erstellen Sie ein AWS-Konto , in dem Dateningenieure und Datenwissenschaftler die Erlaubnis haben, zu experimentieren und ML-Modelle zu erstellen . Anweisungen finden Sie in der AWS Organizations Dokumentation unter Erstellen eines Mitgliedskontos in Ihrer Organisation.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Model Build-Repository.	Erstellen Sie ein Git-Repository in Azure, in dem Datenwissenschaftler ihren Modellerstellungs- und Bereitstellungscode nach Abschluss der Experimentierphase pushen können. Anweisungen finden Sie in der DevOps Azure-Dokumentation unter Ein Git-Repository einrichten.	DevOps Ingenieur, ML-Ingenieur
Erstellen Sie ein Model Deploy-Repository.	Erstellen Sie ein Git-Repository in Azure, in dem Standardbereitstellungscode und Vorlagen gespeichert werden. Es sollte Code für jede Bereitstellungsoption enthalten, die die Organisation verwendet, wie in der Entwurfsphase festgelegt. Es sollte beispielsweise Echtzeit-Endpunkte, asynchrone Endpunkte, serverlose Inferenz oder Batch-Transformationen enthalten. Anweisungen finden Sie in der DevOps Azure-Dokumentation unter Ein Git-Repository einrichten.	DevOps Ingenieur, ML-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon-EC R-Repository.	Richten Sie ein Amazon ECR-Repository ein, das die genehmigten ML-Umgebu ngen als Docker-Images speichert. Ermöglichen Sie Datenwissenschaftlern und ML-Ingenieuren, neue Umgebungen zu definieren. Anweisungen finden Sie in der Amazon ECR-Dokumentation unter Erstellen eines privaten Repositorys.	ML-Ingenieur
Richten Sie SageMaker AI Studio ein.	Richten Sie SageMaker AI Studio auf dem Entwicklu ngskonto gemäß den zuvor definierten Sicherheitsanforde rungen, den bevorzugten Data-Science-Tools (z. B. MLflow) und der bevorzugt en integrierten Entwicklu ngsumgebung (IDE) ein. Verwenden Sie Lebenszyk luskonfigurationen, um die Installation wichtiger Funktione n zu automatisieren und eine einheitliche Entwicklu ngsumgebung für Datenwiss enschaftler zu schaffen. Weitere Informationen finden Sie in der SageMaker KI-Dokumentation unter Amazon AI Studio und MLflow Tracking-Server. SageMaker	Datenwissenschaftler, ML-Ingenieur, Prompt-Ingenieur

Integrieren Sie CI/CD-Pipelines

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Automation-Konto.	Erstellen Sie einen AWS-Konto Ort, an dem automatisierte Pipelines und Jobs ausgeführt werden. Sie können Data-Science-Teams Lesezugriff auf dieses Konto gewähren. Anweisungen finden Sie in der AWS Organizations Dokumentation unter Erstellen eines Mitgliedskontos in Ihrer Organisation.	AWS-Administrator
Richten Sie eine Modellregistrierung ein.	Richten Sie SageMaker AI Model Registry im Automation-Konto ein. Dieses Register speichert die Metadaten für ML-Modelle und hilft bestimmten Datenwissenschaftlern oder Teamleitern, Modelle zu genehmigen oder abzulehnen. Weitere Informationen finden Sie in der SageMaker KI-Dokumentation unter Registrieren und Bereitstellen von Modellen mit Model Registry.	ML-Ingenieur
Erstellen Sie eine Model Build-Pipeline.	Erstellen Sie eine CI/CD-Pipeline in Azure, die manuell oder automatisch gestartet wird, wenn Code in das Model Build-Repository übertragen wird. Die Pipeline sollte	DevOps Ingenieur, ML-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den Quellcode auscheckeⁿ und eine SageMaker KI-Pipeline im Automation-Konto erstellen oder aktualisieren. Die Pipeline sollte der Modellregistrierung ein neues Modell hinzufügen. Weitere Informationen zum Erstellen einer Pipeline finden Sie in der Azure Pipelines-Dokumentation.	

Erstellen Sie den Deployment-Stack

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie AWS Staging- und Deployment-Konten.	Erstellen Sie AWS-Konten für die Bereitstellung und Bereitstellung von ML-Modellen. Diese Konten sollten identisch sein, um genaue Tests der Modelle im Staging-Stadium zu ermöglichen, bevor sie in die Produktion übergehen. Sie können Data-Science-Teams Lesezugriff auf das Staging-Konto gewähren. Anweisungen finden Sie in der AWS Organizations Dokumentation unter Erstellen eines Mitgliedskontos in Ihrer Organisation.	AWS-Administrator
Richten Sie S3-Buckets für die Modellüberwachung ein.	Führen Sie diesen Schritt aus, wenn Sie die Modellübe	ML-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	rwachung für die bereitges tellten Modelle aktiviere n möchten, die von der Model Deploy-Pipeline erstellt wurden. Erstellen Sie Amazon S3 S3-Buckets zum Speichern der Eingabe- und Ausgabedaten. Weitere Informationen zum Erstellen von S3-Buckets finden Sie unter Bucket erstellen in der Amazon S3 S3-Dokume ntation. Richten Sie kontoüber greifende Berechtigungen ein, sodass die automatis ierten Modellüberwachungs aufträge im Automation-Konto ausgeführt werden. Weitere Informationen finden Sie in der SageMaker KI-Dokumentation unter Überwachen der Daten- und Modellqualität.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Model Deploy-Pipeline.	Erstellen Sie eine CI/CD-Pipeline in Azure, die startet, wenn ein Modell in der Modellregistrierung genehmigt wird. Die Pipeline sollte den Quellcode und das Modellartefakt auschecken, die Infrastrukturvorlagen für die Bereitstellung des Modells in den Staging- und Produktionskonten erstellen, das Modell im Staging-Konto bereitstellen, automatisierte Tests ausführen, auf die manuelle Genehmigung warten und das genehmigte Modell im Produktionskonto bereitstellen. Weitere Informationen zum Erstellen einer Pipeline finden Sie in der Dokumentation zu Azure Pipelines.	DevOps Ingenieur, ML-Ingenieur

(Optional) Automatisieren Sie die Infrastruktur der ML-Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen AWS CDK oder CloudFormation Vorlagen.	Definieren Sie AWS Cloud Development Kit (AWS CDK) AWS CloudFormation unsere Vorlagen für alle Umgebungen, die automatisch bereitgestellt werden müssen. Dies kann die Entwicklungsumgebung, die Automatisierungsum	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	gebung sowie die Staging- und Bereitstellungsumgebungen umfassen. Weitere Informationen finden Sie in der CloudFormationDokumentation AWS CDKund.	
Erstellen Sie eine Infrastruktur-Pipeline.	Erstellen Sie in Azure eine CI/CD-Pipeline für die Bereitstellung der Infrastruktur. Ein Administrator kann diese Pipeline initiieren, um neue Umgebungen zu erstellen AWS-Konten und einzurichten, die das ML-Team benötigt.	DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Unzureichende Überwachung und Drifterkennung — Eine unzureichende Überwachung kann dazu führen, dass Probleme mit der Modellleistung oder Datenabweichungen nicht erkannt werden.	Stärken Sie die Monitoring-Frameworks mit Tools wie Amazon CloudWatch, SageMaker AI Model Monitor und SageMaker AI Clarify. Konfigurieren Sie Warnmeldungen für sofortige Maßnahmen bei erkannten Problemen.
Fehler beim Auslösen der CI-Pipeline — Die CI-Pipeline in Azure wird bei der Codezusammenführung aufgrund einer Fehlkonfiguration DevOps möglicherweise nicht ausgelöst.	Überprüfen Sie die DevOps Azure-Projekteinstellungen, um sicherzustellen, dass die Webhooks ordnungsgemäß eingerichtet sind und auf die richtigen SageMaker KI-Endpunkte verweisen.
Verwaltung — Das zentrale Automation-Konto setzt möglicherweise keine Best Practices auf	Prüfen Sie die Automation-Kontoeinstellungen und stellen Sie sicher, dass alle ML-Umgebu

Problem	Lösung
allen ML-Plattformen durch, was zu inkonsist enten Workflows führt.	ngen und -Modelle den vordefinierten Best Practices und Richtlinien entsprechen.
Verzögerungen bei der Genehmigung durch die Modellregistrierung — Dies passiert, wenn es zu Verzögerungen bei der Prüfung und Genehmigung des Modells kommt, entweder weil sich die Mitarbeiter Zeit nehmen, es zu überprüfen, oder weil technische Probleme auftreten.	Implementieren Sie ein Benachrichtigungss ystem, um die Beteiligten über Modelle zu informieren, deren Genehmigung noch aussteht, und um den Überprüfungsprozess zu rationalisieren.
Fehler bei der Modellbereitstellung — Ereigniss e, die an den Start von Pipelines zur Modellber eitstellung gesendet werden, können fehlschla gen und zu Verzögerungen bei der Bereitste llung führen.	Vergewissern Sie sich, dass Amazon EventBrid ge über die richtigen Berechtigungen und Ereignismuster verfügt, um DevOps Azure-Pip elines erfolgreich aufzurufen.
Engpässe bei der Produktionsbereitstellung — Manuelle Genehmigungsprozesse können zu Engpässen führen und die Produktionsbereits tellung von Modellen verzögern.	Optimieren Sie den Genehmigungsablauf innerhalb der Pipeline für die Modellbereitstellu ng und fördern Sie so zeitnahe Überprüfungen und klare Kommunikationskanäle.

Zugehörige Ressourcen

AWS Dokumentation

- Dokumentation zu Amazon SageMaker AI
- Linse für Machine Learning (AWS Well Architected Framework)
- Erfolgreiche Planung MLOps (AWS präskriptive Leitlinien)

Andere Ressourcen AWS

- MLOps Grundlagenplan für Unternehmen mit Amazon SageMaker AI (AWS Blogbeitrag)
- AWS Summit ANZ 2022 — End-to-end MLOps für Architekten (YouTube Video)

- FMOps/LLMOps: Operationalisieren Sie generative KI und Unterschiede mit MLOps (AWS Blogbeitrag)
- Operationalisieren Sie die LLM-Bewertung im großen Maßstab mithilfe von Amazon SageMaker AI Clarify und MLOps Services (AWS Blogbeitrag)
- Die Rolle von Vektordatenbanken in generativen KI-Anwendungen (AWS Blogbeitrag)

Azure-Dokumentation

- DevOps Azure-Dokumentation
- Dokumentation zu Azure Pipelines

Konfigurieren Sie die Protokollierung von Modellaufrufen in Amazon Bedrock mithilfe von AWS CloudFormation

Erstellt von Vikramaditya Bhatnagar (AWS)

Übersicht

Sie können Amazon Bedrock so konfigurieren, dass es Aufrufprotokolle, Modelleingabedaten und Modellausgabedaten für alle Modellaufrufe in Ihrem erfasst. AWS-Konto Dies ist eine bewährte Methode für die Erstellung robuster generativer KI-Anwendungen mit Amazon Bedrock. Sie können Modellaufruf-Logs in einer Amazon CloudWatch Logs-Protokollgruppe, in einem Amazon Simple Storage Service (Amazon S3) -Bucket oder in beiden speichern. Wenn Sie Protokolldaten in CloudWatch Logs haben, können Sie benutzerdefinierte Metrikfilter, Alarme und Dashboards erstellen. Amazon S3 ist ideal für die Replikation von Daten innerhalb AWS-Regionen oder für die Langzeitspeicherung, je nach den Richtlinien Ihres Unternehmens.

Dieses Muster bietet eine AWS CloudFormation Beispielvorlage, die einen Infrastructure-as-Code (IaC) -Ansatz verwendet, um die Protokollierung von Modellaufrufen für Amazon Bedrock zu konfigurieren. Die Vorlage konfiguriert den Protokollspeicher sowohl in CloudWatch Logs als auch in Amazon S3.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Die folgenden Berechtigungen:
  - Berechtigungen zum Erstellen von CloudFormation Stacks
  - Berechtigungen für den Zugriff auf Amazon Bedrock
  - Berechtigungen zum Erstellen und Zugreifen auf Amazon S3 S3-Buckets
  - Berechtigungen zum Erstellen von und Zugreifen auf CloudWatch Logs-Protokollgruppen
  - Berechtigungen zum Erstellen und Zugreifen auf AWS Lambda Funktionen
  - Berechtigungen zum Erstellen von und Zugreifen auf AWS Key Management Service (AWS KMS) -Schlüssel

Einschränkungen

Dieses Muster protokolliert Modellaufrufe sowohl für CloudWatch Logs als auch für Amazon S3. Es unterstützt nicht, nur einen dieser beiden Dienste auszuwählen.

Architektur

Zielarchitektur

Die CloudFormation Vorlage stellt die folgenden Ressourcen in Ihrem Ziel bereit AWS-Konto:

- Eine CloudWatch Logs-Protokollgruppe zum Speichern von Modellaufruf-Logs
- Ein Amazon S3 S3-Bucket zum Speichern von Modellaufrufprotokollen und einer entsprechenden Bucket-Richtlinie
- Ein Amazon S3 S3-Bucket zum Speichern von serverseitigen Zugriffsprotokollen und einer entsprechenden Bucket-Richtlinie
- Eine AWS Lambda Funktion, die die Protokollierungseinstellungen in Amazon Bedrock konfiguriert
- Ein AWS KMS key und ein entsprechender Schlüsselalias
- Eine AWS Identity and Access Management (IAM) -Servicerolle für Amazon Bedrock

Das folgende Diagramm zeigt, wie Aufrufprotokolle gespeichert werden, nachdem Sie den mit diesem Muster verknüpften CloudFormation Stack bereitgestellt haben. Amazon Bedrock veröffentlicht Protokolldaten, wenn das Foundation-Modell Text, ein Bild, ein Video oder eingebettete Daten liefert. Wie im Diagramm dargestellt, sind die Amazon S3 S3-Buckets und die CloudWatch Logs-Protokollgruppe mit einem AWS KMS key verschlüsselt.

Das Diagramm zeigt den folgenden Workflow:

1. Ein Benutzer sendet eine Anfrage an ein Foundation-Modell in Amazon Bedrock.
2. Amazon Bedrock übernimmt die IAM-Servicerolle.
3. Amazon Bedrock generiert Protokolldaten und speichert sie in einer CloudWatch Logs-Protokollgruppe und in einem Amazon S3 S3-Bucket.
4. Wenn ein Benutzer Dateien im Amazon S3 S3-Bucket liest, hochlädt oder löscht, der die Modellaufrufprotokolle enthält, werden diese Aktivitäten in einem anderen Amazon S3 S3-Bucket für serverseitige Zugriffsprotokolle protokolliert.

Automatisierung und Skalierung

Um diese Lösung zu skalieren, können Sie die CloudFormation Vorlage als Stack-Set für mehrere AWS-Regionen und bereitstellen AWS-Konten. Weitere Informationen finden Sie in der CloudFormation Dokumentation unter Konten- und regionsübergreifende Verwaltung von Stacks. StackSets

Tools

AWS-Services

- Amazon Bedrock ist ein vollständig verwalteter Service, der Ihnen leistungsstarke Basismodelle (FMs) von führenden KI-Unternehmen und Amazon über eine einheitliche API zur Verfügung stellt.
- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten AWS-Konten Lebenszyklus über und zu verwalten. AWS-Regionen
- Amazon CloudWatch Logs hilft Ihnen dabei, die Protokolle all Ihrer Systeme und Anwendungen zu zentralisieren, AWS-Services sodass Sie sie überwachen und sicher archivieren können.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Key Management Service (AWS KMS) hilft Ihnen dabei, kryptografische Schlüssel zu erstellen und zu kontrollieren, um Ihre Daten zu schützen.
- Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice, der branchenführende Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet.

Andere Tools

- Git ist ein verteiltes Open-Source-Versionskontrollsystem.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub enable-bedrock-logging-using-cloudformation verfügbar.

Epen

Erstelle den Stapel CloudFormation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die CloudFormation Vorlage herunter.	Laden Sie die CloudFormation Vorlage aus dem GitHub Repository herunter.	Cloud-Architekt
Stellen Sie die Vorlage bereit.	Erstellen Sie einen Stack in Ihrem Zielkonto und Ihrer Region. Geben Sie im Abschnitt Parameter Werte für die Parameter an, die in der Vorlage definiert sind. Anweisungen finden Sie in der CloudFormation Dokumentation unter Einen Stack erstellen.	Cloud-Architekt

Testen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie den Modellzugriff.	Fügen Sie in Amazon Bedrock Zugriff auf das Foundation-Modell hinzu. Anweisungen finden Sie in der Amazon Bedrock-Dokumentation unter Zugriff auf Amazon Bedrock Foundation-Modelle hinzufügen oder entfernen.	Cloud-Architekt
Führen Sie eine Beispielaufforderung aus.	Führen Sie in Amazon Bedrock Playgrounds eine Beispielaufforderung aus.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anweisungen finden Sie in der Amazon Bedrock-Dokumentation unter Generieren von Antworten in der Konsole mithilfe von Playgrounds.	
Überprüfen Sie die Protokollierungskonfiguration.	1. Melden Sie sich bei der Amazon Bedrock-Konsole an. 2. Wählen Sie in der Navigationsleiste den Ort aus, AWS-Region an dem Sie den CloudFormation Stack bereitgestellt haben. 3. Wählen Sie im linken Navigationsbereich unter Bedrock-Konfigurationen die Option Einstellungen aus. 4. Überprüfen Sie Folgendes: • Die Protokollierung von Modellaufrufen ist aktiviert. • Alle Datentypen sind ausgewählt. • Für die Protokollierung von Zielen ist sowohl S3 als auch CloudWatch Logs ausgewählt.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Amazon S3 S3-Bucket.	1. Wählen Sie im Abschnitt S3-Konfigurationen die Option Browse S3 aus. Dadurch wird der Ziel-Bucket in der Amazon S3 S3-Konsole geöffnet. 2. Vergewissern Sie sich, dass für die Beispielaufforderung, die Sie zuvor ausgeführt haben, Protokolldaten vorhanden sind.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Protokoll gruppe.	1. Gehen Sie zurück zur Seite Einstellungen in der Amazon Bedrock-Konsole. 2. Überprüfen Sie im Abschnitt CloudWatch Protokoll konfigurationen die Einstellu ngen für die Protokoll gruppe CloudWatch Logs. Notieren Sie sich den Namen der Protokollgruppe. 3. Öffnen Sie die CloudWatch -Konsole. 4. Wählen Sie im Navigatio nsbereich Protokolle die Option Protokollgruppen. 5. Wählen Sie den Namen der Protokollgruppe, in der Amazon Bedrock Protokoll daten veröffentlicht. 6. Vergewissern Sie sich, dass die Protokolldaten für die Beispielaufforderung, die Sie zuvor ausgeführt haben, vorhanden sind.	Cloud-Architekt

Zugehörige Ressourcen

AWS Dokumentation

- Zugreifen auf einen Amazon S3 S3-Bucket (Amazon S3 S3-Dokumentation)
- Stacks erstellen und verwalten (CloudFormation Dokumentation)
- Modellaufruf überwachen (Amazon Bedrock-Dokumentation)
- Arbeiten mit Protokollgruppen und Protokollströmen (CloudWatch Logs-Dokumentation)

AWS Blog-Beiträge

- Überwachung generativer KI-Anwendungen mithilfe der Amazon Bedrock- und Amazon-Integration CloudWatch
- Bewährte Methoden für die Erstellung robuster generativer KI-Anwendungen mit Amazon Bedrock Agents — Teil 1
- Bewährte Methoden für die Erstellung robuster generativer KI-Anwendungen mit Amazon Bedrock Agents — Teil 2

Erstellen Sie ein benutzerdefiniertes Docker-Container-Image für SageMaker und verwenden Sie es für Modelltrainings in AWS Step Functions

Erstellt von Julia Bluszcz (AWS), Neha Sharma (AWS), Aubrey Oosthuizen (AWS), Mohan Gowda Purushothama (AWS) und Mateusz Zaremba (AWS)

Übersicht

Dieses Muster zeigt, wie Sie ein Docker-Container-Image für Amazon erstellen SageMaker und es für ein Trainingsmodell in AWS Step Functions verwenden. Indem Sie benutzerdefinierte Algorithmen in einem Container verpacken, können Sie fast jeden Code in der SageMaker Umgebung ausführen, unabhängig von Programmiersprache, Framework oder Abhängigkeiten.

In dem bereitgestellten SageMaker Beispiel-Notizbuch wird das benutzerdefinierte Docker-Container-Image in Amazon Elastic Container Registry (Amazon ECR) gespeichert. Step Functions verwendet dann den in Amazon ECR gespeicherten Container, um ein Python-Verarbeitungsskript für SageMaker auszuführen. Anschließend exportiert der Container das Modell nach Amazon Simple Storage Service (Amazon S3).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine AWS Identity and Access Management (IAM) -Rolle für SageMaker mit Amazon S3 S3-Berechtigungen
- Eine IAM-Rolle für Step Functions
- Vertrautheit mit Python
- Vertrautheit mit dem Amazon SageMaker Python SDK
- Vertrautheit mit der AWS-Befehlszeilenschnittstelle (AWS CLI)
- Vertrautheit mit dem AWS-SDK SDK for Python (Boto3)
- Vertrautheit mit Amazon ECR
- Vertrautheit mit Docker

Produktversionen

- AWS Step Functions SDK für Datenwissenschaft, Version 2.3.0
- Amazon SageMaker Python SDK versie 2.78.0

Architektur

Das folgende Diagramm zeigt einen Beispiel-Workflow für die Erstellung eines Docker-Container-Images für und SageMaker dessen anschließende Verwendung für ein Trainingsmodell in Step Functions:

Das Diagramm zeigt den folgenden Workflow:

1. Ein Datenwissenschaftler oder DevOps Ingenieur verwendet ein SageMaker Amazon-Notizbuch, um ein benutzerdefiniertes Docker-Container-Image zu erstellen.
2. Ein Datenwissenschaftler oder DevOps Ingenieur speichert das Docker-Container-Image in einem privaten Amazon ECR-Repository, das sich in einer privaten Registrierung befindet.
3. Ein Datenwissenschaftler oder DevOps Ingenieur verwendet den Docker-Container, um einen SageMaker Python-Verarbeitungsjob in einem Step Functions Functions-Workflow auszuführen.

Automatisierung und Skalierung

Das SageMaker Beispiel-Notizbuch in diesem Muster verwendet einen `ml.m5.xlarge` Notebook-Instanztyp. Sie können den Instanztyp an Ihren Anwendungsfall anpassen. Weitere Informationen zu SageMaker Notebook-Instance-Typen finden Sie unter SageMaker Amazon-Preise.

Tools

- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon SageMaker ist ein verwalteter Service für maschinelles Lernen (ML), der Ihnen hilft, ML-Modelle zu erstellen und zu trainieren und sie dann in einer produktionsbereiten gehosteten Umgebung bereitzustellen.
- Das Amazon SageMaker Python SDK ist eine Open-Source-Bibliothek für das Training und die Bereitstellung von Modellen für maschinelles Lernen. SageMaker

- AWS Step Functions ist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen.
- Das AWS Step Functions Data Science Python SDK ist eine Open-Source-Bibliothek, mit der Sie Step Functions Functions-Workflows erstellen können, die Modelle für maschinelles Lernen verarbeiten und veröffentlichen.

Epen

Erstellen Sie ein benutzerdefiniertes Docker-Container-Image und speichern Sie es in Amazon ECR

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Amazon ECR ein und erstellen Sie eine neue private Registrierung.	Falls Sie dies noch nicht getan haben, richten Sie Amazon ECR ein, indem Sie den Anweisungen unter Einrichtung mit Amazon ECR im Amazon ECR-Benut zerhandbuch folgen. Jedes AWS-Konto ist mit einer standardmäßigen privaten Amazon ECR-Registrierung ausgestattet.	DevOps Ingenieur
Erstellen Sie ein privates Amazon ECR-Repository.	Folgen Sie den Anweisungen unter Erstellen eines privaten Repositorys im Amazon ECR-Benutzerhandbuch. **Note** In dem Repositor y, das Sie erstellen , speichern Sie Ihre benutzerdefinierten	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Docker-Container-Images.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie ein Dockerfile, das die für die Ausführung Ihres SageMaker Verarbeitungsjobs erforderlichen Spezifikationen enthält.	Erstellen Sie ein Dockerfile, das die für die Ausführung Ihres SageMaker Verarbeitungsjobs erforderlichen Spezifikationen enthält, indem Sie ein Dockerfile konfigurieren. Eine Anleitung finden Sie im Amazon SageMaker Developer Guide unter Anpassung Ihres eigenen Trainingscontainers.
	
	Weitere Informationen zu Dockerfiles finden Sie in der Dockerfile-Referenz in der Docker-Dokumentation.
	
	Beispiel: Jupyter-Notebook-Codezellen zum Erstellen eines Dockerfiles
	
	Zelle 1
	
	`# Make docker folder`
	`!mkdir -p docker`
	
	Zelle 2
	
	`%%writefile docker/Dockerfile`
	
	`FROM python:3.7-slim-buster`
	
	`RUN pip3 install pandas==0.25.3 scikit-learn==0.21.3`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`ENV PYTHONUNBUFFERED=TRUE`
	
	`ENTRYPOINT ["python3"]`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Ihr Docker-Container-Image und übertragen Sie es auf Amazon ECR.	1. Erstellen Sie das Container-Image mit der Dockerfile, die Sie durch Ausführen des `docker build` Befehls in der AWS-CLI erstellt haben. 2. Senden Sie das Container-Image an Amazon ECR, indem Sie den `docker push` Befehl ausführen. Weitere Informationen finden Sie unter Container erstellen und registrieren unter Erstellen eines eigenen Algorithmus-Containers auf GitHub. Beispiel für Jupyter-Notebook-Codezellen zum Erstellen und Registrieren eines Docker-Images ⚠ Important Bevor Sie die folgenden Zellen ausführen, stellen Sie sicher, dass Sie ein Dockerfile erstellt und im Verzeichnis namens gespeicherte haben. `docker` Stellen Sie außerdem sicher, dass Sie ein Amazon ECR-	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Repository erstellt haben und dass Sie den `ecr_repository` Wert in der ersten Zelle durch den Namen Ihres Repositorys ersetzen.
	
	Zelle 1
	
	`import boto3`
	`tag = ':latest'`
	`account_id = boto3.client('sts').get_caller_identity().get('Account')`
	`region = boto3.Session().region_name`
	`ecr_repository = 'byoc'`
	
	`image_uri = '{}.dkr.ecr.{}.amazonaws.com/{}'.format(account_id, region, ecr_repository + tag)`
	
	Zelle 2
	
	`# Build docker image`
	`!docker build -t $image_uri docker`
	
	Zelle 3
	
	`# Authenticate to ECR`
	`!aws ecr get-login-password --region`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`{region} | docker login --username AWS --password-stdin {account_id}.dkr.ecr.{region}.amazonaws.com`
	
	Zelle 4
	
	`# Push docker image`
	`!docker push $image_uri`
	
	Note
	Sie müssen Ihren Docker-Client bei Ihrer privaten Registrierung authentifizieren, damit Sie die Befehle `docker push` und `docker pull` verwenden können. Mit diesen Befehlen werden Bilder in und aus den Repositorys in Ihrer Registrierung übertragen und abgerufen.	

Erstellen Sie einen Step Functions Functions-Workflow, der Ihr benutzerdefiniertes Docker-Container-Image verwendet

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie ein Python-Skript, das Ihre benutzerdefinierte Verarbeitungs- und Modelltrainingslogik enthält.	Schreiben Sie eine benutzerdefinierte Verarbeitungslogik, die in Ihrem Datenverarbeitungsskript ausgeführt werden soll. Speichern Sie es dann als Python-Skript mit dem Name `training.py`.
	
	Weitere Informationen finden Sie unter Bringen Sie Ihr eigenes Modell mit aktiviertem SageMaker Skriptmodus mit GitHub.
	
	Beispiel für ein Python-Skript mit benutzerdefinierter Verarbeitungs- und Modelltrainingslogik
	
	`%%writefile training.py`
	`from numpy import empty`
	`import pandas as pd`
	`import os`
	`from sklearn import datasets, svm`
	`from joblib import dump, load`
	
	`if __name__ == '__main__':`
	`digits = datasets.load_digits()`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`    #create classifier object`
	`    clf = svm.SVC(gamma=0.001, C=100.)`
	
	`    #fit the model`
	`    clf.fit(digits.data[:-1], digits.target[:-1])`
	
	`    #model output in binary format`
	`    output_path = os.path.join('/opt/ml/processing/model', "model.joblib")`
	`    dump(clf, output_path)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie einen Step Functions Functions-Workflow, der Ihren SageMaker Verarbeitungsjob als einen der Schritte enthält.	Installieren und importieren Sie das AWS Step Functions Data Science SDK und laden Sie die Datei training.py auf Amazon S3 hoch. Verwenden Sie dann das Amazon SageMaker Python SDK, um einen Verarbeitungsschritt in Step Functions zu definieren.
	
	Important
	Stellen Sie sicher, dass Sie in Ihrem AWS-Konto eine IAM-Ausführungsrolle für Step Functions erstellt haben.
	
	Beispielumgebung einrichten und benutzerdefiniertes Trainingsskript zum Hochladen auf Amazon S3
	
	`!pip install stepfunctions`
	
	`import boto3`
	`import stepfunctions`
	`import sagemaker`
	`import datetime`
	
	`from stepfunctions import steps`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`from stepfunct ions.inputs import ExecutionInput from stepfunct ions.steps import ( Chain ) from stepfunct ions.workflow import Workflow from sagemaker .processing import ScriptProcessor, ProcessingInput, ProcessingOutput`
	
	`sagemaker_session = sagemaker.Session() bucket = sagemaker _session.default_b ucket() role = sagemaker .get_execution_role() prefix = 'byoc-tra ining-model'`
	
	`# See prerequisites section to create this role workflow_execution_rol e = f"arn:aws:iam:: {account_id}:role/Ama zonSageMaker-StepF unctionsWorkflowEx ecutionRole"`
	
	`execution_input = ExecutionInput( schema={ "Preproce ssingJobName": str})`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	``
	input_code = sagemaker
	_session.upload_data(
	    "training.py",
	    bucket=bucket,
	    key_prefix="prepro
	cessing.py",
	)
	``	

	Beispiel für eine Definition eines SageMaker Verarbeitungsschritts, die ein benutzerdefiniertes Amazon ECR-Image und ein Python-Skript verwendet	
	Note Stellen Sie sicher, dass Sie den `execution_input` Parameter verwenden, um den Jobnamen anzugeben. Der Wert des Parameters muss bei jeder Ausführung des Jobs eindeutig sein. Außerdem wird der Code der Datei training.py als `input` Parameter an die übergeben `ProcessingStep`, was bedeutet, dass er in den Container kopiert wird. Das Ziel	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	für den `ProcessingInput` Code ist dasselbe wie das zweite Argument in der `container_entrypoint` .
	
	`script_processor = ScriptProcessor(command=['python3'], image_uri=image_uri, role=role, instance_count=1, instance_type='ml.m5.xlarge')`
	
	`processing_step = steps.ProcessingStep( "training-step", processor=script_processor, job_name=execution_input["PreprocessingJobName"], inputs=[ ProcessingInput( source=input_code, destination="/opt/ml/processing/input/code", input_name="code",`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
        ),
    ],
    outputs=[
        Processin
gOutput(
            source='/
opt/ml/processing/
model',
            destinati
on="s3://{}/{}".fo
rmat(bucket, prefix),
            output_na
me='byoc-example')
    ],
    container_entrypoi
nt=["python3", "/opt/
ml/processing/input/c
ode/training.py"],
)
```

Beispiel Step Functions Functions-Workflow, der einen SageMaker Verarbeitungsjob ausführt

> **Note**
>
> Dieser Beispiel-Workflow umfasst nur den SageMaker Verarbeitungs-Job-Schritt, keinen vollständigen Step Functions Functions -Workflow. Einen vollständigen Beispiel-Workflow finden Sie unter Beispiel-

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Notebooks SageMaker in der AWS Step Functions Data Science SDK-Dokumentation.
	
	`workflow_graph = Chain([processing_step])`
	
	`workflow = Workflow( name="ProcessingWorkflow", definition=workflow_graph, role=workflow_execution_role )`
	
	`workflow.create()`
	`# Execute workflow`
	`execution = workflow.execute( inputs={ "PreprocessingJobName": str(datetime.datetime.now().strftime("%Y%m%d%H%M-%SS")), # Each pre processing job (SageMaker processing job) requires a unique name, } )`
	`execution_output = execution.get_output(wait=True)`	

Zugehörige Ressourcen

- Daten verarbeiten (Amazon SageMaker Developer Guide)
- Anpassung Ihres eigenen Trainingscontainers (Amazon SageMaker Developer Guide)

Verwenden Sie Amazon Bedrock-Agenten, um die Erstellung von Zugriffskontrollen in Amazon EKS durch textbasierte Eingabeaufforderungen zu automatisieren

Erstellt von Keshav Ganesh (AWS) und Sudhanshu Saurav (AWS)

Übersicht

Organizations stehen vor Herausforderungen bei der Verwaltung der Zugriffskontrollen und der Ressourcenbereitstellung, wenn mehrere Teams mit einem gemeinsamen Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster arbeiten müssen. Ein verwalteter Kubernetes-Service wie Amazon EKS hat den Clusterbetrieb vereinfacht. Der Verwaltungsaufwand für die Verwaltung des Teamzugriffs und der Ressourcenberechtigungen bleibt jedoch komplex und zeitaufwändig.

Dieses Muster zeigt, wie Amazon Bedrock-Agenten Ihnen helfen können, die Amazon EKS-Cluster-Zugriffsverwaltung zu automatisieren. Diese Automatisierung ermöglicht es Entwicklungsteams, sich auf die Entwicklung ihrer Kernanwendungen zu konzentrieren, anstatt sich mit der Einrichtung und Verwaltung der Zugriffskontrolle zu befassen. Sie können einen Amazon Bedrock-Agenten so anpassen, dass er mithilfe einfacher Eingabeaufforderungen in natürlicher Sprache Aktionen für eine Vielzahl von Aufgaben ausführt.

Durch die Verwendung von AWS Lambda Funktionen als Aktionsgruppen kann ein Amazon Bedrock-Agent Aufgaben wie das Erstellen von Benutzerzugriffseinträgen und das Verwalten von Zugriffsrichtlinien übernehmen. Darüber hinaus kann ein Amazon Bedrock-Agent Pod-Identitätszuordnungen konfigurieren, die den Zugriff auf AWS Identity and Access Management (IAM-) Ressourcen für die im Cluster laufenden Pods ermöglichen. Mit dieser Lösung können Unternehmen ihre Amazon EKS-Clusterverwaltung mit einfachen textbasierten Eingabeaufforderungen optimieren, den manuellen Aufwand reduzieren und die allgemeine Entwicklungseffizienz verbessern.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver. AWS-Konto
- Etablierte IAM-Rollen und -Berechtigungen für den Bereitstellungsprozess. Dazu gehören Berechtigungen für den Zugriff auf Amazon Bedrock Foundation Models (FM), die Erstellung von Lambda-Funktionen und alle anderen erforderlichen Ressourcen im gesamten Ziel. AWS-Konten

- Der Zugriff auf diese Amazon Bedrock FMs: Amazon Titan Text Embeddings V2 und Anthropic Claude 3 Haiku ist im aktiven AWS-Konto Modus aktiviert.
- AWS Command Line Interface (AWS CLI) Version 2.9.11 oder höher, installiert und konfiguriert.
- eksctl 0.194.0 oder höher, installiert.

Einschränkungen

- Möglicherweise sind Schulungen und Unterlagen erforderlich, um eine reibungslose Einführung und effektive Anwendung dieser Techniken zu gewährleisten. Die Verwendung von Amazon Bedrock, Amazon EKS, Lambda, Amazon OpenSearch Service und OpenAPI erfordert eine erhebliche Lernkurve für Entwickler und Teams. DevOps
- Einige AWS-Services sind nicht in allen verfügbar. AWS-Regionen Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie unter AWS-Services nach Regionen. Informationen zu bestimmten Endpunkten finden Sie unter Service-Endpunkte und Kontingente. Wählen Sie dort den Link für den Service aus.

Architektur

Das folgende Diagramm zeigt den Workflow und die Architekturkomponenten für dieses Muster.

Diese Lösung führt die folgenden Schritte aus:

1. Der Benutzer interagiert mit dem Amazon Bedrock-Agenten, indem er eine Aufforderung oder Anfrage sendet, die dem Agenten als Eingabe zur Bearbeitung und Ergreifung von Maßnahmen dient.
2. Basierend auf der Aufforderung überprüft der Amazon Bedrock-Agent das OpenAPI-Schema, um die richtige API für das Ziel zu identifizieren. Wenn der Amazon Bedrock-Agent den richtigen API-Aufruf findet, wird die Anfrage an die Aktionsgruppe weitergeleitet, die der Lambda-Funktion zugeordnet ist, die diese Aktionen implementiert.
3. Wenn keine relevante API gefunden wird, fragt der Amazon Bedrock-Agent die OpenSearch Sammlung ab. Die OpenSearch Sammlung verwendet indexierte Wissensdatenbankinhalte, die aus dem Amazon S3 S3-Bucket stammen, der das Amazon EKS-Benutzerhandbuch enthält.
4. Die OpenSearch Sammlung sendet relevante Kontextinformationen an den Amazon Bedrock-Mitarbeiter zurück.

5. Bei umsetzbaren Anfragen (solche, die einem API-Vorgang entsprechen) wird der Amazon Bedrock-Agent in einer Virtual Private Cloud (VPC) ausgeführt und löst die Lambda-Funktion aus.
6. Die Lambda-Funktion führt eine Aktion aus, die auf den Eingaben des Benutzers im Amazon EKS-Cluster basiert.
7. Der Amazon S3 S3-Bucket für den Lambda-Code speichert das Artefakt, für das der Code und die Logik für die Lambda-Funktion geschrieben wurden.

Tools

AWS-Services

- Amazon Bedrock ist ein vollständig verwalteter Service, der Ihnen leistungsstarke Basismodelle (FMs) von führenden KI-Startups und Amazon über eine einheitliche API zur Verfügung stellt.
- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten AWS-Konten Lebenszyklus über und zu verwalten. AWS-Regionen
- Mit Amazon Elastic Kubernetes Service (Amazon EKS) können Sie Kubernetes ausführen, AWS ohne dass Sie Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten müssen.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon OpenSearch Service ist ein verwalteter Service, der Sie bei der Bereitstellung, dem Betrieb und der Skalierung von OpenSearch Clustern in der unterstützt AWS Cloud. Die Sammlungsfunktion hilft Ihnen dabei, Ihre Daten zu organisieren und umfassende Wissensdatenbanken aufzubauen, die KI-Assistenten wie Amazon Bedrock-Agenten nutzen können.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere Tools

- eksctl ist ein Befehlszeilenprogramm zum Erstellen und Verwalten von Kubernetes-Clustern auf Amazon EKS.

Code-Repository

Der Code für dieses Muster ist im GitHub eks-access-controls-bedrock-agent-Repository verfügbar.

Bewährte Methoden

- Achten Sie bei der Implementierung dieses Musters auf die höchstmögliche Sicherheit. Stellen Sie sicher, dass der Amazon EKS-Cluster privat ist, über eingeschränkte Zugriffsberechtigungen verfügt und dass sich alle Ressourcen in einer Virtual Private Cloud (VPC) befinden. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden in der Amazon EKS-Dokumentation.
- Verwenden Sie nach Möglichkeit vom AWS KMS Kunden verwaltete Schlüssel und gewähren Sie ihnen eingeschränkte Zugriffsberechtigungen.
- Folgen Sie dem Prinzip der geringsten Rechte und gewähren Sie nur die für die Ausführung einer Aufgabe erforderlichen Mindestberechtigungen. Weitere Informationen finden Sie in der IAM-Dokumentation unter Gewährung der geringsten Rechte und bewährte Methoden zur Sicherheit.

Epen

Richte die Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Um das Repository dieses Musters zu klonen, führen Sie den folgenden Befehl auf Ihrer lokalen Workstation aus: `git clone https://github.com/aws-samples/eks-access-controls-bedrock-agent.git`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Holen Sie sich den AWS-Konto Ausweis.	Gehen Sie wie folgt vor, um die AWS-Konto ID zu erhalten: 1. Öffnen Sie eine Shell im Stammordner des geklonten Repos,. `eks-access-controls-bedrock-agent` 2. Um Ihre AWS-Konto ID zu erhalten, navigieren Sie zum geklonten Verzeichnis und führen Sie den folgenden Befehl aus: `AWS_ACCOUNT=$(aws sts get-caller-identity --query "Account" --output text)` Dieser Befehl speichert Ihre AWS-Konto ID in der `AWS_ACCOUNT` Variablen.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den S3-Bucket für Lambda-Code.	Um diese Lösung zu implementieren, müssen Sie drei Amazon S3 S3-Buckets erstellen, die unterschiedlichen Zwecken dienen, wie im Architekturdiagramm dargestellt. Die S3-Buckets sind für Lambda-Code, eine Wissensdatenbank und ein OpenAPI-Schema vorgesehen.
	
	Gehen Sie wie folgt vor, um den Lambda-Code-Bucket zu erstellen:
	
	1. Führen Sie den folgenden Befehl aus, um einen S3-Bucket für Lambda-Code zu erstellen:
	
	`aws s3 mb s3://bedrock-agent-lambda-artifacts-${AWS_ACCOUNT} --region us-east-1`
	
	2. Führen Sie den folgenden Befehl aus, um die Lambda-Code-Abhängigkeit zu installieren:
	
	`cd eks-lambda`
	`npm install`
	`tsc`
	`cd .. && cd opensearch-lambda`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>npm install
	tsc
	cd ..</pre>
	3. Führen Sie den folgenden Befehl aus, um den Code zu packen und in den S3-Bucket für Lambda hochzuladen:
	<pre>aws cloudformation
	 package \
	 --template-file eks-
	access-controls.yaml
	 \
	 --s3-bucket bedrock-
	agent-lambda-artifa
	cts-${AWS_ACCOUNT} \
	 --output-template-
	file eks-access-
	controls-templat
	e.yaml \
	 --region us-east-1</pre>
	Der Paketbefehl erstellt eine neue CloudFormation Vorlage (`eks-access-control s-template.yaml`), die Folgendes enthält:
	• Verweise auf den Lambda-Funktionscode, der in Ihrem S3-Bucket gespeichert ist.
	• Definitionen für die gesamte erforderliche AWS Infrastruktur, einschlie ßlich VPC, Subnetze,	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon Bedrock-Agent und Sammlung. OpenSearch Sie können diese Vorlage verwenden, um die komplette Lösung bereitzustellen, indem Sie CloudFormation	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den S3-Bucket für die Wissensdatenbank.	Gehen Sie wie folgt vor, um den Amazon S3 S3-Bucket für die Wissensdatenbank zu erstellen:
	
	1. Führen Sie den folgenden Befehl aus, um den Amazon S3 S3-Bucket für die Wissensdatenbank zu erstellen:
	
	`aws s3 mb s3://eks-knowledge-base-${AWS_ACCOUNT} --region us-east-1`
	
	2. Führen Sie die folgenden Befehle aus, um das Amazon EKS-Benut zerhandbuch herunterz uladen und in einem Verzeichnis zu speichern:
	
	`mkdir dataSource`
	`cd dataSource`
	`curl https://docs.aws.amazon.com/pdfs/eks/latest/userguide/eks-ug.pdf -o eks-user-guide.pdf`
	
	3. Führen Sie den folgenden Befehl aus, um das Benutzerhandbuch in den S3-Bucket hochzuladen,
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	den Sie in Schritt 1 erstellt haben:
	
	`aws s3 cp eks-user-guide.pdf s3://eks-knowledge-base-${AWS_ACCOUNT} \ --region us-east-1 \`
	
	4. Führen Sie den folgenden Befehl aus, um zum Stammverzeichnis zurückzukehren:
	
	`cd ..`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den S3-Bucket für das OpenAPI-Schema.	Gehen Sie wie folgt vor, um den Amazon S3 S3-Bucket für das OpenAPI-Schema zu erstellen:
	1. Führen Sie den folgenden Befehl aus, um den S3-Bucket zu erstellen:
	`aws s3 mb s3://eks-openapi-schema-${AWS_ACCOUNT} --region us-east-1`
	2. Führen Sie den folgenden Befehl aus, um das OpenAPI-Schema in den S3-Bucket hochzuladen:
	`aws s3 cp openapi-schema.yaml s3://eks-openapi-schema-${AWS_ACCOUNT} --region us-east-1`
		AWS DevOps

Stellen Sie den CloudFormation Stack bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den CloudFormation Stack bereit.	Verwenden Sie zum Bereitstellen des CloudFormation Stacks die CloudFormation Vorlagendatei`eks-access-controls-template.yaml` , die Sie zuvor erstellt haben. Ausführlichere	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anweisungen finden Sie in der CloudFormation Dokumentation unter Erstellen eines Stacks von der CloudFormation Konsole aus. **Note** Die Bereitstellung des OpenSearch Indexes mit der CloudFormation Vorlage dauert etwa 10 Minuten. Nachdem der Stapel erstellt wurde, notieren Sie sich die `VPC_ID` und `PRIVATE_SUBNET ID` s.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Amazon EKS-Cluster.	Gehen Sie wie folgt vor, um den Amazon EKS-Cluster innerhalb der VPC zu erstellen : 1. Erstellen Sie eine Kopie der `eks-config.yaml` Konfigurationsdatei und benennen Sie die Kopie als`eks-deploy.yaml` . 2. Öffnen Sie `eks-deploy.yaml` in einem Texteditor. Ersetzen Sie dann die folgenden Platzhalt erwerte durch Werte aus dem bereitgestellten Stack:`VPC_ID`,`PRIVATE_SUBNET1` , und `PRIVATE_SUBNET2` 3. Führen Sie den folgenden Befehl aus, um den Cluster mithilfe des eksctl-Dienstprogramms zu erstellen : `eksctl create cluster -f eks-deploy.yaml` **Note** Dieser Clusterer stellungsprozess	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	kann bis zu 15 bis 20 Minuten dauern.
	4. Führen Sie die folgenden Befehle aus, um zu überprüfen, ob der Cluster erfolgreich erstellt wurde:
	`aws eks describe-cluster --name  --query "cluster.status"`
	`aws eks update-kubeconfig --name  --region`
	`kubectl get nodes`
	Die erwarteten Ergebnisse lauten wie folgt:
	• Der Clusterstatus ist`ACTIVE`.
	• Der Befehl `kubectl get nodes` zeigt, dass sich alle Knoten im `Ready` Status befinden.	

Connect die Lambda-Funktion und den Amazon EKS-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie eine Verbindung zwischen dem Amazon EKS-Cluster und der Lambda-Funktion her.	Gehen Sie wie folgt vor, um Netzwerk- und IAM-Berechtigungen einzurichten, damit die Lambda-Funktion mit	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dem Amazon EKS-Cluster kommunizieren kann: 1. Um die IAM-Rolle zu identifizieren, die der Lambda-Funktion zugeordnet ist, öffnen Sie die AWS Management Console und suchen Sie nach der Lambda-Funktion mit dem Namen. `bedrock-agent-eks-access-control` Notieren Sie sich den Amazon-Ressourcennamen (ARN) der IAM-Rolle. 2. Um einen Zugriffseintrag im Amazon EKS-Cluster für die IAM-Rolle der Lambda-Funktion zu erstellen, führen Sie den folgenden Befehl aus: `aws eks create-access-entry --cluster-name eks-testing-cluster --principal-arn <principal-Role-ARN>` 3. Führen Sie den folgenden Befehl aus, um dieser Rolle `AmazonEKSClusterAdminPolicy` Berechtigungen zuzuweisen:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws eks associate -access-policy -- cluster-name eks-testing-cluster --principal-arn <principal-Role-ARN> --policy-arn arn:aws:eks::aws:cluster-access-policy/AmazonEKSClusterAdminPolicy --access-scope type=cluster` Weitere Informationen finden Sie unter Zugriffsrichtlinien mit Zugriffseinträgen verknüpfen und Amazon EKSCluster AdminPolicy in der Amazon EKS-Dokumentation. 4. Suchen Sie die Sicherheitsgruppe des Amazon EKS-Clusters. Fügen Sie eine Regel für eingehenden Datenverkehr hinzu, um eingehenden Netzwerkverkehr von der Lambda-Funktion zum Amazon EKS-Cluster zuzulassen. Verwenden Sie die folgenden Werte für die Regel für eingehenden Datenverkehr: • Typ — HTTPS	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Portbereich — 443 • Quelle — Lambda-Si cherheitsgruppe Weitere Informationen finden Sie unter Sicherhei tsgruppenregeln konfiguri eren in der Amazon VPC-Dokumentation.	

Testen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie den Amazon Bedrock-Agenten.	Bevor Sie den Amazon Bedrock-Agenten testen, stellen Sie sicher, dass Sie Folgendes tun: • Testen Sie zuerst mit Rollen, die nicht zur Produktion gehören. • Dokumentieren Sie alle Änderungen, die am Clusterzugriff vorgenommen wurden. • Planen Sie, die Änderunge n bei Bedarf rückgängig zu machen. Gehen Sie wie folgt vor, um auf den Amazon Bedrock-A genten zuzugreifen:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Melden Sie sich bei der Rolle AWS Management Console Using an IAM mit Amazon Bedrock-Berechtigungen an und öffnen Sie die Amazon Bedrock-Konsole unter. https://console.aws.amazon.com/bedrock/ 2. Wählen Sie im linken Navigationsbereich Agenten aus. Wählen Sie dann im Abschnitt Agents Ihren konfigurierten Agenten aus. 3. Um den Agenten zu testen, probieren Sie die folgenden Beispielaufforderungen aus, in denen Sie den ARN durch einen tatsächlichen IAM-Rollen-ARN `Principal-ARN-OF-ROLE` ersetzen: • Verwenden Sie die folgende Eingabeaufforderung, um einen Zugriffseintrag für eine beliebige IAM-Rolle zu erstellen, der Sie Zugriff auf den EKS-Cluster gewähren möchten: `Create an access entry in cluster eks-testing-new for a role whose principal arn`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`is <Principal-ARN-OF-ROLE> with access policy as AmazonEKS AdminPolicy` Erwartetes Ergebnis: • Der Agent sollte die Erstellung des Zugriffse intrags bestätigen. • Überprüfen Sie zur Überprüfung die Amazon EKS-API AWS Management Console oder verwenden Sie die Amazon EKS-API und führen Sie den folgenden Befehl aus: `aws eks list-access-entrie s --cluster-name ekscluster` • Verwenden Sie die folgende Eingabeaufforderung, um den von Ihnen erstellten Zugriffseintrag zu beschreib en: `Describe an access entry in cluster eks-testing-new whose principal arn is <Principal-ARN-OF-ROLE>` Erwartetes Ergebnis: • Der Agent sollte Details zum Zugriffseintrag zurückgeben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Die Details sollten mit den Angaben übereinstimmen, die Sie zuvor für den Zugriffseintrag konfiguriert haben. • Verwenden Sie die folgende Eingabeaufforderung, um den von Ihnen erstellten Zugriffseintrag zu löschen: `Delete the access entry in cluster eks-testing-new whose principal arn is <Principal-ARN-OF-ROLE>` Erwartetes Ergebnis: • Der Agent sollte das Löschen des Zugangsei ntrags bestätigen. • Überprüfen Sie zur Überprüfung die Amazon EKS-API AWS Management Console oder verwenden Sie die Amazon EKS-API und führen Sie den folgenden Befehl aus: `aws eks list-access-entrie s --cluster-name ekscluster` Sie können den Agenten auch bitten, Aktionen für EKS	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Pod Identity-Verknüpfungen auszuführen. Weitere Informationen finden Sie AWS-Services in der Amazon EKS-Dokumentation unter Erfahren Sie, wie EKS Pod Identity Pods Zugriff gewährt.	

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen von Ressourcen.	Gehen Sie wie folgt vor, um die Ressourcen zu bereinigen, die durch dieses Muster erstellt wurden. Warten Sie, bis jeder Löschschritt abgeschlossen ist, bevor Sie mit dem nächsten Schritt fortfahren. **Warning** Durch dieses Verfahren werden alle Ressourcen, die von diesen Stacks erstellt wurden, dauerhaft gelöscht. Stellen Sie sicher, dass Sie alle wichtigen Daten gesichert haben, bevor Sie fortfahren.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	1. Führen Sie den folgenden Befehl aus, um den Amazon EKS-Cluster zu löschen:
	`eksctl delete cluster -f eks-deploy.yaml`
	Note
	Dieser Vorgang kann 15 bis 20 Minuten in Anspruch nehmen.
	2. Führen Sie die folgenden Befehle aus, um die Amazon S3 S3-Buckets zu löschen:
	• Um den Lambda-Bucket zu leeren:
	`aws s3 rm s3://bedrock-agent-lambda-artifacts-${AWS_ACCOUNT} --recursive`
	• Um den Wissensdatenbank-Bucket zu leeren:
	`aws s3 rm s3://eks-knowledge-base-${AWS_ACCOUNT} –recursive`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	• Um den OpenAPI-S chema-Bucket zu leeren:
	`aws s3 rm s3://bedr ock-agent-openapi- schema-${AWS_ACCOU NT} –recursive`
	• Um die leeren Buckets zu löschen:
	`aws s3 rb s3://bedr ock-agent-lambda-a rtifacts-${AWS_ACC OUNT}`
	`aws s3 rb s3://eks- knowledge-base-${A WS_ACCOUNT}`
	`aws s3 rb s3://bedr ock-agent-openapi- schema-${AWS_ACCOU NT}`
	3. Führen Sie den folgenden Befehl aus, um den CloudFormation Stack zu löschen:
	`aws cloudformation delete-stack \ -- stack-name`
	4. Führen Sie den folgenden Befehl aus, um das Löschen des Amazon EKS-Clusters zu überprüfen:
	`eksctl get clusters`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	5. Führen Sie die folgenden Befehle aus, um das Löschen der Amazon S3 S3-Buckets zu überprüfen:
	• Um das Löschen des Lambda-Buckets zu überprüfen:
	`aws s3 ls | grep "bedrock-agent-lambda-artifacts"`
	• Um das Löschen des Knowledge Base-Buckets zu überprüfen:
	`aws s3 ls | grep "eks-knowledge-base"`
	• Um das Löschen des OpenAPI-Schema-Buckets zu überprüfen:
	`aws s3 ls | grep "bedrock-agent-openapi-schema"`
	6. Führen Sie den folgenden Befehl aus, um das Löschen des Stacks zu überprüfen:
	`aws cloudformation list-stacks \--query 'StackSummaries[?StackName==``]'`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wenn der Stack nicht gelöscht werden kann, finden Sie weitere Informationen unter Problembehandlung.	

Fehlerbehebung

Problem	Lösung
Bei der Einrichtung der Umgebung wird ein Fehlercode ungleich Null zurückgegeben.	Stellen Sie sicher, dass Sie den richtigen Ordner verwenden, wenn Sie einen Befehl zur Bereitstellung dieser Lösung ausführen. Weitere Informationen finden Sie in der Datei First_Deploy.md im Repository dieses Patterns.
Die Lambda-Funktion ist nicht in der Lage, die Aufgabe zu erledigen.	Stellen Sie sicher, dass die Konnektivität zwischen der Lambda-Funktion und dem Amazon EKS-Cluster korrekt eingerichtet ist.
Die Eingabeaufforderungen des Agenten erkennen das nicht. APIs	Stellen Sie die Lösung erneut bereit. Weitere Informationen finden Sie in der Datei RE_DEPLOY.md im Repository dieses Patterns.
Der Stapel kann nicht gelöscht werden.	Ein erster Versuch, den Stapel zu löschen, schlägt möglicherweise fehl. Dieser Fehler kann aufgrund von Abhängigkeitsproblemen mit der benutzerdefinierten Ressource auftreten, die für die OpenSearch Sammlung erstellt wurde, die die Indexierung für die Wissensdatenbank durchführt. Um den Stapel zu löschen, wiederholen Sie den Löschvorgang, indem Sie die benutzerdefinierte Ressource beibehalten.

Zugehörige Ressourcen

AWS Blog

- Ein tiefer Einblick in vereinfachte Amazon EKS-Zugriffsverwaltungskontrollen

Dokumentation zu Amazon Bedrock

- Automatisieren Sie Aufgaben in Ihrer Anwendung mithilfe von KI-Agenten
- So funktioniert Amazon Bedrock Agents
- Testen Sie das Verhalten der Agenten und beheben Sie Fehler
- Verwenden Sie Aktionsgruppen, um Aktionen zu definieren, die Ihr Agent ausführen soll

Amazon EKS-Dokumentation

- Erfahren Sie, wie die Zugriffskontrolle in Amazon EKS funktioniert

Stellen Sie mithilfe AWS von Terraform und Amazon Bedrock einen RAG-Anwendungsfall bereit

Erstellt von Martin Maritsch (AWS), Alice Morano (AWS), Julian Ferdinand Grueber (AWS), Nicolas Jacob Baer (AWS), Olivier Brique (AWS) und Nicola D Orazio (AWS)

Übersicht

AWS bietet verschiedene Optionen zum Erstellen Ihrer generativen KI-Anwendungsfälle, die Retrieval Augmented Generation (RAG) unterstützen. Dieses Muster bietet Ihnen eine Lösung für eine RAG-basierte Anwendung, die auf Amazon Aurora PostgreSQL basiert LangChain und als Vector Store kompatibel ist. Sie können diese Lösung mit Terraform direkt in Ihrem eigenen implementieren AWS-Konto und den folgenden einfachen RAG-Anwendungsfall implementieren:

1. Der Benutzer lädt manuell eine Datei in einen Amazon Simple Storage Service (Amazon S3) - Bucket hoch, z. B. eine Microsoft Excel-Datei oder ein PDF-Dokument. (Weitere Informationen zu den unterstützten Dateitypen finden Sie in der Dokumentation Unstructured.)
2. Der Inhalt der Datei wird extrahiert und in eine Wissensdatenbank eingebettet, die auf dem serverlosen Aurora PostgreSQL-kompatiblen System basiert und die Aufnahme von Dokumenten in den Vector Store nahezu in Echtzeit unterstützt. Dieser Ansatz ermöglicht es dem RAG-Modell, auf relevante Informationen für Anwendungsfälle zuzugreifen und diese abzurufen, bei denen es auf niedrige Latenzen ankommt.
3. Wenn der Benutzer mit dem Textgenerierungsmodell interagiert, verbessert es die Interaktion, indem relevante Inhalte aus den zuvor hochgeladenen Dateien abgerufen und erweitert werden.

Das Muster verwendet Amazon Titan Text Embeddings v2 als Einbettungsmodell und Anthropic Claude 3 Sonnet als Textgenerierungsmodell, beide auf Amazon Bedrock verfügbar.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver. AWS-Konto
- AWS Command Line Interface (AWS CLI) installiert und konfiguriert mit Ihrem AWS-Konto. Installationsanweisungen finden Sie AWS CLI in der AWS CLI Dokumentation unter Installation oder Aktualisierung auf die neueste Version von. Informationen zur Überprüfung Ihrer AWS

Anmeldeinformationen und Ihres Zugriffs auf Ihr Konto finden Sie in der AWS CLI Dokumentation unter Konfiguration und Einstellungen der Anmeldeinformationsdatei.

- Modellzugriff, der für die erforderlichen großen Sprachmodelle (LLMs) in der Amazon Bedrock-Konsole Ihres AWS-Konto aktiviert ist. Für dieses Muster ist Folgendes LLMs erforderlich:
  - `amazon.titan-embed-text-v2:0`
  - `anthropic.claude-3-sonnet-20240229-v1:0`

Einschränkungen

- Diese Beispielarchitektur enthält keine Schnittstelle für die programmatische Beantwortung von Fragen mit der Vektordatenbank. Wenn Ihr Anwendungsfall eine API erfordert, sollten Sie erwägen, Amazon API Gateway mit einer AWS Lambda Funktion hinzuzufügen, die Abruf- und Fragenbeantwortungsaufgaben ausführt.
- Diese Beispielarchitektur beinhaltet keine Überwachungsfunktionen für die bereitgestellte Infrastruktur. Wenn Ihr Anwendungsfall eine Überwachung erfordert, sollten Sie das Hinzufügen von AWS Überwachungsdiensten in Betracht ziehen.
- Wenn Sie viele Dokumente in einem kurzen Zeitraum in den Amazon S3 S3-Bucket hochladen, kann es bei der Lambda-Funktion zu Ratenbegrenzungen kommen. Als Lösung können Sie die Lambda-Funktion von einer Amazon Simple Queue Service (Amazon SQS) -Warteschlange entkoppeln, in der Sie die Geschwindigkeit der Lambda-Aufrufe steuern können.
- Einige sind nicht in allen verfügbar. AWS-Services AWS-Regionen Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie unter Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Produktversionen

- AWS CLI Version 2 oder höher
- Docker-Version 26.0.0 oder höher
- Poesie-Version 1.7.1 oder höher
- Python-Version 3.10 oder höher
- Terraform Version 1.8.4 oder höher

Architektur

Das folgende Diagramm zeigt den Workflow und die Architekturkomponenten für dieses Muster.

Dieses Diagramm veranschaulicht Folgendes:

1. Wenn ein Objekt im Amazon S3 S3-Bucket erstellt wird`bedrock-rag-template-<account_id>`, ruft eine Amazon S3 S3-Benachrichtigung die Lambda-Funktion auf. `data-ingestion-processor`
2. Die Lambda-Funktion `data-ingestion-processor` basiert auf einem Docker-Image, das im Amazon Elastic Container Registry (Amazon ECR) -Repository gespeichert ist. `bedrock-rag-template`

   Die Funktion verwendet LangChain S3, FileLoader um die Datei als Dokument zu lesen. LangChain Dann werden die LangChain RecursiveCharacterTextSplitterChunks jedes Dokument mit a `CHUNK_SIZE` und a versehen, `CHUNK_OVERLAP` die von der maximalen Token-Größe des Amazon Titan Text Embedding V2-Einbettungsmodells abhängen. Als Nächstes ruft die Lambda-Funktion das Einbettungsmodell auf Amazon Bedrock auf, um die Chunks in numerische Vektordarstellungen einzubetten. Schließlich werden diese Vektoren in der Aurora PostgreSQL-Datenbank gespeichert. Um auf die Datenbank zuzugreifen, ruft die Lambda-Funktion zunächst den Benutzernamen und das Passwort von ab. AWS Secrets Manager
3. Auf der Amazon SageMaker AI-Notebook-Instance `aws-sample-bedrock-rag-template` kann der Benutzer eine Fragenaufforderung schreiben. Der Code ruft Claude 3 auf Amazon Bedrock auf und fügt die Wissensdatenbankinformationen dem Kontext der Aufforderung hinzu. Infolgedessen gibt Claude 3 Antworten unter Verwendung der Informationen in den Dokumenten.

Der Ansatz dieses Musters in Bezug auf Netzwerk und Sicherheit lautet wie folgt:

- Die Lambda-Funktion `data-ingestion-processor` befindet sich in einem privaten Subnetz innerhalb der Virtual Private Cloud (VPC). Die Lambda-Funktion darf aufgrund ihrer Sicherheitsgruppe keinen Datenverkehr an das öffentliche Internet senden. Daher wird der Datenverkehr zu Amazon S3 und Amazon Bedrock nur über die VPC-Endpunkte geleitet. Folglich durchquert der Datenverkehr nicht das öffentliche Internet, was die Latenz reduziert und eine zusätzliche Sicherheitsebene auf Netzwerkebene bietet.

- Alle Ressourcen und Daten werden, wann immer möglich, verschlüsselt, indem der Schlüssel AWS Key Management Service (AWS KMS) zusammen mit dem Alias `aws-sample/bedrock-rag-template` verwendet wird.

Automatisierung und Skalierung

Dieses Muster verwendet Terraform, um die Infrastruktur aus dem Code-Repository in einem bereitzustellen. AWS-Konto

Tools

AWS-Services

- Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt. In diesem Muster verwendet Aurora PostgreSQL-kompatibel das pgvector-Plugin als Vektordatenbank.
- Amazon Bedrock ist ein vollständig verwalteter Service, der Ihnen leistungsstarke Basismodelle (FMs) von führenden KI-Startups und Amazon über eine einheitliche API zur Verfügung stellt.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie AWS-Services über Befehle in Ihrer Befehlszeilen-Shell interagieren können.
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist. In diesem Muster hostet Amazon ECR das Docker-Image für die `data-ingestion-processor` Lambda-Funktion.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Key Management Service (AWS KMS) hilft Ihnen dabei, kryptografische Schlüssel zu erstellen und zu kontrollieren, um Ihre Daten zu schützen.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen. In diesem Muster nimmt Lambda Daten in den Vektorspeicher auf.
- Amazon SageMaker AI ist ein verwalteter Service für maschinelles Lernen (ML), mit dem Sie ML-Modelle erstellen und trainieren und sie dann in einer produktionsbereiten, gehosteten Umgebung bereitstellen können.

- Mit AWS Secrets Manager können Sie fest codierte Anmeldeinformationen im Code (einschließlich Passwörter) durch einen API-Aufruf an Secrets Manager ersetzen und das Geheimnis programmgesteuert abrufen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk bereitzustellen. Dieses virtuelle Netzwerk entspricht einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben würden, mit den Vorteilen der Verwendung der skalierbaren Infrastruktur von AWS. Die VPC umfasst Subnetze und Routingtabellen zur Steuerung des Datenverkehrs.

Andere Tools

- Docker ist eine Reihe von Platform-as-a-Service (PaaS) -Produkten, die Virtualisierung auf Betriebssystemebene nutzen, um Software in Containern bereitzustellen.
- HashiCorp Terraform ist ein Infrastructure-as-Code-Tool (IaC), mit dem Sie mithilfe von Code Cloud-Infrastruktur und -Ressourcen bereitstellen und verwalten können.
- Poetry ist ein Tool für Abhängigkeitsmanagement und Paketierung in Python.
- Python ist eine Allzweck-Computerprogrammiersprache.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub terraform-rag-template-using-amazon-bedrock verfügbar.

Bewährte Methoden

- Dieses Codebeispiel kann zwar in allen Bereichen eingesetzt werden AWS-Region, wir empfehlen jedoch, dass Sie US East (Nord-Virginia) — `us-east-1` oder US West (Nordkalifornien) — verwenden. `us-west-1` Diese Empfehlung basiert auf der Verfügbarkeit von Fundament- und Einbettungsmodellen in Amazon Bedrock zum Zeitpunkt der Veröffentlichung dieses Musters. Eine up-to-date Liste der Amazon Bedrock Foundation-Modellunterstützung finden Sie unter Model Support von AWS-Region in der Amazon Bedrock-Dokumentation. AWS-Regionen Informationen zur Bereitstellung dieses Codebeispiels in anderen Regionen finden Sie unter Zusätzliche Informationen.

- Dieses Muster bietet nur eine proof-of-concept (PoC) oder Pilotdemo. Wenn Sie den Code für die Produktion verwenden möchten, sollten Sie unbedingt die folgenden bewährten Methoden anwenden:
  - Aktivieren Sie die Serverzugriffsprotokollierung für Amazon S3.
  - Richten Sie die Überwachung und Warnung für die Lambda-Funktion ein.
  - Wenn Ihr Anwendungsfall eine API erfordert, sollten Sie erwägen, Amazon API Gateway mit einer Lambda-Funktion hinzuzufügen, die Abruf- und Fragenbeantwortungsaufgaben ausführt.
- Folgen Sie dem Prinzip der geringsten Rechte und gewähren Sie die für die Ausführung einer Aufgabe erforderlichen Mindestberechtigungen. Weitere Informationen finden Sie in der IAM-Dokumentation unter Gewährung der geringsten Rechte und bewährte Methoden zur Sicherheit.

Epen

Stellen Sie die Lösung in einem bereit AWS-Konto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Verwenden Sie den folgenden Befehl, um das mit diesem Muster bereitgestellte GitHub Repository zu klonen: `git clone https://github.com/aws-samples/terraform-rag-template-using-amazon-bedrock`	AWS DevOps
Konfigurieren Sie die Variablen.	Gehen Sie wie folgt vor, um die Parameter für dieses Muster zu konfigurieren: 1. Verwenden Sie auf Ihrem Computer im GitHub Repository den folgenden Befehl, um den `terraform` Ordner zu öffnen:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cd terraform` 2. Öffnen Sie die `commons.tfvars` Datei und passen Sie die Parameter an Ihre Bedürfnisse an.	

Stellen Sie die Lösung bereit.	Gehen Sie wie folgt vor, um die Lösung bereitzustellen:
	1. Verwenden Sie im `terraform` Ordner den folgenden Befehl, um Terraform auszuführen und die von Ihnen angepassten Variablen zu übergeben:
	`terraform init`
	`terraform apply -var-file=commons.tfvars`
	2. Vergewissern Sie sich, dass die im Architekturdiagramm angezeigten Ressourcen erfolgreich bereitgestellt wurden.
	
	Die Infrastrukturbereitstellung stellt eine SageMaker KI-Instanz innerhalb der VPC bereit und verfügt über die Berechtigungen für den Zugriff auf die Aurora PostgreSQL-Datenbank.
		AWS DevOps

Testen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Demo aus.	Nachdem die vorherige Infrastrukturbereitstellung erfolgreich war, führen Sie die folgenden Schritte aus, um die Demo in einem Jupyter-Notebook auszuführen: 1. Melden Sie sich bei dem Ort an, AWS Management Console an AWS-Konto dem die Infrastruktur bereitgestellt wird. 2. Öffnen Sie die SageMaker AI-Notebook-Instanz`aws-sample-bedrock-rag-template` . 3. Verschieben Sie das `rag_demo.ipynb` Jupyter-Notizbuch per Drag & Drop auf die SageMaker AI-Notebook-Instanz. 4. Öffnen Sie die Instanz `rag_demo.ipynb` auf der SageMaker AI-Notebook-Instanz und wählen Sie den Kernel aus. `conda_python3` 5. Um die Demo auszuführen, führen Sie die Zellen des Notebooks aus.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Das Jupyter-Notizbuch führt Sie durch den folgenden Prozess: • Anforderungen für die Installation • Definition einbetten • Datenbankverbindungen • Datenaufnahme • Erweiterte Textgenerierung beim Abrufen • Anfragen zu relevanten Dokumenten	

Infrastruktur aufräumen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Säubere die Infrastruktur.	Verwenden Sie den folgenden Befehl, um alle Ressourcen zu entfernen, die Sie erstellt haben, als sie nicht mehr benötigt werden: `terraform destroy -var-file=commons.tfvars`	AWS DevOps

Zugehörige Ressourcen

AWS Ressourcen

- Lambda-Funktionen mit Python erstellen
- Inferenzparameter für Fundamentmodelle

- Zugriff auf Amazon Bedrock Foundation-Modelle
- Die Rolle von Vektordatenbanken in generativen KI-Anwendungen (AWS Datenbank-Blog)
- Arbeiten mit Amazon Aurora PostgreSQL

Sonstige Ressourcen

- pgvector-Dokumentation

Zusätzliche Informationen

Implementierung einer Vektor-Datenbank

Dieses Muster verwendet Aurora PostgreSQL-kompatibel, um eine Vektordatenbank für RAG zu implementieren. Als Alternative zu Aurora PostgreSQL AWS bietet es weitere Funktionen und Dienste für RAG, wie Amazon Bedrock Knowledge Bases und Amazon Service. OpenSearch Sie können die Lösung wählen, die Ihren spezifischen Anforderungen am besten entspricht:

- Amazon OpenSearch Service bietet verteilte Such- und Analyse-Engines, mit denen Sie große Datenmengen speichern und abfragen können.
- Amazon Bedrock Knowledge Bases wurde für den Aufbau und die Bereitstellung von Wissensdatenbanken als zusätzliche Abstraktion entwickelt, um den RAG-Aufnahme- und Abrufprozess zu vereinfachen. Amazon Bedrock Knowledge Bases kann sowohl mit Aurora PostgreSQL als auch mit Amazon Service verwendet werden. OpenSearch

Bereitstellung auf anderen AWS-Regionen

Wie unter Architektur beschrieben, empfehlen wir, für die Bereitstellung dieses Codebeispiels entweder die Region USA Ost (Nord-Virginia) `us-east-1` oder USA West (Nordkalifornien) `us-west-1` zu verwenden. Es gibt jedoch zwei Möglichkeiten, dieses Codebeispiel in anderen Regionen als `us-east-1` und bereitzustellen`us-west-1`. Sie können die Bereitstellungsregion in der `commons.tfvars` Datei konfigurieren. Für den regionsübergreifenden Zugriff auf das Foundation-Modell sollten Sie die folgenden Optionen in Betracht ziehen:

- Durchqueren des öffentlichen Internets — Wenn der Datenverkehr das öffentliche Internet durchqueren kann, fügen Sie der VPC Internet-Gateways hinzu. Passen Sie dann die Sicherheitsgruppe an, die der Lambda-Funktion `data-ingestion-processor` und der

SageMaker AI-Notebook-Instanz zugewiesen ist, um ausgehenden Datenverkehr in das öffentliche Internet zuzulassen.

- Kein Durchqueren des öffentlichen Internets — Gehen Sie wie folgt vor, um dieses Beispiel in einer anderen Region als `us-east-1` oder `us-west-1` bereitzustellen:

1. Erstellen Sie entweder in der `us-west-1` Region `us-east-1` oder eine zusätzliche VPC, einschließlich eines VPC-Endpunkts für. `bedrock-runtime`
2. Stellen Sie mithilfe von VPC-Peering oder einem Transit-Gateway eine Peering-Verbindung zur Anwendungs-VPC her.
3. Wenn Sie den `bedrock-runtime` boto3-Client in einer beliebigen Lambda-Funktion außerhalb von `us-east-1` oder konfigurierenus`-west-1`, übergeben Sie den privaten DNS-Namen des VPC-Endpunkts für `bedrock-runtime` in `us-east-1` oder us-west-1 als den an den boto3-Client. `endpoint_url`

Stellen Sie mithilfe einer Inferenz-Pipeline in Amazon Vorverarbeitungslogik in einem ML-Modell an einem einzigen Endpunkt bereit SageMaker

Erstellt von Mohan Gowda Purushothama (AWS), Gabriel Rodriguez Garcia (AWS) und Mateusz Zaremba (AWS)

Übersicht

Dieses Muster erklärt, wie mehrere Pipeline-Modellobjekte in einem einzigen Endpunkt mithilfe einer Inferenz-Pipeline in Amazon SageMaker bereitgestellt werden. Das Pipeline-Modellobjekt repräsentiert verschiedene Workflow-Phasen des maschinellen Lernens (ML), wie Vorverarbeitung, Modellinferenz und Nachverarbeitung. Um den Einsatz von seriell verbundenen Pipeline-Modellobjekten zu veranschaulichen, zeigt Ihnen dieses Muster, wie Sie einen Scikit-Learn-Vorverarbeitungscontainer und ein Regressionsmodell bereitstellen, das auf dem integrierten linearen Lernalgorithmus basiert. SageMaker Die Bereitstellung wird hinter einem einzigen Endpunkt in gehostet. SageMaker

> **Note**
>
> Die Bereitstellung in diesem Muster verwendet den Instance-Typ ml.m4.2xlarge. Wir empfehlen, einen Instance-Typ zu verwenden, der Ihren Anforderungen an die Datengröße und der Komplexität Ihres Workflows entspricht. Weitere Informationen finden Sie unter SageMaker Amazon-Preise. Dieses Muster verwendet vorgefertigte Docker-Images für Scikit-learn, aber Sie können Ihre eigenen Docker-Container verwenden und sie in Ihren Workflow integrieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Python 3.9
- Amazon SageMaker Python SDK und Boto3-Bibliothek
- Rolle AWS Identity and Access Management (AWS IAM) mit SageMaker Basisberechtigungen und Amazon Simple Storage Service (Amazon S3) -Berechtigungen

Produktversionen

- Amazon SageMaker Python-SDK 2.49.2

Architektur

Zieltechnologie-Stack

- Amazon Elastic Container Registry (Amazon ECR)
- Amazon SageMaker
- Amazon SageMaker Studio
- Amazon Simple Storage Service (Amazon-S3)
- Echtzeit-Inferenzendpunkt für Amazon SageMaker

Zielarchitektur

Das folgende Diagramm zeigt die Architektur für die Bereitstellung eines SageMaker Amazon-Pipeline-Modellobjekts.

Das Diagramm zeigt den folgenden Workflow:

1. Ein SageMaker Notebook stellt ein Pipeline-Modell bereit.
2. Ein S3-Bucket speichert die Modellartefakte.
3. Amazon ECR ruft die Quellcontainer-Images aus dem S3-Bucket ab.

Tools

AWS-Tools

- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon SageMaker ist ein verwalteter ML-Service, der Ihnen hilft, ML-Modelle zu erstellen und zu trainieren und sie dann in einer produktionsbereiten gehosteten Umgebung bereitzustellen.
- Amazon SageMaker Studio ist eine webbasierte, integrierte Entwicklungsumgebung (IDE) für ML, mit der Sie Ihre ML-Modelle erstellen, trainieren, debuggen, bereitstellen und überwachen können.

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code

Der Code für dieses Muster ist in der GitHub Inference Pipeline with Scikit-Learn und Linear Learner Repository verfügbar.

Epen

Bereiten Sie den Datensatz vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bereiten Sie den Datensatz für Ihre Regressionsaufgabe vor.	Öffnen Sie ein Notizbuch in Amazon SageMaker Studio.
	
	Verwenden Sie den folgenden Beispielcode in Ihrem Notizbuch, um alle erforderl ichen Bibliotheken zu importier en und Ihre Arbeitsumgebung zu initialisieren:
	
	`import sagemaker`
	`from sagemaker import`
	` get_execution_role`
	
	`sagemaker_session =`
	` sagemaker.Session()`
	
	`# Get a SageMaker-`
	`compatible role used`
	` by this Notebook`
	` Instance.`
	`role = get_execu`
	`tion_role()`
	
	`# S3 prefix`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`bucket = sagemaker_session.default_bucket()`
	`prefix = "Scikit-LinearLearner-pipeline-abalone-example"`
	
	Um einen Beispieldatensatz herunterzuladen, fügen Sie Ihrem Notizbuch den folgenden Code hinzu:
	
	`! mkdir abalone_data`
	`! aws s3 cp s3://sagemaker-sample-files/datasets/tabular/uci_abalone/abalone.csv ./abalone_data`
	
	Note
	Das Beispiel in diesem Muster verwendet den Abalone-Datensatz aus dem UCI Machine Learning Repository.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Laden Sie den Datensatz in einen S3-Bucket hoch.	Fügen Sie in dem Notizbuch , in dem Sie Ihren Datensatz zuvor vorbereitet haben, den folgenden Code hinzu, um Ihre Beispieldaten in einen S3-Bucket hochzuladen:
	`WORK_DIRECTORY = "abalone_data"`
	
	`train_input = sagemaker_session.upload_data( path="{}/{}".format(WORK_DIRECTORY, "abalone.csv"), bucket=bucket, key_prefix="{}/{}".format(prefix, "train"), )`
		Data Scientist

Erstellen Sie den Datenpräprozessor mit SKLearn

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie das Skript preprocessor.py vor.	1. Kopieren Sie die Vorverarbeitungslogik aus der Python-Datei im Repository GitHub sklearn_abalone_featurizer.py und fügen Sie den Code dann in eine separate Python-Datei mit dem Namen `sklearn_abalone_featurizer.py` ein. Sie können den Code so ändern, dass	Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	er zu Ihrem benutzerd efinierten Datensatz und Ihrem benutzerdefinierten Workflow passt. 2. Speichern Sie die `sklearn_abalone_fe aturizer.py` Datei im Stammverzeichnis Ihres Projekts (d. h. am selben Ort, an dem Sie Ihr SageMaker Notizbuch ausführen).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie das SKLearn Präprozessor-Objekt.	Um ein SKLearn Präprozessor-Objekt (SKLearn Estimator genannt) zu erstellen, das Sie in Ihre endgültige Inferenz-Pipeline integrieren können, führen Sie den folgenden Code in Ihrem Notizbuch aus: SageMaker
	`from sagemaker.sklearn.estimator import SKLearn`
	
	`FRAMEWORK_VERSION = "0.23-1"`
	`script_path = "sklearn_abalone_featurizer.py"`
	
	`sklearn_preprocessor = SKLearn(`
	`entry_point=script_path,`
	`role=role,`
	`framework_version=FRAMEWORK_VERSION,`
	`instance_type="ml.c4.xlarge",`
	`sagemaker_session=sagemaker_session,`
	`)`
	`sklearn_preprocessor.fit({"train": train_input})`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Testen Sie die Inferenz des Präprozessors.	Um zu überprüfen, ob Ihr Präprozessor korrekt definiert ist, starten Sie einen Batch-Transformationsauftrag, indem Sie den folgenden Code in Ihr Notizbuch eingeben: SageMaker
	`# Define a SKLearn Transformer from the trained SKLearn Estimator`
	`transformer = sklearn_preprocessor.transformer(`
	`instance_count=1, instance_type="ml.m5.xlarge", assemble_with="Line", accept="text/csv"`
	`)`
	
	`# Preprocess training input`
	`transformer.transform(train_input, content_type="text/csv")`
	`print("Waiting for transform job: " + transformer.latest_transform_job.job_name)`
	`transformer.wait()`
	`preprocessed_train = transformer.output_path`	

Erstellen Sie ein Modell für maschinelles Lernen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie ein Modellobjekt.	Um ein Modellobjekt zu erstellen, das auf dem linearen Lernalgorithmus basiert, geben Sie den folgenden Code in Ihr SageMaker Notizbuch ein:
	`import boto3`
	`from sagemaker`
	`.image_uris import`
	` retrieve`
	
	`ll_image = retrieve(`
	`"linear-learner",`
	` boto3.Session().re`
	`gion_name)`
	`s3_ll_output_key`
	`_prefix = "ll_train`
	`ing_output"`
	`s3_ll_output_location`
	` = "s3://{}/{}/{}/{}"`
	`.format(`
	`  bucket, prefix,`
	` s3_ll_output_key_p`
	`refix, "ll_model"`
	`)`
	
	`ll_estimator =`
	` sagemaker.estimato`
	`r.Estimator(`
	`  ll_image,`
	`  role,`
	`  instance_count=1,`
	`  instance_type="ml.`
	`m4.2xlarge",`
	`  volume_size=20,`
	`  max_run=3600,`
	`  input_mode="File",`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> output_path=s3_ll_
	output_location,
	    sagemaker_session=
	sagemaker_session,
	)
	
	ll_estimator.s
	et_hyperparameters
	(feature_dim=10,
	 predictor_type="re
	gressor", mini_batc
	h_size=32)
	
	ll_train_data =
	 sagemaker.inputs.T
	rainingInput(
	    preprocessed_train
	,
	    distribution="Full
	yReplicated",
	    content_type="text
	/csv",
	    s3_data_type="S3Pr
	efix",
	)
	
	data_channels =
	 {"train": ll_train_
	data}
	ll_estimator.fit(inpu
	ts=data_channels,
	 logs=True)</pre>	

	Der obige Code ruft das entsprechende Amazon ECR Docker-Image aus der öffentlichen Amazon ECR Registry für das Modell ab, erstellt ein Schätzerobjekt und verwendet dieses Objekt dann, um	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	das Regressionsmodell zu trainieren.	

Stellen Sie die endgültige Pipeline bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie das Pipeline-Modell bereit.	Um ein Pipeline-Modellobj ekt (d. h. ein Präprozessor-Objekt) zu erstellen und das Objekt bereitzustellen, geben Sie den folgenden Code in Ihr SageMaker Notizbuch ein:
	`from sagemaker.model import Model`
	`from sagemaker.pipeline import PipelineModel`
	`import boto3`
	`from time import gmtime, strftime`
	
	`timestamp_prefix = strftime("%Y-%m-%d-%H-%M-%S", gmtime())`
	
	`scikit_learn_inferencee_model = sklearn_preprocessor.create_model()`
	`linear_learner_model = ll_estimator.create_model()`
	
	`model_name = "inferenc e-pipeline-" + timestamp_prefix`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`endpoint_name = "inference-pipeline-ep-" + timestamp_prefix sm_model = PipelineModel( name=model_name, role=role, models= [scikit_learn_inferencee_model, linear_learner_model] )`
	
	`sm_model.deploy(initial_instance_count=1, instance_type="ml.c4.xlarge", endpoint_name=endpoint_name)`
	
	Note
	Sie können den im Modellobjekt verwendeten Instanztyp an Ihre Bedürfnisse anpassen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Testen Sie die Inferenz.	Um zu überprüfen, ob der Endpunkt ordnungsgemäß funktioniert, führen Sie den folgenden Beispiel-Inferenzcode in Ihrem SageMaker Notizbuch aus:
	`from sagemaker.predictor import Predictor`
	`from sagemaker.serializers import CSVSerializer`
	
	`payload = "M, 0.44, 0.365, 0.125, 0.516, 0.2155, 0.114, 0.155"`
	`actual_rings = 10`
	`predictor = Predictor(`
	`endpoint_name=endpoint_name, sagemaker_session=sagemaker_session, serializer=CSVSerializer()`
	`)`
	
	`print(predictor.predict(payload))`
		Data Scientist

Zugehörige Ressourcen

- Vorverarbeitung von Eingabedaten vor dem Treffen von Prognosen mithilfe von SageMaker Amazon-Inferenz-Pipelines und Scikit-Learn (AWS Machine Learning Learning-Blog)
- Durchgängiges Machine Learning mit Amazon SageMaker (GitHub)

Entwickeln Sie mithilfe von RAG und Prompting fortschrittliche, auf KI basierende Chat-Assistenten ReAct

Erstellt von Praveen Kumar Jeyarajan (AWS), Jundong Qiao (AWS), Kara Yang (AWS), Kiowa Jackson (AWS), Noah Hamilton (AWS) und Shuai Cao (AWS)

Übersicht

In einem typischen Unternehmen sind 70 Prozent seiner Daten in isolierten Systemen gespeichert. Mithilfe generativer, KI-gestützter Chat-Assistenten können Sie mithilfe von Interaktionen in natürlicher Sprache Einblicke und Beziehungen zwischen diesen Datensilos gewinnen. Um das Beste aus generativer KI herauszuholen, müssen die Ergebnisse vertrauenswürdig und genau sein und die verfügbaren Unternehmensdaten beinhalten. Erfolgreiche Chat-Assistenten hängen von folgenden Faktoren ab:

- Generative KI-Modelle (wie Anthropic Claude 2)
- Vektorisierung von Datenquellen
- Fortgeschrittene Argumentationstechniken, wie z. B. das ReAct Framework, als Grundlage für das Modell

Dieses Muster bietet Datenabrufansätze aus Datenquellen wie Amazon Simple Storage Service (Amazon S3) -Buckets, AWS Glue und Amazon Relational Database Service (Amazon RDS). Aus diesen Daten wird Wert gewonnen, indem Retrieval Augmented Generation (RAG) mit Methoden verknüpft wird. chain-of-thought Die Ergebnisse unterstützen komplexe Chat-basierte Assistentengespräche, die sich auf die Gesamtheit der in Ihrem Unternehmen gespeicherten Daten stützen.

Dieses Muster verwendet SageMaker Amazon-Handbücher und Preisdatentabellen als Beispiel, um die Funktionen eines generativen KI-Assistenten auf Chatbasis zu untersuchen. Sie werden einen Chat-basierten Assistenten entwickeln, der Kunden hilft, den SageMaker Service zu bewerten, indem er Fragen zur Preisgestaltung und zu den Funktionen des Dienstes beantwortet. Die Lösung verwendet eine Streamlit-Bibliothek für die Erstellung der Frontend-Anwendung und das LangChain Framework für die Entwicklung des Anwendungs-Backends, das auf einem Large Language Model (LLM) basiert.

Anfragen an den Chat-Assistenten werden zunächst mit einer Absichtsklassifizierung beantwortet, sodass sie an einen von drei möglichen Workflows weitergeleitet werden. Der ausgefeilteste

Arbeitsablauf kombiniert allgemeine Beratung mit komplexen Preisanalysen. Sie können das Muster an Anwendungsfälle in Unternehmen, Unternehmen und der Industrie anpassen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- AWS-Befehlszeilenschnittstelle (AWS CLI) installiert und konfiguriert
- AWS Cloud Development Kit (AWS CDK) Toolkit 2.114.1 oder höher installiert und konfiguriert
- Grundkenntnisse in Python und AWS CDK
- Git installiert
- Docker installiert
- Python 3.11 oder höher installiert und konfiguriert (weitere Informationen finden Sie im Abschnitt Tools)
- Ein aktives AWS-Konto, das mithilfe von AWS CDK gestartet wurde
- Der Zugriff auf die Modelle Amazon Titan und Anthropic Claude ist im Amazon Bedrock-Service aktiviert
- AWS-SicherheitsanmeldedatenAWS_ACCESS_KEY_ID, einschließlich korrekt konfigurierter Anmeldeinformationen in Ihrer Terminalumgebung

Einschränkungen

- LangChain unterstützt nicht jedes LLM für Streaming. Die Modelle von Anthropic Claude werden unterstützt, Modelle von AI21 Labs jedoch nicht.
- Diese Lösung wird auf einem einzigen AWS-Konto bereitgestellt.
- Diese Lösung kann nur in AWS-Regionen eingesetzt werden, in denen Amazon Bedrock und Amazon Kendra verfügbar sind. Informationen zur Verfügbarkeit finden Sie in der Dokumentation für Amazon Bedrock und Amazon Kendra.

Produktversionen

- Python-Version 3.11 oder höher
- Streamlit Version 1.30.0 oder höher
- Streamlit-Chat Version 0.1.1 oder höher

- LangChain Version 0.1.12 oder höher
- AWS CDK Version 2.132.1 oder höher

Architektur

Zieltechnologie-Stack

- Amazon Athena
- Amazon Bedrock
- Amazon Elastic Container Service (Amazon ECS)
- AWS Glue
- AWS Lambda
- Amazon S3
- Amazon Kendra
- Elastic Load Balancing

Zielarchitektur

Der AWS-CDK-Code stellt alle Ressourcen bereit, die für die Einrichtung der Chat-basierten Assistentenanwendung in einem AWS-Konto erforderlich sind. Die in der folgenden Abbildung gezeigte Chat-basierte Assistentenanwendung wurde entwickelt, um verwandte Anfragen von Benutzern zu beantworten SageMaker . Benutzer stellen über einen Application Load Balancer eine Verbindung zu einer VPC her, die einen Amazon ECS-Cluster enthält, der die Streamlit-Anwendung hostet. Eine Orchestrierungs-Lambda-Funktion stellt eine Verbindung zur Anwendung her. S3-Bucket-Datenquellen stellen Daten für die Lambda-Funktion über Amazon Kendra und AWS Glue bereit. Die Lambda-Funktion stellt eine Verbindung zu Amazon Bedrock her, um Anfragen (Fragen) von Chat-basierten Assistentenbenutzern zu beantworten.

1. Die Orchestrierungs-Lambda-Funktion sendet die LLM-Prompt-Anfrage an das Amazon Bedrock-Modell (Claude 2).
2. Amazon Bedrock sendet die LLM-Antwort zurück an die Orchestrierungs-Lambda-Funktion.

Logikfluss innerhalb der Orchestrierungs-Lambda-Funktion

Wenn Benutzer über die Streamlit-Anwendung eine Frage stellen, wird die Orchestrierungs-Lambda-Funktion direkt aufgerufen. Das folgende Diagramm zeigt den Logikfluss, wenn die Lambda-Funktion aufgerufen wird.

- Schritt 1 — Die Eingabe `query` (Frage) wird in eine der drei Absichten eingeteilt:
  - Allgemeine SageMaker Orientierungsfragen
  - Allgemeine Fragen zur SageMaker Preisgestaltung (Schulung/Inferenz)
  - Komplexe Fragen im Zusammenhang mit und zur Preisgestaltung SageMaker
- Schritt 2 — Die Eingabe `query` initiiert einen der drei Dienste:
  - `RAG Retrieval service`, das den relevanten Kontext aus der Amazon Kendra Kendra-Vektordatenbank abruft und das LLM über Amazon Bedrock aufruft, um den abgerufenen Kontext als Antwort zusammenzufassen.
  - `Database Query service`, das das LLM, Datenbank-Metadaten und Beispielzeilen aus relevanten Tabellen verwendet, um die Eingabe in eine SQL-Abfrage umzuwandeln. `query` Der Datenbankabfragedienst führt die SQL-Abfrage für die SageMaker Preisdatenbank über Amazon Athena aus und fasst die Abfrageergebnisse als Antwort zusammen.
  - `In-context ReACT Agent service`, der die Eingabe `query` in mehrere Schritte unterteilt, bevor eine Antwort bereitgestellt wird. Der Agent verwendet `RAG Retrieval service` und `Database Query service` als Hilfsmittel, um während des Argumentationsprozesses relevante Informationen abzurufen. Nachdem der Argumentations- und Handlungsprozess abgeschlossen ist, generiert der Agent die endgültige Antwort als Antwort.
- Schritt 3 — Die Antwort der Orchestrierungs-Lambda-Funktion wird als Ausgabe an die Streamlit-Anwendung gesendet.

Tools

AWS-Services

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon Simple Storage Service (Amazon S3) analysieren können.
- Amazon Bedrock ist ein vollständig verwalteter Service, der Ihnen leistungsstarke Basismodelle (FMs) von führenden KI-Startups und Amazon über eine einheitliche API zur Verfügung stellt.
- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Beenden und Verwalten von Containern in einem Cluster vereinfacht.
- AWS Glue ist ein vollständig verwalteter Service zum Extrahieren, Transformieren und Laden (ETL). Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben. Dieses Muster verwendet einen AWS Glue Glue-Crawler und eine AWS Glue Glue-Datenkatalogtabelle.
- Amazon Kendra ist ein intelligenter Suchdienst, der natürliche Sprachverarbeitung und fortschrittliche Algorithmen für maschinelles Lernen verwendet, um spezifische Antworten auf Suchfragen aus Ihren Daten zurückzugeben.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Traffic auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen.

Code-Repository

Der Code für dieses Muster ist im GitHub genai-bedrock-chatbotRepository verfügbar.

Das Code-Repository enthält die folgenden Dateien und Ordner:

- `assets`Ordner — Die statischen Objekte, das Architekturdiagramm und der öffentliche Datensatz.
- `code/lambda-container`folder — Der Python-Code, der in der Lambda-Funktion ausgeführt wird
- `code/streamlit-app`folder — Der Python-Code, der als Container-Image in Amazon ECS ausgeführt wird
- `tests`folder — Die Python-Dateien, die zum Komponententest der AWS-CDK-Konstrukte ausgeführt werden

- `code/code_stack.py`— Das AWS-CDK-Konstrukt Python-Dateien, die zur Erstellung von AWS-Ressourcen verwendet werden
- `app.py`— Die AWS-CDK-Stack-Python-Dateien, die zur Bereitstellung von AWS-Ressourcen im AWS-Zielkonto verwendet werden
- `requirements.txt`— Die Liste aller Python-Abhängigkeiten, die für AWS CDK installiert werden müssen
- `requirements-dev.txt`— Die Liste aller Python-Abhängigkeiten, die installiert werden müssen, damit AWS CDK die Unit-Test-Suite ausführen kann
- `cdk.json`— Die Eingabedatei zur Bereitstellung von Werten, die zum Hochfahren von Ressourcen erforderlich sind

> **Note**
>
> Der AWS-CDK-Code verwendet L3-Konstrukte (Layer 3) und AWS Identity and Access Management (IAM) -Richtlinien, die von AWS für die Bereitstellung der Lösung verwaltet werden.

Bewährte Methoden

- Das hier bereitgestellte Codebeispiel ist nur für eine proof-of-concept (PoC) oder Pilotdemo vorgesehen. Wenn Sie den Code in die Produktionsumgebung übernehmen möchten, sollten Sie unbedingt die folgenden bewährten Methoden anwenden:
  - Die Amazon S3 S3-Zugriffsprotokollierung ist aktiviert.
  - VPC Flow Logs ist aktiviert.
  - Der Amazon Kendra Enterprise Edition-Index ist aktiviert.
- Richten Sie die Überwachung und Warnung für die Lambda-Funktion ein. Weitere Informationen finden Sie unter Überwachung und Problembehandlung von Lambda-Funktionen. Allgemeine bewährte Methoden für die Arbeit mit Lambda-Funktionen finden Sie in der AWS-Dokumentation.

Epen

AWS-Anmeldeinformationen auf Ihrem lokalen Computer einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Exportieren Sie Variablen für das Konto und die AWS-Region, in der der Stack bereitgestellt wird.	Führen Sie die folgenden Befehle aus, um AWS-Anmeldeinformationen für AWS CDK mithilfe von Umgebungsvariablen bereitzustellen.
	`export CDK_DEFAULT_ACCOUNT=<12 Digit AWS Account Number>`
	`export CDK_DEFAULT_REGION=<region>`
		DevOps Ingenieur, AWS DevOps

Richten Sie das AWS-CLI-Profil ein.	Folgen Sie den Anweisungen in der AWS-Dokumentation, um das AWS-CLI-Profil für das Konto einzurichten.	DevOps Ingenieur, AWS DevOps

So richten Sie Ihre Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repo auf Ihrem lokalen Computer.	Um das Repository zu klonen, führen Sie den folgenden Befehl in Ihrem Terminal aus. `git clone https://github.com/awslabs/genai-bedrock-chatbot.git`	DevOps Ingenieur, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie die virtuelle Python-Umgebung ein und installieren Sie die erforderlichen Abhängigkeiten.	Führen Sie die folgenden Befehle aus, um die virtuelle Python-Umgebung einzurichten.
	`cd genai-bedrock-chatbot`
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	Führen Sie den folgenden Befehl aus, um die erforderlichen Abhängigkeiten einzurichten.
	`pip3 install -r requirements.txt`
		DevOps Ingenieur, AWS DevOps

Richten Sie die AWS-CDK-Umgebung ein und synthetisieren Sie den AWS-CDK-Code.	1. Führen Sie den folgenden Befehl aus, um die AWS-CDK-Umgebung in Ihrem AWS-Konto einzurichten. `cdk bootstrap aws://ACCOUNT-NUMBER/REGION` 2. Führen Sie den Befehl aus, um den Code in eine CloudFormation AWS-Stack-Konfiguration zu konvertieren`cdk synth`.	DevOps Ingenieur, AWS DevOps

Konfigurieren und implementieren Sie die Chat-basierte Assistentenanwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gewähren Sie Zugriff auf das Claude-Modell.	Folgen Sie den Anweisungen in der Amazon Bedrock-Dokumentation, um den Zugriff auf das Anthropic-Claude-Modell für Ihr AWS-Konto zu aktivieren.	AWS DevOps
Stellen Sie Ressourcen im Konto bereit.	Gehen Sie wie folgt vor, um Ressourcen im AWS-Konto mithilfe des AWS-CDK bereitzustellen: 1. Geben Sie im Stammverzeichnis des geklonten Repositorys in der `cdk.json` Datei Eingaben für die `logging` Parameter ein. Beispielwerte sind`INFO`, `DEBUGWARN`, und`ERROR`. Diese Werte definieren Nachrichten auf Protokollebene für die Lambda-Funktion und die Streamlit-Anwendung. 2. Die `app.py` Datei im Stammverzeichnis des geklonten Repositorys enthält den CloudFormation AWS-Stack-Namen, der für die Bereitstellung verwendet wird. Der	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Standard-Stack-Name ist`chatbot-stack` . 3. Führen Sie den Befehl aus, um Ressourcen bereitzustellen`cdk deploy`. Der `cdk deploy` Befehl verwendet L3-Konstrukte, um mehrere Lambda-Funktionen zum Kopieren von Dokumenten und CSV-Datensatzdateien in S3-Buckets zu erstellen. 4. Melden Sie sich nach Abschluss des Befehls bei der AWS-Managementkonsole an, öffnen Sie die CloudFormation Konsole und überprüfen Sie, ob der Stack erfolgreich bereitgestellt wurde. Nach erfolgreicher Bereitstellung können Sie über die im Abschnitt CloudFormation Ausgaben angegebene URL auf die Chat-basierte Assistentenanwendung zugreifen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den AWS Glue Glue-Crawler aus und erstellen Sie die Datenkata logtabelle.	Ein AWS Glue Glue-Crawler wird verwendet, um das Datenschema dynamisch zu halten. Die Lösung erstellt und aktualisiert Partitionen in der AWS Glue Data Catalog-Tabelle, indem sie den Crawler bei Bedarf ausführt. Nachdem die CSV-Datensatzdateien in den S3-Bucket kopiert wurden, führen Sie den AWS Glue Glue-Crawler aus und erstellen Sie das Datenkata log-Tabellenschema zum Testen: 1. Navigieren Sie zur AWS Glue Glue-Konsole. 2. Wählen Sie im Navigationsbereich unter Datenkata log die Option Crawlers aus. 3. Wählen Sie den Crawler mit Suffix aus. `sagemaker-pricing-crawler` 4. Führen Sie den Crawler aus. 5. Nachdem der Crawler erfolgreich ausgeführt wurde, erstellt er eine AWS Glue Data Catalog-Tabelle.	DevOps Ingenieur, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Der AWS-CDK-Code konfiguriert den AWS Glue-Crawler so, dass er bei Bedarf ausgeführt wird. Sie können ihn aber auch so planen, dass er regelmäßig ausgeführt wird.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initiieren Sie die Indizierung von Dokumenten.	Nachdem die Dateien in den S3-Bucket kopiert wurden, verwenden Sie Amazon Kendra, um sie zu crawlen und zu indizieren: 1. Navigieren Sie zur Amazon Kendra Kendra-Konsole. 2. Wählen Sie den Index mit dem Suffix aus `chatbot-index` . 3. Wählen Sie im Navigationsbereich Datenquellen und dann den Datenquellenconnector mit dem Suffix aus `chatbot-index` . 4. Wählen Sie Jetzt synchronisieren, um den Indizierungsvorgang zu starten. **Note** Der AWS-CDK-Code konfiguriert die Amazon Kendra-Indexsynchronisierung so, dass sie bei Bedarf ausgeführt wird. Sie können sie jedoch auch regelmäßig ausführen, indem Sie den Schedule-Parameter verwenden.	AWS DevOps, DevOps Ingenieur

Bereinigen Sie alle AWS-Ressourcen in der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die AWS-Ressourcen.	Nachdem Sie die Lösung getestet haben, bereinigen Sie die Ressourcen: 1. Führen Sie den Befehl aus, um die von der Lösung bereitgestellten AWS-Ressourcen zu entfernen `cdk destroy`. 2. Löschen Sie alle Objekte aus den beiden S3-Buckets und entfernen Sie dann die Buckets. Weitere Informationen finden Sie unter Löschen eines Buckets.	DevOps Ingenieur, AWS DevOps

Fehlerbehebung

Problem	Lösung
AWS CDK gibt Fehler zurück.	Hilfe bei Problemen mit AWS CDK finden Sie unter Behebung häufiger Probleme mit AWS CDK.

Zugehörige Ressourcen

- Amazonas-Grundgestein:
  - Modellzugriff
  - Inferenzparameter für Fundamentmodelle

- Lambda-Funktionen mit Python erstellen
- Erste Schritte mit dem AWS CDK
- Arbeiten mit dem AWS CDK in Python
- Generativer KI-Anwendungsgenerator auf AWS
- LangChain Dokumentation
- Optimierte Dokumentation

Zusätzliche Informationen

AWS CDK-Befehle

Beachten Sie bei der Arbeit mit AWS CDK die folgenden nützlichen Befehle:

- Listet alle Stacks in der App auf

```
cdk ls
```

- Gibt die synthetisierte AWS-Vorlage aus CloudFormation

```
cdk synth
```

- Stellt den Stack für Ihr AWS-Standardkonto und Ihre Region bereit

```
cdk deploy
```

- Vergleicht den bereitgestellten Stack mit dem aktuellen Status

```
cdk diff
```

- Öffnet die AWS CDK-Dokumentation

```
cdk docs
```

- Löscht den CloudFormation Stack und entfernt von AWS bereitgestellte Ressourcen

```
cdk destroy
```

Entwickeln Sie mithilfe von Amazon Bedrock-Agenten und Wissensdatenbanken einen vollautomatischen Chat-basierten Assistenten

Erstellt von Jundong Qiao (AWS), Kara Yang (AWS), Kiowa Jackson (AWS), Noah Hamilton (AWS), Praveen Kumar Jeyarajan (AWS) und Shuai Cao (AWS)

Übersicht

Viele Unternehmen stehen vor Herausforderungen, wenn es darum geht, einen Chat-basierten Assistenten zu entwickeln, der in der Lage ist, verschiedene Datenquellen zu orchestrieren, um umfassende Antworten zu bieten. Dieses Muster bietet eine Lösung für die Entwicklung eines Chat-basierten Assistenten, der Anfragen sowohl aus der Dokumentation als auch aus Datenbanken beantworten kann, und das bei einer einfachen Bereitstellung.

Beginnend mit Amazon Bedrock bietet dieser vollständig verwaltete Service für generative künstliche Intelligenz (KI) eine breite Palette fortschrittlicher Basismodelle (FMs). Dies erleichtert die effiziente Erstellung generativer KI-Anwendungen mit einem starken Fokus auf Datenschutz und Sicherheit. Im Zusammenhang mit dem Abruf von Dokumenten ist die Retrieval Augmented Generation (RAG) ein zentrales Merkmal. Es verwendet Wissensdatenbanken, um FM-Eingabeaufforderungen um kontextrelevante Informationen aus externen Quellen zu erweitern. Ein Amazon OpenSearch Serverless-Index dient als Vektordatenbank hinter den Wissensdatenbanken für Amazon Bedrock. Diese Integration wird durch sorgfältiges, zeitnahes Engineering verbessert, um Ungenauigkeiten zu minimieren und sicherzustellen, dass die Antworten in einer sachlichen Dokumentation verankert sind. Für Datenbankabfragen transformieren Amazon Bedrock Textanfragen in strukturierte SQL-Abfragen, die spezifische Parameter enthalten. FMs Dies ermöglicht den präzisen Abruf von Daten aus Datenbanken, die von AWS Glue Glue-Datenbanken verwaltet werden. Amazon Athena wird für diese Abfragen verwendet.

Um kompliziertere Anfragen zu bearbeiten und umfassende Antworten zu erhalten, sind Informationen erforderlich, die sowohl aus der Dokumentation als auch aus Datenbanken stammen. Agents for Amazon Bedrock ist eine generative KI-Funktion, mit der Sie autonome Agenten erstellen können, die komplexe Aufgaben verstehen und sie für die Orchestrierung in einfachere Aufgaben aufteilen können. Die Kombination der Erkenntnisse aus den vereinfachten Aufgaben, die durch die autonomen Agenten von Amazon Bedrock unterstützt werden, verbessert die Informationssynthese und führt zu gründlicheren und umfassenderen Antworten. Dieses Muster zeigt, wie Sie mithilfe von

Amazon Bedrock und den zugehörigen generativen KI-Diensten und -Funktionen innerhalb einer automatisierten Lösung einen chatbasierten Assistenten erstellen können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Docker, installiert
- AWS Cloud Development Kit (AWS CDK), installiert und in die `us-east-1`AWS-Regionen gestartet `us-west-2`
- AWS CDK Toolkit Version 2.114.1 oder höher, installiert
- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert
- Python Version 3.11 oder höher, installiert
- Aktivieren Sie in Amazon Bedrock den Zugriff auf Claude 2, Claude 2.1, Claude Instant und Titan Embeddings G1 — Text

Einschränkungen

- Diese Lösung wird auf einem einzigen AWS-Konto bereitgestellt.
- Diese Lösung kann nur in AWS-Regionen eingesetzt werden, in denen Amazon Bedrock und Amazon OpenSearch Serverless unterstützt werden. Weitere Informationen finden Sie in der Dokumentation für Amazon Bedrock und Amazon OpenSearch Serverless.

Produktversionen

- LLAMA-Index Version 0.10.6 oder höher
- Sqlalchemy Version 2.0.23 oder höher
- OpenSearch-PY Version 2.4.2 oder höher
- Requests_AWS4Auth Version 1.2.3 oder höher
- AWS SDK for Python (Boto3) Version 1.34.57 oder höher

Architektur

Zieltechnologie-Stack

Das AWS Cloud Development Kit (AWS CDK) ist ein Open-Source-Framework für die Softwareentwicklung, mit dem Cloud-Infrastruktur im Code definiert und über AWS bereitgestellt werden kann. CloudFormation Der in diesem Muster verwendete AWS-CDK-Stack stellt die folgenden AWS-Ressourcen bereit:

- AWS Key Management Service (AWS KMS)
- Amazon Simple Storage Service (Amazon-S3)
- AWS Glue Glue-Datenkatalog für die AWS Glue Glue-Datenbankkomponente
- AWS Lambda
- AWS Identity and Access Management (IAM)
- Amazon OpenSearch Serverlos
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)
- AWS Fargate
- Amazon Virtual Private Cloud (Amazon VPC)
- Application Load Balancer

Zielarchitektur

Das Diagramm zeigt ein umfassendes Cloud-natives AWS-Setup innerhalb einer einzigen AWS-Region unter Verwendung mehrerer AWS-Services. Die primäre Schnittstelle für den Chat-basierten Assistenten ist eine Streamlit-Anwendung, die auf einem Amazon ECS-Cluster gehostet wird. Ein Application Load Balancer verwaltet die Barrierefreiheit. Abfragen, die über diese Schnittstelle gestellt werden, aktivieren die `Invocation` Lambda-Funktion, die dann eine Schnittstelle zu Agenten für Amazon Bedrock herstellt. Dieser Agent beantwortet Benutzeranfragen, indem er entweder die Wissensdatenbanken für Amazon Bedrock konsultiert oder eine `Agent executor` Lambda-Funktion aufruft. Diese Funktion löst nach einem vordefinierten API-Schema eine Reihe von Aktionen aus, die dem Agenten zugeordnet sind. Die Wissensdatenbanken für Amazon Bedrock verwenden einen OpenSearch serverlosen Index als Grundlage für ihre Vektordatenbank. Darüber hinaus generiert die `Agent executor` Funktion SQL-Abfragen, die über Amazon Athena für die AWS Glue Glue-Datenbank ausgeführt werden.

Tools

AWS-Services

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon Simple Storage Service (Amazon S3) analysieren können.
- Amazon Bedrock ist ein vollständig verwalteter Service, der Ihnen leistungsstarke Basismodelle (FMs) von führenden KI-Startups und Amazon über eine einheitliche API zur Verfügung stellt.
- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Beenden und Verwalten von Containern in einem Cluster vereinfacht.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Traffic auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen.
- AWS Glue ist ein vollständig verwalteter Service zum Extrahieren, Transformieren und Laden (ETL). Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben. Dieses Muster verwendet einen AWS Glue Glue-Crawler und eine AWS Glue Glue-Datenkatalogtabelle.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon OpenSearch Serverless ist eine serverlose On-Demand-Konfiguration für Amazon OpenSearch Service. In diesem Muster dient ein OpenSearch serverloser Index als Vektordatenbank für die Wissensdatenbanken für Amazon Bedrock.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere Tools

- Streamlit ist ein Open-Source-Python-Framework zur Erstellung von Datenanwendungen.

Code-Repository

Der Code für dieses Muster ist im GitHub genai-bedrock-agent-chatbotRepository verfügbar. Das Code-Repository enthält die folgenden Dateien und Ordner:

- `assets`Ordner — Die statischen Elemente, wie das Architekturdiagramm und der öffentliche Datensatz.
- `code/lambdas/action-lambda`folder — Der Python-Code für die Lambda-Funktion, die als Aktion für den Amazon Bedrock-Agenten fungiert.
- `code/lambdas/create-index-lambda`folder — Der Python-Code für die Lambda-Funktion, die den OpenSearch Serverless-Index erstellt.
- `code/lambdas/invoke-lambda`folder — Der Python-Code für die Lambda-Funktion, die den Amazon Bedrock-Agenten aufruft, der direkt aus der Streamlit-Anwendung aufgerufen wird.
- `code/lambdas/update-lambda`folder — Der Python-Code für die Lambda-Funktion, die Ressourcen aktualisiert oder löscht, nachdem die AWS-Ressourcen über das AWS-CDK bereitgestellt wurden.
- `code/layers/boto3_layer`folder — Der AWS-CDK-Stack, der eine Boto3-Ebene erstellt, die von allen Lambda-Funktionen gemeinsam genutzt wird.
- `code/layers/opensearch_layer`folder — Der AWS-CDK-Stack, der eine OpenSearch serverlose Schicht erstellt, die alle Abhängigkeiten installiert, um den Index zu erstellen.
- `code/streamlit-app`folder — Der Python-Code, der als Container-Image in Amazon ECS ausgeführt wird
- `code/code_stack.py`— Das AWS CDK erstellt Python-Dateien, die AWS-Ressourcen erstellen.
- `app.py`— Der AWS-CDK-Stapel von Python-Dateien, die AWS-Ressourcen im AWS-Zielkonto bereitstellen.
- `requirements.txt`— Die Liste aller Python-Abhängigkeiten, die für das AWS-CDK installiert werden müssen.
- `cdk.json`— Die Eingabedatei zur Bereitstellung der Werte, die für die Erstellung von Ressourcen erforderlich sind. Außerdem können Sie die Lösung in den `context/config` Feldern entsprechend anpassen. Weitere Informationen zur Anpassung finden Sie im Abschnitt Zusätzliche Informationen.

Bewährte Methoden

- Das hier bereitgestellte Codebeispiel dient nur proof-of-concept (PoC) oder Pilotzwecken. Wenn Sie den Code für die Produktion verwenden möchten, sollten Sie unbedingt die folgenden bewährten Methoden anwenden:
  - Amazon S3 S3-Zugriffsprotokollierung aktivieren

  - VPC-Flow-Logs aktivieren
- Richten Sie die Überwachung und Warnung für die Lambda-Funktionen ein. Weitere Informationen finden Sie unter Überwachung und Problembehandlung von Lambda-Funktionen. Bewährte Methoden finden Sie unter Bewährte Methoden für die Arbeit mit AWS Lambda Lambda-Funktionen.

Epen

AWS-Anmeldeinformationen auf Ihrer lokalen Workstation einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Exportieren Sie Variablen für das Konto und die Region.	Führen Sie die folgenden Befehle aus, um AWS-Anmeldeinformationen für das AWS-CDK mithilfe von Umgebungsvariablen bereitzustellen.
	`export CDK_DEFAULT_ACCOUNT=<12-digit AWS account number>`
	`export CDK_DEFAULT_REGION=<Region>`
		AWS DevOps, DevOps Ingenieur

Richten Sie das AWS-CLI mit dem Namen profile ein.	Um das benannte AWS-CLI-Profil für das Konto einzurichten, folgen Sie den Anweisungen unter Konfiguration und Einstellungen der Anmeldeinformationsdatei.	AWS DevOps, DevOps Ingenieur

So richten Sie Ihre Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repo auf Ihre lokale Workstation.	Um das Repository zu klonen, führen Sie den folgenden Befehl in Ihrem Terminal aus. `git clone https://github.com/awslabs/genai-bedrock-agent-chatbot.git`	DevOps Ingenieur, AWS DevOps

Richten Sie die virtuelle Python-Umgebung ein.	Führen Sie die folgenden Befehle aus, um die virtuelle Python-Umgebung einzurichten.
	`cd genai-bedrock-agent-chatbot`
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	Führen Sie den folgenden Befehl aus, um die erforderlichen Abhängigkeiten einzurichten.
	`pip3 install -r requirements.txt`
		DevOps Ingenieur, AWS DevOps

Richten Sie die AWS-CDK-Umgebung ein.	Führen Sie den Befehl `cdk synth` aus, um den Code in eine CloudFormation AWS-Vorlage zu konvertieren.	AWS DevOps, DevOps Ingenieur

Konfiguration und Bereitstellung der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Ressourcen im Konto bereit.	Gehen Sie wie folgt vor, um Ressourcen im AWS-Konto mithilfe des AWS-CDK bereitzustellen: 1. Geben Sie im Stammverz eichnis des geklonten Repositorys in der `cdk.json` Datei Eingaben für die Protokollierungspa rameter ein. Beispielwerte sind`INFO`, `DEBUGWARN`, und`ERROR`. Diese Werte definieren Nachrichten auf Protokoll ebene für die Lambda-Fu nktionen und die Streamlit-Anwendung. 2. Die `cdk.json` Datei im Stammverzeichnis des geklonten Repositorys enthält den CloudForm ation AWS-Stack-Namen, der für die Bereitstellung verwendet wird. Der Standard-Stack-Name ist`chatbot-stack` . Der Standardname des Amazon Bedrock-Agenten ist`ChatbotBedrockAgen t` , und der Standard-Alias für Amazon Bedrock-A	DevOps Ingenieur, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	genten ist. `Chatbot_Agent` 3. Führen Sie den Befehl aus, um Ressourcen bereitzustellen. `cdk deploy` Der `cdk deploy` Befehl verwendet Layer-3-Konstrukte, um mehrere Lambda-Funktionen zum Kopieren von Dokumenten und CSV-Datensatzdateien in S3-Buckets zu erstellen. Außerdem werden der Amazon Bedrock-Agent, die Wissensdatenbanken und die `Action group` Lambda-Funktion für den Amazon Bedrock-Agenten bereitgestellt. 4. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation/. 5. Vergewissern Sie sich, dass der Stack erfolgreich bereitgestellt wurde. Anweisungen finden Sie unter Überprüfen Ihres Stacks auf der CloudFormation AWS-Konsole.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Nach erfolgreicher Bereitstellung können Sie über die URL auf der Registerkarte Outputs in der Konsole auf die Chat-basierte Assistentenanwendung zugreifen. CloudFormation	

Bereinigen Sie alle AWS-Ressourcen in der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die AWS-Ressourcen.	Nachdem Sie die Lösung getestet haben, führen Sie den Befehl aus, um die Ressourcen zu bereinigen`cdk destroy`.	AWS DevOps, DevOps Ingenieur

Zugehörige Ressourcen

AWS-Dokumentation

- Ressourcen von Amazon Bedrock:
  - Modellzugriff
  - Inferenzparameter für Fundamentmodelle
  - Agenten für Amazon Bedrock
  - Wissensdatenbanken für Amazon Bedrock
- Lambda-Funktionen mit Python erstellen
- AWS-CDK-Ressourcen:
  - Erste Schritte mit dem AWS CDK
  - Behebung häufiger AWS-CDK-Probleme
  - Arbeiten mit dem AWS-CDK in Python
- Generativer KI-Anwendungsgenerator auf AWS

Andere AWS-Ressourcen

- Vector Engine für Amazon OpenSearch Serverless

Sonstige Ressourcen

- LlamaIndex Dokumentation
- Rationalisierte Dokumentation

Zusätzliche Informationen

Passen Sie den Chat-basierten Assistenten mit Ihren eigenen Daten an

Folgen Sie diesen strukturierten Richtlinien, um Ihre benutzerdefinierten Daten für die Bereitstellung der Lösung zu integrieren. Diese Schritte sollen einen nahtlosen und effizienten Integrationsprozess gewährleisten, sodass Sie die Lösung effektiv mit Ihren maßgeschneiderten Daten implementieren können.

Für die Datenintegration in der Wissensdatenbank

Datenaufbereitung

1. Suchen Sie das `assets/knowledgebase_data_source/` Verzeichnis.
2. Platzieren Sie Ihren Datensatz in diesem Ordner.

Anpassungen der Konfiguration

1. Öffnen Sie die `cdk.json` Datei.
2. Navigieren Sie zu dem `context/configure/paths/knowledgebase_file_name` Feld und aktualisieren Sie es dann entsprechend.
3. Navigieren Sie zu dem `bedrock_instructions/knowledgebase_instruction` Feld, und aktualisieren Sie es dann, damit es die Nuancen und den Kontext Ihres neuen Datensatzes genau wiedergibt.

Für die Integration von Strukturdaten

Organisation der Daten

1. Erstellen Sie innerhalb des `assets/data_query_data_source/` Verzeichnisses ein Unterverzeichnis, z. B. `tabular_data`
2. Platzieren Sie Ihren strukturierten Datensatz (akzeptable Formate umfassen CSV, JSON, ORC und Parquet) in diesem neu erstellten Unterordner.
3. Wenn Sie eine Verbindung zu einer vorhandenen Datenbank herstellen, aktualisieren Sie die Funktion `create_sql_engine()` unter So stellen Sie eine Verbindung `code/lambda/action-lambda/build_query_engine.py` zu Ihrer Datenbank her.

Konfiguration und Code-Updates

1. Aktualisieren Sie das `context/configure/paths/athena_table_data_prefix` Feld in der `cdk.json` Datei so, dass es dem neuen Datenpfad entspricht.
2. Überarbeiten Sie, `code/lambda/action-lambda/dynamic_examples.csv` indem Sie neue text-to-SQL Beispiele einbeziehen, die Ihrem Datensatz entsprechen.
3. Überarbeiten Sie`code/lambda/action-lambda/prompt_templates.py`, um die Attribute Ihres strukturierten Datensatzes widerzuspiegeln.
4. Aktualisieren Sie das `context/configure/bedrock_instructions/action_group_description` Feld in der `cdk.json` Datei, um den Zweck und die Funktionalität der `Action group` Lambda-Funktion zu erläutern.
5. Erläutern Sie in der `assets/agent_api_schema/artifacts_schema.json` Datei die neuen Funktionen Ihrer `Action group` Lambda-Funktion.

Allgemeines Update

Geben Sie in der `cdk.json` Datei im `context/configure/bedrock_instructions/agent_instruction` Abschnitt eine umfassende Beschreibung der beabsichtigten Funktionalität und des Entwurfszwecks des Amazon Bedrock-Agenten unter Berücksichtigung der neu integrierten Daten.

Dokumentieren Sie institutionelles Wissen anhand von Spracheingaben mithilfe von Amazon Bedrock und Amazon Transcribe

Erstellt von Praveen Kumar Jeyarajan (AWS), Jundong Qiao (AWS), Megan Wu (AWS) und Rajiv Upadhyay (AWS)

Übersicht

Die Erfassung von institutionellem Wissen ist für den Erfolg und die Widerstandsfähigkeit von Organisationen von größter Bedeutung. Institutionelles Wissen steht für das kollektive Wissen, die Erkenntnisse und die Erfahrungen, die Mitarbeiter im Laufe der Zeit gesammelt haben. Diese sind oft stillschweigend und werden informell weitergegeben. Diese Fülle an Informationen umfasst einzigartige Ansätze, bewährte Verfahren und Lösungen für komplizierte Probleme, die möglicherweise an anderer Stelle nicht dokumentiert sind. Durch die Formalisierung und Dokumentation dieses Wissens können Unternehmen das institutionelle Gedächtnis bewahren, Innovationen fördern, Entscheidungsprozesse verbessern und die Lernkurven neuer Mitarbeiter beschleunigen. Darüber hinaus fördert es die Zusammenarbeit, befähigt Einzelpersonen und fördert eine Kultur der kontinuierlichen Verbesserung. Letztlich hilft die Nutzung von institutionellem Wissen Unternehmen dabei, ihr wertvollstes Kapital — die kollektive Intelligenz ihrer Belegschaft — zu nutzen, um Herausforderungen zu bewältigen, Wachstum voranzutreiben und Wettbewerbsvorteile in dynamischen Geschäftsumgebungen zu wahren.

Dieses Muster erklärt, wie institutionelles Wissen mithilfe von Sprachaufzeichnungen von leitenden Mitarbeitern erfasst werden kann. Es verwendet Amazon Transcribe und Amazon Bedrock für die systematische Dokumentation und Überprüfung. Indem Sie dieses informelle Wissen dokumentieren, können Sie es bewahren und an nachfolgende Mitarbeiterkohorten weitergeben. Dieses Bestreben unterstützt betriebliche Exzellenz und verbessert die Effektivität von Schulungsprogrammen durch die Einbeziehung von praktischem Wissen, das durch direkte Erfahrung erworben wurde.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Docker, installiert

- AWS Cloud Development Kit (AWS CDK) Version 2.114.1 oder höher, installiert und in die AWS-Regionen oder als Bootstrapping ausgeführt `us-east-1` `us-west-2`
- AWS CDK Toolkit Version 2.114.1 oder höher, installiert
- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert
- Python Version 3.12 oder höher, installiert
- Berechtigungen zum Erstellen von Ressourcen für Amazon Transcribe, Amazon Bedrock, Amazon Simple Storage Service (Amazon S3) und AWS Lambda

Einschränkungen

- Diese Lösung wird auf einem einzigen AWS-Konto bereitgestellt.
- Diese Lösung kann nur in AWS-Regionen eingesetzt werden, in denen Amazon Bedrock und Amazon Transcribe verfügbar sind. Informationen zur Verfügbarkeit finden Sie in der Dokumentation für Amazon Bedrock und Amazon Transcribe.
- Die Audiodateien müssen in einem Format vorliegen, das Amazon Transcribe unterstützt. Eine Liste der unterstützten Formate finden Sie unter Medienformate in der Transcribe-Dokumentation.

Produktversionen

- AWS-SDK SDK for Python (Boto3) Version 1.34.57 oder höher
- LangChain Version 0.1.12 oder höher

Architektur

Die Architektur stellt einen serverlosen Workflow auf AWS dar. AWS Step Functions orchestriert Lambda-Funktionen für die Audioverarbeitung, Textanalyse und Dokumentgenerierung. Das folgende Diagramm zeigt den Step Functions Functions-Workflow, der auch als Zustandsmaschine bezeichnet wird.

Jeder Schritt in der Zustandsmaschine wird von einer eigenen Lambda-Funktion behandelt. Im Folgenden sind die Schritte im Prozess der Dokumentgenerierung aufgeführt:

1. Die `preprocess` Lambda-Funktion validiert die an Step Functions übergebenen Eingaben und listet alle Audiodateien auf, die im angegebenen Amazon S3 S3-URI-Ordnerpfad vorhanden sind.

Downstream-Lambda-Funktionen im Workflow verwenden die Dateiliste, um das Dokument zu validieren, zusammenzufassen und zu generieren.

2. Die `transcribe` Lambda-Funktion verwendet Amazon Transcribe, um Audiodateien in Texttranskripte umzuwandeln. Diese Lambda-Funktion ist dafür verantwortlich, den Transkriptionsprozess einzuleiten und Sprache präzise in Text umzuwandeln, der dann für die nachfolgende Verarbeitung gespeichert wird.
3. Die `validate` Lambda-Funktion analysiert die Texttranskripte und bestimmt die Relevanz der Antworten auf die ersten Fragen. Durch die Verwendung eines großen Sprachmodells (LLM) über Amazon Bedrock werden themenbezogene Antworten identifiziert und von themenfremden Antworten getrennt.
4. Die `summarize` Lambda-Funktion verwendet Amazon Bedrock, um eine kohärente und präzise Zusammenfassung der themenbezogenen Antworten zu erstellen.
5. Die `generate` Lambda-Funktion fasst die Zusammenfassungen zu einem gut strukturierten Dokument zusammen. Es kann das Dokument gemäß vordefinierten Vorlagen formatieren und alle zusätzlichen erforderlichen Inhalte oder Daten enthalten.
6. Wenn eine der Lambda-Funktionen ausfällt, erhalten Sie eine E-Mail-Benachrichtigung über Amazon Simple Notification Service (Amazon SNS).

Während dieses Prozesses stellt AWS Step Functions sicher, dass jede Lambda-Funktion in der richtigen Reihenfolge initiiert wird. Diese Zustandsmaschine kann parallel verarbeitet werden, um die Effizienz zu erhöhen. Ein Amazon S3 S3-Bucket fungiert als zentrales Speicher-Repository und unterstützt den Arbeitsablauf durch die Verwaltung der verschiedenen beteiligten Medien- und Dokumentenformate.

Tools

AWS-Services

- Amazon Bedrock ist ein vollständig verwalteter Service, der Ihnen leistungsstarke Basismodelle (FMs) von führenden KI-Startups und Amazon über eine einheitliche API zur Verfügung stellt.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Step Functions ist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen.
- Amazon Transcribe ist ein automatischer Spracherkennungsdienst, der Modelle für maschinelles Lernen verwendet, um Audio in Text umzuwandeln.

Andere Tools

- LangChainist ein Framework für die Entwicklung von Anwendungen, die auf großen Sprachmodellen basieren (LLMs).

Code-Repository

Der Code für dieses Muster ist im GitHub genai-knowledge-captureRepository verfügbar.

Das Code-Repository enthält die folgenden Dateien und Ordner:

- `assets`Ordner — Die statischen Ressourcen für die Lösung, z. B. das Architekturdiagramm und der öffentliche Datensatz
- `code/lambdas`folder — Der Python-Code für alle Lambda-Funktionen
  - `code/lambdas/generate`folder — Der Python-Code, der aus den zusammengefassten Daten im S3-Bucket ein Dokument generiert
  - `code/lambdas/preprocess`folder — Der Python-Code, der die Eingaben für die Step Functions Functions-Zustandsmaschine verarbeitet
  - `code/lambdas/summarize`folder — Der Python-Code, der die transkribierten Daten mithilfe des Amazon Bedrock-Service zusammenfasst
  - `code/lambdas/transcribe`folder — Der Python-Code, der Sprachdaten (Audiodatei) mithilfe von Amazon Transcribe in Text konvertiert
  - `code/lambdas/validate`folder — Der Python-Code, der überprüft, ob sich alle Antworten auf dasselbe Thema beziehen
- `code/code_stack.py`— Die AWS-CDK-Konstrukt-Python-Datei, die zur Erstellung von AWS-Ressourcen verwendet wird

- `app.py`— Die Python-Datei der AWS-CDK-App, die zur Bereitstellung von AWS-Ressourcen im AWS-Zielkonto verwendet wird
- `requirements.txt`— Die Liste aller Python-Abhängigkeiten, die für das AWS-CDK installiert werden müssen
- `cdk.json`— Die Eingabedatei zur Bereitstellung von Werten, die für die Erstellung von Ressourcen erforderlich sind

Bewährte Methoden

Das bereitgestellte Codebeispiel dient nur proof-of-concept (PoC) oder Pilotzwecken. Wenn Sie die Lösung in der Produktion einsetzen möchten, wenden Sie die folgenden bewährten Methoden an:

- Amazon S3 S3-Zugriffsprotokollierung aktivieren
- VPC-Flow-Logs aktivieren

Epen

AWS-Anmeldeinformationen auf Ihrer lokalen Workstation einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Exportieren Sie Variablen für das Konto und die AWS-Region.	Führen Sie die folgenden Befehle aus, um AWS-Anmeldeinformationen für das AWS-CDK mithilfe von Umgebungsvariablen bereitzustellen.
	`export CDK_DEFAULT_ACCOUNT=<12-digit AWS account number>`
	`export CDK_DEFAULT_REGION=<Region>`
		AWS DevOps, DevOps Ingenieur

Richten Sie das AWS-CLI mit dem Namen profile ein.	Um das benannte AWS-CLI-Profil für das Konto einzurichten, folgen Sie den Anweisung	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en unter Konfiguration und Einstellungen der Anmeldeinformationsdatei.	

So richten Sie Ihre Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repo auf Ihre lokale Workstation.	Um das genai-knowledge-capture Repository zu klonen, führen Sie den folgenden Befehl in Ihrem Terminal aus. `git clone https://github.com/aws-samples/genai-knowledge-capture`	AWS DevOps, DevOps Ingenieur
(Optional) Ersetzen Sie die Audiodateien.	Gehen Sie wie folgt vor, um die Beispielanwendung so anzupassen, dass sie Ihre eigenen Daten einbezieht: 1. Navigieren Sie zu dem `assets/audio_samples` Ordner im geklonten Repository. 2. Löschen Sie die Ordner, die die Beispiel-Audiodateien enthalten. 3. Erstellen Sie einen Ordner für jedes Thema, das Sie analysieren möchten.	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Übertragen Sie Ihre Audiodateien in die entsprechenden Ordner.	

Richten Sie die virtuelle Python-Umgebung ein.	Führen Sie die folgenden Befehle aus, um die virtuelle Python-Umgebung einzurichten.
	`cd genai-knowledge-capture`
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	`pip install -r requirements.txt`
		AWS DevOps, DevOps Ingenieur

Synthetisieren Sie den AWS-CDK-Code.	Führen Sie den folgenden Befehl aus, um den Code in eine CloudFormation AWS-Stack-Konfiguration zu konvertieren. `cdk synth`	AWS DevOps, DevOps Ingenieur

Konfiguration und Bereitstellung der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Zugriff auf das Basismodell bereit.	Aktivieren Sie den Zugriff auf das Modell Anthropic Claude 3 Sonnet für Ihr AWS-Konto. Anweisungen finden Sie in der Bedrock-Dokumentation unter Modellzugriff hinzufügen.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Ressourcen im Konto bereit.	Gehen Sie wie folgt vor, um Ressourcen im AWS-Konto mithilfe des AWS-CDK bereitzustellen: 1. (Optional) Aktualisieren Sie im Stammverzeichnis des geklonten Repositorys in der `app.py` Datei den CloudFormation AWS-Stack -Namen. Der Standard-Stack-Name lautet`genai-knowledge-capture-stack` . 2. Führen Sie den Befehl aus, um Ressourcen bereitzustellen`cdk deploy`. Der `cdk deploy` Befehl verwendet Layer-3-Konstrukte, um eine Reihe von Lambda-Funktionen, einen S3-Bucket, ein Amazon SNS SNS-Thema und eine Step Functions Functions-Zustandsmaschine zu erstellen. Die Audiodateien im `assets/audio_samples` Ordner werden während der Bereitstellung in den S3-Bucket kopiert. 3. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dann die CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation/. 4. Vergewissern Sie sich, dass der Stack erfolgreich bereitgestellt wurde. Anweisungen finden Sie unter Überprüfen Ihres Stacks auf der CloudFormation AWS-Konsole.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Abonnieren Sie das Amazon-SNS-Thema.	Gehen Sie wie folgt vor, um das Amazon SNS SNS-Thema für Benachrichtigungen zu abonnieren: 1. Wählen Sie in der CloudFormation Konsole im Navigationsbereich Stacks aus. 2. Wählen Sie den `genai-knowledge-capture-stack` Stapel aus. 3. Wählen Sie die Registerkarte Outputs. 4. Suchen Sie den Namen des Amazon SNS SNS-Themas mit dem Schlüssel `SNSTopicName` . 5. Konfigurieren Sie eine E-Mail-Adresse für den Empfang von Benachrichtigungen, indem Sie den Anweisungen unter Abonnieren einer E-Mail-Adresse für ein Amazon SNS SNS-Thema folgen.	Allgemeines AWS

Testen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Zustandsmaschine aus.	1. Öffnen Sie die Step Functions Functions-Konsole. 2. Wählen Sie auf der Seite State Machines die Option genai-knowledge-capture-stack-state-machine. 3. Wählen Sie Start execution (Ausführung starten) aus. 4. (Optional) Geben Sie im Feld Name einen Namen für die Ausführung ein. 5. Geben Sie im Eingabebereich das folgende JSON-Objekt ein, indem Sie den Platzhaltertext ersetzen. Dabei gilt: • <Name>ist der Name, den Sie dem Dokument geben möchten. • <S3 bucket name>ist der Name des Amazon S3 S3-Buckets, der die Audiodateien enthält. • <Folder path>ist das Verzeichnis, das die Audiodateien enthält. `{ "documentName": "<Name>",`	App-Entwickler, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"audioFileFolderUri": "s3://<S3 bucket name>/<Folder path>"
	}</pre>
	6. Wählen Sie Start Execution aus.
	7. Überprüfen Sie auf der Seite mit den Ausführungsdetails die Ergebnisse und warten Sie, bis die Ausführung abgeschlossen ist.	

Bereinigen Sie alle AWS-Ressourcen in der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die AWS-Ressourcen.	Nachdem Sie die Lösung getestet haben, bereinigen Sie die Ressourcen: 1. Löschen Sie alle Objekte aus dem S3-Bucket und anschließend den Bucket. Weitere Informationen finden Sie unter Löschen eines Buckets. 2. Führen Sie im geklonten Repository den Befehl `cdk destroy` aus.	AWS DevOps, DevOps Ingenieur

Zugehörige Ressourcen

AWS-Dokumentation

- Ressourcen von Amazon Bedrock:
  - Modellzugriff
  - Inferenzparameter für Fundamentmodelle
- AWS-CDK-Ressourcen:
  - Erste Schritte mit dem AWS CDK
  - Arbeiten mit dem AWS-CDK in Python
  - Behebung häufiger AWS-CDK-Probleme
  - Toolkit-Befehle
- Ressourcen für AWS Step Functions:
  - Erste Schritte mit AWS Step Functions
  - Fehlersuche
- Lambda-Funktionen mit Python erstellen
- Generativer KI-Anwendungsgenerator auf AWS

Sonstige Ressourcen

- LangChain Dokumentation

Generieren Sie mit Amazon Personalize personalisierte und neu eingestufte Empfehlungen

Erstellt von Mason Cahill (AWS), Matthew Chasse (AWS) und Tayo Olajide (AWS)

Übersicht

Dieses Muster zeigt Ihnen, wie Sie Amazon Personalize verwenden, um personalisierte Empfehlungen — einschließlich neu eingestufter Empfehlungen — für Ihre Benutzer zu generieren, die auf der Erfassung von Benutzerinteraktionsdaten in Echtzeit von diesen Benutzern basieren. Das in diesem Muster verwendete Beispielszenario basiert auf einer Website zur Adoption von Haustieren, die anhand ihrer Interaktionen Empfehlungen für ihre Benutzer generiert (z. B. welche Haustiere ein Benutzer besucht). Anhand des Beispielszenarios lernen Sie, Amazon Kinesis Data Streams zur Erfassung von Interaktionsdaten, AWS Lambda zur Generierung von Empfehlungen und zur Neurangierung der Empfehlungen und Amazon Data Firehose zum Speichern der Daten in einem Amazon Simple Storage Service (Amazon S3) -Bucket zu verwenden. Sie lernen auch, AWS Step Functions zu verwenden, um eine Zustandsmaschine zu erstellen, die die Lösungsversion (d. h. ein trainiertes Modell) verwaltet, die Ihre Empfehlungen generiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit einem Bootstrapping des AWS Cloud Development Kit (AWS CDK)
- AWS-Befehlszeilenschnittstelle (AWS CLI) mit konfigurierten Anmeldeinformationen
- Python 3.9

Produktversionen

- Python 3.9
- AWS CDK 2.23.0 oder höher
- AWS CLI 2.7.27 oder höher

Architektur

Technologie-Stack

- Amazon Data Firehose
- Amazon Kinesis Data Streams
- Amazon Personalize
- Amazon Simple Storage Service (Amazon-S3)
- AWS-Cloud-Entwicklungskit (AWS CDK)
- AWS-Befehlszeilenschnittstelle (AWS Command Line Interface, AWS CLI)
- AWS Lambda
- AWS Step Functions

Zielarchitektur

Das folgende Diagramm zeigt eine Pipeline für die Aufnahme von Echtzeitdaten in Amazon Personalize. Die Pipeline verwendet diese Daten dann, um personalisierte und neu eingestufte Empfehlungen für Benutzer zu generieren.

Das Diagramm zeigt den folgenden Workflow:

1. Kinesis Data Streams nimmt Benutzerdaten in Echtzeit auf (z. B. Ereignisse wie besuchte Haustiere) zur Verarbeitung durch Lambda und Firehose.
2. Eine Lambda-Funktion verarbeitet die Datensätze aus Kinesis Data Streams und führt einen API-Aufruf durch, um die Benutzerinteraktion im Datensatz einem Event-Tracker in Amazon Personalize hinzuzufügen.
3. Eine zeitbasierte Regel ruft eine Step Functions Functions-Zustandsmaschine auf und generiert mithilfe der Ereignisse aus dem Event-Tracker in Amazon Personalize neue Lösungsversionen für die Empfehlungs- und Re-Ranking-Modelle.
4. Amazon Personalize Personalize-Kampagnen werden von der State Machine aktualisiert, um die neue Lösungsversion zu verwenden.
5. Lambda ordnet die Liste der empfohlenen Artikel neu an, indem es die Amazon Personalize-Kampagne zur Neurangierung aufruft.
6. Lambda ruft die Liste der empfohlenen Artikel ab, indem es die Amazon Personalize Personalize-Empfehlungskampagne aufruft.
7. Firehose speichert die Ereignisse in einem S3-Bucket, wo sie als historische Daten abgerufen werden können.

Tools

AWS-Tools

- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Amazon Data Firehose unterstützt Sie bei der Bereitstellung von Echtzeit-Streaming-Daten an andere AWS-Services, benutzerdefinierte HTTP-Endpunkte und HTTP-Endpunkte, die von unterstützten Drittanbietern betrieben werden.
- Amazon Kinesis Data Streams hilft Ihnen dabei, große Datenströme in Echtzeit zu sammeln und zu verarbeiten.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Personalize ist ein vollständig verwalteter Service für maschinelles Lernen (ML), mit dem Sie auf der Grundlage Ihrer Daten Artikelempfehlungen für Ihre Benutzer generieren können.
- AWS Step Functions ist ein serverloser Orchestrierungsservice, mit dem Sie Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen.

Andere Tools

- pytest ist ein Python-Framework zum Schreiben kleiner, lesbarer Tests.
- Python ist eine Allzweck-Computerprogrammiersprache.

Code

Der Code für dieses Muster ist im GitHub Animal Recommender-Repository verfügbar. Sie können die CloudFormation AWS-Vorlage aus diesem Repository verwenden, um die Ressourcen für die Beispiellösung bereitzustellen.

> **Note**
>
> Die Versionen der Amazon Personalize Personalize-Lösung, der Event Tracker und die Kampagnen werden durch benutzerdefinierte Ressourcen (innerhalb der Infrastruktur) unterstützt, die die systemeigenen CloudFormation Ressourcen erweitern.

Epen

Schaffen Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine isolierte Python-Umgebung.	Mac/Linux-Setup 1. Um manuell eine virtuelle Umgebung zu erstellen, führen Sie den `$ python3 -m venv .venv` Befehl von Ihrem Terminal aus. 2. Führen Sie nach Abschluss des Init-Vorgangs den `$ source .venv/bin/activate` Befehl aus, um die virtuelle Umgebung zu aktivieren. Windows-Setup Um manuell eine virtuelle Umgebung zu erstellen, führen Sie den `% .venv\Scripts\activate.bat` Befehl von Ihrem Terminal aus.	DevOps Ingenieur
Synthetisieren Sie die CloudFormation Vorlage.	1. Um die erforderlichen Abhängigkeiten zu installie	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ren, führen Sie den `$ pip install -r requirements.txt` Befehl von Ihrem Terminal aus. 2. Legen Sie in der AWS-CLI die folgenden Umgebungsvariablen fest: • `export ACCOUNT_ID=123456789` • `export CDK_DEPLOY_REGION=us-east-1` • `export CDK_ENVIRONMENT=dev` 3. Aktualisieren Sie die `config/{env}.yml` Datei so, `vpcId` dass sie mit Ihrer Virtual Private Cloud (VPC) -ID übereinstimmt. 4. Führen Sie den Befehl aus, um die CloudFormation Vorlage für diesen Code zu synthetisieren. `$ cdk synth` **Note** `CDK_ENVIRONMENT` Bezieht sich in Schritt 2 auf die	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`config/{env}.yml` Datei.	
Stellen Sie Ressourcen bereit und schaffen Sie eine Infrastruktur.	Führen Sie den `./deploy.sh` Befehl von Ihrem Terminal aus aus, um die Lösungsressourcen bereitzustellen. Dieser Befehl installiert die erforderlichen Python-Abhängigkeiten. Ein Python-Skript erstellt einen S3-Bucket und einen AWS Key Management Service (AWS KMS) -Schlüssel und fügt dann die Startdaten für die ersten Modellerstellungen hinzu. Schließlich wird das Skript ausgeführt, `cdk deploy` um die verbleibende Infrastruktur zu erstellen. **Note** Das anfängliche Modelltraining findet während der Stack-Erstellung statt. Es kann bis zu zwei Stunden dauern, bis der Stack fertig erstellt ist.	DevOps Ingenieur

Zugehörige Ressourcen

- Tierempfehler () GitHub
- AWS-CDK-Referenzdokumentation
- Boto3-Dokumentation
- Optimieren Sie personalisierte Empfehlungen für eine Geschäftskennzahl Ihrer Wahl mit Amazon Personalize (AWS Machine Learning Blog)

Zusätzliche Informationen

Beispiele für Payloads und Antworten

Empfehlung Lambda-Funktion

Um Empfehlungen abzurufen, senden Sie eine Anfrage an die Lambda-Empfehlungsfunktion mit einer Nutzlast im folgenden Format:

```
{
  "userId": "3578196281679609099",
  "limit": 6
}
```

Die folgende Beispielantwort enthält eine Liste von Tiergruppen:

```
[{"id": "1-domestic short hair-1-1"},
{"id": "1-domestic short hair-3-3"},
{"id": "1-domestic short hair-3-2"},
{"id": "1-domestic short hair-1-2"},
{"id": "1-domestic short hair-3-1"},
{"id": "2-beagle-3-3"},
```

Wenn Sie das `userId` Feld weglassen, gibt die Funktion allgemeine Empfehlungen zurück.

Lambda-Funktion neu einordnen

Um Re-Ranking zu verwenden, senden Sie eine Anfrage an die Lambda-Funktion zur Neurangierung. Die Payload enthält alle Elemente, `userId` die neu eingestuft werden IDs sollen, sowie deren Metadaten. In den folgenden Beispieldaten werden die Oxford Pets-Klassen

für `animal_species_id` (1=Katze, 2=Hund) und die Ganzzahlen 1-5 für und verwendet: `animal_age_id` `animal_size_id`

```
{
   "userId":"12345",
   "itemMetadataList":[
      {
         "itemId":"1",
         "animalMetadata":{
            "animal_species_id":"2",
            "animal_primary_breed_id":"Saint_Bernard",
            "animal_size_id":"3",
            "animal_age_id":"2"
         }
      },
      {
         "itemId":"2",
         "animalMetadata":{
            "animal_species_id":"1",
            "animal_primary_breed_id":"Egyptian_Mau",
            "animal_size_id":"1",
            "animal_age_id":"1"
         }
      },
      {
         "itemId":"3",
         "animalMetadata":{
            "animal_species_id":"2",
            "animal_primary_breed_id":"Saint_Bernard",
            "animal_size_id":"3",
            "animal_age_id":"2"
         }
      }
   ]
}
```

Die Lambda-Funktion ordnet diese Artikel neu ein und gibt dann eine geordnete Liste zurück, die den Artikel IDs und die direkte Antwort von Amazon Personalize enthält. Dies ist eine Rangliste der Tiergruppen, zu denen die Artikel gehören, und ihrer Punktzahl. Amazon Personalize verwendet Rezepte für Benutzerpersonalisierung und personalisiertes Ranking, um für jeden Artikel in den Empfehlungen eine Punktzahl anzugeben. Diese Werte stellen die relative Sicherheit dar, die

Amazon Personalize darüber hat, welchen Artikel der Benutzer als Nächstes auswählen wird. Höhere Punktzahlen bedeuten eine größere Gewissheit.


```
{
   "ranking":[
      "1",
      "3",
      "2"
   ],
   "personalizeResponse":{
      "ResponseMetadata":{
         "RequestId":"a2ec0417-9dcd-4986-8341-a3b3d26cd694",
         "HTTPStatusCode":200,
         "HTTPHeaders":{
            "date":"Thu, 16 Jun 2022 22:23:33 GMT",
            "content-type":"application/json",
            "content-length":"243",
            "connection":"keep-alive",
            "x-amzn-requestid":"a2ec0417-9dcd-4986-8341-a3b3d26cd694"
         },
         "RetryAttempts":0
      },
      "personalizedRanking":[
         {
            "itemId":"2-Saint_Bernard-3-2",
            "score":0.8947961
         },
         {
            "itemId":"1-Siamese-1-1",
            "score":0.105204
         }
      ],
      "recommendationId":"RID-d97c7a87-bd4e-47b5-a89b-ac1d19386aec"
   }
}
```


Amazon Kinesis Kinesis-Nutzlast

Die an Amazon Kinesis zu sendende Nutzlast hat das folgende Format:


```
{
    "Partitionkey": "randomstring",
    "Data": {
```

```
        "userId": "12345",
        "sessionId": "sessionId4545454",
        "eventType": "DetailView",
        "animalMetadata": {
            "animal_species_id": "1",
            "animal_primary_breed_id": "Russian_Blue",
            "animal_size_id": "1",
            "animal_age_id": "2"
        },
        "animal_id": "98765"

    }
}
```

> **Note**
>
> Das `userId` Feld für einen nicht authentifizierten Benutzer wurde entfernt.

Optimieren Sie mithilfe von SageMaker KI und Hydra Workflows für maschinelles Lernen — von der lokalen Entwicklung bis hin zu skalierbaren Experimenten

Erstellt von David Sauerwein (AWS), Julian Ferdinand Grueber (AWS) und Marco Geiger (AWS)

Übersicht

Dieses Muster bietet einen einheitlichen Ansatz für die Konfiguration und Ausführung von Algorithmen für maschinelles Lernen (ML) von lokalen Tests bis hin zur Produktion auf Amazon SageMaker AI. ML-Algorithmen stehen im Mittelpunkt dieses Musters, aber sein Ansatz erstreckt sich auch auf Feature-Engineering, Inferenz und ganze ML-Pipelines. Dieses Muster veranschaulicht anhand eines Beispielanwendungsfalls den Übergang von der lokalen Skriptentwicklung zu SageMaker KI-Schulungsaufgaben.

Ein typischer ML-Workflow besteht darin, Lösungen auf einem lokalen Computer zu entwickeln und zu testen, groß angelegte Experimente (z. B. mit unterschiedlichen Parametern) in der Cloud durchzuführen und die genehmigte Lösung in der Cloud bereitzustellen. Anschließend muss die bereitgestellte Lösung überwacht und gewartet werden. Ohne einen einheitlichen Ansatz für diesen Workflow müssen Entwickler ihren Code häufig in jeder Phase neu gestalten. Wenn die Lösung von einer Vielzahl von Parametern abhängt, die sich in jeder Phase dieses Workflows ändern können, kann es immer schwieriger werden, organisiert und konsistent zu bleiben.

Dieses Muster adressiert diese Herausforderungen. Erstens macht es Code-Refactoring zwischen Umgebungen überflüssig, indem ein einheitlicher Workflow bereitgestellt wird, der konsistent bleibt, unabhängig davon, ob er auf lokalen Computern, in Containern oder auf SageMaker KI ausgeführt wird. Zweitens vereinfacht es die Parameterverwaltung durch das Konfigurationssystem von Hydra, bei dem Parameter in separaten Konfigurationsdateien definiert werden, die einfach geändert und kombiniert werden können, wobei die Konfiguration jedes Laufs automatisch protokolliert wird. Weitere Informationen darüber, wie dieses Muster diese Herausforderungen bewältigt, finden Sie unter Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto

- Eine AWS Identity and Access Management (IAM-) Benutzerrolle für die Bereitstellung und den Start der SageMaker KI-Schulungsjobs
- AWS Command Line Interface (AWS CLI) Version 2.0 oder höher installiert und konfiguriert
- Poetry Version 1.8 oder höher, aber früher als 2.0, installiert
- Docker ist installiert
- Python-versie 3.10.x

Einschränkungen

- Der Code zielt derzeit nur auf SageMaker KI-Schulungsjobs ab. Es ist einfach, ihn auf die Verarbeitung von Jobs und ganzen SageMaker KI-Pipelines auszudehnen.
- Für ein vollständig produktionsfähiges SageMaker KI-Setup müssen zusätzliche Details vorhanden sein. Beispiele könnten benutzerdefinierte AWS Key Management Service (AWS KMS) Schlüssel für Rechen- und Speicheranwendungen oder Netzwerkkonfigurationen sein. Sie können diese zusätzlichen Optionen auch konfigurieren, indem Sie Hydra in einem speziellen Unterordner des `config` Ordners verwenden.
- Einige AWS-Services sind nicht in allen verfügbar. AWS-Regionen Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie unter AWS Dienste nach Regionen. Informationen zu bestimmten Endpunkten finden Sie unter Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Architektur

Das folgende Diagramm zeigt die Architektur der Lösung.

Das Diagramm zeigt den folgenden Workflow:

1. Der Datenwissenschaftler kann den Algorithmus in kleinem Maßstab in einer lokalen Umgebung wiederholen, Parameter anpassen und das Trainingsskript schnell testen, ohne dass Docker oder KI erforderlich sind. SageMaker (Weitere Informationen finden Sie unter der Aufgabe „Lokal für schnelle Tests ausführen“ in Epics.)
2. Sobald der Datenwissenschaftler mit dem Algorithmus zufrieden ist, erstellt er das Docker-Image und überträgt es in das angegebene Amazon Elastic Container Registry (Amazon ECR) -Repository. `hydra-sm-artifact` (Weitere Informationen finden Sie unter „Workflows auf SageMaker KI ausführen“ in Epics.)

3. Der Datenwissenschaftler initiiert entweder SageMaker KI-Trainingsjobs oder Hyperparameter-Optimierungsjobs (HPO) mithilfe von Python-Skripten. Für reguläre Trainingsjobs wird die angepasste Konfiguration in den Amazon Simple Storage Service (Amazon S3) Bucket mit dem Namen geschriebenhydra-sample-config. Für HPO-Jobs wird der Standardkonfigurationssatz angewendet, der sich im config Ordner befindet.
4. Der SageMaker KI-Trainingsjob ruft das Docker-Image ab, liest die Eingabedaten aus dem Amazon S3 S3-Bucket hydra-sample-data und ruft entweder die Konfiguration aus dem Amazon S3 S3-Bucket ab hydra-sample-config oder verwendet die Standardkonfiguration. Nach dem Training speichert der Job die Ausgabedaten im Amazon S3 S3-Buckethydra-sample-data.

Automatisierung und Skalierung

- Für automatisierte Schulungen, Umschulungen oder Inferenzen können Sie den AWS CLI Code in Dienste wie AWS LambdaAWS CodePipeline, oder Amazon integrieren. EventBridge
- Die Skalierung kann erreicht werden, indem Konfigurationen für die Instance-Größen geändert oder Konfigurationen für verteilte Schulungen hinzugefügt werden.

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und zu verwalten AWS-Regionen.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie AWS-Services über Befehle in Ihrer Befehlszeilen-Shell interagieren können. Für dieses Muster AWS CLI ist das sowohl für die anfängliche Konfiguration als auch für das Testen von Ressourcen nützlich.
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon SageMaker AI ist ein verwalteter Service für maschinelles Lernen (ML), mit dem Sie ML-Modelle erstellen und trainieren und diese dann in einer produktionsbereiten, gehosteten Umgebung bereitstellen können. SageMaker AI Training ist ein vollständig verwalteter ML-Service innerhalb von SageMaker KI, der das Training von ML-Modellen in großem Maßstab ermöglicht. Das Tool kann die Rechenanforderungen von Trainingsmodellen effizient bewältigen und nutzt dabei die integrierte Skalierbarkeit und Integration mit anderen AWS-Services Modellen.

SageMaker AI Training unterstützt auch benutzerdefinierte Algorithmen und Container und ist somit flexibel für eine Vielzahl von ML-Workflows.

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere Tools

- Docker ist eine Reihe von Platform-as-a-Service (PaaS) -Produkten, die Virtualisierung auf Betriebssystemebene nutzen, um Software in Containern bereitzustellen. Es wurde in diesem Muster verwendet, um konsistente Umgebungen in verschiedenen Phasen sicherzustellen, von der Entwicklung bis zur Bereitstellung, und um Abhängigkeiten und Code zuverlässig zu verpacken. Die Containerisierung von Docker ermöglichte eine einfache Skalierung und Versionskontrolle im gesamten Workflow.
- Hydra ist ein Konfigurationsmanagement-Tool, das Flexibilität bei der Handhabung mehrerer Konfigurationen und dynamisches Ressourcenmanagement bietet. Es ist entscheidend für die Verwaltung von Umgebungskonfigurationen und ermöglicht eine nahtlose Bereitstellung in verschiedenen Umgebungen. Weitere Informationen zu Hydra finden Sie unter Zusätzliche Informationen.
- Python ist eine Allzweck-Computerprogrammiersprache. Python wurde verwendet, um den ML-Code und den Deployment-Workflow zu schreiben.
- Poetry ist ein Tool für Abhängigkeitsmanagement und Paketierung in Python.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub configuring-sagemaker-training-jobs-with-hydra verfügbar.

Bewährte Methoden

- Wählen Sie eine IAM-Rolle für die Bereitstellung und den Start der SageMaker KI-Schulungsjobs, die dem Prinzip der geringsten Rechte folgt, und gewähren Sie die Mindestberechtigungen, die zur Ausführung einer Aufgabe erforderlich sind. Weitere Informationen finden Sie in der IAM-Dokumentation unter Gewährung der geringsten Rechte und bewährte Methoden zur Sicherheit.
- Verwenden Sie temporäre Anmeldeinformationen, um auf die IAM-Rolle im Terminal zuzugreifen.

Epen

Richte die Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen und aktivieren Sie die virtuelle Umgebung.	Um die virtuelle Umgebung zu erstellen und zu aktiviere n, führen Sie die folgenden Befehle im Stammverzeichnis des Repositorys aus:
	`poetry install`
	`poetry shell`
		Allgemeines AWS

Stellen Sie die Infrastruktur bereit.	Führen Sie den folgenden Befehl aus CloudFormation, um die Infrastruktur mithilfe von bereitzustellen: `aws cloudformation deploy --template-file infra/hydra-sagemaker-setup.yaml --stack-name hydra-sagemaker-setup --capabilities CAPABILITY_NAMED_IAM`	General AWS, DevOps Ingenieur
Laden Sie die Beispieldaten herunter.	Führen Sie den folgenden Befehl aus, um die Eingabeda ten von openml auf Ihren lokalen Computer herunterz uladen: `python scripts/download_data.py`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Für schnelle Tests lokal ausführen.	Führen Sie den folgenden Befehl aus, um den Trainings code lokal zum Testen auszuführen: `python mypackage/ train.py data.trai n_data_path=data/t rain.csv evaluatio n.base_dir_path=data` Die Protokolle aller Ausführun gen werden nach Ausführun gszeit sortiert in einem Ordner mit dem Namen `outputs` gespeichert. Weitere Informationen finden Sie im Abschnitt „Ausgabe“ im GitHub Repository. Mithilfe der `--multirun` Funktionalität können Sie auch mehrere Schulungen parallel mit unterschiedlichen Parametern durchführen. Weitere Informationen finden Sie in der Hydra-Dokumentatio n.	Data Scientist

Führen Sie Workflows auf KI SageMaker aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie die Umgebungs variablen fest.	Um Ihren Job auf SageMaker KI auszuführen, legen Sie	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	die folgenden Umgebungs variablen fest und geben Sie dabei Ihre ID AWS-Region und Ihre AWS-Konto ID an:
	
	`export ECR_REPO_NAME=hydra-sm-artifact`
	`export image_tag=latest`
	`export AWS_REGION="<your_aws_region>" # for instance, us-east-1`
	`export ACCOUNT_ID="<your_account_id>"`
	`export BUCKET_NAME_DATA=hydra-sample-data-$ACCOUNT_ID`
	`export BUCKET_NAME_CONFIG=hydra-sample-config-$ACCOUNT_ID`
	`export AWS_DEFAULT_REGION=$AWS_REGION`
	`export ROLE_ARN=arn:aws:iam::${ACCOUNT_ID}:role/hydra-sample-sagemaker`
	`export INPUT_DATA_S3_PATH=s3://$BUCKET_NAME_DATA/hydra-on-sm/input/`
	`export OUTPUT_DATA_S3_PATH=s3://$BUCKET_NAME_DATA/hydra-on-sm/output/`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie ein Docker-Image und übertragen Sie es.	Führen Sie den folgenden Befehl aus, um das Docker-Image zu erstellen und in das Amazon ECR-Repository zu übertragen:
	`chmod +x scripts/create_and_push_image.sh`
	`scripts/create_and_push_image.sh $ECR_REPO_NAME $image_tag $AWS_REGION $ACCOUNT_ID`
	Bei dieser Aufgabe wird davon ausgegangen, dass Sie in Ihrer Umgebung über gültige Anmeldeinformationen verfügen. Das Docker-Image wird in das Amazon ECR-Repository übertragen, das in der vorherigen Aufgabe in der Umgebungsvariablen angegeben wurde, und wird verwendet, um den SageMaker AI-Container zu aktivieren, in dem der Trainingsjob ausgeführt wird.
		ML-Ingenieur, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopieren Sie die Eingabedaten nach Amazon S3.	Der SageMaker KI-Trainingsjob muss die Eingabedaten aufnehmen. Führen Sie den folgenden Befehl aus, um die Eingabedaten in den Amazon S3 S3-Bucket für Daten zu kopieren: `aws s3 cp data/train.csv "${INPUT_DATA_S3_PATH}train.csv"`	Dateningenieur, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Reichen Sie SageMaker KI-Schulungsjobs ein.	Um die Ausführung Ihrer Skripts zu vereinfachen, geben Sie in der `default.yaml` Datei die Standardkonfigurationsparameter an. Dieser Ansatz gewährleistet nicht nur die Konsistenz zwischen den Ausführungen, sondern bietet auch die Flexibilität, die Standardeinstellungen bei Bedarf einfach zu überschreiben. Sehen Sie sich das folgende Beispiel an: `python scripts/start_sagemaker_training_job.py sagemaker.role_arn=$ROLE_ARN sagemaker.config_s3_bucket=$BUCKET_NAME_CONFIG sagemaker.input_data_s3_path=$INPUT_DATA_S3_PATH sagemaker.output_data_s3_path=$OUTPUT_DATA_S3_PATH`	Allgemeiner AWS, ML-Ingenieur, Datenwissenschaftler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das SageMaker KI-Hyperparameter-Tuning durch.	Das Ausführen des SageMaker KI-Hyperparameter-Tunings ähnelt dem Einreichen eines SageMaker AII-Trainingsjobs. Das Ausführungsskript unterscheidet sich jedoch in einigen wichtigen Punkten, wie Sie in der Datei start_sagemaker_hpo_job.py sehen können. Die zu optimierenden Hyperparameter müssen über die boto3-Nutzlast und nicht über einen Kanal an den Trainingsjob weitergeleitet werden. Führen Sie die folgenden Befehle aus, um den Job zur Hyperparameter-Optimierung (HPO) zu starten: `python scripts/start_sagemaker_hpo_job.py sagemaker.role_arn=$ROLE_ARN sagemaker.config_s3_bucket=$BUCKET_NAME_CONFIG sagemaker.input_data_s3_path=$INPUT_DATA_S3_PATH sagemaker.output_data_s3_path=$OUTPUT_DATA_S3_PATH`	Data Scientist

Fehlerbehebung

Problem	Lösung
Abgelaufenes Token	Exportieren Sie neue Anmeldeinformationen AWS .
Fehlende IAM-Berechtigungen	Stellen Sie sicher, dass Sie die Anmeldein formationen einer IAM-Rolle exportieren, die über alle erforderlichen IAM-Berechtigungen verfügt, um die CloudFormation Vorlage bereitzustellen und die SageMaker KI-Schulu ngsjobs zu starten.

Zugehörige Ressourcen

- Trainieren Sie ein Modell mit Amazon SageMaker AI (AWS Dokumentation)
- Was ist Hyperparameter-Tuning?

Zusätzliche Informationen

Dieses Muster befasst sich mit den folgenden Herausforderungen:

Konsistenz von der lokalen Entwicklung bis zur Bereitstellung im großen Maßstab — Mit diesem Muster können Entwickler denselben Workflow verwenden, unabhängig davon, ob sie lokale Python-Skripte verwenden, lokale Docker-Container ausführen, große SageMaker KI-Experimente durchführen oder in der Produktion auf SageMaker KI bereitstellen. Diese Konsistenz ist aus den folgenden Gründen wichtig:

- Schnellere Iteration — Sie ermöglicht schnelles, lokales Experimentieren, ohne dass größere Anpassungen bei der Skalierung erforderlich sind.
- Kein Refactoring — Der Übergang zu größeren Experimenten mit SageMaker KI ist nahtlos und erfordert keine Überarbeitung des bestehenden Setups.
- Kontinuierliche Verbesserung — Die Entwicklung neuer Funktionen und die kontinuierliche Verbesserung des Algorithmus sind unkompliziert, da der Code in allen Umgebungen gleich bleibt.

Konfigurationsmanagement — Dieses Muster nutzt Hydra, ein Konfigurationsmanagement-Tool, um die folgenden Vorteile zu bieten:

- Parameter werden getrennt vom Code in Konfigurationsdateien definiert.
- Verschiedene Parametersätze können einfach ausgetauscht oder kombiniert werden.
- Die Nachverfolgung von Experimenten wird vereinfacht, da die Konfiguration jedes Durchlaufs automatisch protokolliert wird.
- Cloud-Experimente können dieselbe Konfigurationsstruktur wie lokale Läufe verwenden, wodurch Konsistenz gewährleistet wird.

Mit Hydra können Sie die Konfiguration effektiv verwalten und die folgenden Funktionen aktivieren:

- Konfigurationen aufteilen — Teilen Sie Ihre Projektkonfigurationen in kleinere, überschaubare Teile auf, die unabhängig voneinander geändert werden können. Dieser Ansatz erleichtert die Bearbeitung komplexer Projekte.
- Einfache Anpassung der Standardeinstellungen — Ändern Sie Ihre Basiskonfigurationen schnell, sodass Sie neue Ideen leichter testen können.
- CLI-Eingaben und Konfigurationsdateien aufeinander abstimmen — Kombinieren Sie Befehlszeileneingaben problemlos mit Ihren Konfigurationsdateien. Dieser Ansatz reduziert Unordnung und Verwirrung und macht Ihr Projekt im Laufe der Zeit überschaubarer.

Trainieren und implementieren Sie ein benutzerdefiniertes GPU-unterstütztes ML-Modell auf Amazon SageMaker

Erstellt von Ankur Shukla (AWS)

Übersicht

Für das Training und die Implementierung eines Modells für maschinelles Lernen (ML), das von einer Grafikverarbeitungseinheit (GPU) unterstützt wird, müssen zunächst bestimmte Umgebungsvariablen eingerichtet und initialisiert werden, um die Vorteile von NVIDIA voll auszuschöpfen. GPUs Es kann jedoch zeitaufwändig sein, die Umgebung einzurichten und sie mit der SageMaker Amazon-Architektur in der Amazon Web Services (AWS) Cloud kompatibel zu machen.

Dieses Muster hilft Ihnen, mithilfe von Amazon ein benutzerdefiniertes GPU-unterstütztes ML-Modell zu trainieren und zu erstellen. SageMaker Es enthält Schritte zum Trainieren und Bereitstellen eines benutzerdefinierten CatBoost Modells, das auf einem Open-Source-Datensatz mit Amazon-Rezensionen basiert. Anschließend können Sie die Leistung auf einer `p3.16xlarge` Amazon Elastic Compute Cloud (Amazon EC2) -Instance vergleichen.

Dieses Muster ist nützlich, wenn Ihr Unternehmen bestehende GPU-gestützte ML-Modelle einsetzen möchte. SageMaker Ihre Datenwissenschaftler können den Schritten in diesem Muster folgen, um NVIDIA-GPU-unterstützte Container zu erstellen und ML-Modelle auf diesen Containern bereitzustellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein Quell-Bucket von Amazon Simple Storage Service (Amazon S3) zum Speichern der Modellartefakte und Prognosen.
- Ein Verständnis von SageMaker Notebook-Instances und Jupyter-Notebooks.
- Ein Verständnis dafür, wie eine AWS Identity and Access Management (IAM) -Rolle mit grundlegenden SageMaker Rollenberechtigungen, S3-Bucket-Zugriffs- und Aktualisierungsberechtigungen sowie zusätzlichen Berechtigungen für Amazon Elastic Container Registry (Amazon ECR) erstellt wird.

Einschränkungen

- Dieses Muster ist für überwachte ML-Workloads mit einem in Python geschriebenen Train- und Deploy-Code vorgesehen.

Architektur

Technologie-Stack

- SageMaker
- Amazon ECR

Tools

Tools

- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) ist ein von AWS verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon SageMaker — SageMaker ist ein vollständig verwalteter ML-Service.
- Docker — Docker ist eine Softwareplattform zum schnellen Erstellen, Testen und Bereitstellen von Anwendungen.
- Python — Python ist eine Programmiersprache.

Code

Der Code für dieses Muster ist unter GitHub Implementierung eines Bewertungsklassifikationsmodells mit Catboost und SageMaker Repository verfügbar.

Epen

Vorbereitung der Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle und fügen Sie die erforderl ichen Richtlinien hinzu.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die IAM-Konsole und erstellen Sie eine neue IAM-Rolle. Weisen Sie der IAM-Rolle die folgenden Richtlinien zu: • `AmazonEC2Container RegistryFullAccess` • `AmazonS3FullAccess` • `AmazonSageMakerFul lAccess` Weitere Informationen dazu finden Sie in der SageMaker Amazon-Dokumentation unter Eine Notebook-Instance erstellen.	Data Scientist
Erstellen Sie die SageMaker Notebook-Instanz.	Öffnen Sie die SageMaker Konsole, wählen Sie Notebook-Instanzen und dann Notebook-Instanz erstellen aus. Wählen Sie für die IAM-Rolle die IAM-Rolle aus, die Sie zuvor erstellt haben. Konfigurieren Sie die Notebook-Instanz gemäß Ihren Anforderungen und	Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wählen Sie dann Notebook-Instanz erstellen. Ausführliche Schritte und Anweisungen finden Sie in der SageMaker Amazon-Dokumentation unter Eine Notebook-Instance erstellen.	
Klonen Sie das Repository	Öffnen Sie das Terminal in der SageMaker Notebook-Instance und klonen Sie das Klassifizierungsmodell GitHub Implementing a review with Catboost and SageMaker repository, indem Sie den folgenden Befehl ausführen: `git clone https://github.com/aws-samples/review-classification-using-catboost-sagemaker.git`	
Starten Sie das Jupyter-Notebook.	Starten Sie das `Review classification model with Catboost and SageMaker.ipynb` Jupyter-Notebook, das die vordefinierten Schritte enthält.	Data Scientist

Feature-Engineering

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie Befehle im Jupyter-Notebook aus.	Öffnen Sie das Jupyter-Notizbuch und führen Sie die Befehle aus den folgenden Geschichten aus, um die Daten für das Training Ihres ML-Modells vorzubereiten.	Data Scientist

Lesen Sie die Daten aus dem S3-Bucket.	`import pandas as pd`
	`import csv`
	`fname = 's3://amazon-reviews-pds/tsv/amazon_reviews_us_Digital_Video_Download_v1_00.tsv.gz'`
	`df = pd.read_csv(fname, sep='\t',delimiter='\t',error_bad_lines=False)`
		Data Scientist

Verarbeiten Sie die Daten vor.	`import numpy as np`
	`def pre_process(df):`
	
	`  df.fillna(value={'review_body': '', 'review_headline': ''}, inplace=True)`
	`  df.fillna( value={'verified_purchase': 'Unk'}, inplace=True)`
	
	`  df.fillna(0, inplace=True)`
	`  return df`
	`df = pre_process(df)`
	`df.review_date = pd.to_datetime(df.review_date)`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`df['target'] = np.where(df['star_rating']>=4,1,0)` **Note** Dieser Code ersetzt Nullwerte in der `'review_body'` durch eine leere Zeichenfolge und ersetzt die `'verified_purchase'` Spalte durch `'Unk'`, was „unbekannt“ bedeutet.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Teilen Sie die Daten in Trainings-, Validierungs- und Testdatensätze auf.	Um die Verteilung des Ziellabels über die aufgeteilten Datensätze hinweg identisch zu halten, müssen Sie die Stichprobe mithilfe der Scikit-Learn-Bibliothek stratifizieren.
	
	`from sklearn.model_selection import StratifiedShuffleSplit`
	`sss = StratifiedShuffleSplit(n_splits=2, test_size=0.10, random_state=0)`
	`sss.get_n_splits(df, df['target'])`
	`for train_index, test_index in sss.split(df, df['target']):`
	`  X_train_vallid , X_test = df.iloc[train_index], df.iloc[test_index]`
	
	`sss.get_n_splits(X_train_vallid, X_train_vallid['target'])`
	`for train_index, test_index in sss.split(X_train_vallid, X_train_vallid['target']):`
	`  X_train , X_valid = X_train_vallid.iloc[train_index],`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`X_train_vallid.ilo c[test_index]`	

Docker-Image erstellen, ausführen und auf Amazon ECR übertragen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie das Docker-Im age vor und übertragen Sie es.	Führen Sie im Jupyter-N otizbuch die Befehle aus den folgenden Storys aus, um das Docker-Image vorzubereiten und es an Amazon ECR zu übertragen.	ML-Ingenieur

Erstellen Sie ein Repository in Amazon ECR.	`%%sh`
	
	`algorithm_name=s agemaker-catboost- github-gpu-img`
	
	`chmod +x code/train`
	`chmod +x code/serve`
	
	`account=$(aws sts get- caller-identity -- query Account --output text)`
	
	`# Get the region defined in the current configuration (default to us-west-2 if none defined)`
	`region=$(aws configure get region)`
	`region=${region:-us- east-1}`
		ML-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`fullname="${accou nt}.dkr.ecr.${regi on}.amazonaws.com/ ${algorithm_name}: latest"`
	
	`aws ecr create-re pository --repository- name "${algorithm_name} " > /dev/nul`	

Erstellen Sie lokal ein Docker-Image.	`docker build -t "${algorithm_name}" . docker tag ${algorit hm_name} ${fullname}`	ML-Ingenieur
Führen Sie das Docker-Image aus und übertragen Sie es an Amazon ECR.	`docker push ${fullname}`	ML-Ingenieur

Training

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen SageMaker Hyperparameter-Tuning-Job.	Führen Sie im Jupyter-N otebook die Befehle aus den folgenden Storys aus, um mithilfe Ihres Docker-Images einen SageMaker Hyperpara meter-Tuning-Job zu erstellen.	Data Scientist
SageMaker Erstellen Sie einen Schätzer.	Erstellen Sie einen SageMaker Schätzer, indem Sie den Namen des Docker-Im ages verwenden.	Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`import sagemaker as sage`
	`from time import gmtime,`
	` strftime`
	`sess = sage.Session()`
	`from sagemaker.tuner`
	` import IntegerPa`
	`rameter, Categoric`
	`alParameter, Continuou`
	`sParameter, Hyperpara`
	`meterTuner`
	
	`account = sess.boto`
	`_session.client('s`
	`ts').get_caller_id`
	`entity()['Account']`
	`region = sess.boto`
	`_session.region_name`
	`image = '{}.dkr.e`
	`cr.{}.amazonaws.co`
	`m/sagemaker-catboo`
	`st-github-gpu-img:`
	`latest'.format(acc`
	`ount, region)`
	`tree_hpo = sage.esti`
	`mator.Estimator(im`
	`age,`
	
	` role, 1,`
	
	` 'ml.p3.16xlarge',`
	
	`  train_volume_size =`
	` 100,`
	
	`  output_path="s3://`
	`{}/sagemaker/DEMO-`
	`GPU-Catboost/outpu`
	`t".format(bucket),`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`sagemaker_session= sess)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie einen HPO-Job.	Erstellen Sie einen Tuning-Job für Hyperparameter-Optimierung (HPO) mit Parameterbereichen und übergeben Sie die Train- und Validierungssätze als Parameter an die Funktion.
	
	`hyperparameter_ranges = {'iterations': IntegerParameter(80000, 130000),`
	
	`'max_depth': IntegerParameter(6, 10),`
	
	`'max_ctr_complexity': IntegerParameter(4, 10),`
	
	`'learning_rate': ContinuousParameter(0.01, 0.5)}`
	
	`objective_metric_name = 'auc'`
	`metric_definitions = [{'Name': 'auc',`
	
	`'Regex': 'auc: ([0-9\.]+)'}]`
	
	`tuner = HyperparameterTuner(tree_hpo,`
	
	`objective_metric_name,`
	
	`hyperparameter_ranges,`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`    metric_definitions ,`
	
	`    objective_type='Ma ximize',`
	
	`    max_jobs=50,`
	
	`    max_parallel_jobs= 2)`	

Führen Sie den HPO-Job aus.	`train_location =  's3://'+bucket+'/s agemaker/DEMO-GPU- Catboost/data/train/' valid_location =  's3://'+bucket+'/s agemaker/DEMO-GPU- Catboost/data/valid/'`
	
	`tuner.fit({'train':  train_location,  'validati on': valid_location  })`
		Data Scientist

Erhalte den Trainingsjob mit der besten Leistung.	`import sagemaker as sage from time import gmtime,  strftime sess = sage.Session()`
	
	`best_job =tuner.be st_training_job()`
		Data Scientist

Batch-Transformation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen SageMaker Batch-Transformationsjob für Testdaten zur Modellvorhersage.	Führen Sie im Jupyter-Notizbuch die Befehle aus den folgenden Geschichten aus, um das Modell aus Ihrem SageMaker Hyperparameter-Tuning-Job zu erstellen, und senden Sie einen SageMaker Batch-Transformationsjob für die Testdaten zur Modellvorhersage.	Data Scientist

Erstellen Sie das Modell. SageMaker	Erstellen Sie ein Modell im SageMaker Modell mit dem besten Trainingsjob.
	`attached_estimator = sage.estimator.Estimator.attach(best_job)`
	`output_path ='s3://'+bucket+'/sagemaker/DEMO-GPU-Catboost/data/test-predictions/'`
	`input_path ='s3://'+bucket+'/sagemaker/DEMO-GPU-Catboost/data/test/'`
	`transformer = attached_estimator.transformer(instance_count=1,`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`instance_type='ml.p3.16xlarge', assemble_with='Line', accept='text/csv', max_payload=1, output_path=output_path, env = {'SAGEMAKER_MODEL_SERVER_TIMEOUT' : '3600' })`	
Erstellen Sie einen Batch-Transformationsauftrag.	Erstellen Sie einen Batch-Transformationsauftrag für den Testdatensatz. `transformer.transform(input_path, content_type='text/csv', split_type='Line')`	Data Scientist

Analysieren Sie die Ergebnisse

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Lesen Sie die Ergebnisse und bewerten Sie die Leistung des Modells.	Führen Sie im Jupyter-N otizbuch die Befehle aus den folgenden Geschichten aus, um die Ergebnisse zu lesen und die Leistung des Modells anhand der Modellmetriken Area Under the ROC Curve (ROC-AUC) und Area Under the Precision Recall Curve (PR-AUC) zu bewerten. Weitere Informationen dazu finden Sie unter Amazon Machine Learning-Schlüssel konzepte in der Dokumenta tion zu Amazon Machine Learning (Amazon ML).	Data Scientist

Lesen Sie die Ergebnisse der Batch-Transformationsaufträ ge.	Lesen Sie die Ergebnisse des Batch-Transformationsauftra gs in einen Datenrahmen ein.
	
	`file_name = 's3://'+b ucket+'/sagemaker/ DEMO-GPU-Catboost/ data/test-predicti ons/file_1.out'`
	
	`results = pd.read_csv(file_n ame, names=['r eview_id','target' ,'score'] ,sep='\t' ,escapechar ='\\' , quoting=csv.QUOTE_ NONE,`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`lineterminator='\n',quotechar='"').dropna()`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bewerten Sie die Leistungskennzahlen.	Bewerten Sie die Leistung des Modells auf ROC-AUC und PR-AUC.
	
	`from sklearn import metrics`
	`import matplotlib`
	`import pandas as pd`
	`matplotlib.use('agg', warn=False, force=True)`
	`from matplotlib import pyplot as plt`
	
	`%matplotlib inline`
	
	`def analyze_results(labels, predictions):`
	`precision, recall, thresholds = metrics.precision_recall_curve(labels, predictions)`
	`auc = metrics.auc(recall, precision)`
	
	`fpr, tpr, _ = metrics.roc_curve(labels, predictions)`
	`roc_auc_score = metrics.roc_auc_score(labels, predictions)`
	
	`print('Neural-Nets: ROC auc=%.3f' % ( roc_auc_score))`
	
	`plt.plot(fpr, tpr, label="data 1, auc=" + str(roc_auc_score))`
		Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`    plt.xlabel('1-Specificity')`
	`    plt.ylabel('Sensitivity')`
	`    plt.legend(loc=4)`
	`    plt.show()`
	
	`    lr_precision, lr_recall, _ = metrics.precision_recall_curve(labels, predictions)`
	`    lr_auc = metrics.auc(lr_recall, lr_precision)`
	`    # summarize scores`
	`    print('Neural-Nets: PR auc=%.3f' % ( lr_auc))`
	`    # plot the precision-recall curves`
	`    no_skill = len(labels[labels==1.0]) / len(labels)`
	`    plt.plot([0, 1], [no_skill, no_skill], linestyle='--', label='No Skill')`
	
	`    plt.plot(lr_recall, lr_precision, marker='.', label='Neural-Nets')`
	`    # axis labels`
	`    plt.xlabel('Recall')`
	`    plt.ylabel('Precision')`
	`    # show the legend`
	`    plt.legend()`
	`    # show the plot`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`plt.show()`
	
	`return auc`
	
	`analyze_results(results['target'].values,results['score'].values)`	

Zugehörige Ressourcen

- Trainieren und hosten Sie Scikit-Learn-Modelle in Amazon, SageMaker indem Sie einen Scikit-Docker-Container erstellen

Zusätzliche Informationen

Die folgende Liste zeigt die verschiedenen Elemente der Docker-Datei, die im Docker-Image Build, Run und Push in Amazon ECR Epic ausgeführt wird.

Installieren Sie Python mit aws-cli.

```
FROM amazonlinux:1

 RUN yum update -y && yum install -y python36 python36-devel python36-libs python36-
tools python36-pip && \
 yum install gcc tar make wget util-linux kmod man sudo git -y && \
 yum install wget -y && \
 yum install aws-cli -y && \
 yum install nginx -y && \
yum install gcc-c++.noarch -y && yum clean all
```

Installieren Sie die Python-Pakete

```
RUN pip-3.6 install --no-cache-dir --upgrade pip && \pip3 install --no-cache-dir --
upgrade setuptools && \
```

```
pip3 install Cython && \
pip3 install --no-cache-dir numpy==1.16.0 scipy==1.4.1 scikit-learn==0.20.3
 pandas==0.24.2 \
flask gevent gunicorn boto3 s3fs  matplotlib joblib catboost==0.20.2
```

Installieren Sie CUDA und cuDNN

```
RUN wget https://developer.nvidia.com/compute/cuda/9.0/Prod/local_installers/
cuda_9.0.176_384.81_linux-run \
&& chmod u+x cuda_9.0.176_384.81_linux-run \
&& ./cuda_9.0.176_384.81_linux-run --tmpdir=/data --silent --toolkit --override \
&& wget https://custom-gpu-sagemaker-image.s3.amazonaws.com/installation/cudnn-9.0-
linux-x64-v7.tgz \
&& tar -xvzf cudnn-9.0-linux-x64-v7.tgz \
&& cp /data/cuda/include/cudnn.h /usr/local/cuda/include \
&& cp /data/cuda/lib64/libcudnn* /usr/local/cuda/lib64 \

&& chmod a+r /usr/local/cuda/include/cudnn.h /usr/local/cuda/lib64/libcudnn* \
&&  rm -rf /data/*
```

Erstellen Sie die erforderliche Verzeichnisstruktur für SageMaker

```
RUN mkdir /opt/ml /opt/ml/input /opt/ml/input/config /opt/ml/input/data /opt/ml/input/
data/training /opt/ml/model /opt/ml/output /opt/program
```

Stellen Sie die NVIDIA-Umgebungsvariablen ein

```
ENV PYTHONPATH=/opt/program
ENV PYTHONUNBUFFERED=TRUE
ENV PYTHONDONTWRITEBYTECODE=TRUE
ENV PATH="/opt/program:${PATH}"

# Set NVIDIA mount environments
ENV LD_LIBRARY_PATH=/usr/local/nvidia/lib:/usr/local/nvidia/lib64:$LD_LIBRARY_PATH
ENV NVIDIA_VISIBLE_DEVICES="all"
ENV NVIDIA_DRIVER_CAPABILITIES="compute,utility"
ENV NVIDIA_REQUIRE_CUDA "cuda>=9.0"
```

Kopieren Sie Trainings- und Inferenzdateien in das Docker-Image

```
COPY code/* /opt/program/
```

```
WORKDIR /opt/program
```

Translate natürliche Sprache in Abfragen, DSL für OpenSearch und Elasticsearch-Abfragen

Erstellt von Tabby Ward (AWS), Nicholas Switzer (AWS) und Breanne Warner (AWS)

Übersicht

Dieses Muster zeigt, wie umfangreiche Sprachmodelle (LLMs) verwendet werden können, um Abfragen in natürlicher Sprache in abfragedomänenspezifische Sprache (Query DSL) umzuwandeln, was es Benutzern erleichtert, mit Suchdiensten wie OpenSearch Elasticsearch zu interagieren, auch ohne umfassende Kenntnisse der Abfragesprache. Diese Ressource ist besonders wertvoll für Entwickler und Datenwissenschaftler, die suchbasierte Anwendungen mit Funktionen für Abfragen in natürlicher Sprache erweitern und so letztlich die Benutzererfahrung und die Suchfunktionen verbessern möchten.

Das Muster veranschaulicht Techniken für schnelles Engineering, iterative Verfeinerung und Einbindung von Fachwissen, die allesamt für die Generierung synthetischer Daten von entscheidender Bedeutung sind. Dieser Ansatz konzentriert sich zwar hauptsächlich auf die Konvertierung von Abfragen, zeigt aber implizit das Potenzial für Datenerweiterung und skalierbare synthetische Datenproduktion. Diese Grundlage könnte auf umfassendere Aufgaben zur Generierung synthetischer Daten ausgedehnt werden, um zu verdeutlichen, wie wichtig es ist, unstrukturierte Eingaben LLMs in natürlicher Sprache mit strukturierten, anwendungsspezifischen Ausgaben zu verbinden.

Diese Lösung beinhaltet keine Migrations- oder Bereitstellungstools im herkömmlichen Sinne. Stattdessen konzentriert sie sich auf die Demonstration eines Machbarkeitsnachweises (PoC) für die Konvertierung von Abfragen in natürlicher Sprache in Abfragen von DSL mithilfe von. LLMs

- Das Muster verwendet ein Jupyter-Notizbuch als step-by-step Leitfaden für die Einrichtung der Umgebung und die Implementierung der Konvertierung. text-to-query
- Es verwendet Amazon Bedrock für den Zugriff LLMs, die für die Interpretation natürlicher Sprache und die Generierung entsprechender Abfragen von entscheidender Bedeutung sind.
- Die Lösung ist für die Zusammenarbeit mit Amazon OpenSearch Service konzipiert. Sie können einem ähnlichen Prozess für Elasticsearch folgen, und die generierten Abfragen könnten möglicherweise für ähnliche Suchmaschinen angepasst werden.

Query DSL ist eine flexible, JSON-basierte Suchsprache, mit der komplexe Abfragen sowohl in Elasticsearch als auch erstellt werden. OpenSearch Sie ermöglicht es Ihnen, Abfragen in den Abfrageparametern von Suchoperationen anzugeben, und unterstützt verschiedene Abfragetypen. Eine DSL-Abfrage umfasst Blattabfragen und zusammengesetzte Abfragen. Blattabfragen suchen nach bestimmten Werten in bestimmten Feldern und umfassen Volltext-, Begriffsebene-, geografische, verbindende, bereichsübergreifende und spezielle Abfragen. Zusammengesetzte Abfragen dienen als Wrapper für mehrere Blatt- oder zusammengesetzte Klauseln und kombinieren ihre Ergebnisse oder ändern ihr Verhalten. Query DSL unterstützt die Erstellung anspruchsvoller Suchanfragen, die von einfachen Abfragen, die alle Kriterien erfüllen, bis hin zu komplexen Abfragen mit mehreren Klauseln reichen, die zu hochspezifischen Ergebnissen führen. Query DSL ist besonders nützlich für Projekte, die erweiterte Suchfunktionen, flexible Abfragekonstruktion und JSON-basierte Abfragestrukturen erfordern.

Dieses Muster verwendet Techniken wie „Few-Shot Prompting“, Systemaufforderungen, strukturierte Ausgabe, Verkettung von Eingabeaufforderungen, Kontextbereitstellung und aufgabenspezifische Eingabeaufforderungen für die DSL-Konvertierung. text-to-query Definitionen und Beispiele für diese Techniken finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

Um das Jupyter-Notebook effektiv für die Konvertierung von Abfragen in natürlicher Sprache in DSL-Abfragen zu verwenden, benötigen Sie:

- Vertrautheit mit Jupyter-Notebooks. Grundlegendes Verständnis der Navigation und Ausführung von Code in einer Jupyter-Notebook-Umgebung.
- Python-Umgebung. Eine funktionierende Python-Umgebung, vorzugsweise Python 3.x, in der die erforderlichen Bibliotheken installiert sind.
- Elasticsearch oder Wissen OpenSearch . Grundkenntnisse in Elasticsearch oder OpenSearch, einschließlich seiner Architektur und der Durchführung von Abfragen.
- AWS-Konto. Aktiv AWS-Konto für den Zugriff auf Amazon Bedrock und andere verwandte Dienste.
- Bibliotheken und Abhängigkeiten. Installation bestimmter Bibliotheken, die im Notizbuch erwähnt werden, z. B. `boto3` für die AWS Interaktion, und aller anderen Abhängigkeiten, die für die LLM-Integration erforderlich sind.
- Modellieren Sie den Zugriff innerhalb von Amazon Bedrock. In diesem Muster werden drei Claude LLMs von Anthropic verwendet. Öffnen Sie die Amazon Bedrock-Konsole und wählen Sie

Modellzugriff. Wählen Sie auf dem nächsten Bildschirm die Option Bestimmte Modelle aktivieren und wählen Sie diese drei Modelle aus:

- Claude, 3, Sonett
- Claude 3.5 Sonett
- Claude 3 Haiku

- Richtige IAM-Richtlinien und IAM-Rolle. Um das Notebook in Ihrer AWS Identity and Access Management (IAM-) Rolle ausführen zu können AWS-Konto, benötigen Sie die `SagemakerFullAccess` Richtlinie sowie die Richtlinie, die im Abschnitt Zusätzliche Informationen angegeben ist, den Sie benennen können. `APGtext2querydslpolicy` Diese Richtlinie beinhaltet das Abonnieren der drei aufgeführten Claude-Modelle.

Wenn diese Voraussetzungen erfüllt sind, wird ein reibungsloser Ablauf bei der Arbeit mit dem Notebook und der Implementierung der text-to-query Funktionen gewährleistet.

Einschränkungen

- Status des Machbarkeitsnachweises. Dieses Projekt ist in erster Linie als Machbarkeitsnachweis (PoC) gedacht. Es zeigt das Potenzial der Umwandlung von Abfragen LLMs in natürlicher Sprache in Query-DSL, ist jedoch möglicherweise nicht vollständig optimiert oder produktionsbereit.
- Einschränkungen des Modells:

  Einschränkungen des Kontextfensters. Beachten Sie bei der Verwendung der LLMs , die auf Amazon Bedrock verfügbar sind, die Einschränkungen des Kontextfensters:

  Claude-Modelle (Stand September 2024):

  - Claude 3 Opus: 200.000 Tokens
  - Claude 3 Sonnet: 200.000 Wertmarken
  - Claude 3 Haiku: 200.000 Tokens

  Andere Modelle auf Amazon Bedrock haben möglicherweise andere Kontextfenstergrößen. Die neuesten Informationen finden Sie immer in der neuesten Dokumentation.

  Verfügbarkeit des Modells.Die Verfügbarkeit bestimmter Modelle bei Amazon Bedrock kann variieren. Stellen Sie sicher, dass Sie Zugriff auf die erforderlichen Modelle haben, bevor Sie diese Lösung implementieren.
- Zusätzliche Einschränkungen

- Komplexität der Abfrage. Die Effektivität der DSL-Konvertierung von natürlicher Sprache zur Abfrage kann je nach Komplexität der Eingabeabfrage variieren.
- Versionskompatibilität. Die generierte DSL-Abfrage erfordert möglicherweise Anpassungen, die auf der spezifischen Version von Elasticsearch oder OpenSearch der von Ihnen verwendeten Version basieren.
- Leistung. Dieses Muster bietet eine PoC-Implementierung, sodass die Geschwindigkeit und Genauigkeit der Abfragegenerierung für den Einsatz in großen Produktionsmengen möglicherweise nicht optimal sind.
- Kosten. Die Verwendung LLMs in Amazon Bedrock ist kostenpflichtig. Beachten Sie die Preisstruktur für das von Ihnen gewählte Modell. Weitere Informationen finden Sie unter Amazon Bedrock — Preise.
- Wartung. Regelmäßige Aktualisierungen der Eingabeaufforderungen und der Modellauswahl sind möglicherweise erforderlich, um mit den Fortschritten in der LLM-Technologie und den Änderungen der Abfrage-DSL-Syntax Schritt zu halten.

Produktversionen

Diese Lösung wurde in Amazon OpenSearch Service getestet. Wenn Sie Elasticsearch verwenden möchten, müssen Sie möglicherweise einige Änderungen vornehmen, um die genaue Funktionalität dieses Musters zu replizieren.

- OpenSearch Versionskompatibilität. OpenSearch behält die Abwärtskompatibilität innerhalb der Hauptversionen bei. Zum Beispiel:
  - OpenSearch 1.x-Clients sind im Allgemeinen mit OpenSearch 1.x-Clustern kompatibel.
  - OpenSearch 2.x-Clients sind im Allgemeinen mit 2.x-Clustern kompatibel OpenSearch .

  Es ist jedoch immer am besten, wenn möglich dieselbe Nebenversion für Client und Cluster zu verwenden.
- OpenSearch API-Kompatibilität. OpenSearch behält die API-Kompatibilität mit Elasticsearch OSS 7.10.2 für die meisten Operationen bei. Es gibt jedoch einige Unterschiede, insbesondere in neueren Versionen.
- OpenSearch Überlegungen zum Upgrade:
  - Direkte Downgrades werden nicht unterstützt. Verwenden Sie bei Bedarf Snapshots für das Rollback.

- Wenn Sie ein Upgrade durchführen, überprüfen Sie die Kompatibilitätsmatrix und die Versionshinweise auf wichtige Änderungen.

Überlegungen zu Elasticsearch

- Elasticsearch-Version. Die Hauptversion von Elasticsearch, die Sie verwenden, ist entscheidend, da sich die Abfragesyntax und die Funktionen zwischen den Hauptversionen ändern können. Derzeit ist Elasticsearch 8.x die neueste stabile Version. Stellen Sie sicher, dass Ihre Abfragen mit Ihrer spezifischen Elasticsearch-Version kompatibel sind.
- Version der Elasticsearch-Abfrage der DSL-Bibliothek. Wenn Sie die Elasticsearch-Query-DSL-Python-Bibliothek verwenden, stellen Sie sicher, dass ihre Version mit Ihrer Elasticsearch-Version übereinstimmt. Zum Beispiel:
  - Verwenden Sie für Elasticsearch 8.x eine `elasticsearch-dsl` Version, die größer oder gleich 8.0.0, aber kleiner als 9.0.0 ist.
  - Verwenden Sie für Elasticsearch 7.x eine `elasticsearch-dsl` Version, die größer oder gleich 7.0.0, aber kleiner als 8.0.0 ist.
- Version der Client-Bibliothek. Egal, ob Sie den offiziellen Elasticsearch-Client oder einen sprachspezifischen Client verwenden, stellen Sie sicher, dass er mit Ihrer Elasticsearch-Version kompatibel ist.
- Fragen Sie die DSL-Version ab. Query DSL entwickelt sich mit den Elasticsearch-Versionen weiter. Einige Abfragetypen oder Parameter sind möglicherweise veraltet oder wurden in anderen Versionen eingeführt.
- Version zuordnen. Die Art und Weise, wie Sie Zuordnungen für Ihre Indizes definieren und zwischen Versionen wechseln. Schauen Sie immer in der Mapping-Dokumentation für Ihre spezifische Elasticsearch-Version nach.
- Versionen der Analysetools. Wenn Sie Analyzer, Tokenizer oder andere Textanalysetools verwenden, kann sich deren Verhalten oder Verfügbarkeit zwischen den Versionen ändern.

Architektur

Zielarchitektur

Das folgende Diagramm veranschaulicht die Architektur für dieses Muster.

Wobei:

1. Benutzereingabe und Systemaufforderung mit einigen Beispielen für Eingabeaufforderungen. Der Prozess beginnt mit einem Benutzer, der eine Abfrage in natürlicher Sprache oder eine Anfrage zur Schemagenerierung bereitstellt.
2. Amazonas-Grundgestein. Die Eingabe wird an Amazon Bedrock gesendet, das als Schnittstelle für den Zugriff auf das Claude LLM dient.
3. Claude 3 Sonnet LLM. Amazon Bedrock verwendet Claude 3 Sonnet aus der Claude 3-Familie von, um die LLMs Eingabe zu verarbeiten. Es interpretiert und generiert die entsprechende Elasticsearch- oder Query-DSL. OpenSearch Für Schemaanfragen generiert es synthetische Elasticsearch- oder Mappings. OpenSearch
4. DSL-Generierung abfragen. Bei Abfragen in natürlicher Sprache verwendet die Anwendung die Ausgabe des LLM und formatiert sie in eine gültige Elasticsearch- oder OpenSearch Service-Abfrage-DSL.
5. Generierung synthetischer Daten. Die Anwendung verwendet auch Schemas, um synthetisches Elasticsearch zu erstellen, oder OpenSearch Daten, die zu Testzwecken in eine OpenSearch serverlose Sammlung geladen werden.
6. OpenSearch oder Elasticsearch. Die generierte Query-DSL wird anhand einer OpenSearch serverlosen Sammlung für alle Indizes abgefragt. Die JSON-Ausgabe enthält die relevanten Daten und die Anzahl der Treffer aus den Daten, die sich in der Serverless-Sammlung befinden. OpenSearch

Automatisierung und Skalierung

Der Code, der mit diesem Muster bereitgestellt wird, wurde ausschließlich für PoC-Zwecke erstellt. Die folgende Liste enthält einige Vorschläge zur weiteren Automatisierung und Skalierung der Lösung und zur Umstellung des Codes auf die Serienproduktion. Diese Verbesserungen liegen außerhalb des Geltungsbereichs dieses Musters.

- Containerisierung:
  - Dockerisieren Sie die Anwendung, um die Konsistenz in verschiedenen Umgebungen sicherzustellen.
  - Verwenden Sie Container-Orchestrierungsplattformen wie Amazon Elastic Container Service (Amazon ECS) oder Kubernetes für skalierbare Bereitstellungen.
- Serverlose Architektur:
  - Wandeln Sie die Kernfunktionen in AWS Lambda Funktionen um.

    - Verwenden Sie Amazon API Gateway, um RESTful Endpunkte für die Eingabe von Abfragen in natürlicher Sprache zu erstellen.
- Asynchrone Verarbeitung:
    - Implementieren Sie Amazon Simple Queue Service (Amazon SQS), um eingehende Anfragen in die Warteschlange zu stellen.
    - Wird verwendet AWS Step Functions , um den Arbeitsablauf bei der Verarbeitung von Abfragen und der Generierung von Abfrage-DSL zu orchestrieren.
- Zwischenspeichern:
    - Implementieren Sie einen Mechanismus zum Zwischenspeichern der Eingabeaufforderungen.
- Überwachung und Protokollierung:
    - Verwenden Sie Amazon CloudWatch für die Überwachung und Benachrichtigung.
    - Implementieren Sie eine zentrale Protokollierung mit Amazon CloudWatch Logs oder Amazon OpenSearch Service für Protokollanalysen.
- Verbesserungen der Sicherheit:
    - Implementieren Sie IAM-Rollen für eine differenzierte Zugriffskontrolle.
    - Wird verwendet AWS Secrets Manager , um API-Schlüssel und Anmeldeinformationen sicher zu speichern und zu verwalten.
- Einsatz in mehreren Regionen:
    - Erwägen Sie den Einsatz der Lösung auf mehreren Ebenen, AWS-Regionen um die Latenz zu verbessern und die Notfallwiederherstellung zu verbessern.
    - Verwenden Sie Amazon Route 53 für intelligentes Routing von Anfragen.

Durch die Implementierung dieser Vorschläge können Sie diesen PoC in eine robuste, skalierbare und produktionsreife Lösung umwandeln. Wir empfehlen Ihnen, jede Komponente und das gesamte System vor der vollständigen Bereitstellung gründlich zu testen.

Tools

Tools

- Amazon SageMaker AI-Notebooks sind vollständig verwaltete Jupyter-Notebooks für die Entwicklung von maschinellem Lernen. Dieses Muster verwendet Notizbücher als interaktive Umgebung für die Datenexploration, Modellentwicklung und Experimente in Amazon SageMaker

AI. Notebooks bieten eine nahtlose Integration mit anderen SageMaker KI-Funktionen und AWS-Services.

- Python ist eine Allzweck-Computerprogrammiersprache. Dieses Muster verwendet Python als Kernsprache für die Implementierung der Lösung.
- Amazon Bedrock ist ein vollständig verwalteter Service, der Ihnen leistungsstarke Basismodelle (FMs) von führenden KI-Startups und Amazon über eine einheitliche API zur Verfügung stellt. Amazon Bedrock bietet Zugriff auf LLMs für die Verarbeitung natürlicher Sprache. Dieses Muster verwendet Modelle von Anthropic Claude 3.
- AWS SDK für Python (Boto3)ist ein Software-Entwicklungskit, mit dem Sie Ihre Python-Anwendung, -Bibliothek oder Ihr Python-Skript integrieren können AWS-Services, einschließlich Amazon Bedrock.
- Amazon OpenSearch Service ist ein verwalteter Service, der Sie bei der Bereitstellung, dem Betrieb und der Skalierung von OpenSearch Service-Clustern in der AWS-Cloud unterstützt. Dieses Muster verwendet OpenSearch Service als Zielsystem für die Generierung von Abfrage-DSL.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub Prompt Engineering Text-to-QueryDSL Using Claude 3 Models verfügbar. In dem Beispiel wird eine Gesundheits-App für soziale Medien verwendet, die Beiträge für Benutzer und Benutzerprofile erstellt, die mit der Gesundheitsanwendung verknüpft sind.

Bewährte Methoden

Beachten Sie bei der Arbeit mit dieser Lösung Folgendes:

- Für den Zugriff auf Amazon Bedrock sind die richtigen AWS Anmeldeinformationen und Berechtigungen erforderlich
- Mögliche Kosten im Zusammenhang mit der Nutzung von AWS-Services und LLMs
- Wie wichtig es ist, sich mit Query-DSL vertraut zu machen, um die generierten Abfragen zu validieren und gegebenenfalls zu modifizieren

Epen

Richten Sie die Umgebung ein und bereiten Sie die Daten vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Entwicklungsumgebung ein.	**Note** Detaillierte Anweisungen und Code für diesen und die anderen Schritte in diesem Muster finden Sie in der umfassenden exemplarischen Vorgehensweise im GitHub Repository. 1. Installieren Sie die erforderlichen Python-Pakete `boto3`, einschließlich `numpy`, `awscli`, `opensearch-py` , und mithilfe `requests-aws4auth` von pip. 2. Importieren Sie die erforderlichen Module wie `boto3`, `json`, `os`, `opensearch` from `opensearchpy` , `RequestsHttpConnection` from `Opensearchpy` , `bulk` `opensearchpy.helpers` from `sagemaker` , `time`,	Python, Pip, AWS-SDK

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`randomre`, und `AWS4Auth` from`requests_aws4auth` .	
AWS Zugriff einrichten.	Richten Sie den Amazon Bedrock-Client und die SageMaker KI-Sitzung ein. Rufen Sie den Amazon-Ressourcennamen (ARN) für die SageMaker AI-Ausführungsrolle ab, um ihn später bei der Erstellung der OpenSearch Serverless-Sammlung zu verwenden.	IAM, AWS-CLI, Amazon Bedrock, Amazon SageMaker
Laden Sie die Schemas von Gesundheits-Apps.	Lesen und analysieren Sie JSON-Schemas für Gesundheitsposts und Benutzerprofile aus vordefinierten Dateien. Konvertiert Schemas in Zeichenketten für die spätere Verwendung in Eingabeaufforderungen.	DevOps Ingenieur, allgemein AWS, Python, JSON

Generieren Sie synthetische Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen LLM-basierten Datengenerator.	Implementieren Sie die Funktion generate_data (), um die Amazon Bedrock Converse-API mit Claude 3-Modellen aufzurufen. Modell IDs für Sonnet, Sonnet 3.5 und Haiku einrichten:	Python, Amazon Bedrock API, LLM-Aufforderung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`model_id_sonnet3_5 = "anthropic.claude-3-5-sonnet-20240620-v1:0"`
	`model_id_sonnet = "anthropic.claude-3-sonnet-20240229-v1:0"`
	`model_id_haiku = "anthropic.claude-3-haiku-20240307-v1:0"`	

Erstellen Sie synthetische Gesundheitsbeiträge.	Verwenden Sie die Funktion generate_data () mit einer bestimmten Eingabeau fforderung, um synthetische Gesundheitsbeiträge auf der Grundlage des bereitgestellten Schemas zu erstellen. Der Funktionsaufruf sieht wie folgt aus: `health_post_data = generate_data(bedrock_rt, model_id_sonnet, system_prompt, message_healthpost, inference_config)`	Python, JSON

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie synthetische Benutzerprofile.	Verwenden Sie die Funktion generate_data () mit einer bestimmten Meldungsa ufforderung, um synthetische Benutzerprofileinträge auf der Grundlage des bereitges tellten Schemas zu erstellen . Dies ähnelt der Generieru ng von Gesundheitsbeiträgen, verwendet jedoch eine andere Eingabeaufforderung.	Python, JSON

Daten einrichten OpenSearch und aufnehmen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine OpenSearch serverlose Sammlung ein.	Verwenden Sie Boto3, um eine OpenSearch serverlos e Sammlung mit entsprech enden Verschlüsselungs-, Netzwerk- und Zugriffsr ichtlinien zu erstellen. Die Erstellung der Sammlung sieht wie folgt aus: `collection = aoss_clie nt.create_collecti on(name=es_name, type='SEARCH')` Weitere Informationen zu OpenSearch Serverless finden Sie in der AWS Dokumenta tion.	OpenSearch Serverlos, IAM

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie Indizes OpenSearch .	Erstellen Sie mithilfe des OpenSearch Clients Indizes für Gesundheitsposts und Benutzerprofile auf der Grundlage der vordefinierten Schemazuordnungen. Die Indexerstellung sieht wie folgt aus: `response_health = oss_client.indices.create(healthpost_index, body=healthpost_body)`	OpenSearch, JSON
Daten laden in OpenSearch.	Führen Sie die Funktion ingest_data () aus, um die synthetischen Gesundheitsbeiträge und Benutzerprofile massenweise in ihre jeweiligen Indizes einzufügen. OpenSearch Die Funktion verwendet den Bulk-Helper von: `opensearch-py` `success, failed = bulk(oss_client, actions)`	Python, OpenSearch API, Massendatenoperationen

Abfragen generieren und ausführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entwerfen Sie einige Beispiele für Eingabeaufforderungen.	Generieren Sie Beispielabfragen und entsprech	LLM-Aufforderung, DSL abfragen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ende Fragen in natürlicher Sprache, indem Sie Claude-3-Modelle verwenden, die als Beispiele für die Generieru ng von Abfragen dienen. Die Systemaufforderung enthält die folgenden Beispiele: `system_prompt_quer y_generation = [{"text": f"""You are an expert query dsl generator. ... Examples: {example_ prompt} ..."""}]`	
Erstellen Sie einen DSL-Konverter text-to-query.	Implementieren Sie die Systemaufforderung, die Schemas, Daten und einige Beispiele enthält, für die Abfragegenerierung. Verwenden Sie die Systemauf forderung, um Abfragen in natürlicher Sprache in DSL-Abfragen zu konvertieren. Der Funktionsaufruf sieht wie folgt aus: `query_response = generate_data(bedr ock_rt, model_id, system_prompt_quer y_generation, query, inference_config)`	Python, Amazon Bedrock API, LLM-Aufforderung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Abfrage DSL auf. OpenSearch	Führen Sie die Funktion query_oss () aus, um die generierte DSL-Abfrage für die OpenSearch Serverless-Sammlung auszuführen und Ergebnisse zurückzugeben. Die Funktion verwendet die Suchmethode des OpenSearch Clients: `response = oss_client.search(index="_all", body=temp)`	Python, OpenSearch API, DSL abfragen

Testen und auswerten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Testabfragesatz.	Verwenden Sie Claude 3, um einen vielfältigen Satz von Testfragen auf der Grundlage der synthetischen Daten und Schemas zu generieren: `test_queries = generate_data(bedrock_rt, model_id_sonnet, query_system_prompt, query_prompt, inference_config)`	LLM-Aufforderung
Beurteilen Sie die Genauigkeit der DSL-Konvertierung der Abfrage.	Testen Sie die generierte DSL-Abfrage, indem Sie Abfragen ausführen OpenSearch und die	Python, Datenanalyse, Abfrage DSL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zurückgegebenen Ergebnisse auf Relevanz und Genauigkeit analysieren. Dazu gehört das Ausführen der Abfrage und das Überprüfen der Treffer: `output = query_oss (response1) print("Response after running query against Opensearch") print(output)`	
Benchmark Claude 3-Modelle.	Vergleichen Sie die Leistung verschiedener Claude-3-Modelle (Haiku, Sonnet, Sonnet 3.5) bei der Abfragegenerierung in Bezug auf Genauigkeit und Latenz. Ändern Sie zum Vergleich den `model_id` Zeitpunkt, zu dem Sie generate_data () aufrufen, und messen Sie die Ausführungszeit.	Python, Leistungsbenchmarking

Aufräumen und dokumentieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entwickeln Sie einen Bereinigungsprozess.	Löschen Sie nach der Verwendung alle Indizes aus der OpenSearch Serverless-Sammlung.	Python, AWS-SDK, OpenSearch API

Zugehörige Ressourcen

- DSL abfragen (OpenSearch Dokumentation)
- Amazon OpenSearch Service-Dokumentation
- OpenSearch Serverlose Sammlungen
- Dokumentation zu Amazon Bedrock
- Dokumentation zu Amazon SageMaker AI
- AWS SDK für Python (Boto3) Dokumentation

Zusätzliche Informationen

IAM-Richtlinie

Hier ist die `APGtext2querydslpolicy` Richtlinie für die IAM-Rolle, die in diesem Muster verwendet wird:

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Effect": "Allow",
      "Action": [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource": "*"
    },
    { "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::sagemaker-*",
        "arn:aws:s3:::sagemaker-*/*"
      ]
    },
    { "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
```

```
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    { "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "*"
    },
    { "Effect": "Allow",
      "Action": [
        "aoss:*"
      ],
      "Resource": "*"
    },
    { "Effect": "Allow",
      "Action": [
        "iam:PassRole",
        "sagemaker:*"
      ],
      "Resource": [
        "arn:aws:iam::*:role/*", "*"
      ],
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "sagemaker.amazonaws.com"
          }
      }
    },
    { "Effect": "Allow",
      "Action": [
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "codecommit:ListRepositories"
      ],
      "Resource": "*"
    },
    { "Effect": "Allow",
```

```
      "Action": [
        "aws-marketplace:Subscribe"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws-marketplace:ProductId": [
            "prod-6dw3qvchef7zy",
            "prod-m5ilt4siql27k",
            "prod-ozonys2hmmpeu"
          ]
        }
      }
    },
    { "Effect": "Allow",
      "Action": [
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource": "*"
    },
    { "Effect": "Allow",
      "Action": "iam:*",
      "Resource": "*"
    }
  ]
}
```

Schnelle Techniken mit Modellen von Anthropic Claude 3

Dieses Muster veranschaulicht die folgenden Aufforderungstechniken für die text-to-query DSL-Konvertierung unter Verwendung von Claude-3-Modellen.

- Few-Shot-Prompting: Few-Shot-Prompting ist eine leistungsstarke Technik zur Verbesserung der Leistung von Claude 3-Modellen auf Amazon Bedrock. Bei diesem Ansatz wird dem Modell eine kleine Anzahl von Beispielen zur Verfügung gestellt, die die gewünschten input/output behavior before asking it to perform a similar task. When you use Claude 3 models on Amazon Bedrock, few-shot prompting can be particularly effective for tasks that require specific formatting, reasoning patterns, or domain knowledge. To implement this technique, you typically structure your prompt with two main components: the example section and the actual query. The example section contains one or more input/output Paare zur Veranschaulichung der Aufgabe veranschaulichen, und im Abfrageabschnitt wird die neue Eingabe vorgestellt, für die Sie eine Antwort wünschen.

Diese Methode hilft Claude 3, den Kontext und das erwartete Ausgabeformat zu verstehen, und führt häufig zu einer genaueren und konsistenteren Antwort.

Beispiel:

```
"query": {
  "bool": {
    "must": [
      {"match": {"post_type": "recipe"}},
      {"range": {"likes_count": {"gte": 100}}},
      {"exists": {"field": "media_urls"}}
    ]
  }
}
Question: Find all recipe posts that have at least 100 likes and include media URLs.
```

- Systemaufforderungen: Neben der Eingabeaufforderung mit wenigen Eingabeaufforderungen unterstützen die Claude 3-Modelle auf Amazon Bedrock auch die Verwendung von Systemaufforderungen. Systemaufforderungen sind eine Möglichkeit, dem Modell einen allgemeinen Kontext, Anweisungen oder Richtlinien zu geben, bevor es mit spezifischen Benutzereingaben versehen wird. Sie sind besonders nützlich, um den Ton anzugeben, die Rolle des Modells zu definieren oder Einschränkungen für die gesamte Konversation festzulegen. Um eine Systemaufforderung mit Claude 3 auf Amazon Bedrock zu verwenden, fügen Sie sie in den `system` Parameter Ihrer API-Anfrage ein. Dies ist unabhängig von den Benutzernachrichten und gilt für die gesamte Interaktion. Detaillierte Systemaufforderungen werden verwendet, um den Kontext festzulegen und Richtlinien für das Modell bereitzustellen.

  Beispiel:

```
You are an expert query dsl generator. Your task is to take an input question and
 generate a query dsl to answer the question. Use the schemas and data below to
 generate the query.

Schemas: [schema details]
Data: [sample data]
Guidelines:
- Ensure the generated query adheres to DSL query syntax
- Do not create new mappings or other items that aren't included in the provided
 schemas.
```

- Strukturierte Ausgabe: Sie können das Modell anweisen, die Ausgabe in bestimmten Formaten wie JSON oder innerhalb von XML-Tags bereitzustellen.

  Beispiel:

  ```
  Put the query in json tags
  ```

- Verkettung von Eingabeaufforderungen: Das Notizbuch verwendet die Ausgabe eines LLM-Aufrufs als Eingabe für einen anderen, z. B. mithilfe generierter synthetischer Daten, um Beispielfragen zu erstellen.
- Bereitstellung von Kontext: Der relevante Kontext, einschließlich Schemas und Beispieldaten, wird in den Eingabeaufforderungen bereitgestellt.

  Beispiel:

  ```
  Schemas: [schema details]
  Data: [sample data]
  ```

- Aufgabenspezifische Eingabeaufforderungen: Für bestimmte Aufgaben, z. B. das Generieren synthetischer Daten, das Erstellen von Beispielfragen und das Konvertieren von Abfragen in natürlicher Sprache in DSL-Abfragen, werden unterschiedliche Aufforderungen erstellt.

  Beispiel für die Generierung von Testfragen:

  ```
  Your task is to generate 5 example questions users can ask the health app based on
   provided schemas and data. Only include the questions generated in the response.
  ```

Verwenden Sie Amazon Q Developer als Programmierassistenten, um Ihre Produktivität zu steigern

Erstellt von Ram Kandaswamy (AWS)

Übersicht

In diesem Muster wird anhand eines tic-tac-toe Spiels demonstriert, wie Sie Amazon Q Developer für eine Reihe von Entwicklungsaufgaben einsetzen können. Es generiert Code für ein tic-tac-toe Spiel als einseitige Anwendung (SPA), verbessert die Benutzeroberfläche und erstellt Skripts, auf AWS denen die Anwendung bereitgestellt wird.

Amazon Q Developer fungiert als Programmierassistent, um Arbeitsabläufe bei der Softwareentwicklung zu beschleunigen und die Produktivität sowohl für Entwickler als auch für Nicht-Entwickler zu steigern. Unabhängig von Ihrem technischen Fachwissen hilft es Ihnen dabei, Architekturen zu erstellen und Lösungen für Geschäftsprobleme zu entwerfen, Ihre Arbeitsumgebung zu optimieren, neue Funktionen zu implementieren und Testfälle zur Validierung zu generieren. Es verwendet Anweisungen in natürlicher Sprache und KI-Funktionen, um einen konsistenten, qualitativ hochwertigen Code zu gewährleisten und Programmierprobleme zu minimieren, unabhängig von Ihren Programmierkenntnissen.

Der Hauptvorteil von Amazon Q Developer ist seine Fähigkeit, Sie von sich wiederholenden Codierungsaufgaben zu befreien. Wenn Sie die `@workspace` Anmerkung verwenden, erfasst und indexiert Amazon Q Developer alle Codedateien, Konfigurationen und Projektstrukturen in Ihrer integrierten Entwicklungsumgebung (IDE) und bietet maßgeschneiderte Antworten, damit Sie sich auf die kreative Problemlösung konzentrieren können. Sie können mehr Zeit für die Entwicklung innovativer Lösungen und die Verbesserung der Benutzererfahrung aufwenden. Wenn Sie nicht technisch versiert sind, können Sie Amazon Q Developer verwenden, um Arbeitsabläufe zu optimieren und effektiver mit dem Entwicklungsteam zusammenzuarbeiten. Die Amazon Q Developer Explain Code-Funktion bietet detaillierte Anweisungen und Zusammenfassungen, sodass Sie sich in komplexen Codebasen zurechtfinden.

Darüber hinaus bietet Amazon Q Developer einen sprachunabhängigen Ansatz, der jüngeren und mittleren Entwicklern hilft, ihre Fähigkeiten zu erweitern. Sie können sich auf Kernkonzepte und Geschäftslogik statt auf die sprachspezifische Syntax konzentrieren. Dies reduziert die Lernkurve, wenn Sie die Technologie wechseln.

Voraussetzungen und Einschränkungen

Voraussetzungen

- IDE (zum Beispiel WebStorm oder Visual Studio Code) mit installiertem Amazon Q Developer-Plugin. Anweisungen finden Sie unter Installation der Amazon Q Developer-Erweiterung oder des Amazon Q Developer-Plugins in Ihrer IDE in der Amazon Q Developer-Dokumentation.
- Eine aktive AWS-Konto Einrichtung mit Amazon Q Developer. Anweisungen finden Sie unter Erste Schritte in der Amazon Q Developer-Dokumentation.
- npm ist installiert. Anweisungen finden Sie in der npm-Dokumentation. Dieses Muster wurde mit npm Version 10.8 getestet.
- AWS Command Line Interface (AWS CLI) installiert. Anweisungen finden Sie in der AWS CLI Dokumentation.

Einschränkungen

- Amazon Q Developer kann jeweils nur eine Entwicklungsaufgabe ausführen.
- Einige AWS-Services sind nicht in allen verfügbar AWS-Regionen. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie auf der Seite Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Tools

- Für dieses Muster ist eine IDE wie Visual Studio Code oder erforderlich. WebStorm Eine Liste der unterstützten IDEs Produkte finden Sie in der Amazon Q Developer-Dokumentation.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie AWS-Services über Befehle in Ihrer Befehlszeilen-Shell interagieren können.

Bewährte Methoden

Weitere Informationen finden Sie unter Bewährte Programmierpraktiken mit Amazon Q Developer in AWS Prescriptive Guidance. Darüber hinaus gilt:

- Wenn Sie Amazon Q Developer auffordern, stellen Sie sicher, dass Ihre Anweisungen klar und eindeutig sind. Fügen Sie der Aufforderung Codefragmente und Anmerkungen hinzu, `@workspace` um mehr Kontext für Ihre Eingabeaufforderungen bereitzustellen.
- Fügen Sie relevante Bibliotheken hinzu und importieren Sie sie, um Konflikte oder falsche Vermutungen durch das System zu vermeiden.
- Wenn der generierte Code nicht korrekt oder erwartungsgemäß ist, verwenden Sie die Option Feedback geben und neu generieren. Versuchen Sie, die Eingabeaufforderungen in kleinere Anweisungen aufzuteilen.

Epen

Richten Sie die Arbeitsumgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellt ein neues Projekt.	Um ein neues Projekt in Ihrer Arbeitsumgebung zu erstellen , führen Sie den folgenden Befehl aus und akzeptieren Sie die Standardeinstellungen für alle Fragen: `npx create-next-app@latest`	App-Entwickler, Programmierer, Softwareentwickler
Testen Sie die Basisanwendung.	Führen Sie den folgenden Befehl aus und vergewissern Sie sich, dass die Basisanwendung erfolgreich im Browser geladen wurde: `npm run dev`	App-Entwickler, Programmierer, Softwareentwickler
Bereinigen Sie den Basiscode.	Navigieren Sie zu der `page.tsx` Datei im `src/app` Ordner und löschen Sie den	App-Entwickler, Programmierer, Softwareentwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Standardinhalt, um eine leere Seite zu erhalten. Nach dem Löschen sollte die Datei wie folgt aussehen: `export default function Home() { return (<div></div>); }`	

Verwenden Sie Amazon Q Developer, um ein tic-tac-toe Spieleprojekt zu entwerfen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verschaffen Sie sich einen Überblick über die Schritte.	1. Öffnen Sie in Ihrer IDE Ihr Projekt und wählen Sie das Amazon Q-Symbol, um das Chat-Panel zu öffnen. 2. Fragen Sie im Amazon Q Developer-Chat-Panel nach einer Übersicht über die Erstellung einer Single-Page-Anwendung (SPA). Zum Beispiel: `I would like to create a single-page application involving Next.js React framework for tic-tac-toe game. What are the steps?`	App-Entwickler, Programmierer, Softwareentwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Code generieren für tic-tac-toe.	Starten Sie im Chat-Panel eine Entwicklungsaufgabe, indem Sie den `/dev` Befehl gefolgt von der Beschreibung der Aufgabe verwenden. Zum Beispiel:
	`/dev Create a React-based single-page application written in TypeScript for a tic-tac-toe game with the following specifications:`
	`1. Design an aesthetically pleasing interface with the game grid centered vertically and horizontally on the page.`
	`2. Include a heading and clear instructions on how to play the game.`
	`3. Implement color-coding for X and O marks to distinguish them easily.`
	Amazon Q Developer generiert Code auf der Grundlage Ihrer Anweisungen.
		App-Entwickler, Programmierer, Softwareentwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Untersuchen und akzeptieren Sie den generierten Code.	Untersuchen Sie den Code visuell und wählen Sie Code akzeptieren, um die `page.tsx` Datei automatisch zu ersetzen. Wenn Sie auf Probleme stoßen, wählen Sie Feedback geben und erneut generiere n und beschreiben Sie das aufgetretene Problem.	App-Entwickler, Programmi erer, Softwareentwickler
Korrigieren Sie Lint-Fehler.	Das tic-tac-toe Beispiels piel enthält ein Raster. Der Code, den Amazon Q Developer generiert , verwendet möglicher weise den Standardtyp`any`. Sie können Typsicherheit hinzufügen, indem Sie Amazon Q Developer wie folgt auffordern: `/dev Ensure proper TypeScript typing for the onSquare Click event handler to resolve any 'any' type issues.`	App-Entwickler, Programmi erer, Softwareentwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie visuellen Reiz hinzu.	Sie können die ursprüngliche Anforderung in kleinere Fragmente aufteilen. Beispielsweise kannst du die Benutzeroberfläche des Spiels mit den folgenden Eingabeaufforderungen in den Entwickleraufgaben verbessern. Diese Aufforderung verbessert die CSS-Stile (Cascading Style Sheets) und exportiert die App zur Bereitstellung.
	`/dev Debug and fix any CSS issues to correctly display the game grid and overall layout.`
	`Simplify the code by removing game history functionality and related components.`
	`Implement static file export to an 'out' directory for easy deployment. The solution should be fully functional, visually appealing, and free of typing errors or layout issues.`
		App-Entwickler, Programmierer, Softwareentwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Testen Sie erneut.	1. Nachdem Sie den Entwicklungszyklus abgeschlossen haben, testen Sie den Code, um sicherzustellen, dass er wie erwartet funktioniert. Verwenden Sie den folgenden Befehl, um die Anwendung lokal auszuführen:
	`npm run dev`
	2. Wenn die Anwendung erwartungsgemäß funktioniert, verwenden Sie den `build` Befehl, um die gesamte Anwendung zur Vorbereitung der Bereitstellung in den Ausgabeordner zu exportieren:
	`npm run build`
		App-Entwickler, Programmierer, Softwareentwickler

Stellen Sie die Anwendung auf dem bereit AWS Cloud

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Ordner und Dateien für die Bereitstellung.	Erstellen Sie im Projekt in Ihrer Arbeitsumgebung einen Bereitstellungsordner und zwei darin enthaltene Dateien: `pushtos3.sh` und`cloudformation.yml` :	App-Entwickler, Programmierer, Softwareentwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`mkdir deployment && cd deployment`
	`touch pushtos3.sh && chmod +x pushtos3.sh`
	`touch cloudformation.yml`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Generieren Sie Automatisierungscode.	1. Geben Sie im Chat-Panel für Amazon Q Developer die folgende Aufforderung ein:
	
	`/dev Generate a Cloudformation template that creates two resources: tictactoe artifact bucket and CloudFront. CloudFront should be configured with this bucket as origin.`
	`Add cache policy appropriate for Amazon S3 and default root object as index.html.`
	`Ensure that origin access control is used and no public bucket is created.`
	`Output all the resources and their ARNs.`
	
	2. Überprüfen und akzeptieren Sie den generierten Code. Die `cloudformation.yml` Datei, die Sie zuvor erstellt haben, sollte jetzt mit einem AWS CloudFormation Skript gefüllt sein, das die Ressourcen für erstellt AWS Cloud.
		AWS-Administrator, AWS DevOps, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie Skriptinhalte.	Verwenden Sie die folgende Eingabeaufforderung, um ein Bereitstellungsskript zu erstellen: `/dev Modify the pushtos3 shell script so that it can use AWS CLI commands to create a CloudFormation stack named tictactoe-stack if it does not exist already, and use cloudformation.yml as the source template. Wait for the stack to complete and sync the contents from the out folder to the S3 bucket. Perform invalidation of the CloudFront origin.`	App-Entwickler, Programmierer, Softwareentwickler
Stellen Sie die Anwendung auf dem AWS Cloud bereit.	1. Konfigurieren Sie die Arbeitsumgebung mit gültigen AWS Anmeldeinformationen. 2. Führen Sie das Shell-Skript aus, um das voll funktionsfähige tic-tac-toe Spiel auf dem bereitzustellen AWS Cloud.	AWS-Administrator DevOps, AWS, Cloud-Architekt, App-Entwickler

Fehlerbehebung

Problem	Lösung

Der Build erstellt keine einseitige Anwendung und exportiert sie auch nicht in den Ausgabeordner.	Sehen Sie sich den Inhalt der `next.config.mjs` Datei an.
	
	Wenn der Code die folgende Standardkonfiguration hat:
	
	`const nextConfig = {};`
	
	ändere ihn wie folgt:
	
	`const nextConfig = {`
	`  output: 'export',`
	`  distDir: 'out',`
	`};`

Zugehörige Ressourcen

- Ein neues React-Projekt erstellen (React-Dokumentation)
- Überblick über Amazon Q Developer (AWS Dokumentation)
- Bewährte Methoden für Amazon Q Developer (AWS Prescriptive Guidance)
- Installation, Konfiguration und Verwendung von Amazon Q Developer mit JetBrains IDEs (YouTube Video)
- Installation von Amazon Q für die Befehlszeile (AWS Dokumentation)

Verwenden Sie SageMaker Processing für verteiltes Feature-Engineering von ML-Datensätzen im Terabyte-Bereich

Erstellt von Chris Boomhower (AWS)

Übersicht

Viele Datensätze im Terabyte-Bereich oder größer bestehen oft aus einer hierarchischen Ordnerstruktur, und die Dateien im Datensatz weisen manchmal wechselseitige Abhängigkeiten auf. Aus diesem Grund müssen Ingenieure und Datenwissenschaftler für maschinelles Lernen (ML) durchdachte Designentscheidungen treffen, um solche Daten für Modelltraining und Inferenz aufzubereiten. Dieses Muster zeigt, wie Sie manuelle Macrosharding- und Microsharding-Techniken in Kombination mit Amazon SageMaker Processing und virtueller CPU (vCPU) -Parallelisierung verwenden können, um Feature-Engineering-Prozesse für komplizierte Big-Data-ML-Datensätze effizient zu skalieren.

Dieses Muster definiert Macrosharding als die Aufteilung von Datenverzeichnissen auf mehrere Computer zur Verarbeitung und Microsharding als die Aufteilung von Daten auf jedem Computer über mehrere Verarbeitungsthreads. Das Muster demonstriert diese Techniken, indem Amazon SageMaker mit Beispiel-Zeitreihen-Wellenformaufzeichnungen aus dem MIMIC-III-Datensatz verwendet wirdPhysioNet . Durch die Implementierung der Techniken in diesem Muster können Sie die Verarbeitungszeit und die Kosten für das Feature-Engineering minimieren und gleichzeitig die Ressourcennutzung und Durchsatzeffizienz maximieren. Diese Optimierungen basieren auf verteilter SageMaker Verarbeitung auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances und v CPUs für ähnliche, große Datensätze, unabhängig vom Datentyp.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zugriff auf SageMaker Notebook-Instances oder SageMaker Studio, wenn Sie dieses Muster für Ihren eigenen Datensatz implementieren möchten. Wenn Sie Amazon SageMaker zum ersten Mal verwenden, finden Sie weitere Informationen unter Erste Schritte mit Amazon SageMaker in der AWS-Dokumentation.
- SageMaker Studio, wenn Sie dieses Muster mit den PhysioNet MIMIC-III-Beispieldaten implementieren möchten.
- Das Muster verwendet SageMaker Processing, erfordert jedoch keine Erfahrung mit der Ausführung von SageMaker Processing-Jobs.

Einschränkungen

- Dieses Muster eignet sich gut für ML-Datensätze, die voneinander abhängige Dateien enthalten. Diese Interdependenzen profitieren am meisten von manuellem Macrosharding und der parallel Ausführung mehrerer SageMaker Einzelinstanz-Verarbeitungsjobs. Für Datensätze, bei denen solche Interdependenzen nicht existieren, ist die `ShardedByS3Key` Funktion in SageMaker Processing möglicherweise eine bessere Alternative zum Macrosharding, da sie fragmentierte Daten an mehrere Instanzen sendet, die von demselben Verarbeitungsauftrag verwaltet werden. Sie können jedoch die Microsharding-Strategie dieses Musters in beiden Szenarien implementieren, um Instanz v optimal zu nutzen. CPUs

Produktversionen

- Amazon SageMaker Python SDK, Version 2

Architektur

Zieltechnologie-Stack

- Amazon Simple Storage Service (Amazon-S3)
- Amazon SageMaker

Zielarchitektur

Macrosharding und verteilte Instanzen EC2

Die 10 parallel Prozesse, die in dieser Architektur dargestellt werden, spiegeln die Struktur des MIMIC-III-Datensatzes wider. (Prozesse werden zur Vereinfachung des Diagramms durch Ellipsen dargestellt.) Eine ähnliche Architektur gilt für jeden Datensatz, wenn Sie manuelles Macrosharding verwenden. Im Fall von MIMIC-III können Sie die Rohstruktur des Datensatzes zu Ihrem Vorteil nutzen, indem Sie jeden Patientengruppenordner mit minimalem Aufwand separat verarbeiten. In der folgenden Abbildung wird der Block Datensatzgruppen auf der linken Seite angezeigt (1). Da die Daten verteilt sind, ist es sinnvoll, sie nach Patientengruppen aufzuteilen.

Manuelles Sharding nach Patientengruppen bedeutet jedoch, dass für jeden Patientengruppenordner ein separater Verarbeitungsauftrag erforderlich ist, wie Sie im mittleren Abschnitt des Diagramms (2) sehen können, und nicht ein einziger Verarbeitungsauftrag mit mehreren Instanzen. EC2

Da die Daten von MIMIC-III sowohl binäre Wellenformdateien als auch passende textbasierte Header-Dateien enthalten und für die binäre Datenextraktion eine Abhängigkeit von der WFDB-Bibliothek erforderlich ist, müssen alle Datensätze für einen bestimmten Patienten auf derselben Instanz verfügbar gemacht werden. Die einzige Möglichkeit, sicherzustellen, dass die jeder binären Wellenformdatei zugeordnete Header-Datei auch vorhanden ist, besteht darin, manuelles Sharding zu implementieren, um jeden Shard innerhalb seines eigenen Verarbeitungsjobs auszuführen und anzugeben, `s3_data_distribution_type='FullyReplicated'` wann Sie die Eingabe für den Verarbeitungsjob definieren. Wenn alle Daten in einem einzigen Verzeichnis verfügbar wären und es keine Abhängigkeiten zwischen den Dateien gäbe, könnte es alternativ besser sein, einen einzelnen Verarbeitungsauftrag mit mehreren EC2 Instanzen zu starten und anzugeben. `s3_data_distribution_type='ShardedByS3Key'` Wenn Sie `ShardedByS3Key` als Amazon S3 S3-Datenverteilungstyp angeben, wird SageMaker das Daten-Sharding automatisch über Instances hinweg verwaltet.

Das Starten eines Verarbeitungsauftrags für jeden Ordner ist eine kostengünstige Methode zur Vorverarbeitung der Daten, da die gleichzeitige Ausführung mehrerer Instances Zeit spart. Um zusätzliche Kosten und Zeit zu sparen, können Sie Microsharding für jeden Verarbeitungsauftrag verwenden.

Microsharding und Parallel-V CPUs

Innerhalb jedes Verarbeitungsauftrags werden die gruppierten Daten weiter aufgeteilt, um die Nutzung aller verfügbaren V CPUs auf der SageMaker vollständig verwalteten EC2 Instanz zu maximieren. Die Blöcke im mittleren Abschnitt des Diagramms (2) zeigen, was innerhalb der einzelnen primären Verarbeitungsaufträge passiert. Der Inhalt der Patientenaktenordner wird vereinfacht und gleichmäßig auf der Grundlage der Anzahl der verfügbaren V CPUs auf der Instanz aufgeteilt. Nachdem der Ordnerinhalt aufgeteilt wurde, wird der Satz von Dateien mit gleichmäßiger Größe CPUs zur Verarbeitung auf alle V verteilt. Wenn die Verarbeitung abgeschlossen ist, werden die Ergebnisse jeder vCPU in einer einzigen Datendatei für jeden Verarbeitungsauftrag zusammengefasst.

Im beigefügten Code werden diese Konzepte im folgenden Abschnitt der `src/feature-engineering-pass1/preprocessing.py` Datei dargestellt.

```
def chunks(lst, n):
    """
    Yield successive n-sized chunks from lst.

    :param lst: list of elements to be divided
```

```
    :param n: number of elements per chunk
    :type lst: list
    :type n: int
    :return: generator comprising evenly sized chunks
    :rtype: class 'generator'
    """
    for i in range(0, len(lst), n):
        yield lst[i:i + n]


# Generate list of data files on machine
data_dir = input_dir
d_subs = next(os.walk(os.path.join(data_dir, '.')))[1]
file_list = []
for ds in d_subs:
    file_list.extend(os.listdir(os.path.join(data_dir, ds, '.')))
dat_list = [os.path.join(re.split('_|\.', f)[0].replace('n', ''), f[:-4]) for f in
 file_list if f[-4:] == '.dat']

# Split list of files into sub-lists
cpu_count = multiprocessing.cpu_count()
splits = int(len(dat_list) / cpu_count)
if splits == 0: splits = 1
dat_chunks = list(chunks(dat_list, splits))

# Parallelize processing of sub-lists across CPUs
ws_df_list = Parallel(n_jobs=-1, verbose=0)(delayed(run_process)(dc) for dc in
 dat_chunks)

# Compile and pickle patient group dataframe
ws_df_group = pd.concat(ws_df_list)
ws_df_group = ws_df_group.reset_index().rename(columns={'index': 'signal'})
ws_df_group.to_json(os.path.join(output_dir, group_data_out))
```

Eine Funktion,`chunks`, wird zunächst so definiert, dass sie eine bestimmte Liste verarbeitet, indem sie sie in gleich große Längenabschnitte aufteilt `n` und diese Ergebnisse als Generator zurückgibt. Als Nächstes werden die Daten auf alle Patientenordner reduziert, indem eine Liste aller vorhandenen binären Wellenformdateien erstellt wird. Danach wird die Anzahl von `v` ermittelt, die auf der Instanz CPUs verfügbar ist. EC2 Die Liste der binären Wellenformdateien wird CPUs durch Aufruf gleichmäßig auf diese `v` aufgeteilt`chunks`, und dann wird jede Wellenform-Unterliste auf ihrer eigenen vCPU verarbeitet, indem die Parallel-Klasse von joblib verwendet wird. Die Ergebnisse werden vom Verarbeitungsauftrag automatisch zu einer einzigen Liste von Datenrahmen kombiniert,

der SageMaker dann weiter verarbeitet wird, bevor er nach Abschluss des Auftrags in Amazon S3 geschrieben wird. In diesem Beispiel werden von den Verarbeitungsaufträgen 10 Dateien in Amazon S3 geschrieben (eine für jeden Job).

Wenn alle anfänglichen Verarbeitungsaufträge abgeschlossen sind, kombiniert ein sekundärer Verarbeitungsauftrag, der im Block rechts neben dem Diagramm (3) dargestellt ist, die von jedem primären Verarbeitungsauftrag erstellten Ausgabedateien und schreibt die kombinierte Ausgabe in Amazon S3 (4).

Tools

Tools

- Python — Der für dieses Muster verwendete Beispielcode ist Python (Version 3).
- SageMaker Studio — Amazon SageMaker Studio ist eine webbasierte, integrierte Entwicklungsumgebung (IDE) für maschinelles Lernen, mit der Sie Ihre Machine-Learning-Modelle erstellen, trainieren, debuggen, bereitstellen und überwachen können. Sie führen SageMaker Verarbeitungsaufträge mithilfe von Jupyter-Notebooks in Studio aus. SageMaker
- SageMaker Verarbeitung — Amazon SageMaker Processing bietet eine vereinfachte Möglichkeit, Ihre Datenverarbeitungs-Workloads auszuführen. In diesem Muster wird der Feature-Engineering-Code mithilfe von SageMaker Verarbeitungsaufträgen maßstabsgetreu implementiert.

Code

Die angehängte ZIP-Datei enthält den vollständigen Code für dieses Muster. Im folgenden Abschnitt werden die Schritte zum Erstellen der Architektur für dieses Muster beschrieben. Jeder Schritt wird durch einen Beispielcode aus dem Anhang veranschaulicht.

Epen

Richten Sie Ihre SageMaker Studio-Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Greifen Sie auf Amazon SageMaker Studio zu.	Starten Sie SageMaker Studio über Ihr AWS-Konto, indem Sie den Anweisungen in	Datenwissenschaftler, ML-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der SageMaker Amazon-Dokumentation folgen.	
Installieren Sie das Hilfsprogramm wget.	Installieren Sie wget, wenn Sie mit einer neuen SageMaker Studio-Konfiguration vertraut sind oder wenn Sie diese Dienstprogramme noch nie in Studio verwendet haben. SageMaker Öffnen Sie zur Installation ein Terminalfenster in der SageMaker Studio-Konsole und führen Sie den folgenden Befehl aus: `sudo yum install wget`	Datenwissenschaftler, ML-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Laden Sie den Beispielcode herunter und entpacken Sie ihn.	Laden Sie die `attachments.zip` Datei im Bereich Anlagen herunter. Navigieren Sie in einem Terminalfenster zu dem Ordner, in den Sie die Datei heruntergeladen haben, und extrahieren Sie ihren Inhalt:
	`unzip attachment.zip`
	Navigieren Sie zu dem Ordner, in den Sie die ZIP-Datei extrahiert haben, und extrahieren Sie den Inhalt der `Scaled-Processing.zip` Datei.
	`unzip Scaled-Processing.zip`
		Datenwissenschaftler, ML-Ingenieur

Laden Sie den Beispieldatensatz von physionet.org herunter und laden Sie ihn auf Amazon S3 hoch.	Führen Sie das `get_data.ipynb` Jupyter-Notizbuch in dem Ordner aus, der die Dateien enthält. `Scaled-Processing` Dieses Notizbuch lädt einen MIMIC-III-Beispieldatensatz von physionet.org herunter und lädt ihn in Ihren SageMaker Studio-Sitzungs-Bucket in Amazon S3 hoch.	Datenwissenschaftler, ML-Ingenieur

Konfigurieren Sie das erste Vorverarbeitungsskript

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Reduzieren Sie die Dateihier archie in allen Unterverz eichnissen.	In großen Datensätzen wie MIMIC-III sind Dateien häufig auf mehrere Unterverz eichnisse verteilt, selbst innerhalb einer logischen übergeordneten Gruppe. Ihr Skript sollte so konfiguriert sein, dass alle Gruppenda teien in allen Unterverz eichnissen reduziert werden, wie der folgende Code zeigt.
	`# Generate list of .dat files on machine`
	`data_dir = input_dir`
	`d_subs = next(os.w alk(os.path.join(d ata_dir, '.')))[1]`
	`file_list = []`
	`for ds in d_subs:`
	`  file_list.extend(o s.listdir(os.path. join(data_dir, ds, '.')))`
	`dat_list = [os.path. join(re.split('_|\ .', f)[0].replace('n', ''), f[:-4]) for f in file_list if f[-4:] == '.dat']`
	Note
	Die Beispielc odefragmente in diesem Epos stammen
		Datenwissenschaftler, ML-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	aus der `src/feature-engineering-pass1/preprocessing.py` Datei, die im Anhang enthalten ist.	

Teilen Sie Dateien basierend auf der Anzahl der vCPU in Untergruppen auf.	Dateien sollten in gleichmäßig große Untergruppen oder Blöcke aufgeteilt werden, abhängig von der Anzahl der V, die auf der Instanz CPUs vorhanden sind, die das Skript ausführt. Für diesen Schritt können Sie Code implementieren, der dem folgenden ähnelt.
	`# Split list of files into sub-lists`
	`cpu_count = multiprocessing.cpu_count()`
	`splits = int(len(dat_list) / cpu_count)`
	`if splits == 0: splits = 1`
	`dat_chunks = list(chunks(dat_list, splits))`
		Datenwissenschaftler, ML-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Parallelisieren Sie die Verarbeitung von Untergruppen über v. CPUs	Die Skriptlogik sollte so konfiguriert sein, dass alle Untergruppen parallel verarbeitet werden. Verwenden Sie dazu die `Parallel` Klasse und `delayed` Methode der Joblib-Bibliothek wie folgt.
	`# Parallelize processing of sub-lists across CPUs`
	`ws_df_list = Parallel(n_jobs=-1, verbose=0)(delayed(run_process)(dc) for dc in dat_chunks)`
		Datenwissenschaftler, ML-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Speichern Sie die Ausgabe einer einzelnen Dateigruppe in Amazon S3.	Wenn die parallel vCPU-Verarbeitung abgeschlossen ist, sollten die Ergebnisse jeder vCPU kombiniert und in den S3-Bucket-Pfad der Dateigruppe hochgeladen werden. Für diesen Schritt können Sie Code verwenden, der dem folgenden ähnelt.
	`# Compile and pickle patient group dataframe`
	`ws_df_group = pd.concat(ws_df_list)`
	`ws_df_group = ws_df_group.reset_index().rename(columns={'index': 'signal'})`
	`ws_df_group.to_json(os.path.join(output_dir, group_data_out))`
		Datenwissenschaftler, ML-Ingenieur

Konfigurieren Sie das zweite Vorverarbeitungsskript

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kombinieren Sie Datendateien, die bei allen Verarbeitungsaufträgen erstellt wurden, bei denen das erste Skript ausgeführt wurde.	Das vorherige Skript gibt für jeden SageMaker Verarbeitungsjob, der eine Gruppe von Dateien aus dem Datensatz verarbeitet, eine einzelne Datei aus. Als Nächstes müssen Sie diese Ausgabedateien zu einem einzigen	Datenwissenschaftler, ML-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Objekt kombinieren und einen einzigen Ausgabedatensatz in Amazon S3 schreiben. Dies wird in der `src/feature-engineering-pass1p5/preprocessing.py` Datei, die im Anhang bereitgestellt wird, wie folgt demonstriert.
	
	`def write_parquet(wavs_df, path):`
	`"""`
	`Write waveform summary dataframe to S3 in parquet format.`
	
	`:param wavs_df: waveform summary dataframe`
	`:param path: S3 directory prefix`
	`:type wavs_df: pandas dataframe`
	`:type path: str`
	`:return: None`
	`"""`
	`extra_args = {"ServerSideEncryption": "aws:kms"}`
	`wr.s3.to_parquet(`
	`df=wavs_df,`
	`path=path,`
	`compression='snappy',`
	`s3_additional_kwargs=extra_args)`
	
	`def combine_data():`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> """
	    Get combined data
	 and write to parquet.
	
	    :return: waveform
	 summary dataframe
	    :rtype: pandas
	 dataframe
	    """
	    wavs_df = get_data(
	)
	    wavs_df = normalize
	_signal_names(wavs
	_df)
	    write_parquet(wavs
	_df, "s3://{}/{}/
	{}".format(buck
	et_xform, dataset_p
	refix, pass1p5ou
	t_data))
	
	    return wavs_df
	
	wavs_df = combine_d
	ata()</pre>	

Verarbeitungsaufträge ausführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den ersten Verarbeitungsauftrag aus.	Um Macrosharding durchzuführen, führen Sie für jede Dateigruppe einen separaten Verarbeitungsauftrag aus. Microsharding wird innerhalb jedes Verarbeitungsauftrags ausgeführt, da jeder Job Ihr	Datenwissenschaftler, ML-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	erstes Skript ausführt. Der folgende Code zeigt, wie ein Verarbeitungsauftrag für jedes Dateigruppenverzeichnis im folgenden Codeausschnitt (enthalten in) gestartet wird. `notebooks/FeatExtract_Pass1.ipynb`
	
	`pat_groups = list(range(30,40))`
	`ts = str(int(time.time()))`
	
	`for group in pat_groups:`
	`  sklearn_processor = SKLearnProcessor(framework_version='0.20.0',`
	
	`  role=role,`
	
	`  instance_type='ml.m5.4xlarge',`
	
	`  instance_count=1,`
	
	`  volume_size_in_gb=5)`
	`  sklearn_processor.run(`
	`  code='../src/feature-engineering-pass1/preprocessing.py',`
	`  job_name='-'.join(['scaled-`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	processing-p1', str(group), ts]), arguments=["input_path", "/opt/ml/processing/input", "output_path", "/opt/ml/processing/output", "group_data_out", "ws_df_group.json"], inputs= [ProcessingInput(source=f's3://{sess.default_bucket()}/data_inputs/{group}', destination='/opt/ml/processing/input', s3_data_distribution_type='FullyReplicated')], outputs= [ProcessingOutput(source='/opt/ml/processing/output', destination=f's3://{sess.default_bucket()}/data_outputs/{group}'	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>)
	        ],
	        wait=False
	    )</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Führen Sie den zweiten Verarbeitungsauftrag aus.	Um die vom ersten Satz von Verarbeitungsaufträgen generierten Ausgaben zu kombinieren und zusätzliche Berechnungen für die Vorverarbeitung durchzuführen, führen Sie Ihr zweites Skript mit einem einzigen SageMaker Verarbeitungsauftrag aus. Der folgende Code veranschaulicht dies (enthalten in `notebooks/FeatExtract_Pass1p5.ipynb`).
	
	`ts = str(int(time.time()))`
	`bucket = sess.default_bucket()`
	
	`sklearn_processor = SKLearnProcessor(framework_version='0.20.0',`
	
	`role=role,`
	
	`instance_type='ml.t3.2xlarge',`
	
	`instance_count=1,`
	
	`volume_size_in_gb=5)`
	`sklearn_processor.run(`
	`code='../src/feature-engineering-pass1p5/preprocessing.py',`
		Datenwissenschaftler, ML-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`job_name='-'.join(['scaled-processing', 'p1p5', ts]), arguments=['bucket', bucket, 'pass1out_prefix', 'data_outputs', 'pass1out_data', 'ws_df_group.json', 'pass1p5out_data', 'waveform_summary.parquet', 'statsdata_name', 'signal_stats.csv'], wait=True )`	

Zugehörige Ressourcen

- Mit Quick Start in Amazon SageMaker Studio einsteigen (SageMaker Dokumentation)
- Daten verarbeiten (SageMaker Dokumentation)
- Datenverarbeitung mit Scikit-Learn (Dokumentation) SageMaker
- JobLib.Parallel-Dokumentation
- Moody, B., Moody, G., Villarroel, M., Clifford, G.D., & Silva, I. (2020). MIMIC-III-Wellenform-Datenbank (Version 1.0). PhysioNet.
- Johnson, A.E.W., Pollard, T.J., Shen, L., Lehman, L.H., Feng, M., Ghassemi, M., Moody, B., Szolovits, P., Celi, L.A., & Mark, R.G. (2016). MIMIC-III, eine frei zugängliche Datenbank für Intensivpflege. Wissenschaftliche Daten, 3, 160035.
- MIMIC-III Waveform Database-Lizenz

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Visualisieren Sie KI/ML-Modellergebnisse mit Flask und AWS Elastic Beanstalk

Erstellt von Chris Caudill (AWS) und Durga Sury (AWS)

Übersicht

Die Visualisierung der Ergebnisse von Diensten für künstliche Intelligenz und maschinelles Lernen (AI/ML) erfordert häufig komplexe API-Aufrufe, die von Ihren Entwicklern und Ingenieuren angepasst werden müssen. Dies kann ein Nachteil sein, wenn Ihre Analysten schnell einen neuen Datensatz untersuchen möchten.

Sie können die Zugänglichkeit Ihrer Dienste verbessern und eine interaktivere Form der Datenanalyse bereitstellen, indem Sie eine webbasierte Benutzeroberfläche (UI) verwenden, über die Benutzer ihre eigenen Daten hochladen und die Modellergebnisse in einem Dashboard visualisieren können.

Dieses Muster verwendet Flask und Plotly, um Amazon Comprehend in eine benutzerdefinierte Webanwendung zu integrieren und Stimmungen und Entitäten anhand von Benutzerdaten zu visualisieren. Das Muster enthält auch die Schritte zur Bereitstellung einer Anwendung mithilfe von AWS Elastic Beanstalk. Sie können die Anwendung mithilfe der KI-Services von Amazon Web Services (AWS) oder mithilfe eines speziell trainierten Modells anpassen, das auf einem Endpunkt (z. B. einem SageMaker Amazon-Endpunkt) gehostet wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS-Befehlszeilenschnittstelle (AWS CLI), auf Ihrem lokalen Computer installiert und konfiguriert. Weitere Informationen dazu finden Sie unter Grundlagen der Konfiguration in der AWS-CLI-Dokumentation. Sie können auch eine integrierte Entwicklungsumgebung (IDE) von AWS Cloud9 verwenden. Weitere Informationen dazu finden Sie im Python-Tutorial für AWS Cloud9 und unter Vorschau laufender Anwendungen in der AWS Cloud9 Cloud9-IDE in der AWS Cloud9 Cloud9-Dokumentation.

  Hinweis: AWS Cloud9 ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS Cloud9 können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

- Ein Verständnis des Webanwendungs-Frameworks von Flask. Weitere Informationen zu Flask finden Sie im Schnellstart in der Flask-Dokumentation.
- Python Version 3.6 oder höher, installiert und konfiguriert. Sie können Python installieren, indem Sie den Anweisungen unter Einrichten Ihrer Python-Entwicklungsumgebung in der Dokumentation zu AWS Elastic Beanstalk folgen.
- Elastic Beanstalk Command Line Interface (EB CLI), installiert und konfiguriert. Weitere Informationen dazu finden Sie in der Dokumentation zu AWS Elastic Beanstalk unter Installieren der EB-CLI und Konfigurieren der EB-CLI.

Einschränkungen

- Die Flask-Anwendung dieses Musters wurde für die Arbeit mit CSV-Dateien entwickelt, die eine einzige Textspalte verwenden und auf 200 Zeilen beschränkt sind. Der Anwendungscode kann an andere Dateitypen und Datenmengen angepasst werden.
- Die Anwendung berücksichtigt keine Datenspeicherung und aggregiert weiterhin hochgeladene Benutzerdateien, bis sie manuell gelöscht werden. Sie können die Anwendung in Amazon Simple Storage Service (Amazon S3) für persistenten Objektspeicher integrieren oder eine Datenbank wie Amazon DynamoDB für die serverlose Speicherung von Schlüsselwerten verwenden.
- Die Anwendung berücksichtigt nur Dokumente in englischer Sprache. Sie können Amazon Comprehend jedoch verwenden, um die Hauptsprache eines Dokuments zu ermitteln. Weitere Informationen zu den unterstützten Sprachen für jede Aktion finden Sie in der API-Referenz in der Amazon Comprehend Comprehend-Dokumentation.
- Eine Liste zur Fehlerbehebung, die häufig auftretende Fehler und deren Lösungen enthält, finden Sie im Abschnitt Zusätzliche Informationen.

Architektur

Die Architektur der Flask-Anwendung

Flask ist ein leichtes Framework für die Entwicklung von Webanwendungen in Python. Es wurde entwickelt, um die leistungsstarke Datenverarbeitung von Python mit einer umfangreichen Weboberfläche zu kombinieren. Die Flask-Anwendung des Musters zeigt Ihnen, wie Sie eine Webanwendung erstellen, mit der Benutzer Daten hochladen, die Daten zur Inferenz an Amazon Comprehend senden und dann die Ergebnisse visualisieren können. Die Anwendung hat die folgende Struktur:

- `static`— Enthält alle statischen Dateien, die die Weboberfläche unterstützen (z. JavaScript B. CSS und Bilder)
- `templates`— Enthält alle HTML-Seiten der Anwendung
- `userData`— Speichert hochgeladene Benutzerdaten
- `application.py`— Die Flask-Anwendungsdatei
- `comprehend_helper.py`— Funktionen zum Durchführen von API-Aufrufen an Amazon Comprehend
- `config.py`— Die Konfigurationsdatei der Anwendung
- `requirements.txt`— Die von der Anwendung benötigten Python-Abhängigkeiten

Das `application.py` Skript enthält die Kernfunktionalität der Webanwendung, die aus vier Flask-Routen besteht. Das folgende Diagramm zeigt diese Flask-Routen.

- `/`ist das Stammverzeichnis der Anwendung und leitet Benutzer auf die `upload.html` Seite weiter (die im `templates` Verzeichnis gespeichert ist).
- `/saveFile`ist eine Route, die aufgerufen wird, nachdem ein Benutzer eine Datei hochgeladen hat. Diese Route empfängt eine `POST` Anfrage über ein HTML-Formular, das die vom Benutzer hochgeladene Datei enthält. Die Datei wird im `userData` Verzeichnis gespeichert und die Route leitet Benutzer zur `/dashboard` Route weiter.
- `/dashboard`sendet Benutzer auf die `dashboard.html` Seite. Im HTML-Code dieser Seite wird der JavaScript Code ausgeführt, der `static/js/core.js` Daten aus der `/data` Route liest und dann Visualisierungen für die Seite erstellt.
- `/data`ist eine JSON-API, die die zu visualisierenden Daten im Dashboard präsentiert. Diese Route liest die vom Benutzer bereitgestellten Daten und verwendet die Funktionen, um die Benutzerdaten `comprehend_helper.py` zur Stimmungsanalyse und Named Entity Recognition (NER) an Amazon Comprehend zu senden. Die Antwort von Amazon Comprehend wird formatiert und als JSON-Objekt zurückgegeben.

Architektur der Bereitstellung

Überlegungen zum Entwurf

Weitere Informationen zu Designüberlegungen für Anwendungen, die mit Elastic Beanstalk in der AWS-Cloud bereitgestellt werden, finden Sie in der Dokumentation zu AWS Elastic Beanstalk.

Technologie-Stack

- Amazon Comprehend
- Elastic Beanstalk
- Flask

Automatisierung und Skalierung

Elastic Beanstalk Beanstalk-Bereitstellungen werden automatisch mit Load Balancern und Auto Scaling-Gruppen eingerichtet. Weitere Konfigurationsoptionen finden Sie unter Konfiguration von Elastic Beanstalk-Umgebungen in der Dokumentation zu AWS Elastic Beanstalk.

Tools

- AWS Command Line Interface (AWS CLI) ist ein einheitliches Tool, das eine konsistente Schnittstelle für die Interaktion mit allen Teilen von AWS bietet.
- Amazon Comprehend verwendet Natural Language Processing (NLP), um Erkenntnisse über den Inhalt von Dokumenten zu gewinnen, ohne dass eine spezielle Vorverarbeitung erforderlich ist.
- Mit AWS Elastic Beanstalk können Sie Anwendungen in der AWS-Cloud schnell bereitstellen und verwalten, ohne sich mit der Infrastruktur vertraut machen zu müssen, auf der diese Anwendungen ausgeführt werden.
- Elastic Beanstalk CLI (EB CLI) ist eine Befehlszeilenschnittstelle für AWS Elastic Beanstalk, die interaktive Befehle bereitstellt, um die Erstellung, Aktualisierung und Überwachung von Umgebungen aus einem lokalen Repository zu vereinfachen.
- Das Flask-Framework führt Datenverarbeitung und API-Aufrufe mit Python durch und bietet interaktive Webvisualisierung mit Plotly.

Code

Der Code für dieses Muster ist im GitHub Visualize AI/ML-Modellergebnisse mithilfe von Flask und AWS Elastic Beanstalk Repository verfügbar.

Epen

Richten Sie die Flask-Anwendung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	Rufen Sie den Anwendung scode aus den GitHub Visualize AI/ML-Modellergebnissen mithilfe von Flask und dem AWS Elastic Beanstalk Beanstalk-Repository ab, indem Sie den folgenden Befehl ausführen: `git clone git@github.com:aws-samples/aws-comprehend-elasticbeanstalk-for-flask.git` **Note** Stellen Sie sicher, dass Sie Ihre SSH-Schlüssel mit konfigurieren. GitHub	Developer
Installieren Sie die Python-Module.	Nachdem Sie das Repository geklont haben, wird ein neues lokales `aws-comprehend-elasticbeanstalk-for-flask` Verzeichnis erstellt. In diesem Verzeichnis enthält die `requirements.txt` Datei die Python-Module und -Versionen, die	Python-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	die Anwendung ausführen. Verwenden Sie die folgenden Befehle, um die Module zu installieren:
	
	`cd aws-comprehend-elasticbeanstalk-for-flask`
	
	`pip install -r requirements.txt`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Testen Sie die Anwendung lokal.	Starten Sie den Flask-Server, indem Sie den folgenden Befehl ausführen:
	
	`python application.py`
	
	Dies gibt Informationen über den laufenden Server zurück. Sie sollten auf die Anwendung zugreifen können, indem Sie einen Browser öffnen und http://localhost:5000 aufrufen
	
	Note
	Wenn Sie die Anwendung in einer AWS Cloud9 Cloud9-IDE ausführen, müssen Sie den `application.run()` Befehl in der `application.py` Datei durch die folgende Zeile ersetzen:
	
	`application.run(host=os.getenv('IP', '0.0.0.0'),port=int(os.getenv('PORT', 8080)))`
		Python-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie müssen diese Änderung vor der Bereitstellung rückgängig machen.	

Stellen Sie die Anwendung auf Elastic Beanstalk bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Elastic Beanstalk Beanstalk-Anwendung.	Um Ihr Projekt als Elastic Beanstalk Beanstalk-Anwendung zu starten, führen Sie den folgenden Befehl im Stammverzeichnis Ihrer Anwendung aus: `eb init -p python-3.6 comprehend_flask --region us-east-1` ⚠ Important • `comprehend_flask` ist der Name der Elastic Beanstalk Beanstalk-Anwendung und kann entsprechend Ihren Anforderungen geändert werden. • Sie können die AWS-Region durch eine Region Ihrer Wahl ersetzen. Die Standardregion in AWS CLI	Architekt, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wird verwendet, wenn Sie keine Region angeben. • Die Anwendung wurde mit Python Version 3.6 erstellt. Wenn Sie andere Python-Versionen verwenden, können Fehler auftreten. Führen Sie den `eb init -i` Befehl aus, um weitere Konfigurationsoptionen für die Bereitstellung zu erhalten.	
Stellen Sie die Elastic Beanstalk Beanstalk-Umgebung bereit.	Führen Sie den folgenden Befehl im Stammverzeichnis der Anwendung aus: `eb create comprehend-flask-env` **Note** `comprehend-flask-env` ist der Name der Elastic Beanstalk Beanstalk-Umgebung und kann entsprechend Ihren Anforderungen geändert werden. Der Name darf nur Buchstaben, Zahlen und Bindestriche enthalten.	Architekt, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Autorisieren Sie Ihre Bereitstellung für die Verwendung von Amazon Comprehend.	Obwohl Ihre Anwendung möglicherweise erfolgreich bereitgestellt wurde, sollten Sie Ihrer Bereitstellung auch Zugriff auf Amazon Comprehend gewähren. `ComprehendFullAccess` ist eine von AWS verwaltete Richtlinie, die der bereitgestellten Anwendung Berechtigungen zum Durchführen von API-Aufrufen an Amazon Comprehend gewährt. Hängen Sie die `ComprehendFullAccess` Richtlinie an an `aws-elasticbeanstalk-ec2-role` (diese Rolle wird automatisch für die Amazon Elastic Compute Cloud (Amazon EC2) -Instances Ihrer Bereitstellung erstellt), indem Sie den folgenden Befehl ausführen: `aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/ComprehendFullAccess --role-name aws-elasticbeanstalk-ec2-role`	Entwickler, Sicherheitsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Important `aws-elasticbeanstalk-ec2-role` wird erstellt, wenn Ihre Anwendung bereitgestellt wird. Sie müssen den Bereitstellungsprozess abschließen, bevor Sie die AWS Identity and Access Management (IAM) -Richtlinie anhängen können.	
Besuchen Sie Ihre bereitgestellte Anwendung.	Nachdem Ihre Anwendung erfolgreich bereitgestellt wurde, können Sie sie aufrufen, indem Sie den `eb open` Befehl ausführen. Sie können den `eb status` Befehl auch ausführen, um Details zu Ihrer Bereitstellung zu erhalten. Die Bereitstellungs-URL ist unter aufgeführt `CNAME`.	Architekt, Entwickler

(Optional) Passen Sie die Anwendung an Ihr ML-Modell an

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Autorisieren Sie Elastic Beanstalk, auf das neue Modell zuzugreifen.	Stellen Sie sicher, dass Elastic Beanstalk über die erforderlichen Zugriffsb erechtigungen für Ihren neuen Modellendpunkt verfügt. Wenn Sie beispielsweise einen SageMaker Amazon-Endpunkt verwenden, benötigt Ihre Bereitstellung die Erlaubnis, den Endpunkt aufzurufen. Weitere Informationen dazu finden Sie InvokeEndpointin der SageMaker Amazon-Do kumentation.	Entwickler, Sicherheitsarchite kt
Senden Sie die Benutzerdaten an ein neues Modell.	Um das zugrunde liegende ML-Modell in dieser Anwendung zu ändern, müssen Sie die folgenden Dateien ändern: • `comprehend_helper.py` — Dies ist das Python-Skript, das eine Verbindun g mit Amazon Comprehen d herstellt, die Antwort verarbeitet und das Endergebnis an die Anwendung zurückgibt. In diesem Skript können Sie die Daten entweder an einen anderen KI-Service in der AWS-Cloud weiterleiten	Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	oder Sie können die Daten an einen benutzerdefinierten Modellendpunkt senden. Wir empfehlen, dass Sie die Ergebnisse auch in diesem Skript formatieren, um die logische Trennung und die Wiederverwendbarkeit dieses Musters zu gewährleisten. • `application.py` — Wenn Sie den Namen des `comprehend_helper.py` Skripts oder der Funktionen ändern, müssen Sie das `application.py` Anwendungsskript aktualisieren, um diese Änderungen widerzuspiegeln.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Dashboard-Visualisierungen.	In der Regel bedeutet die Integration eines neuen ML-Modells, dass die Visualisierungen aktualisiert werden müssen, um die neuen Ergebnisse widerzuspiegeln. Diese Änderungen werden in den folgenden Dateien vorgenommen: • `templates/dashboard.html` — Die vorgefertigte Anwendung unterstützt nur zwei grundlegende Visualisierungen. Das gesamte Layout der Seite kann in dieser Datei angepasst werden. • `static/js/core.js` — Dieses Skript erfasst die formatierte Ausgabe der `/data` Route des Flask-Servers und verwendet Plotly, um Visualisierungen zu erstellen. Sie können die Diagramme der Seite hinzufügen oder aktualisieren.	Web-Entwickler

(Optional) Stellen Sie die aktualisierte Anwendung bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Anforderungsdatei Ihrer Bewerbung.	Bevor Sie Änderunge n an Elastic Beanstalk senden, aktualisieren Sie die `requirements.txt` Datei, sodass sie alle neuen Python-Module widerspiegelt, indem Sie den folgenden Befehl im Stammverzeichnis Ihrer Anwendung ausführen: `pip freeze > requireme nts.txt`	Python-Entwickler
Stellen Sie die Elastic Beanstalk Beanstalk-Umgebung erneut bereit.	Um sicherzustellen, dass Ihre Anwendungsänderung en in Ihrem Elastic Beanstalk -Deployment widergesp iegelt werden, navigieren Sie zum Stammverzeichnis Ihrer Anwendung und führen Sie den folgenden Befehl aus: `eb deploy` Dadurch wird die neueste Version des Anwendung scodes an Ihr vorhandenes Elastic Beanstalk-Deployment gesendet.	Systemadministrator, Architekt

Zugehörige Ressourcen

- Rufen Sie mit Amazon API Gateway und AWS Lambda einen SageMaker Amazon-Modellendpunkt auf
- Bereitstellung einer Flask-Anwendung auf Elastic Beanstalk
- EB CLI-Befehlsreferenz
- Einrichtung Ihrer Python-Entwicklungsumgebung

Zusätzliche Informationen

Liste der Problemlösungen

Im Folgenden finden Sie sechs häufig auftretende Fehler und deren Lösungen.

Fehler 1

```
Unable to assume role "arn:aws:iam::xxxxxxxxxx:role/aws-elasticbeanstalk-ec2-role".
 Verify that the role exists and is configured correctly.
```

Lösung: Wenn dieser Fehler bei der Ausführung auftritt`eb create`, erstellen Sie eine Beispielanwendung auf der Elastic Beanstalk Beanstalk-Konsole, um das Standard-Instance-Profil zu erstellen. Weitere Informationen dazu finden Sie in der Dokumentation zu AWS Elastic Beanstalk unter Creating an Elastic Beanstalk Environment.

Fehler 2

```
Your WSGIPath refers to a file that does not exist.
```

Lösung: Dieser Fehler tritt in den Bereitstellungsprotokollen auf, weil Elastic Beanstalk erwartet, dass der Flask-Code benannt wird. `application.py` Wenn Sie einen anderen Namen gewählt haben, führen Sie den aus `eb config` und bearbeiten Sie ihn WSGIPath wie im folgenden Codebeispiel gezeigt:

```
aws:elasticbeanstalk:container:python:
     NumProcesses: '1'
     NumThreads: '15'
     StaticFiles: /static/=static/
```

```
    WSGIPath: application.py
```

Stellen Sie sicher, dass Sie es `application.py` durch Ihren Dateinamen ersetzen.

Sie können auch Gunicorn und ein Profil nutzen. Weitere Informationen zu diesem Ansatz finden Sie unter Konfiguration des WSGI-Servers mit einem Profil in der AWS Elastic Beanstalk Beanstalk-Dokumentation.

Fehler 3

```
Target WSGI script '/opt/python/current/app/application.py' does not contain WSGI
 application 'application'.
```

Lösung: Elastic Beanstalk erwartet, dass die Variable, die Ihre Flask-Anwendung repräsentiert, benannt wird. `application` Stellen Sie sicher, dass die `application.py` Datei `application` als Variablennamen verwendet:

```
application = Flask(__name__)
```

Fehler 4

```
The EB CLI cannot find your SSH key file for keyname
```

Lösung: Verwenden Sie die EB-CLI, um anzugeben, welches key pair verwendet werden soll, oder um ein key pair für die EC2 Instances Ihrer Bereitstellung zu erstellen. Um den Fehler zu beheben, führen Sie den Befehl aus `eb init -i` und eine der Optionen wird Sie fragen:

```
Do you want to set up SSH for your instances?
```

Antworten Sie mitY, um entweder ein key pair zu erstellen oder ein vorhandenes key pair anzugeben.

Fehler 5

Ich habe meinen Code aktualisiert und erneut bereitgestellt, aber mein Deployment spiegelt meine Änderungen nicht wider.

Lösung: Wenn du ein Git-Repository mit deiner Bereitstellung verwendest, stelle sicher, dass du deine Änderungen hinzufügst und festschreibst, bevor du sie erneut bereitstellst.

Fehler 6

Sie zeigen eine Vorschau der Flask-Anwendung von einer AWS Cloud9 Cloud9-IDE aus und stoßen auf Fehler.

Lösung: Weitere Informationen dazu finden Sie unter Vorschau laufender Anwendungen in der AWS Cloud9 Cloud9-IDE in der AWS Cloud9 Cloud9-Dokumentation.

Verarbeitung natürlicher Sprache mit Amazon Comprehend

Wenn Sie sich für Amazon Comprehend entscheiden, können Sie benutzerdefinierte Entitäten in einzelnen Textdokumenten erkennen, indem Sie Echtzeitanalysen oder asynchrone Batch-Jobs ausführen. Mit Amazon Comprehend können Sie auch benutzerdefinierte Modelle zur Erkennung von Entitäten und zur Textklassifizierung trainieren, die in Echtzeit verwendet werden können, indem Sie einen Endpunkt erstellen.

Dieses Muster verwendet asynchrone Batch-Jobs, um Stimmungen und Entitäten aus einer Eingabedatei zu erkennen, die mehrere Dokumente enthält. Die in diesem Muster bereitgestellte Beispielanwendung ist so konzipiert, dass Benutzer eine CSV-Datei hochladen können, die eine einzelne Spalte mit einem Textdokument pro Zeile enthält. Die `comprehend_helper.py` Datei im GitHub Visualize AI/ML-Model Results using Flask and AWS Elastic Beanstalk Repository liest die Eingabedatei und sendet die Eingabe zur Verarbeitung an Amazon Comprehend.

BatchDetectEntities

Amazon Comprehend untersucht den Text eines Stapels von Dokumenten auf benannte Entitäten und gibt die erkannte Entität, den Standort, den Entitätstyp und eine Bewertung zurück, die das Vertrauensniveau von Amazon Comprehend angibt. In einem API-Aufruf können maximal 25 Dokumente gesendet werden, wobei jedes Dokument kleiner als 5.000 Byte ist. Sie können die Ergebnisse filtern, sodass nur bestimmte Entitäten angezeigt werden, die auf dem Anwendungsfall basieren. Sie könnten beispielsweise den `'quantity'` Entitätstyp überspringen und einen Schwellenwert für die erkannte Entität festlegen (z. B. 0,75). Wir empfehlen Ihnen, die Ergebnisse für Ihren speziellen Anwendungsfall zu untersuchen, bevor Sie einen Schwellenwert auswählen. Weitere Informationen dazu finden Sie BatchDetectEntitiesin der Amazon Comprehend Comprehend-Dokumentation.

BatchDetectSentiment

Amazon Comprehend prüft einen Stapel eingehender Dokumente und gibt die vorherrschende Stimmung für jedes Dokument zurück (`POSITIVE`,`NEUTRAL`, `MIXED` oder). `NEGATIVE` In einem API-

Aufruf können maximal 25 Dokumente gesendet werden, wobei jedes Dokument kleiner als 5.000 Byte ist. Die Stimmungsanalyse ist unkompliziert, und Sie wählen die Stimmung mit der höchsten Punktzahl aus, die in den Endergebnissen angezeigt werden soll. Weitere Informationen dazu finden Sie BatchDetectSentimentin der Amazon Comprehend Comprehend-Dokumentation.

Handhabung der Flask-Konfiguration

Flask-Server verwenden eine Reihe von Konfigurationsvariablen, um zu steuern, wie der Server läuft. Diese Variablen können Debug-Ausgaben, Sitzungstoken oder andere Anwendungseinstellungen enthalten. Sie können auch benutzerdefinierte Variablen definieren, auf die zugegriffen werden kann, während die Anwendung ausgeführt wird. Es gibt mehrere Ansätze zum Setzen von Konfigurationsvariablen.

In diesem Muster wird die Konfiguration in definiert `config.py` und darin vererbt`application.py`.

- > **Note**
  >
  > `config.py`enthält die Konfigurationsvariablen, die beim Start der Anwendung eingerichtet werden. In dieser Anwendung ist eine `DEBUG` Variable definiert, die der Anwendung mitteilt, den Server im Debug-Modus auszuführen. : Der Debug-Modus sollte nicht verwendet werden, wenn eine Anwendung in einer Produktionsumgebung ausgeführt wird. `UPLOAD_FOLDER`Rist eine benutzerdefinierte Variable, die so definiert ist, dass sie später in der Anwendung referenziert wird und sie darüber informiert, wo hochgeladene Benutzerdaten gespeichert werden sollen.
- `application.py`initiiert die Flask-Anwendung und erbt die in definierten Konfigurationseinstellungen. `config.py` Dies wird durch den folgenden Code ausgeführt:

```
application = Flask(__name__)
application.config.from_pyfile('config.py')
```

Mehr Muster

- Automatisieren Sie den AWS Infrastrukturbetrieb mithilfe von Amazon Bedrock
- Stellen Sie eine ChatOps Lösung zur Verwaltung von SAST-Scanergebnissen bereit, indem Sie Amazon Q Developer in Chat-Anwendungen verwenden, benutzerdefinierte Aktionen und AWS CloudFormation
- Generieren Sie Dateneinblicke mithilfe von AWS Mainframe Modernization und Amazon Q in QuickSight
- Generieren Sie Einblicke in Db2 z/OS-Daten mithilfe von Amazon AWS Mainframe Modernization Q in QuickSight
- Geben Sie SageMaker Notebook-Instances temporären Zugriff auf ein CodeCommit Repository in einem anderen AWS-Konto
- AWS Organizations Richtlinien mithilfe AWS CodePipeline von Amazon Bedrock als Code verwalten
- Migrieren Sie ML-Workloads zum Erstellen, Trainieren und Bereitstellen zu Amazon SageMaker mithilfe der AWS-Entwicklertools
- Modernisieren Sie die CardDemo Mainframe-Anwendung mithilfe von AWS Transform
- Führen Sie erweiterte Analysen mit Amazon Redshift ML durch
- Optimieren Sie die Entwicklung und Bereitstellung von Amazon Lex Lex-Bot mithilfe eines automatisierten Workflows
- Problembehebung bei Zuständen AWS Step Functions mithilfe von Amazon Bedrock

Analysen

Themen

- Analysieren Sie Amazon Redshift Redshift-Daten in Microsoft SQL Server Analysis Services
- Analysieren und visualisieren Sie verschachtelte JSON-Daten mit Amazon Athena und Amazon QuickSight
- Automatisieren Sie die Datenaufnahme aus Amazon AWS Data Exchange S3
- Automatisieren Sie die Durchsetzung von Verschlüsselungen in AWS Glue mithilfe einer CloudFormation AWS-Vorlage
- Erstellen Sie mit dem AWS DataOps Development Kit eine Datenpipeline, um Google Analytics-Daten aufzunehmen, zu transformieren und zu analysieren
- Erstellen Sie mithilfe von Amazon Kinesis Video Streams und AWS Fargate eine Videoverarbeitungspipeline
- Erstellen Sie eine ETL-Servicepipeline, um Daten mithilfe von AWS Glue inkrementell von Amazon S3 nach Amazon Redshift zu laden
- Bauen Sie mit Amazon ein Datennetz für Unternehmen auf DataZone AWS CDK, und AWS CloudFormation
- Value at Risk (VaR) mithilfe von AWS-Services berechnen
- Konfigurieren Sie den kontoübergreifenden Zugriff auf einen gemeinsamen AWS Glue Glue-Datenkatalog mit Amazon Athena
- Konvertieren Sie die temporale Funktion Teradata NORMALIZE in Amazon Redshift SQL
- Konvertieren Sie die Teradata RESET WHEN-Funktion in Amazon Redshift SQL
- Bereitstellen und verwalten Sie einen serverlosen Data Lake in der AWS-Cloud, indem Sie Infrastruktur als Code verwenden
- Erzwingen Sie die Kennzeichnung von Amazon EMR-Clustern beim Start
- Stellen Sie sicher, dass die Amazon EMR-Protokollierung bei Amazon S3 beim Start aktiviert ist
- Generieren Sie Testdaten mit einem AWS Glue Glue-Job und Python
- Mit AWS IoT Greengrass IoT-Daten kostengünstig direkt in Amazon S3 aufnehmen
- Starten Sie einen Spark-Job in einem transienten EMR-Cluster mithilfe einer Lambda-Funktion
- Migrieren Sie Apache Cassandra-Workloads mithilfe von AWS Glue zu Amazon Keyspaces
- Migrieren Sie Hadoop-Daten mithilfe WANdisco LiveData von Migrator zu Amazon S3

- Migrieren Sie Oracle Business Intelligence 12c von lokalen Servern zur AWS-Cloud
- Migrieren Sie einen lokalen Apache Kafka-Cluster zu Amazon MSK mithilfe von MirrorMaker
- Migrieren Sie einen ELK-Stack zu Elastic Cloud auf AWS
- Migrieren Sie Daten mithilfe AWS Cloud von Starburst auf die
- Optimieren Sie die ETL-Erfassung der Eingabedateigröße auf AWS
- Orchestrieren Sie eine ETL-Pipeline mit Validierung, Transformation und Partitionierung mithilfe von AWS Step Functions
- Führen Sie erweiterte Analysen mit Amazon Redshift ML durch
- Abfragen von Amazon DynamoDB-Tabellen mit SQL mithilfe von Amazon Athena
- Mit Athena auf Amazon DynamoDB-Tabellen zugreifen, diese abfragen und verbinden
- Richten Sie einen nutzbaren Mindestdatenraum für die gemeinsame Nutzung von Daten zwischen Organisationen ein
- Richten Sie eine sprachspezifische Sortierung für Amazon Redshift Redshift-Abfrageergebnisse mithilfe einer skalaren Python-UDF ein
- Abonnieren Sie eine Lambda-Funktion für Ereignisbenachrichtigungen von S3-Buckets in verschiedenen AWS-Regionen
- Drei AWS Glue ETL-Auftragstypen für die Konvertierung von Daten in Apache Parquet
- Visualisieren Sie Amazon Redshift Redshift-Prüfprotokolle mit Amazon Athena und Amazon QuickSight
- Visualisieren Sie IAM-Anmeldedaten für alle AWS-Konten mithilfe von Amazon QuickSight
- Mehr Muster

Analysieren Sie Amazon Redshift Redshift-Daten in Microsoft SQL Server Analysis Services

Erstellt von Sunil Vora (AWS)

Übersicht

Dieses Muster beschreibt, wie Amazon Redshift Redshift-Daten in Microsoft SQL Server Analysis Services mithilfe des Intellisoft OLE DB-Anbieters oder CData ADO.NET-Anbieters für den Datenbankzugriff verbunden und analysiert werden.

Amazon Redshift ist ein vollständig verwalteter Data-Warehouse-Service in Petabytegröße in der Cloud. SQL Server Analysis Services ist ein OLAP-Tool (Online Analytical Processing), mit dem Sie Daten aus Data Marts und Data Warehouses wie Amazon Redshift analysieren können. Sie können SQL Server Analysis Services verwenden, um OLAP-Cubes aus Ihren Daten für eine schnelle, erweiterte Datenanalyse zu erstellen.

Voraussetzungen und Einschränkungen

Annahmen

- Dieses Muster beschreibt, wie SQL Server Analysis Services und Intellisoft OLE DB Provider oder CData ADO.NET Provider für Amazon Redshift auf einer Amazon Elastic Compute Cloud (Amazon) -Instance eingerichtet werden. EC2 Alternativ können Sie beide auf einem Host in Ihrem Unternehmensrechenzentrum installieren.

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Amazon Redshift Redshift-Cluster mit Anmeldeinformationen

Architektur

Quelltechnologie-Stack

- Ein Amazon Redshift Redshift-Cluster

Zieltechnologie-Stack

- Microsoft SQL Server-Analysedienste

Quell- und Zielarchitektur

Tools

- Microsoft Visual Studio 2019 (Community-Ausgabe)
- Intellisoft OLE DB Provider für Amazon Redshift (Testversion) oder CData ADO.NET Provider für Amazon Redshift (Testversion)

Epen

Analysieren Sie Tabellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie die zu importierenden Tabellen und Daten.	Identifizieren Sie die zu importierenden Amazon Redshift Redshift-Tabellen und deren Größen.	DBA

EC2 Instanz einrichten und Tools installieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine EC2 Instanz ein.	Erstellen Sie in Ihrem AWS-Konto eine EC2 Instance in einem privaten oder öffentlichen Subnetz.	Systemadministrator
Installieren Sie Tools für den Datenbankzugriff.	Laden Sie den Intellisoft OLE DB Provider für Amazon Redshift (oder CData ADO.NET Provider für	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon Redshift) herunter und installieren Sie ihn.	
Installieren Sie Visual Studio.	Laden Sie Visual Studio 2019 (Community Edition) herunter und installieren Sie es.	Systemadministrator
Installieren Sie Erweiterungen.	Installieren Sie die Microsoft Analysis Services Projects-Erweiterung in Visual Studio.	Systemadministrator
Ein Projekt zu erstellen.	Erstellen Sie ein neues tabellarisches Modellprojekt in Visual Studio, um Ihre Amazon Redshift Redshift-Daten zu speichern. Wählen Sie in Visual Studio die Option Tabular Project von Analysis Services, wenn Sie Ihr Projekt erstellen.	DBA

Erstellen Sie eine Datenquelle und importieren Sie Tabellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon Redshift Redshift-Datenquelle.	Erstellen Sie eine Amazon Redshift-Datenquelle, indem Sie den Intellisoft OLE DB-Anbieter für Amazon Redshift (oder den CData ADO.NET-Anbieter für Amazon Redshift) und Ihre Amazon Redshift Redshift-Anmeldeinformationen verwenden.	Amazon Redshift, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Tabellen importieren.	Wählen Sie Tabellen und Ansichten aus Amazon Redshift aus und importier en Sie sie in Ihr SQL Server Analysis Services-Projekt.	Amazon Redshift, DBA

Nach der Migration aufräumen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die EC2 Instanz.	Löschen Sie die EC2 Instanz, die Sie zuvor gestartet haben.	Systemadministrator

Zugehörige Ressourcen

- Amazon Redshift (AWS-Dokumentation)
- Installieren Sie SQL Server Analysis Services (Microsoft-Dokumentation)
- Tabular Model Designer (Microsoft-Dokumentation)
- Überblick über OLAP-Cubes für erweiterte Analysen (Microsoft-Dokumentation)
- Microsoft Visual Studio 2019 (Community-Ausgabe)
- Intellisoft OLE DB Provider für Amazon Redshift (Testversion)
- CData ADO.NET-Anbieter für Amazon Redshift (Testversion)

Analysieren und visualisieren Sie verschachtelte JSON-Daten mit Amazon Athena und Amazon QuickSight

Erstellt von Anoop Singh (AWS)

Übersicht

Dieses Muster erklärt, wie eine verschachtelte Datenstruktur im JSON-Format mithilfe von Amazon Athena in eine tabellarische Ansicht übersetzt und die Daten anschließend in Amazon visualisiert werden. QuickSight

Sie können Daten im JSON-Format für API-gestützte Datenfeeds von Betriebssystemen verwenden, um Datenprodukte zu erstellen. Diese Daten können Ihnen auch dabei helfen, Ihre Kunden und deren Interaktionen mit Ihren Produkten besser zu verstehen, sodass Sie Benutzererlebnisse maßgeschneidert und Ergebnisse vorhersagen können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Eine JSON-Datei, die eine verschachtelte Datenstruktur darstellt (dieses Muster bietet eine Beispieldatei)

Einschränkungen:

- JSON-Funktionen lassen sich gut in bestehende SQL-orientierte Funktionen in Athena integrieren. Sie sind jedoch nicht ANSI-SQL-kompatibel, und es wird erwartet, dass die JSON-Datei jeden Datensatz in einer separaten Zeile enthält. Möglicherweise müssen Sie die `ignore.malformed.json` Eigenschaft in Athena verwenden, um anzugeben, ob falsch formatierte JSON-Datensätze in Nullzeichen umgewandelt werden sollen oder ob Fehler generiert werden sollen. Weitere Informationen finden Sie in der Athena-Dokumentation unter Bewährte Methoden zum Lesen von JSON-Daten.
- Dieses Muster berücksichtigt nur einfache und kleine Mengen von Daten im JSON-Format. Wenn Sie diese Konzepte in größerem Umfang verwenden möchten, sollten Sie die Datenpartitionierung in Betracht ziehen und Ihre Daten in größeren Dateien konsolidieren.

Architektur

Das folgende Diagramm zeigt die Architektur und den Arbeitsablauf für dieses Muster. Die verschachtelten Datenstrukturen werden in Amazon Simple Storage Service (Amazon S3) im JSON-Format gespeichert. In Athena werden die JSON-Daten einer Athena-Datenstruktur zugeordnet. Anschließend erstellen Sie eine Ansicht, um die Daten zu analysieren und die Datenstruktur in zu visualisieren. QuickSight

Tools

AWS-Services

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt. Dieses Muster verwendet Amazon S3 zum Speichern der JSON-Datei.
- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon S3 analysieren können. Dieses Muster verwendet Athena, um die JSON-Daten abzufragen und zu transformieren. Mit einigen Aktionen in der AWS Management Console können Sie Athena auf Ihre Daten in Amazon S3 verweisen und Standard-SQL verwenden, um einmalige Abfragen auszuführen. Athena ist serverlos, sodass keine Infrastruktur eingerichtet oder verwaltet werden muss, und Sie zahlen nur für die Abfragen, die Sie ausführen. Athena skaliert automatisch und führt Abfragen parallel aus, sodass die Ergebnisse auch bei großen Datensätzen und komplexen Abfragen schnell sind.
- Amazon QuickSight ist ein Business Intelligence (BI) -Service auf Cloud-Ebene, mit dem Sie Ihre Daten auf einem einzigen Dashboard visualisieren, analysieren und melden können. QuickSight ermöglicht es Ihnen, auf einfache Weise interaktive Dashboards zu erstellen und zu veröffentlichen, die Erkenntnisse aus maschinellem Lernen (ML) enthalten. Sie können von jedem Gerät aus auf diese Dashboards zugreifen und sie in Ihre Anwendungen, Portale und Websites einbetten.

Beispiel-Code

Die folgende JSON-Datei bietet eine verschachtelte Datenstruktur, die Sie in diesem Muster verwenden können.

```
{
  "symbol": "AAPL",
```

```
  "financials": [
    {
      "reportDate": "2017-03-31",
      "grossProfit": 20591000000,
      "costOfRevenue": 32305000000,
      "operatingRevenue": 52896000000,
      "totalRevenue": 52896000000,
      "operatingIncome": 14097000000,
      "netIncome": 11029000000,
      "researchAndDevelopment": 2776000000,
      "operatingExpense": 6494000000,
      "currentAssets": 101990000000,
      "totalAssets": 334532000000,
      "totalLiabilities": 200450000000,
      "currentCash": 15157000000,
      "currentDebt": 13991000000,
      "totalCash": 67101000000,
      "totalDebt": 98522000000,
      "shareholderEquity": 134082000000,
      "cashChange": -1214000000,
      "cashFlow": 12523000000,
      "operatingGainsLosses": null
    }
  ]
}
```

Epen

Richten Sie einen S3-Bucket ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Um einen Bucket zum Speichern der JSON-Datei zu erstellen, melden Sie sich bei der an AWS Managemen t Console, öffnen Sie die Amazon S3 S3-Konsole und wählen Sie dann Bucket erstellen. Weitere Informati onen finden Sie in der Amazon	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	S3 S3-Dokumentation unter Bucket erstellen.	
Fügen Sie die verschachtelten JSON-Daten hinzu.	Laden Sie Ihre JSON-Datei in den S3-Bucket hoch. Eine JSON-Beispieldatei finden Sie im vorherigen Abschnitt . Anweisungen finden Sie unter Objekte hochladen in der Amazon S3 S3-Dokumentation.	Systemadministrator

Analysieren Sie Daten in Athena

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Tabelle für die Zuordnung der JSON-Daten.	1. Öffnen Sie die Athena-Konsole. 2. Erstellen Sie eine Datenbank, indem Sie den Anweisungen in der Athena-Dokumentation folgen. 3. Wählen Sie im Datenbankmenü die Datenbank aus, die Sie erstellt haben. 4. Geben Sie im Abfrage-Editor eine `CREATE TABLE` Anweisung wie die folgende ein: `CREATE EXTERNAL TABLE financials_json ( symbol string, financials array<`	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>struct<re
	portdate: string,
	grossprof
	it: bigint,
	totalreve
	nue: bigint,
	totalcash
	: bigint,
	totaldebt
	: bigint,
	researcha
	nddevelopment:
	bigint>>
	)
	ROW FORMAT SERDE
	'org.openx.data.js
	onserde.JsonSerDe'
	LOCATION 's3://s3b
	ucket-for-athena/'</pre> wobei der Speicherort des S3-Buckets `LOCATION` angegeben wird, der die JSON-Datei enthält.
	5. Wählen Sie Ausführen, um die Tabelle zu erstellen.
	
	Weitere Informationen zum Erstellen von Tabellen finden Sie in der Athena-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Ansicht für die Datenanalyse.	1. Öffnen Sie die Athena-Konsole. 2. Erstellen Sie eine Datenbank, indem Sie den Anweisungen in der Athena-Dokumentation folgen. 3. Wählen Sie im Datenbank menü die Datenbank aus, die Sie erstellt haben. 4. Geben Sie im Abfrage-Editor eine `CREATE VIEW` Anweisung wie die folgende ein: `CREATE OR REPLACE VIEW financial_json_view AS SELECT symbol, financials[1].reportdate one_report_date, -- indexes start with 1 financials[1].totalrevenue one_total_revenue, financials[1].reportdate another_report_date, financials[1].totalrevenue another_total_revenue FROM financials_json where symbol='AAPL' ORDER BY 1`	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Wählen Sie Run (Ausführe n), um die Ansicht zu erstellen. Weitere Informationen zum Erstellen von Ansichten finden Sie in der Athena-Dokumentati on.	
Analysieren und validieren Sie die Daten.	1. Öffnen Sie die Athena-Ko nsole. 2. Führen Sie Abfragen im Abfrage-Editor mithilfe der Ansicht aus, die Sie im vorherigen Schritt erstellt haben. 3. Überprüfen Sie die Daten anhand der JSON-Date i, um sicherzustellen, dass Spaltennamen und Datentypen korrekt zugeordnet sind.	Developer

Visualisieren Sie Daten in QuickSight

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Athena als Datenquelle in QuickSight ein.	1. Öffnen Sie die QuickSight - Konsole. 2. Wählen Sie Datensätze, Neuer Datensatz aus. 3. Wählen Sie Athena als Datenquelle.	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie die Datenbank aus, die die von Ihnen erstellte Ansicht enthält. 5. Wählen Sie die Ansicht aus, für die Sie einen Datensatz erstellen möchten. 6. Wählen Sie auf der Seite Datensatzerstellung abschließen die Option Daten direkt abfragen aus. 7. Wählen Sie Visualize aus.	
Visualisieren Sie Daten in QuickSight.	1. Nachdem Sie den Datensatz visualisiert haben, wählen Sie die Grafiken im linken Bereich aus und wählen Sie Felder für den Datensatz aus. Weitere Informationen finden Sie im Tutorial in der QuickSight Dokumentation. 2. Speichern Sie die Änderungen an der Analyse. 3. Wählen Sie Dashboard veröffentlichen, um die von Ihnen erstellten Grafiken zu veröffentlichen.	Datenanalyst

Zugehörige Ressourcen

- Amazon Athena Athena-Dokumentation
- QuickSight Amazon-Tutorials

- Arbeiten mit verschachteltem JSON (Blogbeitrag)

Automatisieren Sie die Datenaufnahme aus Amazon AWS Data Exchange S3

Erstellt von Adnan Alvee (AWS) und Manikanta Gona (AWS)

Übersicht

Dieses Muster bietet eine AWS CloudFormation Vorlage, mit der Sie automatisch Daten aus Ihrem Data Lake AWS Data Exchange in Amazon Simple Storage Service (Amazon S3) aufnehmen können.

AWS Data Exchange ist ein Service, der es einfach macht, dateibasierte Datensätze in der AWS-Cloud sicher auszutauschen. AWS Data Exchange Datensätze sind abonnementbasiert. Als Abonnent können Sie auch auf Änderungen von Datensätzen zugreifen, wenn Anbieter neue Daten veröffentlichen.

Die AWS CloudFormation Vorlage erstellt ein Ereignis in Amazon CloudWatch Events und eine AWS Lambda Funktion. Die Veranstaltung sucht nach Aktualisierungen des Datensatzes, den Sie abonniert haben. Wenn es ein Update gibt, CloudWatch initiiert eine Lambda-Funktion, die die Daten in den von Ihnen angegebenen S3-Bucket kopiert. Wenn die Daten erfolgreich kopiert wurden, sendet Lambda Ihnen eine Amazon Simple Notification Service (Amazon SNS) -Benachrichtigung.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine aktive AWS-Konto
- Abonnement eines Datensatzes in AWS Data Exchange

Einschränkungen

- Die AWS CloudFormation Vorlage muss für jeden abonnierten Datensatz in AWS Data Exchange separat bereitgestellt werden.

Architektur

Zieltechnologie-Stack

- AWS Lambda
- Amazon S3
- AWS Data Exchange
- Amazon CloudWatch
- Amazon SNS

Zielarchitektur

Automatisierung und Skalierung

Sie können die AWS CloudFormation Vorlage mehrfach für die Datensätze verwenden, die Sie in den Data Lake aufnehmen möchten.

Tools

- AWS Data Exchangemacht es AWS Kunden einfach, dateibasierte Datensätze in der sicher auszutauschen. AWS Cloud Als Abonnent können Sie Hunderte von Produkten von qualifizierten Datenanbietern finden und abonnieren. Anschließend können Sie den Datensatz schnell herunterladen oder auf Amazon S3 kopieren, um ihn in einer Vielzahl von AWS Analyse- und Machine-Learning-Diensten zu verwenden. Jeder mit einem AWS-Konto kann AWS Data Exchange Abonnent werden.
- Mit AWS Lambda können Sie Code ausführen, ohne dass Sie Server bereitstellen und verwalten müssen. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie zahlen nur für die Rechenzeit, die Sie verbrauchen. Es fallen keine Gebühren an, wenn Ihr Code nicht ausgeführt wird. Mit Lambda können Sie Code für praktisch jede Art von Anwendung oder Backend-Service ohne Verwaltungsaufwand ausführen. Lambda führt Ihren Code auf einer hochverfügbaren Recheninfrastruktur aus und verwaltet alle Rechenressourcen, einschließlich Server- und Betriebssystemwartung, Kapazitätsbereitstellung und automatische Skalierung, Codeüberwachung und Protokollierung.
- Amazon S3 bietet Speicherplatz für das Internet. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen.
- Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS Ressourcen beschreiben, nahezu in Echtzeit. Mithilfe einfacher Regeln, die Sie schnell einrichten können, können Sie Ereignisse zuordnen und sie an eine oder mehrere Zielfunktionen oder

Streams weiterleiten. CloudWatch Events erkennt betriebliche Änderungen, sobald sie eintreten. Es reagiert auf diese betrieblichen Änderungen und ergreift bei Bedarf Korrekturmaßnahmen, indem es Nachrichten sendet, um auf die Umgebung zu reagieren, Funktionen aktiviert, Änderungen vornimmt und Statusinformationen erfasst. Sie können CloudWatch Ereignisse auch verwenden, um mithilfe von Cron - oder Rate-Ausdrücken automatisierte Aktionen zu planen, die zu bestimmten Zeiten von selbst initiiert werden.

- Amazon Simple Notification Service (Amazon SNS) ermöglicht es Anwendungen, Endbenutzern und Geräten, sofort Benachrichtigungen aus der Cloud zu senden und zu empfangen. Amazon SNS bietet Themen (Kommunikationskanäle) für Push-basiertes Messaging mit hohem Durchsatz. many-to-many Mithilfe von Amazon SNS SNS-Themen können Herausgeber Nachrichten zur parallel Verarbeitung an eine große Anzahl von Abonnenten verteilen, einschließlich Amazon Simple Queue Service (Amazon SQS) -Warteschlangen, Lambda-Funktionen und HTTP/S-Webhooks. Sie können Amazon SNS auch verwenden, um Benachrichtigungen per Push, SMS und E-Mail an Endbenutzer zu senden.

Epen

Abonnieren Sie einen Datensatz

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Abonnieren Sie einen Datensatz.	Abonnieren Sie in der AWS Data Exchange Konsole einen Datensatz . Anweisungen finden Sie AWS Data Exchange in der AWS Dokumentation unter Abonnieren von Datenprodukten.	Allgemeines AWS
Notieren Sie sich die Attribute des Datensatzes.	Notieren Sie AWS-Region sich die ID und die Revisions-ID für den Datensatz. Sie benötigen dies für die AWS CloudFormation Vorlage im nächsten Schritt.	Allgemeines AWS

Stellen Sie die AWS CloudFormation Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket und einen Ordner.	Wenn Sie bereits über einen Data Lake in Amazon S3 verfügen, erstellen Sie einen Ordner, in dem die Daten gespeichert werden, aus AWS Data Exchange denen Sie aufnehmen möchten. Wenn Sie die Vorlage zu Testzweck en bereitstellen, erstellen Sie einen neuen S3-Bucket und notieren Sie sich den Bucket-Namen und das Ordnerpräfix für den nächsten Schritt.	Allgemeines AWS
Stellen Sie die AWS CloudFormation Vorlage bereit.	Stellen Sie die AWS CloudFormation Vorlage bereit, die als Anlage zu diesem Muster bereitgestellt wird. Anweisungen finden Sie in der AWS CloudFormation Dokumentation. Konfigurieren Sie die folgenden Parameter so AWS-Konto, dass sie Ihren Datensatz- und S3-Bucket -Einstellungen entsprech en: Datensatz AWS-Regio n, Datensatz-ID, Revisions -ID, S3-Bucket-Name (zum Beispiel`DOC-EXAMPLE-BUCKET`), Ordnerpräfix (zum Beispiel`myfolder/`)	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und E-Mail für SNS-Benac hrichtigung. Sie können den Parameter Dataset Name auf einen beliebigen Namen festlegen. Wenn Sie die Vorlage bereitstellen, führt sie eine Lambda-Funktion aus, um automatisch den ersten im Datensatz verfügbar en Datensatz aufzunehmen. Die nachfolgende Aufnahme erfolgt dann automatisch, sobald neue Daten in den Datensatz aufgenommen werden.	

Zugehörige Ressourcen

- Abonnieren von Datenprodukten auf AWS Data Exchange (AWS Data Exchange Dokumentation)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Automatisieren Sie die Durchsetzung von Verschlüsselungen in AWS Glue mithilfe einer CloudFormation AWS-Vorlage

Erstellt von Diogo Guedes (AWS)

Übersicht

Dieses Muster zeigt Ihnen, wie Sie mithilfe einer CloudFormation AWS-Vorlage die Durchsetzung von Verschlüsselungen in AWS Glue einrichten und automatisieren. Die Vorlage erstellt alle erforderlichen Konfigurationen und Ressourcen für die Durchsetzung der Verschlüsselung. Zu diesen Ressourcen gehören eine Erstkonfiguration, eine durch eine EventBridge Amazon-Regel erstellte präventive Kontrolle und eine AWS-Lambda-Funktion.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Berechtigungen zur Bereitstellung der CloudFormation Vorlage und ihrer Ressourcen

Einschränkungen

Diese Sicherheitskontrolle ist regional. Sie müssen die Sicherheitskontrolle in jeder AWS-Region bereitstellen, in der Sie die Durchsetzung der Verschlüsselung in AWS Glue einrichten möchten.

Architektur

Zieltechnologie-Stack

- Amazon CloudWatch Logs (von AWS Lambda)
- EventBridge Amazon-Regel
- CloudFormation AWS-Stapel
- AWS CloudTrail
- Von AWS Identity and Access Management (IAM) verwaltete Rolle und Richtlinie
- AWS Key Management Service (AWS KMS)

- AWS-KMS-Alias
- AWS Lambda-Funktion
- AWS Systems Manager Parameter Store

Zielarchitektur

Das folgende Diagramm zeigt, wie die Durchsetzung von Verschlüsselungen in AWS Glue automatisiert werden kann.

Das Diagramm zeigt den folgenden Workflow:

1. Eine CloudFormation Vorlage erstellt alle Ressourcen, einschließlich der Erstkonfiguration und der Erkennungskontrolle für die Durchsetzung der Verschlüsselung in AWS Glue.
2. Eine EventBridge Regel erkennt eine Statusänderung in der Verschlüsselungskonfiguration.
3. Eine Lambda-Funktion wird zur Auswertung und Protokollierung über Logs CloudWatch aufgerufen. Bei der Erkennung von Nichtkonformitäten wird der Parameter Store mit einem Amazon-Ressourcennamen (ARN) für einen AWS-KMS-Schlüssel wiederhergestellt. Der Service wird bei aktivierter Verschlüsselung auf den Status „konform“ zurückgesetzt.

Automatisierung und Skalierung

Wenn Sie AWS Organizations verwenden, können Sie AWS verwenden, CloudFormation StackSets um diese Vorlage in mehreren Konten bereitzustellen, für die Sie die Durchsetzung der Verschlüsselung in AWS Glue aktivieren möchten.

Tools

- Amazon CloudWatch hilft Ihnen dabei, die Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie auf AWS ausführen, in Echtzeit zu überwachen.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel Lambda-Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen AWS-Konten.
- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.

- AWS CloudTrail unterstützt Sie dabei, Betriebs- und Risikoprüfungen, Governance und Compliance Ihres AWS-Kontos zu ermöglichen.
- AWS Glue ist ein vollständig verwalteter Service zum Extrahieren, Transformieren und Laden (ETL). Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben.
- AWS Key Management Service (AWS KMS) unterstützt Sie bei der Erstellung und Kontrolle kryptografischer Schlüssel, um Ihre Daten zu schützen.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Systems Manager unterstützt Sie bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der AWS-Cloud ausgeführt werden. Es vereinfacht das Anwendungs- und Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme und hilft Ihnen, Ihre AWS-Ressourcen sicher und skalierbar zu verwalten.

Code

Der Code für dieses Muster ist im GitHub aws-custom-guardrail-event-gesteuerten Repository verfügbar.

Bewährte Methoden

AWS Glue unterstützt die Datenverschlüsselung im Ruhezustand für die Erstellung von Jobs in AWS Glue und die Entwicklung von Skripten mithilfe von Entwicklungsendpunkten.

Beachten Sie die folgenden bewährten Methoden:

- Konfigurieren Sie ETL-Jobs und Entwicklungsendpunkte so, dass sie AWS-KMS-Schlüssel verwenden, um verschlüsselte Daten im Ruhezustand zu schreiben.
- Verschlüsseln Sie die im AWS Glue Glue-Datenkatalog gespeicherten Metadaten mithilfe von Schlüsseln, die Sie über AWS KMS verwalten.
- Verwenden Sie AWS-KMS-Schlüssel, um Job-Lesezeichen und die von Crawlern und ETL-Jobs generierten Protokolle zu verschlüsseln.

Epen

Starten Sie die Vorlage CloudFormation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation Vorlage bereit.	Laden Sie die `aws-custom-guardrail-event-driven.yaml` Vorlage aus dem GitHub Repository herunter und stellen Sie sie dann bereit. Der `CREATE_COMPLETE` Status gibt an, dass Ihre Vorlage erfolgreich bereitgestellt wurde. **Note** Die Vorlage benötigt keine Eingabeparameter.	Cloud-Architekt

Überprüfen Sie die Verschlüsselungseinstellungen in AWS Glue

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die AWS-KMS-Schlüsselkonfigurationen.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die AWS Glue-Konsole. 2. Wählen Sie im Navigationsbereich unter Datenkatalog die Option Katalogeinstellungen aus.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Vergewissern Sie sich, dass die Einstellungen Metadatenverschlüsselung und Verbindungskennwörter verschlüsseln gekennzeichnet und für die Verwendung konfiguriert sind. `KMSKeyGlue`	

Testen Sie die Durchsetzung der Verschlüsselung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Verschlüsselungseinstellung in CloudFormation.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die CloudFormation Konsole. 2. Wählen Sie im Navigationsbereich Stacks und dann Ihren Stack aus. 3. Wählen Sie die Registerkarte Resources (Ressourcen) aus. 4. Suchen Sie in der Tabelle Ressourcen nach der Verschlüsselungseinstellung nach der logischen ID.	Cloud-Architekt
Versetzen Sie die bereitgestellte Infrastruktur in einen nicht konformen Zustand.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die AWS Glue-Konsole.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie im Navigationsbereich unter Datenkatalog die Option Katalogeinstellungen aus. 3. Deaktivieren Sie das Kontrollkästchen Metadatenverschlüsselung. 4. Deaktivieren Sie das Kontrollkästchen Verbindungskennwörter verschlüsseln. 5. Wählen Sie Speichern. 6. Aktualisieren Sie die AWS Glue Glue-Konsole. Die Guardrail erkennt den Status „Nicht konform“ in AWS Glue, nachdem Sie die Kontrollkästchen deaktiviert haben, und erzwingt dann die Einhaltung der Vorschriften, indem sie die Fehlkonfiguration der Verschlüsselung automatisch behebt. Daher sollten die Kontrollkästchen für die Verschlüsselung nach dem Aktualisieren der Seite erneut aktiviert werden.	

Zugehörige Ressourcen

- Einen Stack auf der CloudFormation AWS-Konsole erstellen (CloudFormation AWS-Dokumentation)

- Erstellen einer CloudWatch Ereignisregel, die bei einem AWS-API-Aufruf mithilfe von AWS ausgelöst wird CloudTrail (CloudWatch Amazon-Dokumentation)
- Verschlüsselung in AWS Glue einrichten (AWS Glue Glue-Dokumentation)

Erstellen Sie mit dem AWS DataOps Development Kit eine Datenpipeline, um Google Analytics-Daten aufzunehmen, zu transformieren und zu analysieren

Erstellt von Anton Kukushkin (AWS) und Rudy Puig (AWS)

Übersicht

Dieses Muster beschreibt, wie Sie eine Datenpipeline zum Erfassen, Transformieren und Analysieren von Google Analytics-Daten mithilfe des AWS DataOps Development Kit (AWS DDK) und anderer Tools aufbauen. AWS-Services Das AWS DDK ist ein Open-Source-Entwicklungsframework, das Sie beim Aufbau von Datenworkflows und moderner Datenarchitektur unterstützt. AWS Eines der Hauptziele des AWS DDK besteht darin, Ihnen Zeit und Mühe zu ersparen, die normalerweise für arbeitsintensive Daten-Pipeline-Aufgaben aufgewendet werden, wie z. B. die Orchestrierung von Pipelines, den Aufbau der Infrastruktur und die Schaffung der dahinter stehenden Infrastruktur. DevOps Sie können diese arbeitsintensiven Aufgaben an AWS DDK auslagern, sodass Sie sich auf das Schreiben von Code und andere wichtige Aktivitäten konzentrieren können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Ein AppFlow Amazon-Connector für Google Analytics, konfiguriert
- Python und Pip (Pythons Paketmanager)
- Git, installiert und konfiguriert
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert
- AWS Cloud Development Kit (AWS CDK), installiert

Produktversionen

- Python 3.7 oder höher
- pip 9.0.3 oder höher

Architektur

Technologie-Stack

- Amazon AppFlow
- Amazon Athena
- Amazon CloudWatch
- Amazon EventBridge
- Amazon Simple Storage Service (Amazon-S3)
- Amazon-Simple-Queue-Service (Amazon SQS)
- AWS DataOps Entwicklungskit (AWS DDK)
- AWS Lambda

Zielarchitektur

Das folgende Diagramm zeigt den ereignisgesteuerten Prozess, der Google Analytics-Daten aufnimmt, transformiert und analysiert.

Das Diagramm zeigt den folgenden Workflow:

1. Eine Amazon-Regel CloudWatch für geplante Ereignisse ruft Amazon AppFlow auf.
2. Amazon AppFlow nimmt Google Analytics-Daten in einen S3-Bucket auf.
3. Nachdem die Daten vom S3-Bucket aufgenommen wurden, EventBridge werden Ereignisbenachrichtigungen generiert, von einer CloudWatch Event-Regel erfasst und dann in eine Amazon SQS SQS-Warteschlange gestellt.
4. Eine Lambda-Funktion verarbeitet Ereignisse aus der Amazon SQS SQS-Warteschlange, liest die entsprechenden S3-Objekte, wandelt die Objekte in das Apache Parquet-Format um, schreibt die transformierten Objekte in den S3-Bucket und erstellt oder aktualisiert dann die Tabellendefinition. AWS Glue Data Catalog
5. Eine Athena-Abfrage wird für die Tabelle ausgeführt.

Tools

AWS Werkzeuge

- Amazon AppFlow ist ein vollständig verwalteter Integrationsservice, der Ihnen den sicheren Datenaustausch zwischen SaaS-Anwendungen (Software as a Service) ermöglicht.
- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon S3 analysieren können.
- Amazon CloudWatch hilft Ihnen dabei, die Kennzahlen Ihrer AWS Ressourcen und der Anwendungen, auf denen Sie laufen, AWS in Echtzeit zu überwachen.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS Lambda Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen. AWS-Konten
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Cloud Development Kit (AWS CDK)ist ein Framework für die Definition der Cloud-Infrastruktur im Code und deren Bereitstellung. AWS CloudFormation
- AWS DataOps Development Kit (AWS DDK) ist ein Open-Source-Entwicklungsframework, das Sie beim Aufbau von Datenworkflows und moderner Datenarchitektur unterstützt. AWS

Code

Der Code für dieses Muster ist in den GitHub AWS DataOps Repositorys Development Kit (AWS DDK) und Analysieren von Google Analytics-Daten mit Amazon AppFlow, Amazon Athena und AWS DataOps Development Kit verfügbar.

Epen

Bereite die Umgebung vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie den Quellcode.	Führen Sie den folgenden Befehl aus, um den Quellcode zu klonen: `git clone https://github.com/aws-samples/aws-ddk-examples.git`	DevOps Ingenieur
Erstellen Sie eine virtuelle Umgebung.	Navigieren Sie zum Quellcode verzeichnis und führen Sie dann den folgenden Befehl aus, um eine virtuelle Umgebung zu erstellen: `cd google-analytics-data-using-appflow/python && python3 -m venv .venv`	DevOps Ingenieur
Installieren Sie die Abhängigkeiten.	Führen Sie den folgenden Befehl aus, um die virtuelle Umgebung zu aktivieren und die Abhängigkeiten zu installieren: `source .venv/bin/activate && pip install -r requirements.txt`	DevOps Ingenieur

Stellen Sie die Anwendung bereit, die Ihre Datenpipeline verwendet

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bootstrap für die Umgebung.	1. Vergewissern Sie AWS CLI sich, dass das mit gültigen Anmeldeinformationen für Ihre AWS-Konto eingerich tet ist. Weitere Informati onen finden Sie in der AWS CLI Dokumentation unter Verwenden benannter Profile. 2. Führen Sie den Befehl `cdk bootstrap --profile [AWS_PROFILE]` aus.	DevOps Ingenieur
Stellen Sie die Daten bereit.	Führen Sie den `cdk deploy --profile [AWS_PROF ILE]` Befehl aus, um die Datenpipeline bereitzustellen.	DevOps Ingenieur

Testen der Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Stack-Sta tus.	1. Öffnen Sie die AWS CloudFormation -Konsole. 2. Vergewissern Sie sich auf der Seite Stacks, dass der Status des Stacks `DdkAppflowAthenaSt ack` lautet`CREATE_CO MPLETE` .	DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Die Bereitstellung schlägt während der Erstellung einer `AWS::AppFlow::Flow` Ressource fehl und Sie erhalten die folgende Fehlermeldung: `Connector Profile with name ga-connection does not exist`	Bestätigen Sie, dass Sie einen AppFlow Amazon-Connector für Google Analytics erstellt und ihm einen Namen gegeben haben `ga-connection` . Anweisungen finden Sie unter Google Analytics in der AppFlow Amazon-Dokumentation.

Zugehörige Ressourcen

- AWS DataOps Entwicklungskit (AWS DDK) (GitHub)
- AWS DDK-Beispiele () GitHub

Zusätzliche Informationen

AWS DDK-Datenpipelines bestehen aus einer oder mehreren Stufen. In den folgenden Codebeispielen verwenden Sie, `AppFlowIngestionStage` um Daten aus Google Analytics aufzunehmen, `SqsToLambdaStage` die Datentransformation durchzuführen und `AthenaSQLStage` die Athena-Abfrage auszuführen.

Zunächst werden die Phasen Datentransformation und Datenaufnahme erstellt, wie das folgende Codebeispiel zeigt:

```
        appflow_stage = AppFlowIngestionStage(
            self,
            id="appflow-stage",
            flow_name=flow.flow_name,
        )
        sqs_lambda_stage = SqsToLambdaStage(
            self,
            id="lambda-stage",
            lambda_function_props={
                "code": Code.from_asset("./ddk_app/lambda_handlers"),
                "handler": "handler.lambda_handler",
```

```
                "layers": [
                    LayerVersion.from_layer_version_arn(
                        self,
                        id="layer",
                        layer_version_arn=f"arn:aws:lambda:
{self.region}:336392948345:layer:AWSDataWrangler-Python39:1",
                    )
                ],
                "runtime": Runtime.PYTHON_3_9,
            },
        )
        # Grant lambda function S3 read & write permissions
        bucket.grant_read_write(sqs_lambda_stage.function)
        # Grant Glue database & table permissions
        sqs_lambda_stage.function.add_to_role_policy(
            self._get_glue_db_iam_policy(database_name=database.database_name)
        )
        athena_stage = AthenaSQLStage(
            self,
            id="athena-sql",
            query_string=[
                (
                    "SELECT year, month, day, device, count(user_count) as cnt "
                    f"FROM {database.database_name}.ga_sample "
                    "GROUP BY year, month, day, device "
                    "ORDER BY cnt DESC "
                    "LIMIT 10; "
                )
            ],
            output_location=Location(
                bucket_name=bucket.bucket_name, object_key="query-results/"
            ),
            additional_role_policy_statements=[
                self._get_glue_db_iam_policy(database_name=database.database_name)
            ],
        )
```

Als Nächstes wird das `DataPipeline` Konstrukt verwendet, um die Stufen mithilfe von EventBridge Regeln miteinander zu verbinden, wie das folgende Codebeispiel zeigt:

```
        (
            DataPipeline(self, id="ingestion-pipeline")
            .add_stage(
```

```
                stage=appflow_stage,
                override_rule=Rule(
                    self,
                    "schedule-rule",
                    schedule=Schedule.rate(Duration.hours(1)),
                    targets=appflow_stage.targets,
                ),
            )
            .add_stage(
                stage=sqs_lambda_stage,
                # By default, AppFlowIngestionStage stage emits an event after the flow
run finishes successfully
                # Override rule below changes that behavior to call the the stage when
data lands in the bucket instead
                override_rule=Rule(
                    self,
                    "s3-object-created-rule",
                    event_pattern=EventPattern(
                        source=["aws.s3"],
                        detail={
                            "bucket": {"name": [bucket.bucket_name]},
                            "object": {"key": [{"prefix": "ga-data"}]},
                        },
                        detail_type=["Object Created"],
                    ),
                    targets=sqs_lambda_stage.targets,
                ),
            )
            .add_stage(stage=athena_stage)
        )
```

Weitere Codebeispiele finden Sie im Repository GitHub [Analysieren von Google Analytics-Daten mit Amazon AppFlow, Amazon Athena und AWS DataOps Development Kit](#).

Erstellen Sie mithilfe von Amazon Kinesis Video Streams und AWS Fargate eine Videoverarbeitungspipeline

Erstellt von Piotr Chotkowski (AWS) und Pushparaju Thangavel (AWS)

Übersicht

Dieses Muster zeigt, wie Amazon Kinesis Video Streams und AWS Fargate verwendet werden, um Frames aus einem Videostream zu extrahieren und sie als Bilddateien für die weitere Verarbeitung in Amazon Simple Storage Service (Amazon S3) zu speichern.

Das Muster bietet eine Beispielanwendung in Form eines Java-Maven-Projekts. Diese Anwendung definiert die AWS-Infrastruktur mithilfe des AWS Cloud Development Kit (AWS CDK). Sowohl die Frame-Verarbeitungslogik als auch die Infrastrukturdefinitionen sind in der Programmiersprache Java geschrieben. Sie können diese Beispielanwendung als Grundlage für die Entwicklung Ihrer eigenen Echtzeit-Videoverarbeitungspipeline oder für die Erstellung des Videovorverarbeitungsschritts einer Pipeline für maschinelles Lernen verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Java SE Development Kit (JDK) 11, installiert
- Apache Maven, installiert
- AWS Cloud Development Kit (AWS CDK), installiert
- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 2, installiert
- Docker (erforderlich für die Erstellung von Docker-Images zur Verwendung in AWS Fargate-Aufgabendefinitionen), installiert

Einschränkungen

Dieses Muster ist als Machbarkeitsnachweis oder als Grundlage für die weitere Entwicklung gedacht. Es sollte in seiner derzeitigen Form nicht in Produktionsbereitstellungen verwendet werden.

Produktversionen

- Dieses Muster wurde mit der AWS-CDK-Version 1.77.0 getestet (siehe AWS-CDK-Versionen)
- JDK 11
- AWS-CLI Version 2

Architektur

Zieltechnologie-Stack

- Amazon Kinesis Video Streams
- AWS Fargate-Aufgabe
- Amazon Simple Queue Service-Warteschlange (Amazon SQS)
- Amazon-S3-Bucket

Zielarchitektur

Der Benutzer erstellt einen Kinesis-Videostream, lädt ein Video hoch und sendet eine JSON-Nachricht, die Details zum Kinesis-Eingabevideostream und zum S3-Ausgabe-Bucket enthält, an eine SQS-Warteschlange. AWS Fargate, das die Hauptanwendung in einem Container ausführt, ruft die Nachricht aus der SQS-Warteschlange ab und beginnt mit dem Extrahieren von Frames. Jeder Frame wird in einer Bilddatei und im Ziel-S3-Bucket gespeichert.

Automatisierung und Skalierung

Die Beispielanwendung kann innerhalb einer einzelnen AWS-Region sowohl horizontal als auch vertikal skaliert werden. Horizontale Skalierung kann erreicht werden, indem die Anzahl der bereitgestellten AWS Fargate-Aufgaben erhöht wird, die aus der SQS-Warteschlange lesen. Vertikale Skalierung kann erreicht werden, indem die Anzahl der Framesplitting- und Image-Publishing-Threads in der Anwendung erhöht wird. Diese Einstellungen werden in der Definition der QueueProcessingFargateServiceRessource im AWS-CDK als Umgebungsvariablen an die Anwendung übergeben. Aufgrund der Art der AWS-CDK-Stack-Bereitstellung können Sie diese Anwendung ohne zusätzlichen Aufwand in mehreren AWS-Regionen und Konten bereitstellen.

Tools

Tools

- AWS CDK ist ein Softwareentwicklungs-Framework zur Definition Ihrer Cloud-Infrastruktur und -Ressourcen mithilfe von Programmiersprachen wie TypeScript,, Python JavaScript, Java und C#/.Net.
- Amazon Kinesis Video Streams ist ein vollständig verwalteter AWS-Service, mit dem Sie Live-Videos von Geräten in die AWS-Cloud streamen oder Anwendungen für Echtzeit-Videoverarbeitung oder stapelorientierte Videoanalysen erstellen können.
- AWS Fargate ist eine serverlose Compute-Engine für Container. Fargate macht die Bereitstellung und Verwaltung von Servern überflüssig, sodass Sie sich auf die Entwicklung Ihrer Anwendungen konzentrieren können.
- Amazon S3 ist ein Objektspeicherservice, der Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet.
- Amazon SQS ist ein vollständig verwalteter Message Queuing-Service, mit dem Sie Microservices, verteilte Systeme und serverlose Anwendungen entkoppeln und skalieren können.

Code

- Eine ZIP-Datei des Beispielanwendungsprojekts () ist angehängt. `frame-splitter-code.zip`

Epen

Stellen Sie die Infrastruktur bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den Docker-Da emon.	Starten Sie den Docker-Daemon auf Ihrem lokalen System. Das AWS CDK verwendet Docker, um das Image zu erstellen, das in der AWS Fargate-Aufgabe verwendet wird. Sie müssen Docker ausführen, bevor Sie mit dem nächsten Schritt fortfahren können.	Entwickler, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Projekt.	Laden Sie die `frame-splitter-code` Beispielanwendung (im Anhang) herunter und extrahieren Sie ihren Inhalt in einen Ordner auf Ihrem lokalen Computer. Bevor Sie die Infrastruktur bereitstellen können, müssen Sie das Java-Maven-Projekt erstellen. Navigieren Sie in einer Befehlszeile zum Stammverzeichnis des Projekts und erstellen Sie das Projekt, indem Sie den folgenden Befehl ausführen: `mvn clean install`	Entwickler, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bootstrap für das AWS-CDK.	(Nur AWS-CDK-Erstbenutzer) Wenn Sie das AWS-CDK zum ersten Mal verwenden, müssen Sie die Umgebung möglicherweise booten, indem Sie den AWS-CLI-Befehl ausführen: `cdk bootstrap --profile "$AWS_PROFILE_NAME"` wo `$AWS_PROFILE_NAME` der Name des AWS-Profils aus Ihren AWS-Anmeldeinformationen gespeichert ist. Sie können diesen Parameter auch entfernen, um das Standardprofil zu verwenden. Weitere Informationen finden Sie in der AWS-CDK-Dokumentation.	Entwickler, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den AWS-CDK-Stack bereit.	In diesem Schritt erstellen Sie die erforderlichen Infrastrukturressourcen (SQS-Warteschlange, S3-Bucket, AWS Fargate-Aufgabendefinition) in Ihrem AWS-Konto, erstellen das Docker-Image, das für die AWS Fargate-Aufgabe erforderlich ist, und stellen die Anwendung bereit. Navigieren Sie an einer Befehlszeile zum Stammverzeichnis des Projekts und führen Sie den folgenden Befehl aus: `cdk deploy --profile "$AWS_PROFILE_NAME" --all` wo `$AWS_PROFILE_NAME` der Name des AWS-Profils aus Ihren AWS-Anmeldeinformationen gespeichert ist. Sie können diesen Parameter auch entfernen, um das Standardprofil zu verwenden. Bestätigen Sie die Bereitstellung. Notieren Sie sich die Werte QueueUrlund Bucket aus der CDK-Bereitstellungsausgabe. Sie werden sie in späteren Schritten benötigen. Das AWS-CDK erstellt die Ressourcen, lädt sie auf Ihr	Entwickler, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	AWS-Konto hoch und erstellt alle Infrastrukturressourcen. Sie können den Prozess der Ressourcenerstellung in der CloudFormation AWS-Konsole beobachten. Weitere Informationen finden Sie in der CloudFormation AWS-Dokumentation und der AWS-CDK-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Videostream.	In diesem Schritt erstellen Sie einen Kinesis-Videostream, der als Eingangsstream für die Videoverarbeitung dient. Stellen Sie sicher, dass Sie die AWS-CLI installiert und konfiguriert haben. Führen Sie in der AWS-CLI Folgendes aus: `aws kinesisvideo --profile "$AWS_PROFILE_NAME" create-stream --stream-name "$STREAM_NAME" --data-retention-in-hours "24"` wobei der `$AWS_PROFILE_NAME` Name des AWS-Profils aus Ihren AWS-Anmeldeinformationen enthalten ist (oder entfernen Sie diesen Parameter, um das Standardprofil zu verwenden) und `$STREAM_NAME` ein beliebiger gültiger Streamname ist. Alternativ können Sie mithilfe der Kinesis-Konsole einen Videostream erstellen, indem Sie die Schritte in der Kinesis Video Streams-Dokumentation befolgen. Notieren Sie sich den AWS-Ressourcennamen	Entwickler, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(ARN) des erstellten Streams. Sie benötigen ihn später.	

Führen Sie ein Beispiel aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das Video in den Stream hoch.	Öffnen Sie im Projektordner für die `frame-splitter-code` Beispielanwendung die `ProcessingTaskTest.java` Datei im `src/test/java/amazon/awscdk/examples/splitter` Ordner. Ersetzen Sie die `streamName` Variablen `profileName` und durch die Werte, die Sie in den vorherigen Schritten verwendet haben. Um das Beispielvideo in den Kinesis-Videostream hochzuladen, den Sie im vorherigen Schritt erstellt haben, führen Sie folgenden Befehl aus: `amazon.awscdk.examples.splitter.ProcessingTaskTest#testExample test` Alternativ können Sie Ihr Video mit einer der in der Kinesis Video Streams Streams-Dokumentation	Entwickler, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	beschriebenen Methoden hochladen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Initiieren Sie die Videoverarbeitung.	Nachdem Sie ein Video in den Kinesis-Videostream hochgeladen haben, können Sie mit der Verarbeitung beginnen. Um die Verarbeitungslogik zu initiieren, müssen Sie eine Nachricht mit Details an die SQS-Warteschlange senden, die das AWS-CDK während der Bereitstellung erstellt hat. Um eine Nachricht mit der AWS-CLI zu senden, führen Sie Folgendes aus:
	`aws sqs --profile "$AWS_PROFILE_NAME" send-message --queue-url QUEUE_URL --message-body MESSAGE`
	wobei `$AWS_PROFILE_NAME` der Name des AWS-Profils aus Ihren AWS-Anmeldeinformationen (entfernen Sie diesen Parameter, um das Standardprofil zu verwenden), `QUEUE_URL` der QueueUrlWert aus der AWS-CDK-Ausgabe `MESSAGE` ist und eine JSON-Zeichenfolge im folgenden Format ist:
	`{ "streamARN": "STREAM_ARN", "bucket": "BUCKET_N`
		Entwickler, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`AME", "s3Directory": "test-output" }` Dabei `STREAM_ARN` handelt es sich um den ARN des Videostreams, den Sie in einem früheren Schritt erstellt haben, und `BUCKET_NAME` um den Bucket-Wert aus der AWS-CDK-Ausgabe. Durch das Senden dieser Nachricht wird die Videoverarbeitung eingeleitet. Alternativ können Sie eine Nachricht mithilfe der Amazon SQS SQS-Konsole senden, wie in der Amazon SQS SQS-Dokumentation beschrieben.	
Bilder der Videoframes anzeigen.	Sie können die resultierenden Bilder im S3-Ausgabe-Bucket sehen, `s3://BUCKET_NAME/test-output` wo `BUCKET_NAME` sich der Bucket-Wert aus der AWS-CDK-Ausgabe befindet.	Entwickler, Ingenieur DevOps

Zugehörige Ressourcen

- AWS-CDK-Dokumentation
- AWS-CDK-API-Referenz
- AWS CDK Einführungsworkshop
- Dokumentation zu Amazon Kinesis Video Streams

- Beispiel: Identifizieren von Objekten in Videostreams mithilfe von SageMaker
- Beispiel: Analysieren und Rendern von Kinesis-Videostream-Fragmenten
- Analysieren Sie Live-Videos in großem Maßstab in Echtzeit mit Amazon Kinesis Video Streams und Amazon SageMaker (Blogbeitrag zu AWS Machine Learning)
- AWS Fargate — Erste Schritte

Zusätzliche Informationen

Eine IDE auswählen

Wir empfehlen Ihnen, Ihre bevorzugte Java-IDE zu verwenden, um dieses Projekt zu erstellen und zu erkunden.

Bereinigen

Nachdem Sie dieses Beispiel ausgeführt haben, entfernen Sie alle bereitgestellten Ressourcen, um zusätzliche AWS-Infrastrukturkosten zu vermeiden.

Verwenden Sie diese beiden Befehle in der AWS-CLI, um die Infrastruktur und den Videostream zu entfernen:

```
cdk destroy --profile "$AWS_PROFILE_NAME" --all
```

```
aws kinesisvideo --profile "$AWS_PROFILE_NAME" delete-stream --stream-arn "$STREAM_ARN"
```

Alternativ können Sie die Ressourcen manuell entfernen, indem Sie die CloudFormation AWS-Konsole verwenden, um den CloudFormation AWS-Stack zu entfernen, und die Kinesis-Konsole, um den Kinesis-Videostream zu entfernen. Beachten Sie, dass der Ausgabe-S3-Bucket oder die Bilder in den Amazon Elastic Container Registry (Amazon ECR) -Repositorys (`aws-cdk/assets`) `cdk destroy` nicht entfernt werden. Sie müssen sie manuell entfernen.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Erstellen Sie eine ETL-Servicepipeline, um Daten mithilfe von AWS Glue inkrementell von Amazon S3 nach Amazon Redshift zu laden

Erstellt von Rohan Jamadagni (AWS) und Arunabha Datta (AWS)

Übersicht

Dieses Muster enthält Anleitungen zur Konfiguration von Amazon Simple Storage Service (Amazon S3) für eine optimale Data-Lake-Leistung und zum anschließenden Laden inkrementeller Datenänderungen von Amazon S3 in Amazon Redshift mithilfe von AWS Glue, wobei Extraktions-, Transformations- und Ladevorgänge (ETL) ausgeführt werden.

Die Quelldateien in Amazon S3 können verschiedene Formate haben, darunter kommagetrennte Werte (CSV), XML- und JSON-Dateien. Dieses Muster beschreibt, wie Sie AWS Glue verwenden können, um die Quelldateien in ein kosten- und leistungsoptimiertes Format wie Apache Parquet zu konvertieren. Sie können Parquet-Dateien direkt von Amazon Athena und Amazon Redshift Spectrum aus abfragen. Sie können Parquet-Dateien auch in Amazon Redshift laden, sie aggregieren und die aggregierten Daten mit Verbrauchern teilen oder die Daten mithilfe von Amazon visualisieren. QuickSight

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein S3-Quell-Bucket mit den richtigen Rechten, der CSV-, XML- oder JSON-Dateien enthält.

Annahmen

- Die CSV-, XML- oder JSON-Quelldateien wurden bereits in Amazon S3 geladen und sind von dem Konto aus zugänglich, in dem AWS Glue und Amazon Redshift konfiguriert sind.
- Bewährte Methoden für das Laden der Dateien, das Teilen der Dateien, die Komprimierung und die Verwendung eines Manifests werden befolgt, wie in der Amazon Redshift Redshift-Dokumentation beschrieben.
- Die Struktur der Quelldatei ist unverändert.
- Das Quellsystem kann Daten in Amazon S3 aufnehmen, indem es der in Amazon S3 definierten Ordnerstruktur folgt.

- Der Amazon Redshift Redshift-Cluster erstreckt sich über eine einzige Availability Zone. (Diese Architektur ist angemessen, da AWS Lambda, AWS Glue und Amazon Athena serverlos sind.) Um eine hohe Verfügbarkeit zu gewährleisten, werden Cluster-Snapshots in regelmäßigen Abständen erstellt.

Einschränkungen

- Die Dateiformate sind auf diejenigen beschränkt, die derzeit von AWS Glue unterstützt werden.
- Downstream-Berichte in Echtzeit werden nicht unterstützt.

Architektur

Quelltechnologie-Stack

- S3-Bucket mit CSV-, XML- oder JSON-Dateien

Zieltechnologie-Stack

- S3-Datensee (mit partitioniertem Parquet-Dateispeicher)
- Amazon Redshift

Zielarchitektur

Datenfluss

Tools

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice. Amazon S3 kann für eine Vielzahl von Speicherlösungen verwendet werden, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- AWS Lambda — Mit AWS Lambda können Sie Code ausführen, ohne Server bereitzustellen oder zu verwalten. AWS Lambda ist ein ereignisgesteuerter Service. Sie können Ihren Code so einrichten, dass er automatisch von anderen AWS-Services initiiert wird.

- Amazon Redshift — Amazon Redshift ist ein vollständig verwalteter Data-Warehouse-Service im Petabyte-Bereich. Mit Amazon Redshift können Sie Petabyte an strukturierten und halbstrukturierten Daten in Ihrem Data Warehouse und Ihrem Data Lake mithilfe von Standard-SQL abfragen.
- AWS Glue — AWS Glue ist ein vollständig verwalteter ETL-Service, der das Aufbereiten und Laden von Daten für Analysen erleichtert. AWS Glue erkennt Ihre Daten und speichert die zugehörigen Metadaten (z. B. Tabellendefinitionen und Schema) im AWS Glue Glue-Datenkatalog. Ihre katalogisierten Daten sind sofort durchsuchbar, können abgefragt werden und sind für ETL verfügbar.
- AWS Secrets Manager — AWS Secrets Manager erleichtert den Schutz und die zentrale Verwaltung von Geheimnissen, die für den Anwendungs- oder Servicezugriff benötigt werden. Der Service speichert Datenbankanmeldedaten, API-Schlüssel und andere Geheimnisse und macht es überflüssig, vertrauliche Informationen im Klartextformat fest zu codieren. Secrets Manager bietet auch eine Schlüsselrotation, um Sicherheits- und Compliance-Anforderungen zu erfüllen. Es verfügt über eine integrierte Integration für Amazon Redshift, Amazon Relational Database Service (Amazon RDS) und Amazon DocumentDB. Sie können Geheimnisse speichern und zentral verwalten, indem Sie die Secrets Manager-Konsole, die Befehlszeilenschnittstelle (CLI) oder die Secrets Manager API und verwenden. SDKs
- Amazon Athena — Amazon Athena ist ein interaktiver Abfrageservice, der die Analyse von in Amazon S3 gespeicherten Daten vereinfacht. Athena ist serverlos und in AWS Glue integriert, sodass es die mit AWS Glue katalogisierten Daten direkt abfragen kann. Athena ist elastisch skaliert, um interaktive Abfrageleistung zu bieten.

Epen

Erstellen Sie die S3-Buckets und die Ordnerstruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie Quellsysteme auf Datenstruktur und Attribute .	Führen Sie diese Aufgabe für jede Datenquelle aus, die zum Amazon S3 S3-Data Lake beiträgt.	Dateningenieur
Definieren Sie die Partitions- und Zugriffsstrategie.	Diese Strategie sollte auf der Häufigkeit der Datenerfa	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ssung, der Delta-Verarbeitung und den Nutzungsanforderungen basieren. Stellen Sie sicher, dass S3-Buckets nicht öffentlich zugänglich sind und dass der Zugriff nur durch spezifische, auf Servicerollen basierende Richtlinien gesteuert wird. Weitere Informationen finden Sie in der Amazon S3-Dokumentation.	
Erstellen Sie separate S3-Buckets für jeden Datenquellentyp und einen separaten S3-Bucket pro Quelle für die verarbeiteten (Parquet-) Daten.	Erstellen Sie für jede Quelle einen separaten Bucket und anschließend eine Ordnerstruktur, die auf der Datenaufnahmefrequenz des Quellsystems basiert, z. B. `s3://source-system-name/date/hour` Erstellen Sie für die verarbeiteten (in das Parquet-Format konvertierten) Dateien eine ähnliche Struktur, z. B. `s3://source-processed-bucket/date/hour` Weitere Informationen zum Erstellen von S3-Buckets finden Sie in der Amazon S3 S3-Dokumentation.	Dateningenieur

Erstellen Sie ein Data Warehouse in Amazon Redshift

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den Amazon Redshift Redshift-Cluster mit den entsprechenden Parametergruppen und der Wartungs- und Sicherung sstrategie.	Verwenden Sie das Secrets Manager Manager-D atenbankgeheimnis für Administratoranmeldedaten, während Sie den Amazon Redshift Redshift-Cluster erstellen. Informationen zur Erstellung und Dimension ierung eines Amazon Redshift Redshift-Clusters finden Sie in der Amazon Redshift Redshift-Dokumentation und im Whitepaper Sizing Cloud Data Warehouses.	Dateningenieur
Erstellen Sie die IAM-Servi cerolle und fügen Sie sie dem Amazon Redshift Redshift-Cluster hinzu.	Die Servicerolle AWS Identity and Access Management (IAM) gewährleistet den Zugriff auf Secrets Manager und die S3-Quell-Buckets. Weitere Informationen finden Sie in der AWS-Dokumentation zur Autorisierung und zum Hinzufügen einer Rolle.	Dateningenieur
Erstellen Sie das Datenbank schema.	Folgen Sie den Best Practices von Amazon Redshift für das Tabellendesign. Wählen Sie je nach Anwendungsfall die geeigneten Sortier- und Verteilungsschlüssel sowie die bestmögliche Komprimie rungskodierung aus. Bewährte	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Methoden finden Sie in der AWS-Dokumentation.	
Konfigurieren Sie das Workload-Management.	Konfigurieren Sie je nach Ihren Anforderungen Warteschlangen für Workload Management (WLM), Short Query Acceleration (SQA) oder Parallelitätsskalierung. Weitere Informationen finden Sie unter Implementieren des Workload-Managements in der Amazon Redshift Redshift-Dokumentation.	Dateningenieur

Erstellen Sie ein Geheimnis in Secrets Manager

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein neues Geheimnis, um die Amazon Redshift Redshift-Anmeldeinformationen in Secrets Manager zu speichern.	In diesem Secret werden die Anmeldeinformationen für den Admin-Benutzer sowie für einzelne Benutzer des Datenbankdienstes gespeichert. Anweisungen finden Sie in der Secrets Manager Manager-Dokumentation. Wählen Sie Amazon Redshift Cluster als geheimen Typ. Aktivieren Sie außerdem auf der Seite „Secret Rotation“ die Rotation. Dadurch wird der entsprechende Benutzer im Amazon Redshift Redshift-Cluster erstellt und die	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Schlüsselgeheimnisse werden in definierten Intervallen rotiert.	
Erstellen Sie eine IAM-Richtlinie, um den Zugriff auf Secrets Manager einzuschränken.	Beschränken Sie den Secrets Manager Manager-Zugriff nur auf Amazon Redshift Redshift-Administratoren und AWS Glue.	Dateningenieur

AWS Glue konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie im AWS Glue Glue-Datenkatalog eine Verbindung für Amazon Redshift hinzu.	Anweisungen finden Sie in der AWS Glue Glue-Dokumentation.	Dateningenieur
Erstellen Sie eine IAM-Servicerolle für AWS Glue und fügen Sie sie hinzu, um auf Secrets Manager-, Amazon Redshift- und S3-Buckets zuzugreifen.	Weitere Informationen finden Sie in der AWS Glue Glue-Dokumentation.	Dateningenieur
Definieren Sie den AWS Glue Glue-Datenkatalog für die Quelle.	Dieser Schritt beinhaltet die Erstellung einer Datenbank und der erforderlichen Tabellen im AWS Glue Glue-Datenkatalog. Sie können entweder einen Crawler verwenden, um die Tabellen in der AWS Glue Glue-Datenbank zu katalogisieren, oder sie als externe Amazon	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Athena Athena-Tabellen definieren. Sie können auch über den AWS Glue Glue-Datenkatalog auf die in Athena definierten externen Tabellen zugreifen. Weitere Informationen zur Definition des Datenkatalogs und zur Erstellung einer externen Tabelle in Athena finden Sie in der AWS-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen AWS Glue Glue-Job zur Verarbeitung von Quelldaten.	Bei dem AWS Glue Glue-Job kann es sich um eine Python-Shell handeln oder PySpark um die Quelldatendateien zu standardisieren, zu deduplizieren und zu bereinigen. Um die Leistung zu optimieren und zu vermeiden, dass der gesamte S3-Quell-Bucket abgefragt werden muss, partitionieren Sie den S3-Bucket nach Datum, aufgeschlüsselt nach Jahr, Monat, Tag und Stunde als Pushdown-Prädikat für den AWS Glue Glue-Job. Weitere Informationen finden Sie in der AWS Glue Glue-Dokumentation. Laden Sie die verarbeiteten und transformierten Daten im Parquet-Format in die verarbeiteten S3-Bucket-Partitionen. Sie können die Parquet-Dateien von Athena abfragen.	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen AWS Glue Glue-Job, um Daten in Amazon Redshift zu laden.	Der AWS Glue Glue-Job kann eine Python-Shell sein oder PySpark die Daten laden, indem die Daten aktualisiert werden, gefolgt von einer vollständigen Aktualisierung. Einzelheiten finden Sie in der AWS Glue Glue-Dokumentation und im Abschnitt Zusätzliche Informationen.	Dateningenieur
(Optional) Planen AWS Glue Glue-Jobs, indem Sie bei Bedarf Trigger verwenden.	Die inkrementelle Datenlast wird hauptsächlich durch ein Amazon S3 S3-Ereignis ausgelöst, das eine AWS Lambda Lambda-Funktion veranlasst, den AWS Glue Glue-Job aufzurufen. Verwenden Sie die triggerbasierte Planung von AWS Glue für alle Datenladungen, die eine zeitbasierte statt einer ereignisbasierten Planung erfordern.	Dateningenieur

Erstellen einer Lambda-Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine mit dem IAM-Service verknüpfte Rolle für AWS Lambda, um auf S3-Buckets und den AWS Glue	Erstellen Sie eine mit dem IAM-Service verknüpfte Rolle für AWS Lambda mit einer Richtlinie zum Lesen von Amazon S3 S3-Objekten und	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Glue-Job zuzugreifen, und fügen Sie sie hinzu.	-Buckets und einer Richtlini e für den Zugriff auf die AWS Glue Glue-API, um einen AWS Glue Glue-Job zu starten. Weitere Informationen finden Sie im Knowledge Center.	
Erstellen Sie eine Lambda-Funktion, um den AWS Glue Glue-Job auf der Grundlage des definierten Amazon S3 S3-Ereignisses auszuführen.	Die Lambda-Funktion sollte durch die Erstellung der Amazon S3-Manifestdatei initiiert werden. Die Lambda-Funktion sollte den Speichero rt des Amazon S3 S3-Ordner s (z. B. source_bucket/ year/month/date/hour) als Parameter an den AWS Glue Glue-Job übergeben . Der AWS Glue Glue-Job verwendet diesen Parameter als Pushdown-Prädikat, um den Dateizugriff und die Auftragsverarbeitungsleistu ng zu optimieren. Weitere Informationen finden Sie in der AWS Glue Glue-Doku mentation.	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon S3 S3-PUT-Objektereignis, um die Objekterstellung zu erkennen, und rufen Sie die entsprechende Lambda-Funktion auf.	Das Amazon S3 S3-PUT-Objektereignis sollte nur durch die Erstellung der Manifestdatei ausgelöst werden. Die Manifestdatei steuert die Lambda-Funktion und die Parallelität des AWS Glue Glue-Jobs und verarbeitet den Ladevorgang als Batch, anstatt einzelne Dateien zu verarbeiten, die in einer bestimmten Partition des S3-Quell-Buckets ankommen. Weitere Informationen finden Sie in der Lambda-Dokumentation.	Dateningenieur

Zugehörige Ressourcen

- Amazon S3 S3-Dokumentation
- Dokumentation zu AWS Glue
- Amazon Redshift Redshift-Dokumentation
- AWS Lambda
- Amazon Athena
- AWS Secrets Manager

Zusätzliche Informationen

Detaillierter Ansatz für Upsert und Complete Refresh

Upsert: Dies ist für Datensätze vorgesehen, die je nach geschäftlichem Anwendungsfall eine historische Aggregation erfordern. Folgen Sie je nach Ihren Geschäftsanforderungen einem der unter

Aktualisieren und Einfügen neuer Daten (Amazon Redshift Redshift-Dokumentation) beschriebenen Methoden.

Vollständige Aktualisierung: Dies ist für kleine Datensätze vorgesehen, für die keine historischen Aggregationen erforderlich sind. Folgen Sie einem der folgenden Ansätze:

1. Kürzen Sie die Amazon Redshift Redshift-Tabelle.
2. Lädt die aktuelle Partition aus dem Staging-Bereich

oder:

1. Erstellen Sie eine temporäre Tabelle mit aktuellen Partitionsdaten.
2. Löschen Sie die Amazon Redshift Redshift-Zieltabelle.
3. Benennen Sie die temporäre Tabelle in die Zieltabelle um.

Bauen Sie mit Amazon ein Datennetz für Unternehmen auf DataZone AWS CDK, und AWS CloudFormation

Erstellt von Dhrubajyoti Mukherjee (AWS), Adjoa Taylor (AWS), Ravi Kumar (AWS) und Weizhou Sun (AWS)

Übersicht

Bei Amazon Web Services (AWS) wissen Kunden, dass Daten der Schlüssel zur Beschleunigung von Innovationen und zur Steigerung des Geschäftswerts für ihr Unternehmen sind. Um diese riesigen Datenmengen zu verwalten, können Sie eine dezentrale Architektur wie Data Mesh einsetzen. Eine Data-Mesh-Architektur erleichtert das Produktdenken, eine Denkweise, die Kunden, Ziele und den Markt berücksichtigt. Data Mesh hilft auch dabei, ein föderiertes Governance-Modell zu etablieren, das einen schnellen und sicheren Zugriff auf Ihre Daten ermöglicht.

Unter Strategien für den Aufbau einer auf Datennetzen basierenden Unternehmenslösung AWS wird erläutert, wie Sie das Data Mesh Strategy Framework verwenden können, um eine Data-Mesh-Strategie für Ihr Unternehmen zu formulieren und zu implementieren. Mithilfe des Data Mesh Strategy Framework können Sie die Organisation von Teams und deren Interaktionen optimieren, um Ihre Datennetzentwicklung zu beschleunigen.

Dieses Dokument enthält Anleitungen zum Aufbau eines Unternehmensdatennetzes mit Amazon DataZone. Amazon DataZone ist ein Datenverwaltungsservice für die Katalogisierung, Erkennung, gemeinsame Nutzung und Verwaltung von Daten, die vor Ort und in AWS Quellen von Drittanbietern gespeichert sind. Das Muster umfasst Code-Artefakte, die Ihnen helfen, die auf Datennetzen basierende Datenlösungsinfrastruktur mithilfe von und bereitzustellen. AWS Cloud Development Kit (AWS CDK) AWS CloudFormation Dieses Muster ist für Cloud-Architekten und -Techniker vorgesehen. DevOps

Informationen zu den Zielen dieses Musters und zum Lösungsumfang finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Mindestens zwei aktive Konten AWS-Konten: eines für das zentrale Governance-Konto und ein weiteres für das Mitgliedskonto

- AWS Administratoranmeldedaten für das zentrale Governance-Konto in Ihrer Entwicklungsumgebung
- AWS Command Line Interface (AWS CLI) wurde installiert, um Ihre über die AWS-Services Befehlszeile zu verwalten
- Node.js und Node Package Manager (npm) wurden installiert, um Anwendungen zu verwalten AWS CDK
- AWS CDK Das Toolkit wurde mithilfe von npm global in Ihrer Entwicklungsumgebung installiert, um Anwendungen zu synthetisieren und bereitzustellen AWS CDK

```
npm install -g aws-cdk
```

- Python Version 3.12 ist in Ihrer Entwicklungsumgebung installiert
- TypeScript in Ihrer Entwicklungsumgebung installiert oder global mit dem npm-Compiler installiert:

```
npm install -g typescript
```

- Docker ist in Ihrer Entwicklungsumgebung installiert
- Ein Versionskontrollsystem wie Git zur Pflege des Quellcodes der Lösung (empfohlen)
- Eine integrierte Entwicklungsumgebung (IDE) oder ein Texteditor mit Unterstützung für Python und TypeScript (dringend empfohlen)

Einschränkungen

- Die Lösung wurde nur auf Maschinen getestet, auf denen Linux oder macOS ausgeführt wird.
- In der aktuellen Version unterstützt die Lösung standardmäßig nicht die Integration AWS IAM Identity Center von Amazon DataZone . Sie können es jedoch so konfigurieren, dass es diese Integration unterstützt.

Produktversionen

- Python-versie 3.12

Architektur

Das folgende Diagramm zeigt eine Data-Mesh-Referenzarchitektur. Die Architektur basiert auf Amazon DataZone und verwendet Amazon Simple Storage Service (Amazon S3) und AWS

Glue Data Catalog als Datenquellen. Die AWS-Services , die Sie mit Amazon DataZone in Ihrer Data Mesh-Implementierung verwenden, kann je nach den Anforderungen Ihres Unternehmens unterschiedlich sein.

1. In den Erzeugerkonten sind die Rohdaten entweder in ihrer aktuellen Form verbrauchstauglich oder sie werden durch Nutzung für den Verbrauch transformiert AWS Glue. Die technischen Metadaten der Daten werden in Amazon S3 gespeichert und mithilfe eines AWS Glue Datencrawlers ausgewertet. Die Datenqualität wird mithilfe von AWS Glue Data Quality gemessen. Die Quelldatenbank im Datenkatalog ist als Asset im DataZone Amazon-Katalog registriert. Der DataZone Amazon-Katalog wird mithilfe von DataZone Amazon-Datenquellenjobs im zentralen Governance-Konto gehostet.
2. Das zentrale Governance-Konto hostet die DataZone Amazon-Domain und das DataZone Amazon-Datenportal. Die AWS-Konten Datenproduzenten und -verbraucher sind mit der DataZone Amazon-Domain verknüpft. Die DataZone Amazon-Projekte der Datenproduzenten und -verbraucher sind unter den entsprechenden DataZone Amazon-Domaineinheiten organisiert.
3. Endbenutzer der Datenbestände melden sich mit ihren AWS Identity and Access Management (IAM-) Anmeldeinformationen oder Single Sign-On (mit Integration über IAM Identity Center) beim DataZone Amazon-Datenportal an. Sie suchen, filtern und zeigen Asset-Informationen (z. B. Datenqualitätsinformationen oder geschäftliche und technische Metadaten) im DataZone Amazon-Datenkatalog an.
4. Nachdem ein Endbenutzer den gewünschten Datenbestand gefunden hat, verwendet er die DataZone Amazon-Abonnementfunktion, um Zugriff anzufordern. Der Dateneigentümer im Produzententeam erhält eine Benachrichtigung und bewertet die Abonnementanfrage im DataZone Amazon-Datenportal. Der Dateneigentümer genehmigt oder lehnt die Abonnementanfrage auf der Grundlage ihrer Gültigkeit ab.
5. Nachdem die Abonnementanfrage genehmigt und erfüllt wurde, wird im Kundenkonto für die folgenden Aktivitäten auf das Asset zugegriffen:
   - Entwicklung von KI/ML-Modellen mithilfe von Amazon AI SageMaker
   - Analytik und Berichterstattung mithilfe von Amazon Athena und Amazon QuickSight

Tools

AWS-Services

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon Simple Storage Service (Amazon S3) analysieren können.
- AWS Cloud Development Kit (AWS CDK)ist ein Softwareentwicklungs-Framework, das Ihnen hilft, AWS Cloud Infrastruktur im Code zu definieren und bereitzustellen.
- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und zu verwalten AWS-Regionen.
- Amazon DataZone ist ein Datenverwaltungsservice, der Sie dabei unterstützt, Daten zu katalogisieren, zu entdecken, gemeinsam zu nutzen und zu verwalten AWS, die vor Ort und in Quellen von Drittanbietern gespeichert sind.
- Amazon QuickSight ist ein Business Intelligence (BI) -Service auf Cloud-Ebene, mit dem Sie Ihre Daten in einem einzigen Dashboard visualisieren, analysieren und melden können.
- Amazon SageMaker AI ist ein verwalteter Service für maschinelles Lernen (ML), mit dem Sie ML-Modelle erstellen und trainieren und diese dann in einer produktionsbereiten, gehosteten Umgebung bereitstellen können.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code-Repository

Die Lösung ist im Repository GitHub data-mesh-datazone-cdk-cloudformation verfügbar.

Epen

Richte die Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Um das Repository zu klonen, führen Sie den folgenden Befehl in Ihrer lokalen	Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Entwicklungsumgebung (Linux oder macOS) aus: `git clone https://github.com/aws-samples/data-mesh-datazone-cdk-cloudformation`	

Erstellen Sie die Umgebung.	Führen Sie die folgenden Befehle aus, um die virtuelle Python-Umgebung zu erstellen:
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	`pip install -r requirements.txt`
		Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bootstrap für das Konto.	Führen Sie den folgenden Befehl aus AWS CDK, um das zentrale Governance-Konto mithilfe von zu booten: `cdk bootstrap aws://<GOVERNANCE_ACCOUNT_ID>/<AWS_REGION>` Melden Sie sich bei der an AWS Management Console, öffnen Sie die zentrale Governance-Kontokonsole und rufen Sie den Amazon-Ressourcennamen (ARN) der AWS CDK Ausführungsrolle ab.	Cloud-Architekt, DevOps Ingenieur
Konstruieren Sie die `DzDataMeshMemberStackSet.yaml` Datei.	Um die `DzDataMeshMemberStackSet.yaml` Datei aus dem Stammverzeichnis des Repositorys zu erstellen, starten Sie das folgende Bash-Skript: `./lib/scripts/create_dz_data_mesh_member_stack_set.sh`	Cloud-Architekt, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie die Erstellung der Vorlage.	Stellen Sie sicher, dass die AWS CloudFormation Vorlagendatei am `lib/cfn-templates/DzDataMeshMemberStackSet.yaml` Speicherort erstellt wurde.	Cloud-Architekt, DevOps Ingenieur

Stellen Sie Ressourcen im zentralen Governance-Konto bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Ändern Sie die Konfiguration.	Ändern Sie in der `config/Config.ts` Datei die folgenden Parameter:
	`DZ_APPLICATION_NAME - Name of the application.`
	`DZ_STAGE_NAME - Name of the stage.`
	`DZ_DOMAIN_NAME - Name of the Amazon DataZone domain`
	`DZ_DOMAIN_DESCRIPTION - Description of the Amazon DataZone domain`
	`DZ_DOMAIN_TAG - Tag of the Amazon DataZone domain`
	`DZ_ADMIN_PROJECT_NAME - Name of the Amazon DataZone project for administrators`
	`DZ_ADMIN_PROJECT_DESCRIPTION - Description of the Amazon DataZone project for administrators`
		Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`CDK_EXEC_ROLE_ARN - ARN of the cdk execution role`
	`DZ_ADMIN_ROLE_ARN - ARN of the administrator role`
	
	Lassen Sie die verbleibenden Parameter leer.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die DataZone Amazon-Glossarkonfiguration.	Verwenden Sie die folgende Beispielkonfiguration, um die DataZone Amazon-Glossarkonfiguration in der `lib/utils/glossary_config.json` Datei zu aktualisieren: `{ "GlossaryName": "PII Data", "GlossaryDescription": "If data source contains PII attributes", "GlossaryTerms": [{ "Name": "Yes", "ShortDescription": "Yes", "LongDescription": "Yes Glossary Term" }, { "Name": "No", "ShortDescription": "No", "LongDescription": "No Glossary Term" } ] }`	Cloud-Architekt, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Konfiguration des DataZone Amazon-Metadatenformulars.	Verwenden Sie die folgende Beispielkonfiguration`lib/utils/metadata_form_config.json file`, um die Konfiguration des DataZone Amazon-Metadatenformulars in zu aktualisieren: `{ "FormName": "ScheduleDataRefresh", "FormDescription": "Form for data refresh schedule", "FormSmithyModel": "@amazon.datazone#displayname(defaultName: \"Data Refresh Schedule\")\nstructure ScheduleDataRefresh {\n @documentation(\"Schedule of Data Refresh\")\n @required\n @amazon.datazone#searchable\n @amazon.datazone#displayname(defaultName: \"Data Refresh Schedule\")\n data_refresh_schedule: String\n}" }`	Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Exportieren Sie die AWS Anmeldeinformationen.	Verwenden Sie das folgende Format, um AWS Anmeldeinformationen für die IAM-Rolle mit Administratorrechten in Ihre Entwicklungsumgebung zu exportieren:
	`export AWS_ACCESS_KEY_ID=`
	`export AWS_SECRET_ACCESS_KEY=`
	`export AWS_SESSION_TOKEN=`
		Cloud-Architekt, Ingenieur DevOps

Synthetisieren Sie die Vorlage.	Führen Sie den folgenden Befehl aus, um die AWS CloudFormation Vorlage zu synthetisieren: `npx cdk synth`	Cloud-Architekt, Ingenieur DevOps
Stellen Sie die Lösung bereit.	Führen Sie den folgenden Befehl aus, um die Lösung bereitzustellen: `npx cdk deploy --all`	Cloud-Architekt, DevOps Ingenieur

Neue Mitgliedskonten konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Vorlage bereit.	Stellen Sie die AWS CloudFormation Vorlage, die sich `lib/cfn-templates/`	Cloud-Architekt, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`DzDataMeshCfnStackSetExecutionRole.yaml` im Mitgliedskonto befindet, mit den folgenden Eingabeparametern bereit: • `GovernanceAccountID` – Konto-ID des Governance-Kontos • `DataZoneKMSKeyID` – ID des AWS Key Management Service (AWS KMS) -Schlüssels, der die DataZone Amazon-Metadaten verschlüsselt • `NotificationQueueName` – Name der Amazon SQS SQS-Benachrichtigungswarteschlange im Governance-Konto	
Aktualisieren Sie die ARNs.	Verwenden Sie den folgenden Code, um die Liste der AWS CloudFormation StackSet Ausführungsrollen ARNs für die Mitgliedskonten zu aktualisieren: `DZ_MEMBER_STACK_SET_EXEC_ROLE_LIST - List of Stack set execution role arns for the member accounts.`	Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Synthetisieren und bereitstellen.	Führen Sie die folgenden Befehle aus, um die AWS CloudFormation Vorlage zu synthetisieren und die Lösung bereitzustellen:
	`npx cdk synth`
	`npx cdk deploy --all`
		Cloud-Architekt, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ordnen Sie das Mitgliedskonto zu.	Gehen Sie wie folgt vor, um das Mitgliedskonto mit dem zentralen Governance-Konto zu verknüpfen: 1. Melden Sie sich bei der Konsole des zentralen Governance-Kontos an und öffnen Sie die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone/. 2. Wählen Sie die Domain aus, die Sie erstellt haben. 3. Scrollen Sie zum Tab „Zugeordnete Konten“ und wählen Sie „Zuordnung beantragen“. 4. Geben Sie die AWS-Konto-ID an und wählen Sie AWSRAMPermissionDataZonePortalReadWrite als RAM-Richtlinie aus. 5. Wählen Sie „Zuordnung anfordern“. 6. Warten Sie, bis Sie eine E-Mail-Benachrichtigung erhalten, dass Ihr Konto erfolgreich gestartet wurde.	Cloud-Architekt, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Parameter.	Verwenden Sie das folgende Format, um die für das Mitgliedskonto spezifischen Parameter in der Konfigurationsdatei unter zu `config/Config.ts` aktualisieren: `export const DZ_MEMBER_ACCOUNT_CONFIG: memberAccountConfig = { '123456789012' : { PROJECT_NAME: 'TEST-PROJECT-123456789012', PROJECT_DESCRIPTION: 'TEST-PROJECT-123456789012', PROJECT_EMAIL: 'user@xyz.com' } }`	Cloud-Architekt, Ingenieur DevOps

Synthetisieren Sie die Vorlage und stellen Sie sie bereit.	Führen Sie die folgenden Befehle aus, um die AWS CloudFormation Vorlage zu synthetisieren und die Lösung bereitzustellen:
	`npx cdk synth`
	`npx cdk deploy --all`
		Cloud-Architekt, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Mitgliedskonten hinzufügen.	Um zusätzliche Mitglieds konten in der Datenlösung zu erstellen und zu konfigurieren, wiederholen Sie die vorherige n Schritte für jedes Mitglieds konto. Diese Lösung unterscheidet nicht zwischen Datenprod uzenten und Verbrauchern.	Cloud-Architekt, DevOps Ingenieur

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Trennen Sie die Zuordnung der Mitgliedskonten.	Gehen Sie wie folgt vor, um die Verknüpfung der Konten aufzuheben: 1. Melden Sie sich bei der Konsole an und öffnen Sie die DataZone Amazon-Ko nsole. 2. Wählen Sie „Domains anzeigen“. 3. Wählen Sie die Domain aus, die Sie erstellt haben. 4. Wählen Sie den Tab Kontozuordnungen aus. 5. Wählen Sie das Mitglieds konto aus, dessen Verknüpfung Sie aufheben möchten.	Cloud-Architekt, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Wählen Sie „Verbindung trennen“ und geben Sie `disassociate` zur Bestätigung die Eingabetaste ein. 7. Wiederholen Sie die Schritte 3-6 für alle Mitgliedskonten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die Stack-Instanzen.	Gehen Sie wie folgt vor, um die AWS CloudFormation Stack-Instances zu löschen: 1. Öffnen Sie die AWS CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation/. 2. Wählen Sie im Navigationsbereich StackSets aus. 3. Wählen Sie das Stack-Set mit dem Namen StackSetDataZone- - DataMesh - Member und dann den Tab Stack-Instances aus. 4. Kopieren Sie die AWS-Konto ID des Mitgliedskontos, das Sie aus der Mitgliedschaft entfernen möchten. 5. Wählen Sie „Aktionen“, wählen Sie „Stapel löschen aus StackSet“ und behalten Sie die Standardoptionen bei. 6. Geben Sie im Feld Kontonummern die Konto-ID ein. 7. Wählen Sie in der Dropdownliste Regionen angeben die AWS-Region Option.	Cloud-Architekt, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Wählen Sie Weiter und anschließend Absenden aus. 9. Vergewissern Sie sich auf der Registerkarte Vorgänge, dass der Vorgang erfolgreich war. Das Löschen des Stacks kann einige Zeit dauern. 10. Wiederholen Sie die Schritte 2-9 für alle Mitgliedskonten.	
Zerstöre alle Ressourcen.	Um Ressourcen zu vernichten, implementieren Sie die folgenden Schritte in Ihrer lokalen Entwicklungsumgebung (Linux oder macOS): 1. Navigieren Sie zum Stammverzeichnis Ihres Repositorys. 2. Exportieren Sie die AWS Anmeldeinformationen für die IAM-Rolle, mit der Sie den AWS CDK Stack erstellt haben. 3. Führen Sie den folgenden Befehl aus, um die Cloud-Ressourcen zu löschen: `npx cdk destroy --all`	Cloud-Architekt, DevOps Ingenieur

Zugehörige Ressourcen

- DataZone Amazon-Schnellstart mit Daten AWS Glue
- Tutorial: Erstelle deine erste App AWS CDK
- Erste Schritte mit AWS CloudFormation
- Strategien für den Aufbau einer auf Datennetzen basierenden Unternehmenslösung auf AWS

Zusätzliche Informationen

Ziele

Durch die Implementierung dieses Musters wird Folgendes erreicht:

- Dezentrales Eigentum an Daten – Verlagern Sie die Datenverantwortung von einem zentralen Team auf Teams, die die Quellsysteme, Geschäftsbereiche oder Anwendungsfälle Ihres Unternehmens repräsentieren.
- Produktdenken – Führen Sie bei der Betrachtung der Datenbestände in Ihrem Unternehmen eine produktorientierte Denkweise ein, die Kunden, den Markt und andere Faktoren einbezieht.
- Föderierte Verwaltung – Verbessern Sie die Sicherheitsvorkehrungen, Kontrollen und die Einhaltung von Vorschriften für alle Datenprodukte Ihres Unternehmens.
- Support für mehrere Konten und Projekte – Unterstützen Sie den effizienten und sicheren Datenaustausch und die Zusammenarbeit zwischen den Geschäftsbereichen oder Projekten Ihres Unternehmens.
- Zentralisierte Überwachung und Benachrichtigungen – Überwachen Sie die Cloud-Ressourcen Ihres Datennetzes mithilfe von Amazon und benachrichtigen Sie Benutzer CloudWatch, wenn ein neues Mitgliedskonto verknüpft wird.
- Skalierbarkeit und Erweiterbarkeit – Fügen Sie dem Data Mesh neue Anwendungsfälle hinzu, während sich Ihr Unternehmen weiterentwickelt.

Umfang der Lösung

Wenn Sie diese Lösung verwenden, können Sie klein anfangen und sie dann skalieren, wenn Sie auf Ihrem Weg zum Data Mesh vorankommen. Wenn ein Mitgliedskonto die Datenlösung verwendet, enthält sie häufig Kontokonfigurationen, die für die Organisation, das Projekt oder die Geschäftseinheit spezifisch sind. Diese Lösung berücksichtigt diese unterschiedlichen AWS-Konto Konfigurationen, indem sie die folgenden Funktionen unterstützt:

- AWS Glue Data Catalog als Datenquelle für Amazon DataZone
- Verwaltung der DataZone Amazon-Datendomäne und des zugehörigen Datenportals
- Verwaltung des Hinzufügens von Mitgliedskonten zur auf Datennetzen basierenden Datenlösung
- Verwaltung von DataZone Amazon-Projekten und -Umgebungen
- Verwaltung von DataZone Amazon-Glossaren und Metadatenformularen
- Verwaltung von IAM-Rollen, die den Benutzern der Data Mesh-basierten Datenlösung entsprechen
- Benachrichtigung der Benutzer einer auf Datennetzen basierenden Datenlösung
- Überwachung der bereitgestellten Cloud-Infrastruktur

  Diese Lösung verwendet AWS CDK und implementiert AWS CloudFormation die Cloud-Infrastruktur. Sie macht AWS CloudFormation früher Folgendes:

  - Definieren und implementieren Sie Cloud-Ressourcen auf einer niedrigeren Abstraktionsebene.
  - Stellen Sie Cloud-Ressourcen aus dem AWS Management Console bereit. Mit diesem Ansatz können Sie eine Infrastruktur ohne Entwicklungsumgebung bereitstellen.

  Die Data-Mesh-Lösung verwendet AWS CDK , um Ressourcen auf einer höheren Abstraktionsebene zu definieren. Dadurch bietet die Lösung einen entkoppelten, modularen und skalierbaren Ansatz, bei dem das entsprechende Tool für die Bereitstellung der Cloud-Ressourcen ausgewählt wird.

Nächste Schritte

Sie können sich an AWSExperten wenden, um Unterstützung beim Aufbau eines Datennetzes mit Amazon zu erhalten DataZone.

Der modulare Charakter dieser Lösung unterstützt den Aufbau von Datenmanagementlösungen mit unterschiedlichen Architekturen, wie Data Fabric und Data Lakes. Darüber hinaus können Sie die Lösung je nach den Anforderungen Ihres Unternehmens auf andere DataZone Amazon-Datenquellen ausdehnen.

Value at Risk (VaR) mithilfe von AWS-Services berechnen

Erstellt von Sumon Samanta (AWS)

Übersicht

Dieses Muster beschreibt, wie ein Value-at-Risk-Berechnungssystem (VaR) mithilfe von AWS-Services implementiert wird. In einer lokalen Umgebung verwenden die meisten VaR-Systeme eine große, dedizierte Infrastruktur und eine interne oder kommerzielle Netzplanungssoftware, um Batch-Prozesse auszuführen. Dieses Muster stellt eine einfache, zuverlässige und skalierbare Architektur für die VaR-Verarbeitung in der AWS-Cloud dar. Es baut eine serverlose Architektur auf, die Amazon Kinesis Data Streams als Streaming-Service, Amazon Simple Queue Service (Amazon SQS) als verwalteten Warteschlangenservice, Amazon ElastiCache als Caching-Service und AWS Lambda zur Bearbeitung von Bestellungen und zur Risikoberechnung verwendet.

VaR ist ein statistisches Maß, das Händler und Risikomanager verwenden, um potenzielle Verluste in ihrem Portfolio ab einem bestimmten Konfidenzniveau abzuschätzen. Die meisten VaR-Systeme beinhalten die Durchführung einer großen Anzahl mathematischer und statistischer Berechnungen und die Speicherung der Ergebnisse. Diese Berechnungen erfordern erhebliche Rechenressourcen, sodass VaR-Batchprozesse in kleinere Gruppen von Rechenaufgaben aufgeteilt werden müssen. Das Aufteilen eines großen Batches in kleinere Aufgaben ist möglich, da diese Aufgaben größtenteils unabhängig voneinander sind (d. h. Berechnungen für eine Aufgabe hängen nicht von anderen Aufgaben ab).

Eine weitere wichtige Anforderung an eine VaR-Architektur ist die Skalierbarkeit der Rechenleistung. Dieses Muster verwendet eine serverlose Architektur, die je nach Rechenlast automatisch ein- oder ausskaliert wird. Da der Bedarf an Batch- oder Online-Rechenleistung schwer vorherzusagen ist, ist eine dynamische Skalierung erforderlich, um den Prozess innerhalb des in einem Service Level Agreement (SLA) festgelegten Zeitrahmens abzuschließen. Außerdem sollte eine kostenoptimierte Architektur in der Lage sein, jede Rechenressource herunterzuskalieren, sobald die Aufgaben auf dieser Ressource abgeschlossen sind.

AWS-Services eignen sich hervorragend für VaR-Berechnungen, da sie skalierbare Rechen- und Speicherkapazität, Analyseservices für eine kostenoptimierte Verarbeitung und verschiedene Arten von Schedulern für die Ausführung Ihrer Risikomanagement-Workflows bieten. Außerdem zahlen Sie nur für die Rechen- und Speicherressourcen, die Sie auf AWS nutzen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eingabedateien, die von Ihren Geschäftsanforderungen abhängen. Ein typischer Anwendungsfall umfasst die folgenden Eingabedateien:
  - Marktdatendatei (Eingabe in die VaR-Berechnungsmaschine)
  - Handelsdatendatei (es sei denn, Handelsdaten werden über einen Stream übertragen).
  - Konfigurationsdatendatei (Modell und andere statische Konfigurationsdaten)
  - Modelldateien für die Berechnungsengine (quantitative Bibliotheken)
  - Zeitreihendatendatei (für historische Daten wie den Aktienkurs der letzten fünf Jahre)
- Wenn die Marktdaten oder andere Eingaben über einen Stream eingehen, werden Amazon Kinesis Data Streams eingerichtet und Amazon Identity and Access Management (IAM) -Berechtigungen konfiguriert, um in den Stream zu schreiben.

Dieses Muster bildet eine Architektur, in der Handelsdaten von einem Handelssystem in einen Kinesis-Datenstrom geschrieben werden. Anstatt einen Streaming-Dienst zu verwenden, können Sie Ihre Handelsdaten in kleinen Batch-Dateien speichern, sie in einem Amazon Simple Storage Service (Amazon S3) -Bucket speichern und ein Ereignis aufrufen, um die Verarbeitung der Daten zu starten.

Einschränkungen

- Die Kinesis-Datenstream-Sequenzierung ist für jeden Shard garantiert, sodass Handelsaufträge, die auf mehrere Shards geschrieben werden, nicht garantiert in derselben Reihenfolge wie Schreibvorgänge geliefert werden.
- Das AWS Lambda Lambda-Laufzeitlimit beträgt derzeit 15 Minuten. (Weitere Informationen finden Sie in den häufig gestellten Fragen zu Lambda.)

Architektur

Zielarchitektur

Das folgende Architekturdiagramm zeigt die AWS-Services und -Workflows für das Risikobewertungssystem.

Das Diagramm veranschaulicht folgende Vorgänge:

1. Geschäfte werden aus dem Auftragsverwaltungssystem eingelesen.
2. Die Lambda-Funktion „Ticket Position Netting“ verarbeitet die Bestellungen und schreibt konsolidierte Nachrichten für jeden Ticker in eine Risikowarteschlange in Amazon SQS.
3. Die Lambda-Funktion der Risikoberechnungs-Engine verarbeitet die Nachrichten von Amazon SQS, führt Risikoberechnungen durch und aktualisiert die VaR-Gewinn- und Verlustinformationen (PnL) im Risiko-Cache in Amazon. ElastiCache
4. Die Lambda-Funktion zum Lesen von ElastiCache Daten ruft die Risikoergebnisse ab ElastiCache und speichert sie in einer Datenbank und einem S3-Bucket.

Weitere Informationen zu diesen Diensten und Schritten finden Sie im Abschnitt Epics.

Automatisierung und Skalierung

Sie können die gesamte Architektur mithilfe des AWS Cloud Development Kit (AWS CDK) oder CloudFormation AWS-Vorlagen bereitstellen. Die Architektur kann sowohl die Batch-Verarbeitung als auch die Intraday-Verarbeitung (Echtzeit) unterstützen.

Die Skalierung ist in die Architektur integriert. Da immer mehr Trades in den Kinesis-Datenstrom geschrieben werden und auf ihre Verarbeitung warten, können zusätzliche Lambda-Funktionen aufgerufen werden, um diese Trades zu verarbeiten, und nach Abschluss der Verarbeitung nach unten skaliert werden. Die Verarbeitung mehrerer Amazon SQS SQS-Warteschlangen zur Risikoberechnung ist ebenfalls eine Option. Wenn eine strikte Reihenfolge oder Konsolidierung in allen Warteschlangen erforderlich ist, kann die Verarbeitung nicht parallelisiert werden. Bei einem end-of-the-day Batch oder einem Mini-Intraday-Batch können die Lambda-Funktionen jedoch parallel verarbeiten und die Endergebnisse in speichern. ElastiCache

Tools

AWS-Dienste

- Amazon Aurora MySQL-Compatible Edition ist eine vollständig verwaltete, MySQL-kompatible relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von MySQL-Bereitstellungen unterstützt. Dieses Muster verwendet MySQL als Beispiel, aber Sie können jedes RDBMS-System zum Speichern von Daten verwenden.
- Amazon ElastiCache unterstützt Sie bei der Einrichtung, Verwaltung und Skalierung verteilter In-Memory-Cache-Umgebungen in der AWS-Cloud.

- Amazon Kinesis Data Streams hilft Ihnen dabei, große Datenströme in Echtzeit zu sammeln und zu verarbeiten.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code

Dieses Muster bietet eine Beispielarchitektur für ein VaR-System in der AWS-Cloud und beschreibt, wie Sie Lambda-Funktionen für VaR-Berechnungen verwenden können. Informationen zum Erstellen Ihrer Lambda-Funktionen finden Sie in den Codebeispielen in der Lambda-Dokumentation. Wenn Sie Hilfe benötigen, wenden Sie sich an AWS Professional Services.

Bewährte Methoden

- Halten Sie jede VaR-Rechenaufgabe so klein und leicht wie möglich. Experimentieren Sie mit einer unterschiedlichen Anzahl von Trades in jeder Rechenaufgabe, um herauszufinden, welcher am besten in Bezug auf Rechenzeit und Kosten optimiert ist.
- Bewahren Sie wiederverwendbare Objekte bei Amazon auf ElastiCache. Verwenden Sie ein Framework wie Apache Arrow, um die Serialisierung und Deserialisierung zu reduzieren.
- Beachten Sie die Zeitbegrenzung von Lambda. Wenn Sie glauben, dass Ihre Rechenaufgaben mehr als 15 Minuten dauern könnten, versuchen Sie, sie in kleinere Aufgaben aufzuteilen, um das Lambda-Timeout zu vermeiden. Wenn dies nicht möglich ist, könnten Sie eine Container-Orchestrierungslösung mit AWS Fargate, Amazon Elastic Container Service (Amazon ECS) und Amazon Elastic Kubernetes Service (Amazon EKS) in Betracht ziehen.

Epen

Handelsfluss zum Risikosystem

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fange an, Trades zu schreiben.	Neue, abgewickelte oder teilweise abgewickelte Geschäfte werden aus dem Auftragsverwaltungssystem in einen Risikostream geschrieb en. Dieses Muster verwendet Amazon Kinesis als verwaltet en Streaming-Service. Der Hash des Handelsorder-Tickers wird verwendet, um Handelsaufträge auf mehrere Shards zu verteilen.	Amazon Kinesis

Führen Sie Lambda-Funktionen für die Auftragsabwicklung aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Risikover arbeitung mit Lambda.	Führen Sie eine AWS Lambda Lambda-Funktion für die neuen Bestellungen aus. Basierend auf der Anzahl der ausstehenden Handelsau fträge skaliert Lambda automatisch. Jede Lambda-In stance hat eine oder mehrere Bestellungen und ruft die aktuelle Position für jeden Ticker von Amazon ab. ElastiCache (Sie können eine CUSIP-ID, einen Kurvennam	Amazon Kinesis, AWS Lambda, Amazon ElastiCache

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en oder einen Indexnamen für andere Finanzderivate als Schlüssel zum Speichern und Abrufen von Daten verwenden .) ElasticCache In ElastiCac he werden die Gesamtposition (Menge) und das Schlüssel-Wert-Paar < Ticker, Nettoposi tion >, wobei die Nettoposition der Skalierungsfaktor ist, für jeden Ticker einmal aktualisi ert.	

Schreiben Sie Nachrichten für jeden Ticker in die Warteschlange

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schreiben Sie konsolidierte Nachrichten in die Risikowar teschlange.	Schreiben Sie die Nachricht in eine Warteschlange. Dieses Muster verwendet Amazon SQS als verwalteten Warteschlangenservice. Eine einzelne Lambda-Instance kann zu einem bestimmte n Zeitpunkt einen kleinen Stapel von Handelsaufträgen erhalten, schreibt jedoch nur eine einzige Nachricht für jeden Ticker an Amazon SQS. Es wird ein Skalierungsfaktor berechnet: (alte Nettoposi tion + aktuelle Position) /alte Nettoposition.	Amazon SQS, AWS Lambda

Rufen Sie die Risk Engine auf

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie Risikober echnungen.	Die Lambda-Funktion für das Risk-Engine-Lambda wird aufgerufen. Jede Position wird von einer einzigen Lambda-Funktion verarbeitet. Zu Optimierungszwecken kann jede Lambda-Funktion jedoch mehrere Nachrichten von Amazon SQS verarbeiten.	Amazon SQS, AWS Lambda

Rufen Sie Risikoergebnisse aus dem Cache ab

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie den Risiko-Cache ab und aktualisieren Sie ihn.	Lambda ruft die aktuelle Nettoposition für jeden Ticker von ab. ElastiCache Es ruft auch ein VaR-Array für Gewinn und Verlust (PnL) für jeden Ticker von ab. ElastiCac he Wenn das PnL-Array bereits existiert, aktualisiert die Lambda-Funktion das Array und den VaR mit einer Skala, die aus der Amazon SQS SQS-Nachricht stammt, die von der Netting Lambda-Fu nktion geschrieben wurde. Wenn das PnL-Array nicht vorhanden ist ElasticCache,	Amazon SQS, AWS Lambda, Amazon ElastiCache

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	werden ein neuer PnL und ein neuer VaR anhand simuliert er Tickerpreisreihendaten berechnet.	

Daten im Elastic Cache aktualisieren und in der Datenbank speichern

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Speichern Sie Risikoerg ebnisse.	Nachdem die VaR- und PnL-Nummern aktualisiert wurden ElastiCache, wird alle fünf Minuten eine neue Lambda-Funktion aufgerufe n. Diese Funktion liest alle gespeicherten Daten aus einer Aurora MySQL-kom patiblen Datenbank ElastiCac he und in einem S3-Bucket und speichert sie dort.	AWS Lambda, Amazon ElastiCache

Zugehörige Ressourcen

- Basler VaR-Framework

Konfigurieren Sie den kontoübergreifenden Zugriff auf einen gemeinsamen AWS Glue Glue-Datenkatalog mit Amazon Athena

Erstellt von Denis Avdonin (AWS)

Übersicht

Dieses Muster enthält step-by-step Anweisungen, einschließlich Richtlinienbeispielen für AWS Identity and Access Management (IAM), um die kontoübergreifende gemeinsame Nutzung eines in einem Amazon Simple Storage Service (Amazon S3) -Bucket gespeicherten Datensatzes mithilfe des AWS Glue Glue-Datenkatalogs zu konfigurieren. Sie können den Datensatz in einem S3-Bucket speichern. Die Metadaten werden von einem AWS Glue Glue-Crawler gesammelt und in den AWS Glue Glue-Datenkatalog aufgenommen. Der S3-Bucket und der AWS Glue Glue-Datenkatalog befinden sich in einem AWS-Konto, das als Datenkonto bezeichnet wird. Sie können den Zugriff auf IAM-Prinzipale in einem anderen AWS-Konto gewähren, das als Verbraucherkonto bezeichnet wird. Benutzer können die Daten im Verbraucherkonto mithilfe der serverlosen Amazon Athena Athena-Abfrage-Engine abfragen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zwei aktive AWS-Konten
- Ein S3-Bucket in einem der AWS-Konten
- Athena-Engine-Version 2
- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert (oder AWS CloudShell für die Ausführung von AWS-CLI-Befehlen)

Produktversionen

Dieses Muster funktioniert nur mit Athena-Engine-Version 2 und Athena-Engine-Version 3. Wir empfehlen Ihnen, auf Athena-Engine-Version 3 zu aktualisieren. Wenn Sie kein Upgrade von Athena-Engine-Version 1 auf Athena-Engine-Version 3 durchführen können, folgen Sie dem unter Kontoübergreifender Zugriff auf den AWS Glue-Datenkatalog mit Amazon Athena im AWS Big Data-Blog beschriebenen Ansatz.

Architektur

Zieltechnologie-Stack

- Amazon Athena
- Amazon Simple Storage Service (Amazon-S3)
- AWS Glue
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (AWS KMS)

Das folgende Diagramm zeigt eine Architektur, die IAM-Berechtigungen verwendet, um Daten in einem S3-Bucket in einem AWS-Konto (Datenkonto) mit einem anderen AWS-Konto (Verbraucherkonto) über den AWS Glue-Datenkatalog zu teilen.

Das Diagramm zeigt den folgenden Workflow:

1. Die S3-Bucket-Richtlinie im Datenkonto gewährt Berechtigungen für eine IAM-Rolle im Verbraucherkonto und für die AWS Glue Glue-Crawler-Servicerolle im Datenkonto.
2. Die AWS KMS KMS-Schlüsselrichtlinie im Datenkonto gewährt Berechtigungen für die IAM-Rolle im Verbraucherkonto und für die AWS Glue Glue-Crawler-Servicerolle im Datenkonto.
3. Der AWS Glue Glue-Crawler im Datenkonto erkennt das Schema der Daten, die im S3-Bucket gespeichert sind.
4. Die Ressourcenrichtlinie des AWS Glue Glue-Datenkatalogs im Datenkonto gewährt Zugriff auf die IAM-Rolle im Verbraucherkonto.
5. Ein Benutzer erstellt mithilfe eines AWS-CLI-Befehls eine benannte Katalogreferenz im Verbraucherkonto.
6. Eine IAM-Richtlinie gewährt einer IAM-Rolle im Verbraucherkonto Zugriff auf Ressourcen im Datenkonto. Die Vertrauensrichtlinie der IAM-Rolle ermöglicht es Benutzern im Verbraucherkonto, die IAM-Rolle zu übernehmen.
7. Ein Benutzer im Verbraucherkonto übernimmt die IAM-Rolle und greift mithilfe von SQL-Abfragen auf Objekte im Datenkatalog zu.
8. Die serverlose Athena Engine führt die SQL-Abfragen aus.

> **Note**
>
> Bewährte Methoden für IAM empfehlen, einer IAM-Rolle Berechtigungen zu erteilen und einen Identitätsverbund zu verwenden.

Tools

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon S3 analysieren können.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Glue ist ein vollständig verwalteter Service zum Extrahieren, Transformieren und Laden (ETL). Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Key Management Service (AWS KMS) unterstützt Sie bei der Erstellung und Kontrolle kryptografischer Schlüssel zum Schutz Ihrer Daten.

Epen

Richten Sie Berechtigungen im Datenkonto ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gewähren Sie Zugriff auf Daten im S3-Bucket.	Erstellen Sie eine S3-Bucket-Richtlinie auf der Grundlage der folgenden Vorlage und weisen Sie die Richtlinie dem Bucket zu, in dem die Daten gespeichert sind. `{`	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Principal": { "AWS": ["arn:aws:iam::<consumer account id>:role/<role name>", "arn:aws:iam::<data account id>:role/service-role/AWSGlueServiceRole-data-bucket-crawler"] }, "Action": "s3:GetObject", "Resource": "arn:aws:s3:::data-bucket/*" }, { "Effect": "Allow", "Principal": { "AWS": ["arn:aws:iam::<consumer account id>:role/<role name>", "arn:aws:iam::<data account id>:role/service-role/AWSGl	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ueServiceRole-data-bucket-crawler"] }, "Action": "s3:ListBucket", "Resource": "arn:aws:s3:::data-bucket" }] } Die Bucket-Richtlinie gewährt Berechtigungen für die IAM-Rolle im Verbraucherkonto und für die AWS Glue Glue-Crawler-Servicerolle im Datenkonto.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Falls erforderlich) Gewähren Sie Zugriff auf den Datenverschlüsselungsschlüssel.	Wenn der S3-Bucket mit einem AWS-KMS-Schlüssel verschlüsselt ist, `kms:Decrypt` erteilen Sie der IAM-Rolle im Verbraucherkonto und der AWS Glue Glue-Crawler-Servicerolle im Datenkonto die Erlaubnis für den Schlüssel. Aktualisieren Sie die Schlüsselrichtlinie mit der folgenden Aussage: `{ "Effect": "Allow", "Principal": { "AWS": [ "arn:aws:iam::<consumer account id>:role/<role name>", "arn:aws:iam::<data account id>:role/service-role/AWSGlueServiceRole-data-bucket-crawler" ] }, "Action": "kms:Decrypt", "Resource": "arn:aws:kms:<region>:<data account id>:key/<key id>" }`	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gewähren Sie dem Crawler Zugriff auf die Daten.	Fügen Sie der Servicerolle des Crawlers die folgende IAM-Richtlinie hinzu: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::data-bucket/*" }, { "Effect": "Allow", "Action": "s3:ListBucket", "Resource": "arn:aws:s3:::data-bucket" } ] }`	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Falls erforderlich) Gewähren Sie dem Crawler Zugriff auf den Datenverschlüsselungsschlüssel.	Wenn der S3-Bucket mit einem AWS-KMS-Schlüssel verschlüsselt ist, erteilen Sie der Service-Rolle des Crawlers die `kms:Decrypt` Erlaubnis für den Schlüssel, indem Sie ihm die folgende Richtlinie anhängen: `{ "Effect": "Allow", "Action": "kms:Decrypt", "Resource": "arn:aws:kms:<region>:<data account id>:key/<key id>" }`	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gewähren Sie der IAM-Rolle im Verbraucherkonto und dem Crawler Zugriff auf den Datenkatalog.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS Glue-Konsole. 2. Wählen Sie im Navigationsbereich unter Datenkatalog die Option Einstellungen aus. 3. Fügen Sie im Abschnitt Berechtigungen die folgende Anweisung hinzu, und wählen Sie dann Speichern aus. `{ "Version" : "2012-10-17", "Statement" : [ { "Effect" : "Allow", "Principal" : { "AWS" : [ "arn:aws:iam::<consumer account id>:role/<role name>", "arn:aws:iam::<data account id>:role/service-role/AWSGlueServiceRole-data-bucket-crawler" ] }, ...`	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"Action" : "glue:*", "Resource" : ["arn:aws:glue:<region>:<data account id>:catalog", "arn:aws:glue:<region>:<data account id>:database/*", "arn:aws:glue:<region>:<data account id>:table/*"] }] }</pre> Diese Richtlinie erlaubt alle AWS Glue Glue-Aktionen für alle Datenbanken und Tabellen im Datenkonto. Sie können die Richtlinie so anpassen, dass den Benutzerprinzipalen nur die erforderlichen Berechtigungen gewährt werden. Sie können beispielsweise schreibgeschützten Zugriff auf bestimmte Tabellen oder Ansichten in einer Datenbank gewähren.	

Greifen Sie über das Verbraucherkonto auf Daten zu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine benannte Referenz für den Datenkata log.	Um eine benannte Datenkata logreferenz zu erstellen, verwenden Sie CloudShel loder eine lokal installierte AWS-CLI, um den folgenden Befehl auszuführen: `aws athena create-da ta-catalog --name <shared catalog name> --type GLUE --paramet ers catalog-id=<data account id>`	Cloud-Administrator
Gewähren Sie der IAM-Rolle im Verbraucherkonto Zugriff auf die Daten.	Fügen Sie der IAM-Rolle im Verbraucherkonto die folgende Richtlinie hinzu, um der Rolle kontoübergreifenden Zugriff auf die Daten zu gewähren: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::data-bucket/*" }, { "Effect": "Allow",`	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"Action": "s3:ListBucket", "Resource": "arn:aws:s3:::data-bucket" }, { "Effect": "Allow", "Action": "glue:*", "Resource": ["arn:aws:glue:<region>:<data account id>:catalog", "arn:aws:glue:<region>:<data account id>:database/*", "arn:aws:glue:<region>:<data account id>:table/*"] }] }</pre> Verwenden Sie als Nächstes die folgende Vorlage, um anzugeben, welche Benutzer die IAM-Rolle in ihrer Vertrauensrichtlinie akzeptieren können: <pre>{ "Version": "2012-10-17",</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>{
	    "Statement": [
	       {
	            "Effect":
	 "Allow",
	            "Principa
	l": {
	                "AWS":
	 "arn:aws:iam::<con
	sumer account id>:user/
	<IAM user>"
	            },
	            "Action":
	 "sts:AssumeRole"
	        }
	    ]
	}</pre>
	Erteilen Sie den Benutzern abschließend Berechtigungen zur Übernahme der IAM-Rolle, indem Sie dieselbe Richtlinie an die Benutzergruppe anhängen, zu der sie gehören.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Falls erforderlich) Gewähren Sie der IAM-Rolle im Verbraucherkonto Zugriff auf den Datenverschlüsselungsschlüssel.	Wenn der S3-Bucket mit einem AWS-KMS-Schlüssel verschlüsselt ist, erteilen Sie der IAM-Rolle im Verbrauch erkonto die `kms:Decrypt` Erlaubnis für den Schlüssel, indem Sie ihm die folgende Richtlinie anhängen: `{ "Effect": "Allow", "Action": "kms:Decrypt", "Resource": "arn:aws:kms:<region>:<data account id>:key/<key id>" }`	Cloud-Administrator
Wechseln Sie im Verbrauch erkonto zur IAM-Rolle, um auf Daten zuzugreifen.	Wechseln Sie als Datenverbraucher zur IAM-Rolle, um auf Daten im Datenkonto zuzugreifen.	Datenkonsument

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Greifen Sie auf die Daten zu.	Fragen Sie Daten mit Athena ab. Öffnen Sie beispielsweise den Athena-Abfrage-Editor und führen Sie die folgende Abfrage aus:
	`SELECT * FROM <shared catalog name>.<database name>.<table name>`
	Anstatt eine benannte Katalogreferenz zu verwenden, können Sie auch anhand seines Amazon-Ressourcennamens (ARN) auf den Katalog verweisen.
	Note
	Wenn Sie in einer Abfrage oder Ansicht eine dynamische Katalogreferenz verwenden, setzen Sie den Verweis in doppelte Anführungszeichen (\“). Zum Beispiel:
	`SELECT * FROM \"glue:arn:aws:glue:<region>:<data account id>:catalog\".<dat`
		Datenverbraucher

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`abase name>.<table name>` Weitere Informationen finden Sie unter Kontoübergreifender Zugriff auf AWS Glue Glue-Datenkataloge im Amazon Athena Athena-Benutzerhandbuch.	

Zugehörige Ressourcen

- Kontoübergreifender Zugriff auf AWS Glue Glue-Datenkataloge (Athena-Dokumentation)
- (AWS CLI) create-data-catalog (AWS CLI-Befehlsreferenz)
- Kontoübergreifender Zugriff auf den AWS Glue-Datenkatalog mit Amazon Athena (AWS Big Data Blog)
- Bewährte Sicherheitsmethoden in IAM (IAM-Dokumentation)

Zusätzliche Informationen

Verwendung von Lake Formation als Alternative für kontenübergreifendes Teilen

Sie können AWS Lake Formation auch verwenden, um den Zugriff auf AWS Glue Glue-Katalogobjekte für mehrere Konten gemeinsam zu nutzen. Lake Formation bietet eine detaillierte Zugriffskontrolle auf Spalten- und Zeilenebene, Tag-basierte Zugriffskontrolle, gesteuerte Tabellen für ACID-Transaktionen und andere Funktionen. Lake Formation ist zwar gut in Athena integriert, erfordert jedoch eine zusätzliche Konfiguration im Vergleich zum reinen IAM-Ansatz dieses Musters. Wir empfehlen Ihnen, die Entscheidung, Lake Formation oder reine IAM-Zugriffskontrollen zu verwenden, im breiteren Kontext Ihrer gesamten Lösungsarchitektur zu berücksichtigen. Zu den Überlegungen gehören auch, um welche anderen Dienste es sich handelt und wie sie sich in beide Ansätze integrieren lassen.

Konvertieren Sie die temporale Funktion Teradata NORMALIZE in Amazon Redshift SQL

Erstellt von Po Hong (AWS)

Übersicht

NORMALIZE ist eine Teradata-Erweiterung des ANSI SQL-Standards. Wenn eine SQL-Tabelle eine Spalte mit dem Datentyp PERIOD enthält, kombiniert NORMALIZE Werte, die sich in dieser Spalte treffen oder sich überschneiden, zu einer einzigen Periode, die mehrere einzelne Periodenwerte konsolidiert. Um NORMALIZE verwenden zu können, muss mindestens eine Spalte in der SQL SELECT-Liste den temporalen PERID-Datentyp von Teradata haben. Weitere Informationen zu NORMALIZE finden Sie in der Teradata-Dokumentation.

Amazon Redshift unterstützt NORMALIZE nicht, aber Sie können diese Funktionalität mithilfe der systemeigenen SQL-Syntax und der LAG-Fensterfunktion in Amazon Redshift implementieren. Dieses Muster konzentriert sich auf die Verwendung der Teradata NORMALIZE-Erweiterung mit der Bedingung ON MEETS OR OVERLAPS, dem beliebtesten Format. Es erklärt, wie diese Funktion in Teradata funktioniert und wie sie in die native SQL-Syntax von Amazon Redshift konvertiert werden kann.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Grundkenntnisse und Erfahrung mit Teradata SQL
- Wissen und Erfahrung mit Amazon Redshift

Architektur

Quelltechnologie-Stack

- Teradata-Datawarehouse

Zieltechnologie-Stack

- Amazon Redshift

Zielarchitektur

Eine übergeordnete Architektur für die Migration einer Teradata-Datenbank zu Amazon Redshift finden Sie im Muster Migrieren einer Teradata-Datenbank zu Amazon Redshift mithilfe von AWS SCT-Datenextraktionsagenten. Bei der Migration wird die Teradata NORMALIZE-Phrase nicht automatisch in Amazon Redshift SQL konvertiert. Sie können diese Teradata-Erweiterung konvertieren, indem Sie die Richtlinien in diesem Muster befolgen.

Tools

Code

Sehen Sie sich die folgende Tabellendefinition in Teradata an, um das Konzept und die Funktionalität von NORMALIZE zu veranschaulichen:

```
CREATE TABLE systest.project
     (    emp_id        INTEGER,
          project_name  VARCHAR(20),
          dept_id       INTEGER,
          duration      PERIOD(DATE)
     );
```

Führen Sie den folgenden SQL-Code aus, um Beispieldaten in die Tabelle einzufügen:

```
BEGIN TRANSACTION;

INSERT INTO systest.project VALUES (10, 'First Phase', 1000,  PERIOD(DATE '2010-01-10',
 DATE '2010-03-20') );
INSERT INTO systest.project VALUES (10, 'First Phase', 2000,  PERIOD(DATE '2010-03-20',
 DATE '2010-07-15') );

INSERT INTO systest.project VALUES (10, 'Second Phase', 2000,  PERIOD(DATE
 '2010-06-15', DATE '2010-08-18') );
INSERT INTO systest.project VALUES (20, 'First Phase', 2000,  PERIOD(DATE '2010-03-10',
 DATE '2010-07-20') );

INSERT INTO systest.project VALUES (20, 'Second Phase', 1000,  PERIOD(DATE
 '2020-05-10', DATE '2020-09-20') );

END TRANSACTION;
```

Ergebnisse:

```
select * from systest.project order by 1,2,3;

 *** Query completed. 4 rows found. 4 columns returned.
 *** Total elapsed time was 1 second.

     emp_id  project_name              dept_id  duration
-----------  --------------------  -----------  ------------------------
         10  First Phase                  1000  ('10/01/10', '10/03/20')
         10  First Phase                  2000  ('10/03/20', '10/07/15')
         10  Second Phase                 2000  ('10/06/15', '10/08/18')
         20  First Phase                  2000  ('10/03/10', '10/07/20')
         20  Second Phase                 1000  ('20/05/10', '20/09/20')
```

Anwendungsfall Teradata NORMALIZE

Fügen Sie nun die Teradata NORMALIZE SQL-Klausel zur SELECT-Anweisung hinzu:

```
SELECT NORMALIZE ON MEETS OR OVERLAPS emp_id, duration
FROM systest.project
ORDER BY 1,2;
```

Diese NORMALIZE-Operation wird für eine einzelne Spalte (emp_id) ausgeführt. Für emp_id=10 verschmelzen die drei sich überschneidenden Periodenwerte in der Angabe Dauer wie folgt zu einem einzigen Periodenwert:

```
     emp_id  duration
-----------  ------------------------
         10  ('10/01/10', '10/08/18')
         20  ('10/03/10', '10/07/20')
         20  ('20/05/10', '20/09/20')
```

Die folgende SELECT-Anweisung führt eine NORMALIZE-Operation für project_name und dept_id aus. Beachten Sie, dass die SELECT-Liste nur eine PERIOD-Spalte, nämlich die Dauer, enthält.

```
SELECT NORMALIZE project_name, dept_id, duration
FROM systest.project;
```

Ausgabe:

```
project_name              dept_id  duration
```

```
--------------------  -----------  ------------------------
First Phase                   1000  ('10/01/10', '10/03/20')
Second Phase                  1000  ('20/05/10', '20/09/20')
First Phase                   2000  ('10/03/10', '10/07/20')
Second Phase                  2000  ('10/06/15', '10/08/18')
```

Amazon Redshift Redshift-äquivalentes SQL

Amazon Redshift unterstützt derzeit den PERIOD-Datentyp in einer Tabelle nicht. Stattdessen müssen Sie ein Teradata PERIOD-Datenfeld wie folgt in zwei Teile unterteilen: start_date, end_date:

```
CREATE TABLE systest.project
     (    emp_id        INTEGER,
          project_name  VARCHAR(20),
          dept_id       INTEGER,
          start_date  DATE,
          end_date    DATE
     );
```

Fügen Sie Beispieldaten in die Tabelle ein:

```
BEGIN TRANSACTION;

INSERT INTO systest.project VALUES (10, 'First Phase', 1000,  DATE '2010-01-10', DATE
 '2010-03-20' );
INSERT INTO systest.project VALUES (10, 'First Phase', 2000,  DATE '2010-03-20', DATE
 '2010-07-15');

INSERT INTO systest.project VALUES (10, 'Second Phase', 2000,  DATE '2010-06-15', DATE
 '2010-08-18' );
INSERT INTO systest.project VALUES (20, 'First Phase', 2000,  DATE '2010-03-10', DATE
 '2010-07-20' );

INSERT INTO systest.project VALUES (20, 'Second Phase', 1000,  DATE '2020-05-10', DATE
 '2020-09-20' );

END TRANSACTION;
```

Ausgabe:

```
 emp_id | project_name | dept_id | start_date |  end_date
--------+--------------+---------+------------+------------
```

```
     10 | First Phase  |    1000 | 2010-01-10 | 2010-03-20
     10 | First Phase  |    2000 | 2010-03-20 | 2010-07-15
     10 | Second Phase |    2000 | 2010-06-15 | 2010-08-18
     20 | First Phase  |    2000 | 2010-03-10 | 2010-07-20
     20 | Second Phase |    1000 | 2020-05-10 | 2020-09-20
(5 rows)
```

Um die NORMALIZE-Klausel von Teradata neu zu schreiben, können Sie die LAG-Fensterfunktion in Amazon Redshift verwenden. Diese Funktion gibt die Werte für eine Zeile mit einem bestimmten Offset über (vor) der aktuellen Zeile in der Partition zurück.

Sie können die LAG-Funktion verwenden, um jede Zeile zu identifizieren, mit der eine neue Periode beginnt, indem Sie ermitteln, ob eine Periode mit der vorherigen Periode übereinstimmt oder sich mit ihr überschneidet (0, wenn ja und 1, wenn nein). Wenn dieses Flag kumulativ zusammengefasst wird, stellt es eine Gruppen-ID bereit, die in der äußeren Group By-Klausel verwendet werden kann, um das gewünschte Ergebnis in Amazon Redshift zu erzielen.

Hier ist ein Beispiel für eine Amazon Redshift SQL-Anweisung, die LAG () verwendet:

```
SELECT emp_id, start_date, end_date,
            (CASE WHEN start_date <= LAG(end_date) OVER (PARTITION BY emp_id ORDER BY
 start_date, end_date) THEN 0 ELSE 1 END) AS GroupStartFlag
FROM systest.project
ORDER BY 1,2;
```

Ausgabe:

```
 emp_id | start_date |  end_date  | groupstartflag
--------+------------+------------+----------------
     10 | 2010-01-10 | 2010-03-20 |              1
     10 | 2010-03-20 | 2010-07-15 |              0
     10 | 2010-06-15 | 2010-08-18 |              0
     20 | 2010-03-10 | 2010-07-20 |              1
     20 | 2020-05-10 | 2020-09-20 |              1
(5 rows)
```

Die folgende Amazon Redshift SQL-Anweisung normalisiert nur die Spalte emp_id:

```
SELECT T2.emp_id, MIN(T2.start_date) as new_start_date, MAX(T2.end_date) as
 new_end_date
FROM
```

```
( SELECT T1.*, SUM(GroupStartFlag) OVER (PARTITION BY emp_id ORDER BY start_date ROWS
 UNBOUNDED PRECEDING) As GroupID
FROM ( SELECT emp_id, start_date, end_date,
            (CASE WHEN start_date <= LAG(end_date) OVER (PARTITION BY emp_id ORDER BY
 start_date, end_date) THEN 0 ELSE 1 END) AS GroupStartFlag
FROM systest.project ) T1
) T2
GROUP BY T2.emp_id, T2.GroupID
ORDER BY 1,2;
```

Ausgabe:

```
 emp_id | new_start_date | new_end_date
--------+----------------+----------------------------------
     10 | 2010-01-10     | 2010-08-18
     20 | 2010-03-10     | 2010-07-20
     20 | 2020-05-10     | 2020-09-20
(3 rows)
```

Die folgende Amazon Redshift SQL-Anweisung normalisiert die Spalten project_name und dept_id:

```
SELECT T2.project_name, T2.dept_id, MIN(T2.start_date) as new_start_date,
 MAX(T2.end_date) as new_end_date
FROM
( SELECT T1.*, SUM(GroupStartFlag) OVER (PARTITION BY project_name, dept_id ORDER BY
 start_date ROWS UNBOUNDED PRECEDING) As GroupID
FROM ( SELECT project_name, dept_id, start_date, end_date,
            (CASE WHEN start_date <= LAG(end_date) OVER (PARTITION BY project_name,
 dept_id ORDER BY start_date, end_date) THEN 0 ELSE 1 END) AS GroupStartFlag
FROM systest.project ) T1
) T2
GROUP BY T2.project_name, T2.dept_id, T2.GroupID
ORDER BY 1,2,3;
```

Ausgabe:

```
 project_name | dept_id | new_start_date | new_end_date
--------------+---------+----------------+--------------
 First Phase  |    1000 | 2010-01-10     | 2010-03-20
 First Phase  |    2000 | 2010-03-10     | 2010-07-20
```

```
 Second Phase |    1000 | 2020-05-10     | 2020-09-20
 Second Phase |    2000 | 2010-06-15     | 2010-08-18
(4 rows)
```

Epen

NORMALIZE nach Amazon Redshift SQL konvertieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Ihren Teradata-SQL-Code.	Verwenden Sie die NORMALIZE-Phrase entsprechend Ihren Bedürfnissen.	SQL Developer
Konvertieren Sie den Code in Amazon Redshift SQL.	Folgen Sie den Richtlinien im Abschnitt „Tools“ dieses Musters, um Ihren Code zu konvertieren.	SQL Developer
Führen Sie den Code in Amazon Redshift aus.	Erstellen Sie Ihre Tabelle, laden Sie Daten in die Tabelle und führen Sie Ihren Code in Amazon Redshift aus.	SQL Developer

Zugehörige Ressourcen

Referenzen

- Temporale Funktion „Teradata NORMALIZE“ (Teradata-Dokumentation)
- LAG-Fensterfunktion (Amazon Redshift Redshift-Dokumentation)
- Migrieren Sie zu Amazon Redshift (AWS-Website)
- Migrieren Sie eine Teradata-Datenbank mithilfe von AWS SCT-Datenextraktionsagenten zu Amazon Redshift (AWS Prescriptive Guidance)
- Konvertieren Sie die Teradata RESET WHEN-Funktion auf Amazon Redshift SQL (AWS Prescriptive Guidance)

Tools

- AWS-Schemakonvertierungstool (AWS SCT)

Partner

- AWS-Kompetenzpartner für Migration

Konvertieren Sie die Teradata RESET WHEN-Funktion in Amazon Redshift SQL

Erstellt von Po Hong (AWS)

Übersicht

RESET WHEN ist eine Teradata-Funktion, die in analytischen Fensterfunktionen von SQL verwendet wird. Es ist eine Erweiterung des ANSI SQL-Standards. RESET WHEN bestimmt die Partition, über die eine SQL-Fensterfunktion ausgeführt wird, basierend auf einer bestimmten Bedingung. Wenn die Bedingung TRUE ergibt, wird eine neue, dynamische Unterpartition innerhalb der vorhandenen Fensterpartition erstellt. Weitere Informationen zu RESET WHEN finden Sie in der Teradata-Dokumentation.

Amazon Redshift unterstützt RESET WHEN in SQL-Fensterfunktionen nicht. Um diese Funktionalität zu implementieren, müssen Sie RESET WHEN in die native SQL-Syntax in Amazon Redshift konvertieren und mehrere verschachtelte Funktionen verwenden. Dieses Muster zeigt, wie Sie die Teradata RESET WHEN-Funktion verwenden und sie in die Amazon Redshift SQL-Syntax konvertieren können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Grundkenntnisse des Teradata Data Warehouse und seiner SQL-Syntax
- Gutes Verständnis von Amazon Redshift und seiner SQL-Syntax

Architektur

Quelltechnologie-Stack

- Teradata-Datawarehouse

Zieltechnologie-Stack

- Amazon Redshift

Architektur

Eine allgemeine Architektur für die Migration einer Teradata-Datenbank zu Amazon Redshift finden Sie im Muster Migrieren einer Teradata-Datenbank zu Amazon Redshift mithilfe von AWS SCT-Datenextraktionsagenten. Die Migration konvertiert die Teradata RESET WHEN-Phrase nicht automatisch in Amazon Redshift SQL. Sie können diese Teradata-Erweiterung konvertieren, indem Sie die Richtlinien im nächsten Abschnitt befolgen.

Tools

Code

Sehen Sie sich die folgende Tabellendefinition in Teradata an, um das Konzept von RESET WHEN zu veranschaulichen:

```
create table systest.f_account_balance
( account_id integer NOT NULL,
  month_id integer,
  balance integer )
unique primary index (account_id, month_id);
```

Führen Sie den folgenden SQL-Code aus, um Beispieldaten in die Tabelle einzufügen:

```
BEGIN TRANSACTION;
Insert Into systest.f_account_balance values (1,1,60);
Insert Into systest.f_account_balance values (1,2,99);
Insert Into systest.f_account_balance values (1,3,94);
Insert Into systest.f_account_balance values (1,4,90);
Insert Into systest.f_account_balance values (1,5,80);
Insert Into systest.f_account_balance values (1,6,88);
Insert Into systest.f_account_balance values (1,7,90);
Insert Into systest.f_account_balance values (1,8,92);
Insert Into systest.f_account_balance values (1,9,10);
Insert Into systest.f_account_balance values (1,10,60);
Insert Into systest.f_account_balance values (1,11,80);
Insert Into systest.f_account_balance values (1,12,10);
END TRANSACTION;
```

Die Beispieltabelle enthält die folgenden Daten:

account_id	month_id	Saldo

1	1	60
1	2	99
1	3	94
1	4	90
1	5	80
1	6	88
1	7	90
1	8	92
1	9	10
1	10	60
1	11	80
1	12	10

Nehmen wir an, Sie möchten für jedes Konto die Reihenfolge der aufeinanderfolgenden monatlichen Saldoerhöhungen analysieren. Wenn der Saldo eines Monats kleiner oder gleich dem Saldo des Vormonats ist, müssen Sie den Zähler auf Null zurücksetzen und neu starten.

Anwendungsfall Teradata RESET WHEN

Um diese Daten zu analysieren, verwendet Teradata SQL eine Fensterfunktion mit einem verschachtelten Aggregat und einer RESET WHEN-Phrase wie folgt:

```
SELECT account_id, month_id, balance,
 ( ROW_NUMBER() OVER (PARTITION BY account_id ORDER BY month_id
RESET WHEN balance <= SUM(balance) over (PARTITION BY account_id ORDER BY month_id ROWS
 BETWEEN 1 PRECEDING AND 1 PRECEDING) ) -1 ) as balance_increase
FROM systest.f_account_balance
ORDER BY 1,2;
```

Ausgabe:

account_id	month_id	Saldo	gleichgewicht_erhöhen
1	1	60	0
1	2	99	1
1	3	94	0
1	4	90	0
1	5	80	0
1	6	88	1
1	7	90	2
1	8	92	3
1	9	10	0
1	10	60	1
1	11	80	2
1	12	10	0

Die Abfrage wird in Teradata wie folgt verarbeitet:

1. Die Aggregatfunktion SUM (Saldo) berechnet die Summe aller Salden für ein bestimmtes Konto in einem bestimmten Monat.
2. Wir prüfen, ob ein Saldo in einem bestimmten Monat (für ein bestimmtes Konto) höher ist als der Saldo des Vormonats.
3. Wenn der Saldo gestiegen ist, erfassen wir einen kumulierten Zählwert. Wenn die Bedingung RESET WHEN als falsch ausgewertet wird, was bedeutet, dass der Saldo in aufeinanderfolgenden Monaten gestiegen ist, erhöhen wir die Anzahl weiter.
4. Die geordnete analytische Funktion ROW_NUMBER () berechnet den Zählwert. Wenn wir einen Monat erreichen, dessen Saldo kleiner oder gleich dem Saldo des Vormonats ist, wird die RESET WHEN-Bedingung als wahr ausgewertet. Falls ja, starten wir eine neue Partition

und ROW_NUMBER () setzt die Zählung bei 1 neu an. Wir verwenden ROWS BETWEEN 1 PREVIODING UND 1 PREVIODING, um auf den Wert der vorherigen Zeile zuzugreifen.

5. Wir subtrahieren 1, um sicherzustellen, dass der Zählwert mit 0 beginnt.

SQL entspricht Amazon Redshift

Amazon Redshift unterstützt die RESET WHEN-Phrase in einer SQL-Analysefensterfunktion nicht. Um dasselbe Ergebnis zu erzielen, müssen Sie Teradata SQL mithilfe der nativen SQL-Syntax von Amazon Redshift und verschachtelten Unterabfragen wie folgt neu schreiben:

```
SELECT account_id, month_id, balance,
   (ROW_NUMBER() OVER(PARTITION BY account_id, new_dynamic_part ORDER BY month_id) -1)
 as balance_increase
FROM
( SELECT account_id, month_id, balance, prev_balance,
SUM(dynamic_part) OVER (PARTITION BY account_id ORDER BY month_id ROWS BETWEEN
 UNBOUNDED PRECEDING AND CURRENT ROW) As new_dynamic_part
FROM ( SELECT account_id, month_id, balance,
SUM(balance) over (PARTITION BY account_id ORDER BY month_id ROWS BETWEEN 1 PRECEDING
 AND 1 PRECEDING) as prev_balance,
(CASE When balance <= prev_balance Then 1 Else 0 END) as dynamic_part
FROM systest.f_account_balance ) A
) B
ORDER BY 1,2;
```

Da Amazon Redshift keine Funktionen für verschachtelte Fenster in der SELECT-Klausel einer einzelnen SQL-Anweisung unterstützt, müssen Sie zwei verschachtelte Unterabfragen verwenden.

- In der inneren Unterabfrage (Alias A) wird ein dynamischer Partitionsindikator (dynamic_part) erstellt und gefüllt. dynamic_part wird auf 1 gesetzt, wenn der Saldo eines Monats kleiner oder gleich dem Saldo des Vormonats ist. Andernfalls wird er auf 0 gesetzt.
- In der nächsten Ebene (Alias B) wird ein new_dynamic_part-Attribut als Ergebnis einer SUM-Fensterfunktion generiert.
- Schließlich fügen Sie new_dynamic_part als neues Partitionsattribut (dynamische Partition) zum vorhandenen Partitionsattribut (account_id) hinzu und wenden dieselbe Fensterfunktion ROW_NUMBER () wie in Teradata an (und minus eins).

Nach diesen Änderungen generiert Amazon Redshift SQL dieselbe Ausgabe wie Teradata.

Epen

RESET WHEN nach Amazon Redshift SQL konvertieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Ihre Teradata-Fensterfunktion.	Verwenden Sie je nach Bedarf verschachtelte Aggregate und die RESET WHEN-Phrase.	SQL Developer
Konvertieren Sie den Code in Amazon Redshift SQL.	Folgen Sie den Richtlinien im Abschnitt „Tools“ dieses Musters, um Ihren Code zu konvertieren.	SQL Developer
Führen Sie den Code in Amazon Redshift aus.	Erstellen Sie Ihre Tabelle, laden Sie Daten in die Tabelle und führen Sie Ihren Code in Amazon Redshift aus.	SQL Developer

Zugehörige Ressourcen

Referenzen

- RESET WHEN-Phrase (Teradata-Dokumentation)
- Erklärung RESET WHEN (Stack Overflow)
- Zu Amazon Redshift migrieren (AWS-Website)
- Migrieren Sie eine Teradata-Datenbank mithilfe von AWS SCT-Datenextraktionsagenten zu Amazon Redshift (AWS Prescriptive Guidance)
- Konvertieren Sie die temporale Funktion Teradata NORMALIZE in Amazon Redshift SQL (AWS Prescriptive Guidance)

Tools

- AWS-Schemakonvertierungstool (AWS SCT)

Partner

- AWS-Kompetenzpartner für Migration

Bereitstellen und verwalten Sie einen serverlosen Data Lake in der AWS-Cloud, indem Sie Infrastruktur als Code verwenden

Erstellt von Kirankumar Chandrashekar (AWS) und Abdel Jaidi (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Dieses Muster beschreibt, wie Serverless Computing und Infrastructure as Code (IaC) verwendet werden, um einen Data Lake in der Amazon Web Services (AWS) -Cloud zu implementieren und zu verwalten. Dieses Muster basiert auf dem von AWS entwickelten Workshop zum Serverless Data Lake Framework (SDLF).

SDLF ist eine Sammlung wiederverwendbarer Ressourcen, die die Bereitstellung von Unternehmensdatenseen in der AWS-Cloud beschleunigen und zu einer schnelleren Bereitstellung in der Produktion beitragen. Es wird verwendet, um die grundlegende Struktur eines Data Lakes unter Befolgung bewährter Methoden zu implementieren.

SDLF implementiert einen CI/CD-Prozess (Continuous Integration/Continuous Deployment) während der gesamten Code- und Infrastrukturbereitstellung mithilfe von AWS-Services wie AWS CodePipeline, AWS und AWS CodeBuild. CodeCommit

Dieses Muster verwendet mehrere serverlose AWS-Services, um das Data Lake-Management zu vereinfachen. Dazu gehören Amazon Simple Storage Service (Amazon S3) und Amazon DynamoDB für die Speicherung, AWS Lambda und AWS Glue für die Datenverarbeitung sowie Amazon CloudWatch Events, Amazon Simple Queue Service (Amazon SQS) und AWS Step Functions für die Orchestrierung.

AWS CloudFormation - und AWS-Code-Services fungieren als IaC-Schicht und bieten reproduzierbare und schnelle Bereitstellungen mit einfachem Betrieb und einfacher Verwaltung.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.

- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert.
- Ein Git-Client, installiert und konfiguriert.
- Der SDLF-Workshop wird in einem Webbrowser-Fenster geöffnet und ist sofort einsatzbereit.

Architektur

Das Architekturdiagramm veranschaulicht einen ereignisgesteuerten Prozess mit den folgenden Schritten.

1. Nachdem eine Datei zum Rohdaten-S3-Bucket hinzugefügt wurde, wird eine Amazon S3 S3-Ereignisbenachrichtigung in eine SQS-Warteschlange gestellt. Jede Benachrichtigung wird als JSON-Datei zugestellt, die Metadaten wie den S3-Bucket-Namen, den Objektschlüssel oder den Zeitstempel enthält.
2. Diese Benachrichtigung wird von einer Lambda-Funktion verarbeitet, die das Ereignis auf der Grundlage der Metadaten an den richtigen Extraktions-, Transformations- und Ladeprozess (ETL) weiterleitet. Die Lambda-Funktion kann auch kontextbezogene Konfigurationen verwenden, die in einer Amazon DynamoDB-Tabelle gespeichert sind. Dieser Schritt ermöglicht die Entkopplung und Skalierung auf mehrere Anwendungen im Data Lake.
3. Das Ereignis wird an die erste Lambda-Funktion im ETL-Prozess weitergeleitet, die Daten transformiert und aus dem Rohdatenbereich in den Staging-Bereich für den Data Lake verschiebt. Der erste Schritt besteht darin, den umfassenden Katalog zu aktualisieren. Dies ist eine DynamoDB-Tabelle, die alle Dateimetadaten des Data Lake enthält. Jede Zeile in dieser Tabelle enthält Betriebsmetadaten zu einem einzelnen Objekt, das in Amazon S3 gespeichert ist. Es wird synchron eine Lambda-Funktion aufgerufen, die eine leichte Transformation für das S3-Objekt durchführt. Dabei handelt es sich um einen rechenintensiven Vorgang (z. B. das Konvertieren einer Datei von einem Format in ein anderes). Da dem Staging-S3-Bucket ein neues Objekt hinzugefügt wurde, wird der umfassende Katalog aktualisiert und eine Nachricht an die SQS-Warteschlange gesendet, in der auf die nächste ETL-Phase gewartet wird.
4. Eine CloudWatch Ereignisregel löst alle 5 Minuten eine Lambda-Funktion aus. Diese Funktion prüft, ob Nachrichten aus der vorherigen ETL-Phase an die SQS-Warteschlange zugestellt wurden. Wenn eine Nachricht zugestellt wurde, startet die Lambda-Funktion die zweite Funktion von AWS Step Functions im ETL-Prozess.
5. Anschließend wird eine umfangreiche Transformation auf einen Stapel von Dateien angewendet. Diese umfangreiche Transformation ist ein rechenintensiver Vorgang, z. B. ein synchroner Aufruf

eines AWS Glue-Jobs, einer AWS Fargate-Aufgabe, eines Amazon EMR-Schritts oder eines Amazon-Notebooks. SageMaker Tabellenmetadaten werden mithilfe eines AWS Glue-Crawlers, der den AWS Glue-Katalog aktualisiert, aus den Ausgabedateien extrahiert. Dateimetadaten werden auch der umfassenden Katalogtabelle in DynamoDB hinzugefügt. Schließlich wird auch ein Datenqualitätsschritt ausgeführt, der Deequ nutzt.

Technologie-Stack

- CloudWatch Amazon-Veranstaltungen
- AWS CloudFormation
- AWS CodePipeline
- AWS CodeBuild
- AWS CodeCommit
- Amazon-DynamoDB
- AWS Glue
- AWS Lambda
- Amazon S3
- Amazon SQS
- AWS Step Functions

Tools

- Amazon CloudWatch Events — CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit.
- AWS CloudFormation — CloudFormation hilft bei der vorhersehbaren und wiederholten Erstellung und Bereitstellung von AWS-Infrastrukturbereitstellungen.
- AWS CodeBuild — CodeBuild ist ein vollständig verwalteter Build-Service, der Ihren Quellcode kompiliert, Komponententests durchführt und Artefakte erzeugt, die sofort einsatzbereit sind.
- AWS CodeCommit — CodeCommit ist ein von AWS gehosteter Service zur Versionskontrolle, mit dem Sie Ressourcen (wie Quellcode und Binärdateien) privat speichern und verwalten können.
- AWS CodePipeline — CodePipeline ist ein Continuous Delivery Service, mit dem Sie die Schritte modellieren, visualisieren und automatisieren können, die für die kontinuierliche Veröffentlichung Ihrer Softwareänderungen erforderlich sind.

- Amazon DynamoDB — DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der schnelle und vorhersehbare Leistung mit Skalierbarkeit bietet.
- AWS Glue — AWS Glue ist ein vollständig verwalteter ETL-Service, der das Aufbereiten und Laden von Daten für Analysen erleichtert.
- AWS Lambda — Lambda unterstützt die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice. Amazon S3 kann für eine Vielzahl von Speicherlösungen verwendet werden, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- AWS Step Functions — AWS Step Functions ist ein serverloser Funktionsorchestrator, der es einfach macht, AWS Lambda Lambda-Funktionen und mehrere AWS-Services in geschäftskritischen Anwendungen zu sequenzieren.
- Amazon SQS — Amazon Simple Queue Service (Amazon SQS) ist ein vollständig verwalteter Message Queuing-Service, mit dem Sie Microservices, verteilte Systeme und serverlose Anwendungen entkoppeln und skalieren können.
- Deequ — Deequ ist ein Tool, das Ihnen dabei hilft, Datenqualitätskennzahlen für große Datenmengen zu berechnen, Datenqualitätsbeschränkungen zu definieren und zu überprüfen und über Änderungen bei der Datenverteilung auf dem Laufenden zu bleiben.

Code-Repository

Der Quellcode und die Ressourcen für das SDLF sind im AWS GitHub Labs-Repository verfügbar.

Epen

Richten Sie die CI/CD-Pipeline für die Bereitstellung von IaC ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die CI/CD-Pipeline ein, um IaC für den Data Lake zu verwalten.	Melden Sie sich bei der AWS-Managementkonsole an und folgen Sie den Schritten aus dem Abschnitt Ersteinrichtung des SDLF-Work	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	shops. Dadurch werden die ersten CI/CD-Ressourcen wie CodeCommit Repositorys, CodeBuild Umgebungen und CodePipeline Pipelines erstellt, die IaC für den Data Lake bereitstellen und verwalten.	

Versionskontrolle des IaC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das CodeCommit Repository auf Ihrem lokalen Computer.	Folgen Sie den Anweisungen aus dem Abschnitt Einführung der Grundlagen des SDLF-Workshops. Auf diese Weise können Sie das Git-Repository, das IaC hostet, in Ihre lokale Umgebung klonen. Weitere Informationen finden Sie in der Dokumentation unter Verbindung zu CodeCommit Repositorys herstellen. CodeCommit	DevOps Ingenieur
Ändern Sie die CloudFormation Vorlagen.	Verwenden Sie Ihre lokale Workstation und einen Code-Editor, um die CloudFormation Vorlagen an Ihre Anwendungsfälle oder Anforderungen anzupassen. Übergeben Sie sie in das lokal geklonte Git-Repository.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie in der CloudFormation AWS-Dokumentation unter Arbeiten mit CloudFormation AWS-Vorlagen.	
Übertragen Sie die Änderungen in das CodeCommit Repository.	Ihr Infrastrukturcode unterliegt jetzt der Versionskontrolle und Änderungen an Ihrer Codebasis werden nachverfolgt. Wenn Sie eine Änderung per Push in das CodeCommit Repository übertragen, CodePipeline wird sie automatisch auf Ihre Infrastruktur angewendet und an diese weitergeleitet CodeBuild. **Important** Wenn Sie die AWS SAM-CLI in verwenden CodeBuild, führen Sie die `sam deploy` Befehle `sam package` und aus. Wenn Sie die AWS-CLI verwenden, führen Sie die `aws cloudformation deploy` Befehle `aws cloudformation package` und aus.	DevOps Ingenieur

Zugehörige Ressourcen

Richten Sie die CI/CD-Pipeline für die Bereitstellung von IaC ein

- SDLF-Workshop — Erste Einrichtung

Versionskontrolle des IaC

- SDLF-Workshop — Bereitstellung der Grundlagen
- Verbindung zu Repositorien herstellen CodeCommit
- Arbeiten mit CloudFormation AWS-Vorlagen

Sonstige Ressourcen

- Referenzarchitektur für die serverlose Datenanalyse-Pipeline von AWS
- SDLF-Dokumentation

Erzwingen Sie die Kennzeichnung von Amazon EMR-Clustern beim Start

Erstellt von Priyanka Chaudhary (AWS)

Übersicht

Dieses Muster bietet eine Sicherheitskontrolle, die sicherstellt, dass Amazon EMR-Cluster bei ihrer Erstellung markiert werden.

Amazon EMR ist ein Service von Amazon Web Services (AWS) zur Verarbeitung und Analyse großer Datenmengen. Amazon EMR bietet einen erweiterbaren Service mit geringer Konfiguration als einfachere Alternative zum Betrieb interner Cluster-Datenverarbeitung. Mithilfe von Tagging können Sie AWS-Ressourcen auf unterschiedliche Weise kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Sie können beispielsweise Ihre Amazon EMR-Cluster taggen, indem Sie jedem Cluster benutzerdefinierte Metadaten zuweisen. Ein Tag besteht aus einem Schlüssel und einem Wert, die Sie definieren. Wir empfehlen Ihnen, einen konsistenten Satz von Stichwörtern zu erstellen, um die Anforderungen Ihrer Organisation zu erfüllen. Wenn Sie einem Amazon EMR-Cluster ein Tag hinzufügen, wird das Tag auch an jede aktive Amazon Elastic Compute Cloud (Amazon EC2) -Instance weitergegeben, die dem Cluster zugeordnet ist. Wenn Sie ein Tag aus einem Amazon EMR-Cluster entfernen, wird dieses Tag auch von jeder zugehörigen aktiven EC2 Instance entfernt.

Die Detective Control überwacht API-Aufrufe und initiiert ein Amazon CloudWatch Events-Ereignis für RunJobFlow, AddTagsRemoveTags, und CreateTags APIs. Das Ereignis ruft AWS Lambda auf, das ein Python-Skript ausführt. Die Python-Funktion ruft die Amazon EMR-Cluster-ID aus der JSON-Eingabe des Ereignisses ab und führt die folgenden Prüfungen durch:

- Prüfen Sie, ob der Amazon EMR-Cluster mit den von Ihnen angegebenen Tag-Namen konfiguriert ist.
- Falls nicht, senden Sie dem Benutzer eine Amazon Simple Notification Service (Amazon SNS) -Benachrichtigung mit den entsprechenden Informationen: dem Namen des Amazon EMR-Clusters, den Details zum Verstoß, der AWS-Region, dem AWS-Konto und dem Amazon-Ressourcennamen (ARN) für Lambda, von dem diese Benachrichtigung stammt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket zum Hochladen des bereitgestellten Lambda-Codes. Oder Sie können zu diesem Zweck einen S3-Bucket erstellen, wie im Abschnitt Epics beschrieben.
- Eine aktive E-Mail-Adresse, an die Sie Benachrichtigungen über Verstöße erhalten möchten.
- Eine Liste der obligatorischen Stichwörter, nach denen Sie suchen möchten.

Einschränkungen

- Diese Sicherheitskontrolle ist regional. Sie müssen es in jeder AWS-Region bereitstellen, die Sie überwachen möchten.

Produktversionen

- Amazon EMR Version 4.8.0 und höher.

Architektur

Workflow-Architektur

Automatisierung und Skalierung

- Wenn Sie AWS Organizations verwenden, können Sie AWS Cloudformation verwenden, StackSets um diese Vorlage in mehreren Konten bereitzustellen, die Sie überwachen möchten.

Tools

AWS-Services

- AWS CloudFormation — AWS CloudFormation hilft Ihnen dabei, Ihre AWS-Ressourcen zu modellieren und einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus zu verwalten. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben und sie zusammen als Stack zu starten und zu konfigurieren, anstatt Ressourcen einzeln zu verwalten. Sie können Stacks für mehrere AWS-Konten und AWS-Regionen verwalten und bereitstellen.

- Amazon CloudWatch Events — Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit.
- Amazon EMR — Amazon EMR ist ein Webservice, der die Ausführung von Big-Data-Frameworks und die effiziente Verarbeitung großer Datenmengen vereinfacht.
- AWS Lambda — AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Code

Dieses Muster umfasst die folgenden Anlagen:

- `EMRTagValidation.zip`— Der Lambda-Code für die Sicherheitskontrolle.
- `EMRTagValidation.yml`— Die CloudFormation Vorlage, die das Ereignis und die Lambda-Funktion einrichtet.

Epen

Richten Sie den S3-Bucket ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Wählen oder erstellen Sie in der Amazon S3 S3-Konsole einen S3-Bucket, um die Lambda-Code-ZIP-Datei zu hosten. Dieser S3-Bucket muss sich in derselben AWS-	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Region befinden wie der Amazon EMR-Cluster, den Sie überwachen möchten. Der Name eines Amazon S3-Buckets ist global eindeutig, und der Namespace wird von allen AWS-Konten verwendet . Der S3-Bucket-Name darf keine führenden Schrägstriche enthalten.	
Laden Sie den Lambda-Code hoch.	Laden Sie die Lambda-Code-ZIP-Datei, die im Abschnitt Anlagen bereitgestellt wird, in den S3-Bucket hoch.	Cloud-Architekt

Stellen Sie die CloudFormation AWS-Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die CloudFormation AWS-Vorlage.	Öffnen Sie die CloudFormation AWS-Konsole in derselben AWS-Region wie Ihr S3-Bucket und stellen Sie die Vorlage bereit. Weitere Informationen zur Bereitstellung von CloudFormation AWS-Vorlagen finden Sie in der CloudFormation Dokumentation unter Erstellen eines Stacks auf der CloudFormation AWS-Konsole.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vervollständigen Sie die Parameter in der Vorlage.	Wenn Sie die Vorlage starten, werden Sie zur Eingabe der folgenden Informationen aufgefordert: • S3-Bucket: Geben Sie den Bucket an, den Sie im ersten Epic erstellt oder ausgewählt haben. Hier haben Sie den angehängten Lambda-Code (.zip-Datei) hochgeladen. • S3-Schlüssel: Geben Sie den Speicherort der Lambda-ZIP-Datei in Ihrem S3-Bucket an (z. B. Dateiname .zip oder controls/ filename .zip). Fügen Sie keine führenden Schrägstriche ein. • Benachrichtigungs-E-Mail: Geben Sie eine aktive E-Mail-Adresse an, unter der Sie Amazon SNS SNS-Benachrichtigungen erhalten möchten. • Schlüsselnamen kennzeichnen: Geben Sie die Tags, nach denen Sie suchen möchten, in einer durch Kommas getrennten Liste an (z. B.,,`Applicati onID`). `Environme nt Owner` Das Ereignis	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CloudWatch Ereignisse überwacht den Cluster auf diese Tags und sendet eine Benachrichtigung, wenn sie nicht gefunden werden. • Lambda-Protokollierungsebene: Geben Sie die Protokollierungsebene und die Häufigkeit für die Lambda-Funktion an. Verwenden Sie Info, um detaillierte Informationsmeldungen über den Fortschritt, Fehler für Fehlerereignisse, die die Fortsetzung der Bereitstellung dennoch ermöglichen würden, und Warnmeldungen für potenziell schädliche Situationen zu protokollieren.	

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die CloudFormation Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail an die von Ihnen angegebene E-Mail-Adresse. Sie müssen dieses E-Mail-Abonnement bestätige	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	n, um Benachrichtigungen über Verstöße zu erhalten.	

Zugehörige Ressourcen

- AWS Lambda Lambda-Entwicklerhandbuch
- Kennzeichnen von Clustern in Amazon EMR

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Stellen Sie sicher, dass die Amazon EMR-Protokollierung bei Amazon S3 beim Start aktiviert ist

Erstellt von Priyanka Chaudhary (AWS)

Übersicht

Dieses Muster bietet eine Sicherheitskontrolle, die die Protokollierungskonfiguration für Amazon EMR-Cluster überwacht, die auf Amazon Web Services (AWS) ausgeführt werden.

Amazon EMR ist ein AWS-Tool für die Verarbeitung und Analyse großer Datenmengen. Amazon EMR bietet den erweiterbaren Service mit niedriger Konfiguration als Alternative zum Betrieb interner Cluster-Datenverarbeitung. Amazon EMR bietet zwei Arten von EMR-Clustern.

- Transiente Amazon EMR-Cluster: Transiente Amazon EMR-Cluster werden automatisch heruntergefahren und es fallen keine Kosten mehr an, wenn die Verarbeitung abgeschlossen ist.
- Persistente Amazon EMR-Cluster: Persistente Amazon EMR-Cluster werden weiterhin ausgeführt, nachdem der Datenverarbeitungsauftrag abgeschlossen ist.

Sowohl Amazon EMR als auch Hadoop erstellen Protokolldateien, die Aufschluss über den jeweiligen Status des Clusters geben. Standardmäßig werden diese auf den Master-Knoten im Verzeichnis/mnt/var/log/geschrieben. Je nachdem, wie Sie den Cluster beim Start konfigurieren, können Sie diese Protokolle auch in Amazon Simple Storage Service (Amazon S3) speichern und sie über das grafische Debugging-Tool anzeigen. Beachten Sie, dass die Amazon S3 S3-Protokollierung nur angegeben werden kann, wenn der Cluster gestartet wird. Bei dieser Konfiguration werden alle 5 Minuten Protokolle vom primären Knoten an den Amazon S3 S3-Standort gesendet. Für transiente Cluster ist die Amazon S3 S3-Protokollierung wichtig, da die Cluster nach Abschluss der Verarbeitung verschwinden und diese Protokolldateien zum Debuggen fehlgeschlagener Jobs verwendet werden können.

Das Muster verwendet eine CloudFormation AWS-Vorlage, um eine Sicherheitskontrolle bereitzustellen, die API-Aufrufe überwacht und Amazon CloudWatch Events auf "" startetRunJobFlow. Der Trigger ruft AWS Lambda auf, das ein Python-Skript ausführt. Die Lambda-Funktion ruft die EMR-Cluster-ID aus der JSON-Eingabe des Ereignisses ab und sucht auch nach einer Amazon S3 S3-Protokoll-URI. Wenn kein Amazon S3 S3-URI gefunden wird, sendet die Lambda-Funktion eine Amazon Simple Notification Service (Amazon SNS) -Benachrichtigung, in der der EMR-Clustername, die Verstoßdetails, die AWS-Region, das AWS-Konto und der Lambda

Amazon Resource Name (ARN), von dem die Benachrichtigung stammt, detailliert beschrieben werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein S3-Bucket für die Lambda-Code-.zip-Datei
- Eine E-Mail-Adresse, an die Sie die Benachrichtigung über den Verstoß erhalten möchten

Einschränkungen

- Diese Detective Control ist regional und muss in den AWS-Regionen eingesetzt werden, die Sie überwachen möchten.

Produktversionen

- Amazon EMR Version 4.8.0 und höher

Architektur

Zieltechnologie-Stack

- Veranstaltung Amazon CloudWatch Events
- Amazon EMR
- Lambda-Funktion
- S3-Bucket
- Amazon SNS

Zielarchitektur

Automatisierung und Skalierung

- Wenn Sie AWS Organizations verwenden, können Sie AWS verwenden, CloudFormation StackSets um diese Vorlage in mehreren Konten bereitzustellen, die Sie überwachen möchten.

Tools

Tools

- AWS CloudFormation — AWS CloudFormation unterstützt Sie bei der Modellierung und Einrichtung von AWS-Ressourcen mithilfe von Infrastructure as Code.
- AWS Cloudwatch Events — AWS CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit.
- Amazon EMR — Amazon EMR ist eine verwaltete Cluster-Plattform, die den Betrieb von Big-Data-Frameworks vereinfacht.
- AWS Lambda — AWS Lambda unterstützt die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon S3 — Amazon S3 ist eine Webservice-Schnittstelle, mit der Sie beliebige Datenmengen von überall im Internet speichern und abrufen können.
- Amazon SNS — Amazon SNS ist ein Webservice, der die Zustellung oder den Versand von Nachrichten zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen, koordiniert und verwaltet.

Code

- Eine ZIP-Datei des Projekts ist als Anhang verfügbar.

Epen

Definieren Sie den S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Um die Lambda-Code-ZIP-Datei zu hosten, wählen oder erstellen Sie einen S3-Bucket mit einem eindeutigen Namen, der keine führenden Schrägstriche enthält. Ein S3-Bucket-Name ist weltweit eindeutig,	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und der Namespace wird von allen AWS-Konten gemeinsam genutzt. Ihr S3-Bucket muss sich in derselben AWS-Regio n befinden wie der Amazon EMR-Cluster, der bewertet wird.	

Laden Sie den Lambda-Code in den S3-Bucket hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Lambda-Code in den S3-Bucket hoch.	Laden Sie die Lambda-Code-ZIP-Datei, die im Abschnitt „Anlagen“ bereitgestellt wird, in den S3-Bucket hoch. Der S3-Bucket muss sich in derselben Region befinden wie der Amazon EMR-Cluster, der bewertet wird.	Cloud-Architekt

Stellen Sie die CloudFormation AWS-Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudForm ation AWS-Vorlage bereit.	Stellen Sie auf der CloudForm ation AWS-Konsole, in derselben Region wie Ihr S3-Bucket, die CloudFormation AWS-Vorlage bereit, die als Anlage zu diesem Muster bereitgestellt wird. Geben Sie im nächsten Epic die Werte für die Parameter an.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen zur Bereitstellung von CloudFormation AWS-Vorlagen finden Sie im Abschnitt „Verwandte Ressourcen“.	

Vervollständigen Sie die Parameter in der CloudFormation AWS-Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Nennen Sie den S3-Bucket.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epic erstellt haben.	Cloud-Architekt
Geben Sie den Amazon S3 S3-Schlüssel ein.	<file-name>Geben Sie den Speicherort der Lambda-Code-ZIP-Datei in Ihrem S3-Bucket ohne führende Schrägstriche an (z. B.<directory>/.zip).	Cloud-Architekt
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine aktive E-Mail-Adresse an, um Amazon SNS SNS-Benachrichtigungen zu erhalten.	Cloud-Architekt
Definieren Sie die Protokollierungsebene.	Definieren Sie die Protokollierungsebene und die Häufigkeit für Ihre Lambda-Funktion. „Info“ bezeichnet detaillierte Informationsmeldungen über den Fortschritt der Anwendung. „Fehler“ bezeichnet Fehlerereignisse, die dazu führen könnten, dass	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Anwendung weiterhin ausgeführt werden kann. „Warnung“ steht für potenziell schädliche Situationen.	

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail-Nachricht an die angegebene E-Mail-Adresse. Sie müssen dieses E-Mail-Abonnement bestätigen, um Benachric htigungen über Verstöße zu erhalten.	Cloud-Architekt

Zugehörige Ressourcen

- AWS Lambda
- Amazon EMR-Protokollierung
- Bereitstellen von CloudFormation AWS-Vorlagen

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Generieren Sie Testdaten mit einem AWS Glue Glue-Job und Python

Erstellt von Moinul Al-Mamun (AWS)

Übersicht

Dieses Muster zeigt Ihnen, wie Sie schnell und einfach Millionen von Beispieldateien gleichzeitig generieren können, indem Sie einen in Python geschriebenen AWS Glue Glue-Job erstellen. Die Beispieldateien werden in einem Amazon Simple Storage Service (Amazon S3) -Bucket gespeichert. Die Fähigkeit, schnell eine große Anzahl von Beispieldateien zu generieren, ist wichtig für das Testen oder Evaluieren von Services in der AWS-Cloud. Sie können beispielsweise die Leistung von AWS Glue Studio- oder AWS Glue DataBrew Glue-Jobs testen, indem Sie Datenanalysen für Millionen kleiner Dateien in einem Amazon S3 S3-Präfix durchführen.

Sie können zwar andere AWS-Services verwenden, um Beispieldatensätze zu generieren, wir empfehlen Ihnen jedoch, AWS Glue zu verwenden. Sie müssen keine Infrastruktur verwalten, da AWS Glue ein serverloser Datenverarbeitungsservice ist. Sie können einfach Ihren Code mitbringen und ihn in einem AWS Glue Glue-Cluster ausführen. Darüber hinaus stellt AWS Glue die Ressourcen bereit, konfiguriert und skaliert sie, die für die Ausführung Ihrer Jobs erforderlich sind. Sie zahlen nur für die Ressourcen, die Ihre Jobs während der Ausführung verbrauchen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS-Befehlszeilenschnittstelle (AWS CLI), für die Verwendung mit dem AWS-Konto installiert und konfiguriert

Produktversionen

- Python 3.9
- AWS-CLI Version 2

Einschränkungen

Die maximale Anzahl von AWS Glue Glue-Jobs pro Trigger beträgt 50. Weitere Informationen finden Sie unter AWS Glue Glue-Endpunkte und Kontingente.

Architektur

Das folgende Diagramm zeigt eine Beispielarchitektur, in deren Mittelpunkt ein AWS Glue Glue-Job steht, der seine Ausgabe (d. h. Beispieldateien) in einen S3-Bucket schreibt.

Das Diagramm umfasst den folgenden Workflow:

1. Sie verwenden die AWS-CLI, die AWS-Managementkonsole oder eine API, um den AWS Glue-Job zu initiieren. Mit der AWS-CLI oder API können Sie die Parallelisierung des aufgerufenen Jobs automatisieren und die Laufzeit für die Generierung von Beispieldateien reduzieren.
2. Der AWS Glue Glue-Job generiert Dateiinhalte nach dem Zufallsprinzip, konvertiert den Inhalt in das CSV-Format und speichert den Inhalt dann als Amazon S3 S3-Objekt unter einem gemeinsamen Präfix. Jede Datei ist kleiner als ein Kilobyte. Der AWS Glue Glue-Job akzeptiert zwei benutzerdefinierte Auftragsparameter: `START_RANGE` und`END_RANGE`. Sie können diese Parameter verwenden, um Dateinamen und die Anzahl der Dateien festzulegen, die in Amazon S3 bei jeder Auftragsausführung generiert werden. Sie können mehrere Instanzen dieses Jobs parallel ausführen (z. B. 100 Instanzen).

Tools

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS Glue ist ein vollständig verwalteter Service zum Extrahieren, Transformieren und Laden (ETL). Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.

Bewährte Methoden

Beachten Sie bei der Implementierung dieses Musters die folgenden bewährten Methoden für AWS Glue:

- Verwenden Sie den richtigen AWS Glue Glue-Worker-Typ, um die Kosten zu senken. Wir empfehlen Ihnen, sich mit den verschiedenen Eigenschaften von Workertypen vertraut zu machen und dann anhand der CPU- und Speicheranforderungen den richtigen Worker-Typ für Ihre Arbeitslast auszuwählen. Für dieses Muster empfehlen wir, einen Python-Shell-Job als Jobtyp zu verwenden, um die DPU zu minimieren und die Kosten zu senken. Weitere Informationen finden Sie unter Hinzufügen von Aufträgen in AWS Glue im AWS Glue Developer Guide.
- Verwenden Sie das richtige Parallelitätslimit, um Ihren Job zu skalieren. Wir empfehlen Ihnen, die maximale Parallelität Ihres AWS Glue Glue-Auftrags auf Ihrem Zeitbedarf und der erforderlichen Anzahl von Dateien festzulegen.
- Generieren Sie zunächst eine kleine Anzahl von Dateien. Um Kosten und Zeit beim Erstellen Ihrer AWS Glue Glue-Jobs zu sparen, beginnen Sie mit einer kleinen Anzahl von Dateien (z. B. 1.000). Dies kann die Fehlerbehebung erleichtern. Wenn das Generieren einer kleinen Anzahl von Dateien erfolgreich ist, können Sie auf eine größere Anzahl von Dateien skalieren.
- Führen Sie es zuerst lokal aus. Um Kosten und Zeit bei der Erstellung Ihrer AWS Glue Glue-Jobs zu sparen, starten Sie die Entwicklung lokal und testen Sie Ihren Code. Anweisungen zur Einrichtung eines Docker-Containers, der Ihnen helfen kann, AWS Glue Glue-ETL-Jobs (Extrahieren, Transformieren und Laden) sowohl in einer Shell als auch in einer integrierten Entwicklungsumgebung (IDE) zu schreiben, finden Sie im Beitrag Entwickeln von AWS Glue Glue-ETL-Jobs lokal mithilfe eines Containers im AWS Big Data-Blog.

Weitere bewährte Methoden für AWS Glue finden Sie unter Bewährte Methoden in der AWS Glue Glue-Dokumentation.

Epen

Erstellen Sie einen S3-Ziel-Bucket und eine IAM-Rolle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket zum Speichern der Dateien.	Erstellen Sie einen S3-Bucket und ein darin enthaltenes Präfix.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Dieses Muster verwendet den `s3://{your-s3-bucket-name}/small-files/` Standort zu Demonstrationszwecken.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und konfigurieren Sie eine IAM-Rolle.	Sie müssen eine IAM-Rolle erstellen, die Ihr AWS Glue Glue-Job verwenden kann, um in Ihren S3-Bucket zu schreiben. 1. Erstellen Sie eine IAM-Rolle (z. B. genannt `"AWSGlueServiceRole-smallfiles"`). 2. Wählen Sie AWS Glue als vertrauenswürdige Entität der Richtlinie. 3. Fügen Sie der Rolle eine von AWS verwaltete Richtlinie `"AWSGlueServiceRole"` hinzu, die aufgerufen wird. 4. Erstellen Sie eine Inline-Richtlinie oder eine vom Kunden verwaltete Richtlinie, die auf der `"s3-small-file-access"` Grundlage der folgenden Konfiguration aufgerufen wird. `"{bucket}"` Ersetzen Sie es durch Ihren Bucket-Namen. `{ "Version": "2012-10-17", "Statement": [ {`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"Effect": "Allow", "Action": ["s3:GetObject", "s3:PutObject"], "Resource": ["arn:aws:s3:::{bucket}/small-files/input/*"] }] }</pre> 5. Hängen Sie die `"s3-small-file-access"` Richtlinie an Ihre Rolle an.	

Erstellen und konfigurieren Sie einen AWS Glue Glue-Job zur Verarbeitung gleichzeitiger Läufe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen AWS Glue Glue-Job.	Sie müssen einen AWS Glue Glue-Job erstellen, der Ihre Inhalte generiert und in einem S3-Bucket speichert. Erstellen Sie einen AWS Glue Glue-Job und konfigurieren Sie dann Ihren Job, indem Sie die folgenden Schritte ausführen:	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS Glue-Konsole. 2. Wählen Sie im Navigatio nsbereich unter Dateninte gration und ETL die Option Jobs aus. 3. Wählen Sie im Abschnitt Job erstellen die Option Python-Shell-Skripteditor aus. 4. Wählen Sie im Abschnitt Optionen die Option Neues Skript mit Standardcode erstellen und dann Erstellen aus. 5. Wählen Sie Jobdetails. 6. Geben Sie als Namen create_small_files ein. 7. Wählen Sie für IAM-Rolle die IAM-Rolle aus, die Sie zuvor erstellt haben. 8. Wählen Sie im Abschnitt Dieser Job wird ausgeführt die Option Ein neues Skript, das von Ihnen erstellt werden soll aus. 9. Erweitern Sie Erweiterte Eigenschaften. 10. Geben Sie zu Demonstra tionszwecken für Maximale Parallelität den Wert 100	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ein. Hinweis: Die maximale Parallelität definiert, wie viele Instanzen des Jobs Sie parallel ausführen können. 11. Wählen Sie Speichern.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisieren Sie den Jobcode.	1. Öffnen Sie die AWS Glue Glue-Konsole.
	2. Wählen Sie im Navigationsbereich die Option Jobs (Aufträge) aus.
	3. Wählen Sie im Bereich Ihre Jobs den Job aus, den Sie zuvor erstellt haben.
	4. Wählen Sie die Registerkarte Skript und aktualisieren Sie dann das Skript auf der Grundlage des folgenden Codes. Aktualisieren Sie die `text_str` Variablen `BUCKET_NAME PREFIX`, und mit Ihren Werten.
	`from awsglue.utils import getResolvedOptions`
	`import sys`
	`import boto3`
	`from random import randrange`
	
	`# Two arguments`
	`args = getResolvedOptions(sys.argv, ['START_RANGE', 'END_RANGE'])`
	
	`START_RANGE = int(args['START_RANGE'])`
	`END_RANGE = int(args['END_RANGE'])`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>BUCKET_NAME = '{BUCKET_NAME}'
	PREFIX = 'small-files/input/'
	s3 = boto3.resource('s3')
	for x in range(START_RANGE, END_RANGE):
	    # generate file name
	    file_name = f"input_{x}.txt"
	    # generate text
	    text_str = str(randrange(100000))+","+str(randrange(100000))+", " + str(randrange(10000000)) + "," + str(randrange(10000))
	    # write in s3
	s3.Object(BUCKET_NAME, PREFIX + file_name).put(Body=text_str)</pre> 5. Wählen Sie Speichern.	

Führen Sie den AWS Glue Glue-Job über die Befehlszeile oder Konsole aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den AWS Glue Glue-Job von der Befehlszeile aus.	Um Ihren AWS Glue Glue-Job über die AWS-CLI auszuführen, führen Sie den folgenden Befehl mit Ihren Werten aus:	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`cmd:~$ aws glue start-job-run --job-name create_small_files --arguments '{"--START_RANGE":"0","--END_RANGE":"1000000"}'`
	`cmd:~$ aws glue start-job-run --job-name create_small_files --arguments '{"--START_RANGE":"1000000","--END_RANGE":"2000000"}'`
	
	Note
	Anweisungen zur Ausführung des AWS Glue Glue-Jobs von der AWS-Managementkonsole aus finden Sie in der Geschichte Ausführen des AWS Glue-Jobs in der AWS-Managementkonsole in diesem Muster.
	
	Tip
	Wir empfehlen die Verwendung der AWS-CLI zur Ausführung von AWS Glue-Jobs, wenn Sie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	mehrere Ausführungen gleichzeitig mit unterschiedlichen Parametern ausführen möchten, wie im obigen Beispiel gezeigt.
	
	Um alle AWS-CLI-Befehle zu generieren, die zum Generieren einer definierten Anzahl von Dateien unter Verwendung eines bestimmten Parallelisierungsfaktors erforderlich sind, führen Sie den folgenden Bash-Code aus (unter Verwendung Ihrer Werte):
	
	`# define parameters`
	`NUMBER_OF_FILES=10000000;`
	`PARALLELIZATION=50;`
	
	`# initialize`
	`_SB=0;`
	
	`# generate commands`
	`for i in $(seq 1 $PARALLELIZATION);`
	`do`
	`echo aws glue start-job-run --job-name create_small_files --arguments '"'{"--START_RANGE":"'$(((NUMBER_OF`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
_FILES/PARALLELIZA
TION) * (i-1) +
 _SB))'","--END_RAN
GE":"'$(((NUMBER_O
F_FILES/PARALLELIZ
ATION) * (i)))'"}'"'";
      _SB=1;
done
```

Wenn Sie das obige Skript verwenden, sollten Sie Folgendes beachten:

- Das Skript vereinfacht das Aufrufen und Generieren kleiner Dateien in großem Maßstab.
- Aktualisiere `NUMBER_OF_FILES` und `PARALLELIZATION` mit deinen Werten.
- Das obige Skript druckt eine Liste von Befehlen, die Sie ausführen müssen. Kopieren Sie diese Ausgabebefehle und führen Sie sie dann in Ihrem Terminal aus.
- Wenn Sie die Befehle direkt aus dem Skript heraus ausführen möchten, entfernen Sie die `echo` Anweisung in Zeile 11.

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Ein Beispiel für die Ausgabe des obigen Skripts finden Sie unter Shell-Skriptausgabe im Abschnitt Zusätzliche Informationen dieses Musters.	
Führen Sie den AWS Glue Glue-Job in der AWS-Managementkonsole aus.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS Glue-Konsole. 2. Wählen Sie im Navigationsbereich unter Datenintegration und ETL die Option Jobs aus. 3. Wählen Sie im Bereich „Ihre Jobs“ Ihren Job aus. 4. Aktualisieren Sie im Abschnitt Parameter (optional) Ihre Parameter. 5. Wählen Sie Aktion und dann Job ausführen aus. 6. Wiederholen Sie die Schritte 3 bis 5 so oft Sie möchten. Um beispielsweise 10 Millionen Dateien zu erstellen, wiederholen Sie diesen Vorgang zehnmal.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Status Ihres AWS Glue Glue-Auftrags.	1. Öffnen Sie die AWS Glue Glue-Konsole. 2. Wählen Sie im Navigationsbereich die Option Jobs (Aufträge) aus. 3. Wählen Sie im Bereich „Ihre Jobs“ den Job aus, den Sie zuvor erstellt haben (d. h. `create_small_files`). 4. Informationen zum Fortschritt und zur Generierung Ihrer Dateien finden Sie in den Spalten Run-ID, Run Status und anderen.	App-Developer

Zugehörige Ressourcen

Referenzen

- Register für offene Daten auf AWS
- Datensätze für Analysen
- Daten auf AWS öffnen
- Jobs in AWS Glue hinzufügen
- Erste Schritte mit AWS Glue

Anleitungen und Muster

- Bewährte Methoden für AWS Glue
- Anwendungen für Lasttests

Zusätzliche Informationen

Benchmarking-Test

Dieses Muster wurde verwendet, um im Rahmen eines Benchmark-Tests 10 Millionen Dateien mit unterschiedlichen Parallelisierungsparametern zu generieren. Die folgende Tabelle zeigt die Ergebnisse des Tests:

Parallelisierung	Anzahl der Dateien, die durch einen Joblauf generiert wurden	Dauer des Job	Geschwindigkeit
10	1 000 000	6 Stunden, 40 Minuten	Sehr langsam
50	200 000	80 Minuten	Mittel
100	100 000	40 Minuten	Schnell

Wenn Sie den Prozess beschleunigen möchten, können Sie in Ihrer Jobkonfiguration mehr gleichzeitige Läufe konfigurieren. Sie können die Auftragskonfiguration ganz einfach an Ihre Anforderungen anpassen. Beachten Sie jedoch, dass es ein Kontingent für den AWS Glue Glue-Service gibt. Weitere Informationen finden Sie unter AWS Glue Glue-Endpunkte und Kontingente.

Shell-Skriptausgabe

Das folgende Beispiel zeigt die Ausgabe des Shell-Skripts aus dem Job Run the AWS Glue von der Befehlszeile aus in diesem Muster.

```
user@MUC-1234567890 MINGW64 ~
  $ # define parameters
  NUMBER_OF_FILES=10000000;
  PARALLELIZATION=50;
  # initialize
  _SB=0;

  # generate commands
  for i in $(seq 1 $PARALLELIZATION);
   do
```

```
        echo aws glue start-job-run --job-name create_small_files --arguments
 "'"'{"--START_RANGE":"'$(((NUMBER_OF_FILES/PARALLELIZATION)  (i-1) + SB))'","--
ENDRANGE":"'$(((NUMBER_OF_FILES/PARALLELIZATION)  (i)))'"}'"'";
        _SB=1;
   done

  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"0","--END_RANGE":"200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"200001","--END_RANGE":"400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"400001","--END_RANGE":"600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"600001","--END_RANGE":"800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"800001","--END_RANGE":"1000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1000001","--END_RANGE":"1200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1200001","--END_RANGE":"1400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1400001","--END_RANGE":"1600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1600001","--END_RANGE":"1800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1800001","--END_RANGE":"2000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2000001","--END_RANGE":"2200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2200001","--END_RANGE":"2400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2400001","--END_RANGE":"2600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2600001","--END_RANGE":"2800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2800001","--END_RANGE":"3000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3000001","--END_RANGE":"3200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3200001","--END_RANGE":"3400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3400001","--END_RANGE":"3600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3600001","--END_RANGE":"3800000"}'
```

```
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3800001","--END_RANGE":"4000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4000001","--END_RANGE":"4200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4200001","--END_RANGE":"4400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4400001","--END_RANGE":"4600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4600001","--END_RANGE":"4800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4800001","--END_RANGE":"5000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5000001","--END_RANGE":"5200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5200001","--END_RANGE":"5400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5400001","--END_RANGE":"5600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5600001","--END_RANGE":"5800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5800001","--END_RANGE":"6000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6000001","--END_RANGE":"6200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6200001","--END_RANGE":"6400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6400001","--END_RANGE":"6600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6600001","--END_RANGE":"6800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6800001","--END_RANGE":"7000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7000001","--END_RANGE":"7200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7200001","--END_RANGE":"7400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7400001","--END_RANGE":"7600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7600001","--END_RANGE":"7800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7800001","--END_RANGE":"8000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8000001","--END_RANGE":"8200000"}'
```

```
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8200001","--END_RANGE":"8400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8400001","--END_RANGE":"8600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8600001","--END_RANGE":"8800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8800001","--END_RANGE":"9000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9000001","--END_RANGE":"9200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9200001","--END_RANGE":"9400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9400001","--END_RANGE":"9600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9600001","--END_RANGE":"9800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9800001","--END_RANGE":"10000000"}'

  user@MUC-1234567890 MINGW64 ~
```

HÄUFIG GESTELLTE FRAGEN

Wie viele gleichzeitige Läufe oder parallel Jobs sollte ich verwenden?

Die Anzahl der gleichzeitigen Läufe und parallel Jobs hängt von Ihrem Zeitbedarf und der gewünschten Anzahl von Testdateien ab. Wir empfehlen Ihnen, die Größe der Dateien, die Sie erstellen, zu überprüfen. Prüfen Sie zunächst, wie viel Zeit ein AWS Glue Glue-Job benötigt, um die gewünschte Anzahl von Dateien zu generieren. Verwenden Sie dann die richtige Anzahl gleichzeitiger Läufe, um Ihre Ziele zu erreichen. Wenn Sie beispielsweise davon ausgehen, dass 100.000 Dateien 40 Minuten benötigen, um den Lauf abzuschließen, Ihre Zielzeit jedoch 30 Minuten beträgt, müssen Sie die Parallelitätseinstellung für Ihren AWS Glue Glue-Job erhöhen.

Welche Art von Inhalt kann ich mit diesem Muster erstellen?

Sie können jede Art von Inhalt erstellen, z. B. Textdateien mit unterschiedlichen Trennzeichen (z. B. PIPE, JSON oder CSV). Dieses Muster verwendet Boto3, um in eine Datei zu schreiben, und speichert die Datei dann in einem S3-Bucket.

Welche IAM-Berechtigungen benötige ich für den S3-Bucket?

Sie benötigen eine identitätsbasierte Richtlinie, die den `Write` Zugriff auf Objekte in Ihrem S3-Bucket ermöglicht. Weitere Informationen finden Sie unter Amazon S3: Erlaubt Lese- und Schreibzugriff auf Objekte in einem S3-Bucket in der Amazon S3 S3-Dokumentation.

Mit AWS IoT Greengrass IoT-Daten kostengünstig direkt in Amazon S3 aufnehmen

Erstellt von Sebastian Viviani (AWS) und Rizwan Syed (AWS)

Übersicht

Dieses Muster zeigt Ihnen, wie Sie mithilfe eines AWS IoT Greengrass Version 2-Geräts kostengünstig Daten aus dem Internet der Dinge (IoT) direkt in einen Amazon Simple Storage Service (Amazon S3) -Bucket aufnehmen können. Auf dem Gerät wird eine benutzerdefinierte Komponente ausgeführt, die die IoT-Daten liest und die Daten in einem persistenten Speicher (d. h. einer lokalen Festplatte oder einem lokalen Volume) speichert. Anschließend komprimiert das Gerät die IoT-Daten in eine Apache Parquet-Datei und lädt die Daten regelmäßig in einen S3-Bucket hoch.

Die Menge und Geschwindigkeit der IoT-Daten, die Sie aufnehmen, ist nur durch Ihre Edge-Hardwarekapazitäten und Ihre Netzwerkbandbreite begrenzt. Sie können Amazon Athena verwenden, um Ihre aufgenommenen Daten kostengünstig zu analysieren. Athena unterstützt komprimierte Apache Parquet-Dateien und Datenvisualisierung mithilfe von Amazon Managed Grafana.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Edge-Gateway, das auf AWS IoT Greengrass Version 2 läuft und Daten von Sensoren sammelt (Die Datenquellen und der Datenerfassungsprozess würden den Rahmen dieses Musters sprengen, aber Sie können fast jede Art von Sensordaten verwenden. Dieses Muster verwendet einen lokalen MQTT-Broker mit Sensoren oder Gateways, die Daten lokal veröffentlichen.)
- Komponenten, Rollen und SDK-Abhängigkeiten von AWS IoT Greengrass
- Eine Stream-Manager-Komponente zum Hochladen der Daten in den S3-Bucket
- AWS SDK for Java, AWS-SDK für JavaScript oder AWS-SDK SDK for Python (Boto3) zur Ausführung des APIs

Einschränkungen

- Die Daten in diesem Muster werden nicht in Echtzeit in den S3-Bucket hochgeladen. Es gibt eine Verzögerungszeit, und Sie können die Verzögerungszeit konfigurieren. Daten werden vorübergehend auf dem Edge-Gerät zwischengespeichert und nach Ablauf des Zeitraums hochgeladen.
- Das SDK ist nur in Java, Node.js und Python verfügbar.

Architektur

Zieltechnologie-Stack

- Amazon S3
- AWS IoT Greengrass
- MQTT-Broker
- Stream Manager-Komponente

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur, die darauf ausgelegt ist, IoT-Sensordaten aufzunehmen und diese Daten in einem S3-Bucket zu speichern.

Das Diagramm zeigt den folgenden Workflow:

1. Aktualisierungen mehrerer Sensoren (z. B. Temperatur und Ventil) werden auf einem lokalen MQTT-Broker veröffentlicht.
2. Der Parquet-Dateikomprimierer, der diese Sensoren abonniert hat, aktualisiert Themen und empfängt diese Updates.
3. Der Parquet-Dateikomprimierer speichert die Updates lokal.
4. Nach Ablauf des Zeitraums werden die gespeicherten Dateien zu Parquet-Dateien komprimiert und an den Stream-Manager weitergegeben, damit sie in den angegebenen S3-Bucket hochgeladen werden.
5. Der Stream-Manager lädt die Parquet-Dateien in den S3-Bucket hoch.

> **Note**
>
> Der Stream-Manager (`StreamManager`) ist eine verwaltete Komponente. Beispiele für den Export von Daten nach Amazon S3 finden Sie unter Stream Manager in der AWS IoT Greengrass-Dokumentation. Sie können einen lokalen MQTT-Broker als Komponente oder einen anderen Broker wie Eclipse Mosquitto verwenden.

Tools

AWS-Tools

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon S3 analysieren können.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS IoT Greengrass ist ein Open-Source-IoT-Edge-Laufzeit- und Cloud-Service, mit dem Sie IoT-Anwendungen auf Ihren Geräten erstellen, bereitstellen und verwalten können.

Andere Tools

- Apache Parquet ist ein spaltenorientiertes Open-Source-Datendateiformat, das zum Speichern und Abrufen entwickelt wurde.
- MQTT (Message Queuing Telemetry Transport) ist ein einfaches Messaging-Protokoll, das für eingeschränkte Geräte entwickelt wurde.

Bewährte Methoden

Verwenden Sie das richtige Partitionsformat für hochgeladene Daten

Es gibt keine spezifischen Anforderungen für die Root-Präfixnamen im S3-Bucket (z. B. `"myAwesomeDataSet/"` oder`"dataFromSource"`), aber wir empfehlen, eine aussagekräftige Partition und ein aussagekräftiges Präfix zu verwenden, damit der Zweck des Datensatzes leicht zu verstehen ist.

Wir empfehlen außerdem, die richtige Partitionierung in Amazon S3 zu verwenden, damit die Abfragen für den Datensatz optimal ausgeführt werden. Im folgenden Beispiel werden die Daten im

HIVE-Format partitioniert, sodass die von jeder Athena-Abfrage gescannte Datenmenge optimiert wird. Dies verbessert die Leistung und senkt die Kosten.

```
s3://<ingestionBucket>/<rootPrefix>/year=YY/month=MM/day=DD/
HHMM_<suffix>.parquet
```

Epen

So richten Sie Ihre Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	1. Erstellen Sie einen S3-Bucket oder verwenden Sie einen vorhandenen Bucket. 2. Erstellen Sie ein aussagekräftiges Präfix für den S3-Bucket, in den Sie die IoT-Daten aufnehmen möchten (z. B. `s3:\\<bucket>\<prefix>`). 3. Notieren Sie sich Ihr Präfix für die spätere Verwendung.	App-Developer
Fügen Sie dem S3-Bucket IAM-Berechtigungen hinzu.	Um Benutzern Schreibzugriff auf den S3-Bucket und das Präfix zu gewähren, die Sie zuvor erstellt haben, fügen Sie Ihrer AWS IoT Greengrass-Rolle die folgende IAM-Richtlinie hinzu: `{ "Version": "2012-10-17", "Statement": [ {`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"Sid": "S3DataUpload", "Effect": "Allow", "Action": ["s3:List*", "s3:Put*"], "Resource": ["arn:aws:s3:::<ingestionBucket>", "arn:aws:s3:::<ingestionBucket>/<prefix>/*"] }] }</pre> Weitere Informationen finden Sie in der Aurora-Dokumentation unter Erstellen einer IAM-Richtlinie für den Zugriff auf Amazon S3 S3-Ressourcen. Aktualisieren Sie als Nächstes die Ressourcenrichtlinie (falls erforderlich) für den S3-Bucket, um Schreibzugriff mit den richtigen AWS-Prinzipalen zu ermöglichen.	

Erstellen und implementieren Sie die AWS IoT Greengrass-Komponente

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie das Rezept der Komponente.	Aktualisieren Sie die Komponentenkonfiguration, wenn Sie eine Bereitstellung anhand des folgenden Beispiels erstellen: `{ "region": "<region>", "parquet_period": <period>, "s3_bucket": "<s3Bucket>", "s3_key_prefix": "<s3prefix>" }` `<region>`Ersetzen Sie durch Ihre AWS-Region, `<period>` durch Ihr periodisches Intervall , `<s3Bucket>` durch Ihren S3-Bucket und `<s3prefix>` durch Ihr Präfix.	App-Developer
Erstellen Sie die Komponente.	Führen Sie eine der folgenden Aktionen aus: • Erstellen Sie die Komponente. • Fügen Sie die Komponente der CI/CD-Pipeline hinzu (falls vorhanden). Achten Sie darauf, das Artefakt aus dem Artefakt-Repository in den AWS IoT Greengrass-	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Artefakt-Bucket zu kopieren. Erstellen oder aktualisieren Sie anschließend Ihre AWS IoT Greengrass-Kompone nte. • **Note** Fügen Sie den MQTT-Broker als Komponente hinzu oder fügen Sie ihn später manuell hinzu. : Diese Entscheidung wirkt sich auf das Authentifizierungs schema aus, das Sie mit dem Broker verwenden können. Durch manuelles Hinzufügen eines Brokers wird der Broker von AWS IoT Greengrass entkoppelt und jedes unterstützte Authentifizierungs schema des Brokers aktiviert. Die von AWS bereitges tellten Broker-Ko mponenten verfügen über vordefinierte Authentifizierungs schemata. Weitere	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Informationen finden Sie unter MQTT 3.1.1 Broker (Moquette) und MQTT 5 Broker (EMQX).	
Aktualisieren Sie den MQTT-Client.	Der Beispielcode verwendet keine Authentifizierung, da die Komponente eine lokale Verbindung zum Broker herstellt. Wenn sich Ihr Szenario unterscheidet, aktualisieren Sie den MQTT-Client-Bereich nach Bedarf. Gehen Sie zusätzlich wie folgt vor: 1. Aktualisieren Sie die MQTT-Themen im Abonnement. 2. Aktualisieren Sie den MQTT-Nachrichtenparser nach Bedarf, da sich die Nachrichten aus den einzelnen Quellen unterscheiden können.	App-Developer

Fügen Sie die Komponente dem AWS IoT Greengrass Version 2-Kerngerät hinzu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Bereitstellung des Kerngeräts.	Wenn die Bereitstellung des AWS IoT Greengrass Version 2-Kerngeräts bereits	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	vorhanden ist, überarbeiten Sie die Bereitstellung. Wenn die Bereitstellung nicht existiert, erstellen Sie eine neue Bereitstellung. Um der Komponente den richtigen Namen zu geben, aktualisieren Sie die Log Manager-Konfiguration für die neue Komponente (falls erforderlich) auf der Grundlage der folgenden Kriterien: `{ "logsUploaderConfiguration": { "systemLogsConfiguration": { ... }, "componentLogsConfigurationMap": { "<com.iot.ingest.parquet>": { "minimumLogLevel": "INFO", "diskSpaceLimit": "20", "diskSpaceLimitUnit": "MB", "deleteLogFileAfterCloudUpload": "false" } ... } }, ...`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"periodicUploadInt ervalSec": "300" }</pre> Schließen Sie abschließ end die Überarbeitung der Bereitstellung für Ihr AWS IoT Greengrass-Kerngerät ab.	

Überprüfen Sie die Datenaufnahme in den S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Protokolle für das AWS IoT Greengrass-Volume.	Überprüfen Sie Folgendes: • Der MQTT-Client wurde erfolgreich mit dem lokalen MQTT-Broker verbunden. • Der MQTT-Client hat die richtigen Themen abonniert. • Der Broker erhält Nachricht en über Sensoraktualisieru ngen zu den MQTT-Them en. • Die Komprimierung von Parkett erfolgt in jedem periodischen Intervall.	App-Developer
Überprüfen Sie den S3-Bucket .	Überprüfen Sie, ob die Daten in den S3-Bucket hochgelad en werden. Sie können sehen, wie die Dateien zu jedem Zeitpunkt hochgeladen werden.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie können auch überprüfen, ob die Daten in den S3-Bucket hochgeladen wurden, indem Sie die Daten im nächsten Abschnitt abfragen.	

Abfragen von Athena einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Datenbank und eine Tabelle.	1. Erstellen Sie eine AWS Glue Glue-Datenbank (falls erforderlich). 2. Erstellen Sie eine Tabelle in AWS Glue manuell oder indem Sie einen Crawler in AWS Glue ausführen.	App-Developer
Gewähren Sie Athena Zugriff auf die Daten.	1. Aktualisieren Sie die Berechtigungen, damit Athena auf den S3-Bucket zugreifen kann. Weitere Informationen finden Sie unter Detaillierter Zugriff auf Datenbanken und Tabellen im AWS Glue Glue-Datenkatalog in der Athena-Dokumentation. 2. Fragen Sie die Tabelle in Ihrer Datenbank ab.	App-Developer

Fehlerbehebung

Problem	Lösung
Der MQTT-Client kann keine Verbindung herstellen	• Überprüfen Sie die Berechtigungen auf dem MQTT-Broker. Wenn Sie einen MQTT-Broker von AWS haben, finden Sie weitere Informationen unter MQTT 3.1.1 Broker (Moquette) und MQTT 5 Broker (EMQX). • Überprüfen Sie die Anmeldeinformationen auf dem MQTT-Client. Wenn Sie einen MQTT-Broker von AWS haben, finden Sie weitere Informationen unter MQTT 3.1.1 Broker (Moquette) und MQTT 5 Broker (EMQX).
Der MQTT-Client kann nicht abonnieren	Überprüfen Sie die Berechtigungen auf dem MQTT-Broker. Wenn Sie einen MQTT-Broker von AWS haben, finden Sie weitere Informationen unter MQTT 3.1.1 Broker (Moquette) und MQTT 5 Broker (EMQX).
Parquet-Dateien werden nicht erstellt	• Stellen Sie sicher, dass die MQTT-Themen korrekt sind. • Stellen Sie sicher, dass die MQTT-Nachrichten von den Sensoren das richtige Format haben.
Objekte werden nicht in den S3-Bucket hochgeladen	• Stellen Sie sicher, dass Sie über Internet- und Endpunktkonnektivität verfügen. • Stellen Sie sicher, dass die Ressourcenrichtlinie für Ihren S3-Bucket korrekt ist. • Überprüfen Sie die Berechtigungen für die Kerngeräterolle AWS IoT Greengrass Version 2.

Zugehörige Ressourcen

- DataFrame(Pandas-Dokumentation)
- Apache Parquet-Dokumentation (Parquet-Dokumentation)
- Entwickeln von AWS IoT Greengrass-Komponenten (AWS IoT Greengrass-Entwicklerhandbuch, Version 2)
- Bereitstellen von AWS IoT Greengrass-Komponenten auf Geräten (AWS IoT Greengrass Developer Guide, Version 2)
- Interagieren Sie mit lokalen IoT-Geräten (AWS IoT Greengrass Developer Guide, Version 2)
- MQTT 3.1.1 Broker (Moquette) (AWS IoT Greengrass Entwicklerhandbuch, Version 2)
- MQTT 5-Broker (EMQX) (AWS IoT Greengrass-Entwicklerhandbuch, Version 2)

Zusätzliche Informationen

Kostenanalyse

Das folgende Kostenanalyseszenario zeigt, wie sich der in diesem Muster behandelte Ansatz zur Datenaufnahme auf die Datenaufnahmekosten in der AWS-Cloud auswirken kann. Die Preisbeispiele in diesem Szenario basieren auf den Preisen zum Zeitpunkt der Veröffentlichung. Die Preise sind freibleibend. Darüber hinaus können Ihre Kosten je nach AWS-Region, AWS-Servicekontingenten und anderen Faktoren im Zusammenhang mit Ihrer Cloud-Umgebung variieren.

Eingangssignal eingestellt

Diese Analyse verwendet die folgenden Eingangssignale als Grundlage für den Vergleich der IoT-Aufnahmekosten mit anderen verfügbaren Alternativen.

Anzahl der Signale	Frequency (Frequenz)	Daten pro Signal
125	25 Hz	8 Bytes

In diesem Szenario empfängt das System 125 Signale. Jedes Signal ist 8 Byte groß und tritt alle 40 Millisekunden (25 Hz) auf. Diese Signale können einzeln oder gruppiert in einer gemeinsamen Nutzlast übertragen werden. Sie haben die Möglichkeit, diese Signale nach Ihren Bedürfnissen aufzuteilen und zu bündeln. Sie können auch die Latenz bestimmen. Die Latenz besteht aus dem Zeitraum für den Empfang, die Akkumulation und die Aufnahme der Daten.

Zu Vergleichszwecken basiert der Aufnahmevorgang für dieses Szenario auf der `us-east-1` AWS-Region. Der Kostenvergleich gilt nur für AWS-Services. Andere Kosten, wie Hardware oder Konnektivität, werden bei der Analyse nicht berücksichtigt.

Kostenvergleiche

Die folgende Tabelle zeigt die monatlichen Kosten in US-Dollar (USD) für jede Aufnahmemethode.

Methode	Monatliche Kosten
SiteWiseAWS-IoT*	331,77 USD
AWS IoT SiteWise Edge mit Datenverarbeitungspaket (alle Daten werden am Netzwerkrand aufbewahrt)	200 USD
AWS IoT Core- und Amazon S3 S3-Regeln für den Zugriff auf Rohdaten	84,54 USD
Parquet-Dateikomprimierung am Edge und Hochladen auf Amazon S3	0.5 USD

*Daten müssen heruntergerechnet werden, um die Servicekontingenten einzuhalten. Das bedeutet, dass es bei dieser Methode zu Datenverlusten kommt.

Alternative Methoden

In diesem Abschnitt werden die entsprechenden Kosten für die folgenden alternativen Methoden aufgeführt:

- AWS IoT SiteWise — Jedes Signal muss in einer individuellen Nachricht hochgeladen werden. Daher beträgt die Gesamtzahl der Nachrichten pro Monat 125×25×3600×24×30 oder 8,1 Milliarden Nachrichten pro Monat. AWS IoT SiteWise kann jedoch nur 10 Datenpunkte pro Sekunde pro Eigenschaft verarbeiten. Unter der Annahme, dass die Daten auf 10 Hz heruntergerechnet werden, wird die Anzahl der Nachrichten pro Monat auf 125×10×3600×24×30 oder 3,24 Milliarden reduziert. Wenn Sie die Publisher-Komponente verwenden, die Messungen in Gruppen von 10 zusammenfasst (bei 1 USD pro Million Nachrichten), fallen monatliche Kosten in Höhe von 324 USD pro Monat an. Unter der Annahme, dass jede Nachricht 8 Byte (1 Kb/125) umfasst, sind das 25,92 GB Datenspeicher. Dadurch fallen monatliche Kosten in Höhe von 7,77 USD pro Monat an.

Die Gesamtkosten für den ersten Monat betragen 331,77 USD und steigen jeden Monat um 7,77 USD.

- AWS IoT SiteWise Edge mit Datenverarbeitungspaket, einschließlich aller Modelle und Signale, die vollständig am Edge verarbeitet werden (d. h. keine Cloud-Aufnahme) — Sie können das Datenverarbeitungspaket als Alternative verwenden, um die Kosten zu senken und alle Modelle zu konfigurieren, die am Edge berechnet werden. Dies kann nur zur Speicherung und Visualisierung funktionieren, auch wenn keine echte Berechnung durchgeführt wird. In diesem Fall ist es notwendig, leistungsstarke Hardware für das Edge-Gateway zu verwenden. Es gibt feste Kosten von 200 USD pro Monat.
- Direkte Aufnahme in AWS IoT Core durch MQTT und eine IoT-Regel zum Speichern der Rohdaten in Amazon S3 — Unter der Annahme, dass alle Signale in einer gemeinsamen Nutzlast veröffentlicht werden, beträgt die Gesamtzahl der auf AWS IoT Core veröffentlichten Nachrichten 25×3600×24×30 oder 64,8 Millionen pro Monat. Bei 1 USD pro Million Nachrichten sind das monatliche Kosten von 64,8 USD pro Monat. Bei 0,15 USD pro Million Regelaktivierungen und einer Regel pro Nachricht fallen dadurch monatliche Kosten in Höhe von 19,44 USD pro Monat an. Bei einem Preis von 0,023 USD pro GB Speicherplatz in Amazon S3 fallen weitere 1,5 USD pro Monat an (was jeden Monat steigt, um den neuen Daten Rechnung zu tragen). Die Gesamtkosten für den ersten Monat belaufen sich auf 84,54 USD und steigen jeden Monat um 1,5 USD.
- Komprimieren von Daten am Edge in einer Parquet-Datei und Hochladen auf Amazon S3 (vorgeschlagene Methode) — Das Komprimierungsverhältnis hängt vom Datentyp ab. Bei denselben Industriedaten, die für MQTT getestet wurden, belaufen sich die Gesamtausgabedaten für einen ganzen Monat auf 1,2 Gb. Das kostet 0,03 USD pro Monat. Die in anderen Benchmarks beschriebenen Kompressionsraten (unter Verwendung zufälliger Daten) liegen in der Größenordnung von 66 Prozent (was eher einem Worst-Case-Szenario entspricht). Die Gesamtdaten belaufen sich auf 21 GB und kosten 0,5 USD pro Monat.

Parkett-Dateigenerator

Das folgende Codebeispiel zeigt die Struktur eines Parquet-Dateigenerators, der in Python geschrieben ist. Das Codebeispiel dient nur zur Veranschaulichung und funktioniert nicht, wenn es in Ihre Umgebung eingefügt wird.

```
import queue
import paho.mqtt.client as mqtt
import pandas as pd

#queue for decoupling the MQTT thread
```

```
messageQueue = queue.Queue()
client = mqtt.Client()
streammanager = StreamManagerClient()

def feederListener(topic, message):
    payload = {
        "topic" : topic,
        "payload" : message,
    }
    messageQueue.put_nowait(payload)

def on_connect(client_instance, userdata, flags, rc):
    client.subscribe("#",qos=0)

def on_message(client, userdata, message):
    feederListener(topic=str(message.topic),
 message=str(message.payload.decode("utf-8")))


filename = "tempfile.parquet"
streamname = "mystream"
destination_bucket= "amzn-s3-demo-bucket"
keyname="mykey"
period= 60

client.on_connect = on_connect
client.on_message = on_message
streammanager.create_message_stream(
            MessageStreamDefinition(name=streamname,
 strategy_on_full=StrategyOnFull.OverwriteOldestData)
        )


while True:
   try:
       message = messageQueue.get(timeout=myArgs.mqtt_timeout)
   except (queue.Empty):
       logger.warning("MQTT message reception timed out")

   currentTimestamp = getCurrentTime()
   if currentTimestamp >= nextUploadTimestamp:
       df = pd.DataFrame.from_dict(accumulator)
       df.to_parquet(filename)
```

```
      s3_export_task_definition = S3ExportTaskDefinition(input_url=filename,
bucket=destination_bucket, key=key_name)
      streammanager.append_message(streamname,
Util.validate_and_serialize_to_json_bytes(s3_export_task_definition))
      accumulator = {}
      nextUploadTimestamp += period
  else:
       accumulator.append(message)
```

Starten Sie einen Spark-Job in einem transienten EMR-Cluster mithilfe einer Lambda-Funktion

Erstellt von Dhrubajyoti Mukherjee (AWS)

Übersicht

Dieses Muster verwendet die Amazon RunJobFlow EMR-API-Aktion, um einen transienten Cluster zu starten, um einen Spark-Job von einer Lambda-Funktion aus auszuführen. Ein transienter EMR-Cluster ist so konzipiert, dass er beendet wird, sobald der Job abgeschlossen ist oder wenn ein Fehler auftritt. Ein transienter Cluster bietet Kosteneinsparungen, da er nur während der Rechenzeit ausgeführt wird, und er bietet Skalierbarkeit und Flexibilität in einer Cloud-Umgebung.

Der transiente EMR-Cluster wird mithilfe der Boto3-API und der Programmiersprache Python in einer Lambda-Funktion gestartet. Die Lambda-Funktion, die in Python geschrieben ist, bietet die zusätzliche Flexibilität, den Cluster bei Bedarf zu initiieren.

Um ein Beispiel für eine Batchberechnung und -ausgabe zu demonstrieren, startet dieses Muster einen Spark-Job in einem EMR-Cluster von einer Lambda-Funktion aus und führt eine Batch-Berechnung anhand der Beispielvertriebsdaten eines fiktiven Unternehmens durch. Die Ausgabe des Spark-Jobs wird eine Datei mit kommagetrennten Werten (CSV) in Amazon Simple Storage Service (Amazon S3) sein. Die Eingabedatendatei, die Spark-JAR-Datei, ein Codeausschnitt und eine CloudFormation AWS-Vorlage für eine Virtual Private Cloud (VPC) und AWS Identity and Access Management (IAM) -Rollen zur Ausführung der Berechnung werden als Anlage bereitgestellt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

Einschränkungen

- Aus dem Code kann jeweils nur ein Spark-Job initiiert werden.

Produktversionen

- Auf Amazon EMR 6.0.0 getestet

Architektur

Zieltechnologie-Stack

- Amazon EMR
- AWS Lambda
- Amazon S3
- Apache Spark

Zielarchitektur

Automatisierung und Skalierung

Um die Spark-EMR-Batchberechnung zu automatisieren, können Sie eine der folgenden Optionen verwenden.

- Implementieren Sie eine EventBridge Amazon-Regel, die die Lambda-Funktion in einem Cron-Zeitplan initiieren kann. Weitere Informationen finden Sie unter Tutorial: AWS Lambda Lambda-Funktionen planen mit EventBridge.
- Konfigurieren Sie Amazon S3 S3-Ereignisbenachrichtigungen so, dass die Lambda-Funktion bei Dateieingang ausgelöst wird.
- Übergeben Sie die Eingabeparameter über den Ereignistext und die Lambda-Umgebungsvariablen an die AWS-Lambda-Funktion.

Tools

AWS-Services

- Amazon EMR ist eine verwaltete Cluster-Plattform, die die Ausführung von Big-Data-Frameworks auf AWS vereinfacht, um große Datenmengen zu verarbeiten und zu analysieren.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere Tools

- Apache Spark ist eine mehrsprachige Analyse-Engine für die Verarbeitung großer Datenmengen.

Epen

Erstellen Sie die Amazon EMR- und Lambda IAM-Rollen und die VPC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Rollen und die VPC.	Wenn Sie bereits über die IAM-Rollen AWS Lambda und Amazon EMR und eine VPC verfügen, können Sie diesen Schritt überspringen. Um den Code auszuführen, benötigen sowohl der EMR-Cluster als auch die Lambda-Funktion IAM-Rollen. Der EMR-Cluster benötigt außerdem eine VPC mit einem öffentlichen Subnetz oder ein privates Subnetz mit einem NAT-Gateway. Um automatisch alle IAM-Rolle n und eine VPC zu erstellen , stellen Sie die angehängte CloudFormation AWS-Vorla ge unverändert bereit, oder Sie können die Rollen und die VPC manuell erstellen, wie im Abschnitt Zusätzliche Informati onen angegeben.	Cloud-Architekt
Notieren Sie sich die CloudFormation Ausgabesc hlüssel der AWS-Vorlage.	Nachdem die CloudFormation Vorlage erfolgreich bereitges tellt wurde, navigieren Sie in der CloudFormation AWS-	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Konsole zur Registerkarte Outputs. Beachten Sie die fünf Ausgabetasten: • `S3Bucket` • `LambdaExecutionRole` • `ServiceRole` • `JobFlowRole` • `Ec2SubnetId` Sie werden die Werte aus diesen Schlüsseln verwenden , wenn Sie die Lambda-Fu nktion erstellen.	

Laden Sie die Spark-.jar-Datei hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Spark-.jar-Datei hoch.	Laden Sie die Spark-.jar-Datei in den S3-Bucket hoch, den der CloudFormation AWS-Stack erstellt hat. Der Bucket-Name ist derselbe wie der Ausgabeschlüssel`S3Bucket`.	Allgemeines AWS

Erstellen Sie die Lambda-Funktion, um den EMR-Cluster zu starten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Lambda-Fu nktion.	Erstellen Sie auf der Lambda-Konsole eine Python 3.9+ Lambda-Funktion mit einer	Dateningenieur, Cloud-Ing enieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ausführungsrolle. Die Ausführungsrollenrichtlinie muss es Lambda ermöglichen, einen EMR-Cluster zu starten. (Siehe die beigefügte CloudFormation AWS-Vorlage.)	
Kopieren Sie den Code und fügen Sie ihn ein.	Ersetzen Sie den Code in der `lambda_function.py` Datei durch den Code aus dem Abschnitt Zusätzliche Informationen dieses Musters.	Dateningenieur, Cloud-Ingenieur
Ändern Sie die Parameter im Code.	Folgen Sie den Kommentaren im Code, um die Parameterwerte so zu ändern, dass sie Ihrem AWS-Konto entsprechen.	Dateningenieur, Cloud-Ingenieur
Starten Sie die Funktion, um den Cluster zu initiieren.	Starten Sie die Funktion, um die Erstellung eines transienten EMR-Clusters mit der bereitgestellten Spark-.jar-Datei zu initiieren. Sie führt den Spark-Job aus und wird automatisch beendet, wenn der Job abgeschlossen ist.	Dateningenieur, Cloud-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den EMR-Clusterstatus.	Nachdem der EMR-Clust er initiiert wurde, wird er in der Amazon EMR-Konso le unter der Registerkarte Cluster angezeigt. Alle Fehler beim Starten des Clusters oder beim Ausführen des Jobs können entsprechend überprüft werden.	Dateningenieur, Cloud-Ing enieur

Richten Sie die Beispieldemo ein und führen Sie sie aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Spark-.jar-Datei hoch.	Laden Sie die Spark-.jar-Datei aus dem Bereich Anlagen herunter und laden Sie sie in den S3-Bucket hoch.	Dateningenieur, Cloud-Ing enieur
Laden Sie den Eingabeda tensatz hoch.	Laden Sie die angehängte `fake_sales_data.csv` Datei in den S3-Bucket hoch.	Dateningenieur, Cloud-Ing enieur
Fügen Sie den Lambda-Co de ein und ändern Sie die Parameter.	Kopieren Sie den Code aus dem Abschnitt Tools und fügen Sie den Code in eine Lambda-Funktion ein, wodurch die `lambda_fu nction.py` Codedatei ersetzt wird. Ändern Sie die Parameterwerte so, dass sie Ihrem Konto entsprechen.	Dateningenieur, Cloud-Ing enieur
Starten Sie die Funktion und überprüfen Sie die Ausgabe.	Nachdem die Lambda-Fu nktion den Cluster mit dem	Dateningenieur, Cloud-Ing enieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bereitgestellten Spark-Job initiiert hat, generiert sie eine .csv-Datei im S3-Bucket.	

Zugehörige Ressourcen

- Spark bauen
- Apache Spark und Amazon EMR
- Boto3 Docs run_job_flow-Dokumentation
- Informationen und Dokumentation zu Apache Spark

Zusätzliche Informationen

Code

```
"""
Copy paste the following code in your Lambda function. Make sure to change the
 following key parameters for the API as per your account

-Name (Name of Spark cluster)
-LogUri (S3 bucket to store EMR logs)
-Ec2SubnetId (The subnet to launch the cluster into)
-JobFlowRole (Service role for EC2)
-ServiceRole (Service role for Amazon EMR)

The following parameters are additional parameters for the Spark job itself. Change the
 bucket name and prefix for the Spark job (located at the bottom).

-s3://your-bucket-name/prefix/lambda-emr/SparkProfitCalc.jar (Spark jar file)
-s3://your-bucket-name/prefix/fake_sales_data.csv (Input data file in S3)
-s3://your-bucket-name/prefix/outputs/report_1/ (Output location in S3)
"""
import boto3

client = boto3.client('emr')
```

```
def lambda_handler(event, context):
    response = client.run_job_flow(
        Name='spark_job_cluster',
        LogUri='s3://your-bucket-name/prefix/logs',
        ReleaseLabel='emr-6.0.0',
        Instances={
            'MasterInstanceType': 'm5.xlarge',
            'SlaveInstanceType': 'm5.large',
            'InstanceCount': 1,
            'KeepJobFlowAliveWhenNoSteps': False,
            'TerminationProtected': False,
            'Ec2SubnetId': 'subnet-XXXXXXXXXXXXX'
        },
        Applications=[{'Name': 'Spark'}],
        Configurations=[
            {'Classification': 'spark-hive-site',
             'Properties': {
                 'hive.metastore.client.factory.class':
 'com.amazonaws.glue.catalog.metastore.AWSGlueDataCatalogHiveClientFactory'}
             }
        ],
        VisibleToAllUsers=True,
        JobFlowRole='EMRLambda-EMREC2InstanceProfile-XXXXXXXXX',
        ServiceRole='EMRLambda-EMRRole-XXXXXXXXX',
        Steps=[
            {
                'Name': 'flow-log-analysis',
                'ActionOnFailure': 'TERMINATE_CLUSTER',
                'HadoopJarStep': {
                    'Jar': 'command-runner.jar',
                    'Args': [
                        'spark-submit',
                        '--deploy-mode', 'cluster',
                        '--executor-memory', '6G',
                        '--num-executors', '1',
                        '--executor-cores', '2',
                        '--class', 'com.aws.emr.ProfitCalc',
                        's3://your-bucket-name/prefix/lambda-emr/SparkProfitCalc.jar',
                        's3://your-bucket-name/prefix/fake_sales_data.csv',
                        's3://your-bucket-name/prefix/outputs/report_1/'
                    ]
                }
            }
        ]
```

```
    )
```

IAM-Rollen und VPC-Erstellung

Um den EMR-Cluster in einer Lambda-Funktion zu starten, sind eine VPC und IAM-Rollen erforderlich. Sie können die VPC- und IAM-Rollen mithilfe der CloudFormation AWS-Vorlage im Abschnitt Anlagen dieses Musters einrichten, oder Sie können sie mithilfe der folgenden Links manuell erstellen.

Die folgenden IAM-Rollen sind für die Ausführung von Lambda und Amazon EMR erforderlich.

Lambda-Ausführungsrolle

Die Ausführungsrolle einer Lambda-Funktion gewährt ihr die Erlaubnis, auf AWS-Services und -Ressourcen zuzugreifen.

Servicerolle für Amazon EMR

Die Amazon EMR-Rolle definiert die zulässigen Aktionen für Amazon EMR bei der Bereitstellung von Ressourcen und der Ausführung von Service-Level-Aufgaben, die nicht im Kontext einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance ausgeführt werden, die innerhalb eines Clusters ausgeführt wird. Die Service-Rolle wird beispielsweise verwendet, um EC2 Instances bereitzustellen, wenn ein Cluster gestartet wird.

Servicerolle für EC2 Instanzen

Die Servicerolle für EC2 Cluster-Instances (auch EC2 Instance-Profil für Amazon EMR genannt) ist eine spezielle Art von Servicerolle, die jeder EC2 Instance in einem Amazon EMR-Cluster zugewiesen wird, wenn die Instance gestartet wird. Anwendungsprozesse, die auf Apache Hadoop ausgeführt werden, übernehmen diese Rolle für Berechtigungen zur Interaktion mit anderen AWS-Services.

VPC- und Subnetzerstellung

Sie können eine VPC von der VPC-Konsole aus erstellen.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Migrieren Sie Apache Cassandra-Workloads mithilfe von AWS Glue zu Amazon Keyspaces

Erstellt von Nikolai Kolesnikov (AWS), Karthiga Priya Chandran (AWS) und Samir Patel (AWS)

Übersicht

Dieses Muster zeigt Ihnen, wie Sie Ihre vorhandenen Apache Cassandra-Workloads mithilfe CQLReplicator von AWS Glue zu Amazon Keyspaces (für Apache Cassandra) migrieren. Sie können CQLReplicator auf AWS Glue verwenden, um die Replikationsverzögerung bei der Migration Ihrer Workloads auf wenige Minuten zu reduzieren. Sie erfahren auch, wie Sie einen Amazon Simple Storage Service (Amazon S3) -Bucket verwenden, um Daten zu speichern, die für die Migration erforderlich sind, einschließlich Apache Parquet-Dateien, Konfigurationsdateien und Skripts. Bei diesem Muster wird davon ausgegangen, dass Ihre Cassandra-Workloads auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances in einer Virtual Private Cloud (VPC) gehostet werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Cassandra-Cluster mit einer Quelltabelle
- Zieltabelle in Amazon Keyspaces zur Replikation der Arbeitslast
- S3-Bucket zum Speichern von Parquet-Zwischendateien, die inkrementelle Datenänderungen enthalten
- S3-Bucket zum Speichern von Job-Konfigurationsdateien und Skripten

Einschränkungen

- CQLReplicator auf AWS Glue benötigt einige Zeit, um Datenverarbeitungseinheiten (DPUs) für die Cassandra-Workloads bereitzustellen. Die Replikationsverzögerung zwischen dem Cassandra-Cluster und dem Zielschlüsselraum und der Zieltabelle in Amazon Keyspaces wird wahrscheinlich nur wenige Minuten andauern.

Architektur

Quelltechnologie-Stack

- Apache Cassandra
- DataStax Server
- ScyllaDB

Zieltechnologie-Stack

- Amazon Keyspaces

Migrationsarchitektur

Das folgende Diagramm zeigt eine Beispielarchitektur, bei der ein Cassandra-Cluster auf EC2 Instanzen gehostet und auf drei Availability Zones verteilt ist. Die Cassandra-Knoten werden in privaten Subnetzen gehostet.

Das Diagramm zeigt den folgenden Workflow:

1. Eine benutzerdefinierte Servicerolle bietet Zugriff auf Amazon Keyspaces und den S3-Bucket.
2. Ein AWS Glue Glue-Job liest die Jobkonfiguration und die Skripts im S3-Bucket.
3. Der AWS Glue Glue-Job stellt über Port 9042 eine Verbindung her, um Daten aus dem Cassandra-Cluster zu lesen.
4. Der AWS Glue Glue-Job stellt über Port 9142 eine Verbindung her, um Daten in Amazon Keyspaces zu schreiben.

Tools

AWS-Services und -Tools

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS CloudShell ist eine browserbasierte Shell, mit der Sie AWS-Services mithilfe der AWS-Befehlszeilenschnittstelle (AWS CLI) und einer Reihe vorinstallierter Entwicklungstools verwalten können.
- AWS Glue ist ein vollständig verwalteter ETL-Service, mit dem Sie Daten zuverlässig kategorisieren, bereinigen, anreichern und zwischen Datenspeichern und Datenströmen verschieben können.

- Amazon Keyspaces (für Apache Cassandra) ist ein verwalteter Datenbankservice, der Sie bei der Migration, Ausführung und Skalierung Ihrer Cassandra-Workloads in der AWS-Cloud unterstützt.

Code

Der Code für dieses Muster ist im Repository verfügbar. GitHub CQLReplicator

Bewährte Methoden

- Um die erforderlichen AWS Glue Glue-Ressourcen für die Migration zu ermitteln, schätzen Sie die Anzahl der Zeilen in der Cassandra-Quelltabelle. Zum Beispiel 250.000 Zeilen pro 0,25 DPU (2 VCPUs, 4 GB Arbeitsspeicher) mit 84 GB Festplatte.
- Wärmen Sie Amazon Keyspaces-Tabellen vor der Ausführung vor. CQLReplicator Beispielsweise können acht CQLReplicator Kacheln (AWS Glue Glue-Jobs) bis zu 22 K WCUs pro Sekunde schreiben, sodass das Ziel auf 25-30 K WCUs pro Sekunde vorgewärmt werden sollte.
- Um die Kommunikation zwischen AWS Glue Glue-Komponenten zu ermöglichen, verwenden Sie eine selbstreferenzierende Regel für eingehenden Datenverkehr für alle TCP-Ports in Ihrer Sicherheitsgruppe.
- Verwenden Sie die Strategie für den inkrementellen Datenverkehr, um die Migrationslast im Laufe der Zeit zu verteilen.

Epen

Bereitstellen CQLReplicator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Zielschlü sselraum und eine Zieltabelle.	1. Erstellen Sie einen Schlüsselraum und eine Tabelle in Amazon Keyspaces. Weitere Informationen zur Schreibkapazität finden Sie unter Berechnungen von Schreibeinheiten im Abschnitt Zusätzlic	App-Besitzer, AWS-Admin istrator, DBA, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	he Informationen dieses Musters. Sie können einen Schlüsselraum auch mithilfe der Cassandra Query Language (CQL) erstellen. Weitere Informationen finden Sie unter Erstellen eines Schlüsselraums mithilfe von CQL im Abschnitt Zusätzliche Informationen dieses Musters. **Note** Nachdem Sie die Tabelle erstellt haben, sollten Sie erwägen, die Tabelle in den On-Demand-Kapazitätsmodus umzuschalten, um unnötige Gebühren zu vermeiden. 2. Führen Sie das folgende Skript aus, um auf den Durchsatzmodus zu aktualisieren: `ALTER TABLE target_keyspace.target_table WITH CUSTOM_PR`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`OPERTIES = { 'capacity_mode': { 'throughput_mode': 'PAY_PER_REQUEST'} }`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Cassandra-Treiber für die Verbindung mit Cassandra.	Verwenden Sie das folgende Konfigurationsskript: `Datastax-java-driver { basic.request.consistency = “LOCAL_QUORUM” basic.contact-points = [“127.0.0.1:9042”] advanced.reconnect-on-init = true basic.load-balancing-policy { local-datacenter = “datacenter1” } advanced.auth-provider = { class = PlainTextAuthProvider username = “user-at-sample” password = “S@MPLE=PASSWORD=” } }` **Note** Das vorherige Skript verwendet den Spark Cassandra Connector. Weitere Informationen finden Sie in der Referenzkonfiguration für Cassandra.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Cassandra-Treiber für die Verbindung mit Amazon Keyspaces.	Verwenden Sie das folgende Konfigurationsskript: `datastax-java-driver { basic { load-balancing-pol icy { local-datacenter = us-west-2 } contact-points = ["cassandr a.us-west-2.amazon aws.com:9142"] request { page-size = 2500 timeout = 360 seconds consistency = LOCAL_QUORUM } } advanced { control-connection { timeout = 360 seconds } session-leak.thres hold = 6 connection { connect-timeout = 360 seconds init-query-timeout = 360 seconds warn-on-init-error = false } auth-provider = { class = software. aws.mcs.auth.SigV4 AuthProvider`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> aws-region = us-
	west-2
	 }
	
	 ssl-engine-factory {
	  class = DefaultSs
	lEngineFactory
	  }
	  }
	}</pre>
	Note
	Das vorherige Skript verwendet den Spark Cassandra Connector . Weitere Informati onen finden Sie in der Referenzkonfiguration für Cassandra.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle für den AWS Glue Glue-Job.	Erstellen Sie eine neue AWS-Servicerolle `glue-cassandra-migration` mit dem Namen AWS Glue als vertrauenswürdige Entität. **Note** Das `glue-cassandra-migration` sollte Lese- und Schreibzugriff auf den S3-Bucket und Amazon Keyspaces bieten. Der S3-Bucket enthält die .jar-Dateien, die Konfigurationsdateien für Amazon Keyspaces und Cassandra sowie die Parquet-Zwischendateien. Er enthält beispielsweise die verwalteten Richtlinien `AWSGlueServiceRole`, `AmazonS3FullAccess`, und `AmazonKeyspacesFullAccess`.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

CQLReplicator In AWS herunterladen CloudShell.	Laden Sie das Projekt in Ihren Home-Ordner herunter, indem Sie den folgenden Befehl ausführen:
	`git clone https://github.com/aws-samples/cql-replicator .git`
	`cd cql-replicator/glue`
	`# Only for AWS CloudShell, the bc package includes bc and dc. Bc is an arbitrary precision numeric processing arithmetic language`
	`sudo yum install bc -y`	

Ändern Sie die Referenzkonfigurationsdateien.	Kopieren `Keyspaces Connector.conf` Sie `CassandraConnector .conf` und in das `../glue/conf` Verzeichnis im Projektordner.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Initiieren Sie den Migration sprozess.	Der folgende Befehl initialisiert die CQLReplicator Umgebung. Die Initialisierung umfasst das Kopieren von .jar-Artefakten und das Erstellen eines AWS Glue Glue-Connectors, eines S3-Buckets, eines AWS Glue Glue-Jobs, des `migration` Schlüsselraums und der Tabelle: `ledger`
	
	`cd cql-replicator/glue/bin`
	`./cqlreplicator --state init --sg '"sg-1","sg-2"' \ --subnet "subnet-XXXXXXXXXXXX" \ --az us-west-2a --region us-west-2 \ --glue-iam-role glue-cassandra-migration \ --landing-zone s3://cql-replicator-1234567890-us-west-2`
	
	Das Skript enthält die folgenden Parameter:
	
	• `--sg`— Die Sicherheitsgruppen, die den Zugriff auf den Cassandra-Cluster von AWS Glue aus ermöglichen und die
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	selbstreferenzierende Regel für eingehenden Datenverkehr enthalten • `--subnet`— Das Subnetz, zu dem der Cassandra-Cluster gehört • `--az`— Die Availability Zone des Subnetzes • `--region`— Die AWS-Region, in der der Cassandra-Cluster bereitgestellt wird • `--glue-iam-role` — Die IAM-Rollenberechtigungen, die AWS Glue übernehmen kann, wenn Sie Amazon Keyspaces und Amazon S3 in Ihrem Namen aufrufen • `--landing zone`— Ein optionaler Parameter für die Wiederverwendung eines S3-Buckets (Wenn Sie keinen Wert für den `--landing zone` Parameter angeben, versucht der `init` Prozess, einen neuen Bucket zum Speichern der Konfigurationsdateien, .jar-Artefakte und Zwischendateien zu erstellen.)	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Bereitstellung.	Nachdem Sie den vorherigen Befehl ausgeführt haben, sollte das AWS-Konto Folgendes enthalten: • Der CQLReplicator AWS Glue-Job und der AWS Glue Glue-Konnektor in AWS Glue • Der S3-Bucket, in dem die Artefakte gespeichert sind • Der Zielschlüsselraum `migration` und die `ledger` Tabelle in Amazon Keyspaces	AWS DevOps

Lauf CQLReplicator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den Migrationsprozess.	Um mit CQLReplicator AWS Glue zu arbeiten, müssen Sie den `--state run` Befehl verwenden, gefolgt von einer Reihe von Parametern. Die genaue Konfiguration dieser Parameter wird in erster Linie von Ihren individuellen Migrationsanforderungen bestimmt. Diese Einstellungen können beispielsweise variieren, wenn Sie sich dafür entscheiden, TTL-Werte und Aktualisierungen (Time to	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Live) zu replizieren, oder wenn Sie Objekte, die 1 MB überschreiten, nach Amazon S3 auslagern. Führen Sie den folgenden Befehl aus, um die Arbeitsla st vom Cassandra-Cluster nach Amazon Keyspaces zu replizieren: `./cqlreplicator --state run --tiles 8 \ --landing-zone s3://cql-replicator-1234567890-us-west-2 \ --region us-west-2 \ --src-keyspace source_keyspace \ --src-table source_table \ --trg-keyspace taget_keyspace \ --writetime-column column_name \ --trg-table target_table --inc-traffic` Ihr Quellschlüsselraum und Ihre Tabelle befinden sich `source_keyspace.source_table` im Cassandra	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	-Cluster. Ihr Zielschlüsselraum und Ihre Zieltabelle befinden sich `target_keyspace.target_table` in Amazon Keyspaces. Der Parameter `--inc-traffic` verhindert, dass inkrementeller Verkehr den Cassandra-Cluster und Amazon Keyspaces mit einer hohen Anzahl von Anfragen überlastet. Um Updates zu replizieren, fügen Sie sie zu Ihrer Befehlszeile hinzu`--writetime-column regular_column_name` . Die reguläre Spalte wird als Quelle für den Schreibzeitstempel verwendet.	

Überwachen Sie den Migrationsprozess

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie migrierte Cassandra-Zeilen während der historischen Migrationsphase.	Führen Sie den folgenden Befehl aus, um die Anzahl der Zeilen zu ermitteln, die während der Backfilling-Phase repliziert wurden: `./cqlreplicator --statestats \ --landing-zone s3://cql-`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`replicator-1234567890-us-west-2 \ --src-keyspace source_keyspace --src-table source_table --region us-west-2`	

Beenden Sie den Migrationsprozess

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie den `cqlreplicator` Befehl oder die AWS Glue Glue-Konsole.	Führen Sie den folgenden Befehl aus, um den Migration sprozess ordnungsgemäß zu beenden: `./cqlreplicator --state request-stop --tiles 8 \ --landing-zone s3://cql-replicator-1234567890-us-west-2 \ --region us-west-2 \ --src-keyspace source_keyspace --src-table source_table` Verwenden Sie die AWS Glue Glue-Konsole, um den Migrationsprozess sofort zu beenden.	AWS DevOps

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die bereitgestellten Ressourcen.	Der folgende Befehl löscht den AWS Glue Glue-Job, den Connector, den S3-Bucket und die Keyspaces-Tabelle `ledger`: `./cqlreplicator --state cleanup --landing-zone s3://cql-replicator-1234567890-us-west-2`	AWS DevOps

Fehlerbehebung

Problem	Lösung
AWS Glue Glue-Jobs schlugen fehl und gaben einen OOM-Fehler (Out of Memory) zurück.	1. Ändern Sie den Workertyp (Scale Up). Ändern Sie beispielsweise `G0.25X` zu `G.1X` oder `G.1X` zu `G.2X`. Sie können auch die Anzahl der DPUs pro AWS Glue Glue-Auftrag (Scale Out) in erhöhen CQLReplicator. 2. Starten Sie den Migrationsprozess an dem Punkt, an dem er unterbrochen wurde. Um fehlgeschlagene CQLReplicator Jobs neu zu starten, führen `--state run` Sie den Befehl erneut mit denselben Parametern aus.

Zugehörige Ressourcen

- CQLReplicator mit AWS Glue README.MD

- Dokumentation zu AWS Glue
- Dokumentation zu Amazon Keyspaces
- Apache Cassandra

Zusätzliche Informationen

Überlegungen zur Migration

Sie können AWS Glue verwenden, um Ihren Cassandra-Workload zu Amazon Keyspaces zu migrieren, während Ihre Cassandra-Quelldatenbanken während des Migrationsprozesses voll funktionsfähig bleiben. Nach Abschluss der Replikation können Sie wählen, ob Sie Ihre Anwendungen mit minimaler Replikationsverzögerung (weniger als Minuten) zwischen dem Cassandra-Cluster und Amazon Keyspaces auf Amazon Keyspaces übertragen möchten. Um die Datenkonsistenz aufrechtzuerhalten, können Sie auch eine ähnliche Pipeline verwenden, um die Daten von Amazon Keyspaces zurück in den Cassandra-Cluster zu replizieren.

Schreiben Sie Berechnungen für Einheiten

Stellen Sie sich als Beispiel vor, Sie beabsichtigen, innerhalb einer Stunde 500.000.000 mit einer Zeilengröße von 1 KiB zu schreiben. Die Gesamtzahl der Amazon Keyspaces-Schreibeinheiten (WCUs), die Sie benötigen, basiert auf dieser Berechnung:

```
(number of rows/60 mins 60s) 1 WCU per row = (500,000,000/(60*60s) * 1 WCU)
= 69,444 WCUs required
```

69.444 WCUs pro Sekunde ist der Tarif für 1 Stunde, aber Sie könnten etwas mehr Aufwandspolster hinzufügen. `69,444 * 1.10 = 76,388 WCUs`Hat zum Beispiel 10 Prozent Gemeinkosten.

Erstellen Sie einen Schlüsselraum mithilfe von CQL

Führen Sie die folgenden Befehle aus, um einen Schlüsselraum mithilfe von CQL zu erstellen:

```
CREATE KEYSPACE target_keyspace WITH replication = {'class': 'SingleRegionStrategy'}
CREATE TABLE target_keyspace.target_table ( userid uuid, level text, gameid int,
 description text, nickname text, zip text, email text, updatetime text, PRIMARY KEY
 (userid, level, gameid) ) WITH default_time_to_live = 0 AND CUSTOM_PROPERTIES =
 {'capacity_mode':{ 'throughput_mode':'PROVISIONED', 'write_capacity_units':76388,
 'read_capacity_units':3612 }} AND CLUSTERING ORDER BY (level ASC, gameid ASC)
```

Migrieren Sie Hadoop-Daten mithilfe WANdisco LiveData von Migrator zu Amazon S3

Erstellt von Tony Velcich

Übersicht

Dieses Muster beschreibt den Prozess für die Migration von Apache Hadoop-Daten von einem Hadoop Distributed File System (HDFS) zu Amazon Simple Storage Service (Amazon S3). Es verwendet WANdisco LiveData Migrator, um den Datenmigrationsprozess zu automatisieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Hadoop-Cluster-Edge-Knoten, auf dem LiveData Migrator installiert wird. Der Knoten sollte die folgenden Anforderungen erfüllen:
  - Mindestspezifikation: 4 CPUs, 16 GB RAM, 100 GB Speicher.
  - Netzwerk mit mindestens 2 Gbit/s.
  - Port 8081, auf den auf Ihrem Edge-Knoten zugegriffen werden kann, um auf die WANdisco Benutzeroberfläche zuzugreifen.
  - Java 1.8 64-Bit.
  - Auf dem Edge-Knoten installierte Hadoop-Clientbibliotheken.
  - Möglichkeit, sich als HDFS-Superuser zu authentifizieren (z. B. „hdfs“).
  - Wenn Kerberos auf Ihrem Hadoop-Cluster aktiviert ist, muss auf dem Edge-Knoten ein gültiger Keytab verfügbar sein, der einen geeigneten Principal für den HDFS-Superuser enthält.
- Ein aktives AWS-Konto mit Zugriff auf einen S3-Bucket.
- Eine AWS Direct Connect, die zwischen Ihrem lokalen Hadoop-Cluster (insbesondere dem Edge-Knoten) und AWS hergestellt wird.

Produktversionen

- LiveData Migrator 1.8.6
- WANdisco Benutzeroberfläche (OneUI) 5.8.0

Architektur

Quelltechnologie-Stack

- Lokaler Hadoop-Cluster

Zieltechnologie-Stack

- Amazon S3

Architektur

Das folgende Diagramm zeigt die Architektur der LiveData Migrator-Lösung.

Der Workflow besteht aus vier Hauptkomponenten für die Datenmigration von lokalem HDFS zu Amazon S3.

- LiveData Migrator — Automatisiert die Migration von Daten von HDFS zu Amazon S3 und befindet sich auf einem Edge-Knoten des Hadoop-Clusters.
- HDFS — Ein verteiltes Dateisystem, das Zugriff auf Anwendungsdaten mit hohem Durchsatz ermöglicht.
- Amazon S3 — Ein Objektspeicherservice, der Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet.
- AWS Direct Connect — Ein Service, der eine dedizierte Netzwerkverbindung von Ihren lokalen Rechenzentren zu AWS herstellt.

Automatisierung und Skalierung

In der Regel erstellen Sie mehrere Migrationen, sodass Sie bestimmte Inhalte aus Ihrem Quelldateisystem nach Pfad oder Verzeichnis auswählen können. Sie können Daten auch in mehrere unabhängige Dateisysteme gleichzeitig migrieren, indem Sie mehrere Migrationsressourcen definieren.

Epen

Amazon S3 S3-Speicher in Ihrem AWS-Konto konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie sich bei Ihrem AWS-Konto an.	Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.	AWS-Erfahrung
Erstellen Sie einen S3-Bucket.	Wenn Sie noch keinen vorhandenen S3-Bucket haben, den Sie als Zielspeicher verwenden können, wählen Sie in der Amazon S3 S3-Konsole die Option „Bucket erstellen“ und geben Sie einen Bucket-Namen, eine AWS-Region und Bucket-Einstellungen für den Block Public Access an. AWS und WANdisco empfehlen Ihnen, die Optionen zum Blockieren des öffentlichen Zugriffs für den S3-Bucket zu aktivieren und die Bucket-Zugriffs- und Benutzerberechtigungsrichtlinien so einzurichten, dass sie den Anforderungen Ihrer Organisation entsprechen. Ein AWS-Beispiel finden Sie unter https://docs.aws.amazon.com/AmazonS3/ latest/dev/example - walkthroughs-	AWS-Erfahrung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	managing-access-example 1.html.	

Installieren Sie LiveData Migrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das LiveData Migrator-Installationsprogr amm herunter.	Laden Sie das LiveData Migrator-Installationsprogr amm herunter und laden Sie es auf den Hadoop Edge-Knoten hoch. Sie können eine kostenlose Testversion von LiveData Migrator unter / aws.amazon. herunterladen. https://www2.wandisco.com/l dm-trial. You can also obtain access to LiveData Migrator from AWS Marketplace, at https:/ com/marketplace/pp/ B07B8. SZND9	Hadoop-Administrator, Besitzer der Anwendung
Installieren Sie LiveData Migrator.	Verwenden Sie das heruntergeladene Installationsprogramm und installieren Sie LiveData Migrator als HDFS-Superuser auf einem Edge-Knoten in Ihrem Hadoop-Cluster. Die Installationsbefehle finden Sie im Abschnitt „Zusätzliche Informationen“.	Hadoop-Administrator, Besitzer der Anwendung
Überprüfen Sie den Status von LiveData Migrator und anderen Diensten.	Überprüfen Sie den Status von LiveData Migrator, Hive Migrator und WANdisco	Hadoop-Administrator, Anwendungsbesitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	UI mithilfe der Befehle im Abschnitt „Zusätzliche Informationen“.	

Konfigurieren Sie den Speicher über die Benutzeroberfläche WANdisco

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Registrieren Sie Ihr LiveData Migrator-Konto.	Melden Sie sich über einen Webbrowser auf Port 8081 (auf dem Hadoop Edge-Knoten) bei der WANdisco Benutzeroberfläche an und geben Sie Ihre Daten für die Registrierung ein. Wenn Sie LiveData Migrator beispielsweise auf einem Host namens myldmhost.example.com ausführen, lautet die URL: http://myldmhost.example.com:8081	Besitzer der Anwendung
Konfigurieren Sie Ihren HDFS-Quellspeicher.	Geben Sie die Konfigurationsdetails an, die für Ihren HDFS-Quellspeicher erforderlich sind. Dazu gehören der Wert „fs.defaultFS“ und ein benutzerdefinierter Speichername. Wenn Kerberos aktiviert ist, geben Sie den Principal- und den Keytab-Speicherort an, den LiveData Migrator verwenden soll. Wenn NameNode HA auf dem Cluster aktiviert	Hadoop-Administrator, Anwendungsbesitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ist, geben Sie einen Pfad zu den Dateien core-site.xml und hdfs-site.xml auf dem Edge-Knoten an.	
Konfigurieren Sie Ihren Amazon S3 S3-Zielspeicher.	Fügen Sie Ihren Zielspeicher als Typ S3a hinzu. Geben Sie den benutzerdefinierten Speichernamen und den S3-Bucket-Namen an. Geben Sie „org.apache.hadoop .fs.s3a.Simple AWSCreden tials Provider“ für die Option Credentials Provider ein und geben Sie den AWS-Zugriff und die geheimen Schlüssel für den S3-Bucket ein. Zusätzliche S3a-Eigen schaften werden ebenfalls benötigt. Einzelheiten finden Sie im Abschnitt „S3a-Eige nschaften“ in der LiveData Migrator-Dokumentation unter https://docs.wandisco.com/l ive-data-migrator/ docs/comm and-reference/# 3a. filesyste m-add-s	AWS, Inhaber der Anwendung

Bereiten Sie sich auf die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Ausschlüsse hinzu (falls erforderlich).	Wenn Sie bestimmte Datensätze von der Migration ausschließen möchten,	Hadoop-Administrator, Anwendungsbesitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	fügen Sie Ausnahmen für den HDFS-Quellspeicher hinzu. Diese Ausnahmen können auf der Dateigröße, den Dateinamen (basierend auf Regex-Mustern) und dem Änderungsdatum basieren.	

Erstellen und starten Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und konfigurieren Sie die Migration.	Erstellen Sie eine Migration im Dashboard der WANdisco Benutzeroberfläche. Wählen Sie Ihre Quelle (HDFS) und Ihr Ziel (den S3-Bucket). Fügen Sie neue Ausnahmen hinzu, die Sie im vorherigen Schritt definiert haben. Wählen Sie entweder die Option „Überschreiben“ oder die Option „Überspringen, wenn die Größe übereinstimmt“. Erstellen Sie die Migration, wenn alle Felder vollständig sind.	Hadoop-Administrator, Besitzer der Anwendung
Starten Sie die Migration.	Wählen Sie im Dashboard die Migration aus, die Sie erstellt haben. Klicken Sie hier, um die Migration zu starten. Sie können eine Migration auch automatisch starten, indem Sie bei der Erstellung der	Besitzer der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Migration die Option Autostart auswählen.	

Bandbreite verwalten (optional)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie ein Netzwerkb andbreitenlimit zwischen Quelle und Ziel fest.	Wählen Sie in der Speicherl iste auf dem Dashboard Ihren Quellspeicher aus und wählen Sie in der Gruppierungsliste „Bandbreitenverwaltung“ aus. Deaktivieren Sie die Option „Unbegrenzt“ und definieren Sie das maximale Bandbreit enlimit und die maximale Bandbreiteneinheit. Wählen Sie „Anwenden“.	Inhaber der Anwendung, Netzwerk

Überwachen und verwalten Sie Migrationen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Zeigen Sie Migrationsinformat ionen über die WANdisco Benutzeroberfläche an.	Verwenden Sie die WANdisco Benutzeroberfläche, um Lizenz-, Bandbreiten-, Speicher- und Migration sinformationen anzuzeige n. Die Benutzeroberfläche bietet auch ein Benachric htigungssystem, sodass Sie Benachrichtigungen über Fehler, Warnungen oder	Hadoop-Administrator, Anwendungsbesitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wichtige Meilensteine Ihrer Nutzung erhalten können.	
Migrationen beenden, fortsetzen und löschen.	Sie können verhindern, dass bei einer Migration Inhalte an das Ziel übertragen werden, indem Sie sie in den Status STOPPED versetzen . Gestoppte Migrationen können wieder aufgenomm en werden. Migrationen im Status STOPPED können auch gelöscht werden.	Hadoop-Administrator, Anwendungsbesitzer

Zugehörige Ressourcen

- LiveData Migrator-Dokumentation
- LiveData Migrator im AWS Marketplace
- WANdisco LiveData Migrator-Demonstration (Video)

Zusätzliche Informationen

Installation von Migrator LiveData

Sie können LiveData Migrator mit den folgenden Befehlen installieren, vorausgesetzt, das Installationsprogramm befindet sich in Ihrem Arbeitsverzeichnis:

```
su - hdfs
chmod +x livedata-migrator.sh && sudo ./livedata-migrator.sh
```

Überprüfen Sie den Status von LiveData Migrator und anderen Diensten nach der Installation

Verwenden Sie die folgenden Befehle, um den Status von LiveData Migrator, Hive Migrator und UI zu überprüfen: WANdisco

```
service livedata-migrator status
service hivemigrator status
service livedata-ui status
```

Migrieren Sie Oracle Business Intelligence 12c von lokalen Servern zur AWS-Cloud

Erstellt von Lanre (Lan-Ray) showunmi (AWS) und Patrick Huang (AWS)

Übersicht

Dieses Muster zeigt, wie Oracle Business Intelligence Enterprise Edition 12c mithilfe von AWS von lokalen Servern in die AWS-Cloud migriert wird. CloudFormation Außerdem wird beschrieben, wie Sie andere AWS-Services verwenden können, um Oracle BI 12c-Komponenten zu implementieren, die hohe Verfügbarkeit, Sicherheit, Flexibilität und die Fähigkeit zur dynamischen Skalierung bieten.

Eine Liste der bewährten Methoden im Zusammenhang mit der Migration von Oracle BI 12c zur AWS-Cloud finden Sie im Abschnitt Zusätzliche Informationen dieses Musters.

> **Note**
>
> Es hat sich bewährt, mehrere Testmigrationen durchzuführen, bevor Sie Ihre vorhandenen Oracle BI 12c-Daten in die Cloud übertragen. Diese Tests helfen Ihnen dabei, Ihren Migrationsansatz zu optimieren, potenzielle Probleme zu identifizieren und zu beheben und die Ausfallzeiten genauer einzuschätzen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Sichere Netzwerkkonnektivität zwischen Ihren lokalen Servern und AWS über AWS Virtual Private Network (AWS VPN) -Services oder AWS Direct Connect
- Softwarelizenzen für Ihr Oracle-Betriebssystem, Oracle BI 12c, Oracle Database, Oracle WebLogic Server und Oracle HTTP Server

Einschränkungen

Informationen zu Speichergrößenbeschränkungen finden Sie in der Dokumentation zu Amazon Relational Database Service (Amazon RDS) für Oracle.

Produktversionen

- Oracle Business Intelligence Enterprise Ausgabe 12c
- Oracle WebLogic Server 12c
- Oracle HTTP-Server 12c
- Oracle Database 12c (oder neuer)
- Oracle Java SE 8

Architektur

Das folgende Diagramm zeigt eine Beispielarchitektur für die Ausführung von Oracle BI 12c-Komponenten in der AWS-Cloud:

Dieses Diagramm zeigt die folgende Architektur:

1. Amazon Route 53 bietet eine DNS-Konfiguration (Domain Name Service).
2. Elastic Load Balancing (ELB) verteilt den Netzwerkverkehr, um die Skalierbarkeit und Verfügbarkeit der Oracle BI 12c-Komponenten auf mehrere Availability Zones zu verbessern.
3. Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen hosten die Oracle HTTP-Server, den Weblogic Admin-Server und verwaltete BI-Server in mehreren Availability Zones.
4. Amazon Relational Database Service (Amazon RDS) für Oracle-Datenbanken speichert BI-Server-Metadaten in mehreren Availability Zones.
5. Amazon Elastic File System (Amazon EFS) wird auf jeder Oracle BI 12c-Komponente zur gemeinsamen Dateispeicherung bereitgestellt.

Technologie-Stack

- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic File System (Amazon EFS)
- Amazon RDS für Oracle
- AWS Certificate Manager (ACM)

- Elastic Load Balancing (ELB)
- Oracle BI 12c
- Oracle WebLogic Server 12c
- Oracle HTTP-Server (OHS)

Tools

- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.
- AWS Certificate Manager (ACM) unterstützt Sie bei der Erstellung, Speicherung und Erneuerung von öffentlichen und privaten SSL/TLS X.509-Zertifikaten und Schlüsseln, die Ihre AWS-Websites und -Anwendungen schützen.
- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS-Cloud oder zwischen Kombinationen von Cloud- und lokalen Setups.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server starten, wie Sie benötigen, und diese schnell nach oben oder unten skalieren.
- Amazon EC2 Auto Scaling hilft Ihnen dabei, die Anwendungsverfügbarkeit aufrechtzuerhalten, und ermöglicht es Ihnen, EC2 Amazon-Instances gemäß den von Ihnen definierten Bedingungen automatisch hinzuzufügen oder zu entfernen.
- Amazon Elastic File System (Amazon EFS) unterstützt Sie bei der Erstellung und Konfiguration gemeinsam genutzter Dateisysteme in der AWS-Cloud.
- Elastic Load Balancing verteilt den eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Traffic auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der AWS-Cloud.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.

- Mit Oracle Data Pump können Sie Daten und Metadaten mit hoher Geschwindigkeit von einer Datenbank in eine andere verschieben.
- Oracle Fusion Middleware ist eine Suite von Tools für die Anwendungsentwicklung und Integrationslösungen für Identitätsmanagement, Zusammenarbeit und Business Intelligence-Reporting.
- Oracle GoldenGate unterstützt Sie bei der Entwicklung, Ausführung, Orchestrierung und Überwachung Ihrer Datenreplikations- und Streaming-Datenverarbeitungslösungen in der Oracle Cloud-Infrastruktur.
- Das Oracle WebLogic Scripting Tool (WLST) bietet eine Befehlszeilenschnittstelle, mit der Sie Ihre Cluster horizontal skalieren können. WebLogic

Epen

Beurteilen Sie die Quellumgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sammeln Sie Informationen zum Softwareinventar.	Identifizieren Sie Versionen und Patch-Levels für alle Softwarekomponenten Ihres Quelltechnologie-Stacks, einschließlich der folgenden: • Oracle-Betriebssystem • Oracle Database • Oracle BI 12c • Oracle-Server WebLogic • Oracle-HTTP-Server • Java	Migrationsarchitekt, Lösungsarchitekt, Anwendungseigentümer, Oracle BI-Administrator
Sammeln Sie Informationen zum Datenverarbeitungs- und Speicherbestand.	Überprüfen Sie in Ihrer Quellumgebung aktuelle und historische Nutzungskennzahlen auf Folgendes: • CPU-Verwendung	Migrationsarchitekt, Lösungsarchitekt, Anwendungseigentümer, Oracle BI-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Speicherauslastung • Speichernutzung ⚠ Important Vergewissern Sie sich, dass Sie historische Auslastungsspitzen berücksichtigen.	
Sammeln Sie Informationen über die Architektur der Quellumgebung und ihre Anforderungen.	Verschaffen Sie sich ein umfassendes Verständnis der Architektur Ihrer Quellumgebung und ihrer Anforderungen, einschließlich der folgenden Kenntnisse: • Konfiguration der WebLogic Oracle-Server-Domäne • Clustering • Load Balancing • Konnektivität • Verfügbarkeit • Anforderungen für die Notfallwiederherstellung	Migrationsarchitekt, Lösungsarchitekt, Anwendungseigentümer, Oracle BI-Administrator
Identifizieren Sie die Datenquellen von Java Database Connectivity (JDBC).	Sammeln Sie Informationen über die JDBC-Datenquellen und -Treiber Ihrer Quellumgebung für jede verwendete Datenbank-Engine.	Migrationsarchitekt, Anwendungsbesitzer, Oracle BI-Administrator, Datenbankingenieur oder Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sammeln Sie Informationen über umgebungsspezifische Einstellungen.	Sammeln Sie Informationen zu Einstellungen und Konfigurationen, die für Ihre Quellumgebung spezifisch sind, einschließlich der folgenden: • Benutzerdefinierte Skripts zum Starten und Herunterfahren • Java und andere Umgebungsvariablen • Zertifikate	Migrationsarchitekt, Lösungsarchitekt, Anwendungseigentümer, Oracle BI-Administrator
Identifizieren Sie alle Abhängigkeiten von anderen Anwendungen.	Sammeln Sie Informationen über Integrationen in Ihrer Quellumgebung, die Abhängigkeiten zu anderen Anwendungen schaffen. **Important** Stellen Sie sicher, dass Sie alle LDAP-Integrationen (Lightweight Directory Access Protocol) und andere Netzwerkanforderungen identifizieren.	Migrationsarchitekt, Lösungsarchitekt, Anwendungseigentümer, Oracle BI-Administrator

Entwerfen Sie Ihre Zielumgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Designdok ument auf hoher Ebene.	Erstellen Sie ein Dokument zum Entwurf einer Zielarchi tektur. Stellen Sie sicher, dass Sie die Informationen, die Sie bei der Bewertung Ihrer Quellumgebung gesammelt haben, als Grundlage für das Entwurfsdokument verwenden .	Lösungsarchitekt, Anwendung sarchitekt, Datenbank ingenieur, Migrationsarchitekt
Holen Sie die Genehmigung für das Entwurfsdokument ein.	Prüfen Sie das Entwurfsd okument mit den Beteiligten und holen Sie die erforderl ichen Genehmigungen ein.	Inhaber der Anwendung oder des Dienstes, Lösungsar chitekt, Anwendungsarchitekt

Stellen Sie die Infrastruktur bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie den Infrastru kturcode in vor CloudForm ation.	Erstellen Sie CloudFormation Vorlagen für die Bereitste llung Ihrer Oracle BI 12c-Infra struktur in der AWS-Cloud. Weitere Informationen finden Sie unter Arbeiten mit CloudFormation AWS-Vorla gen im CloudFormation AWS-Benutzerhandbuch.	Cloud-Infrastrukturarchitekt, Lösungsarchitekt, Anwendung sarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Es hat sich bewährt, modulare CloudFormation Vorlagen für jede Oracle BI 12c-Stufe zu erstellen, anstatt eine große Vorlage für all Ihre Ressourcen zu erstellen. Weitere Informationen zu CloudFormation bewährten Methoden finden Sie im AWS-Blog unter 8 bewährte Methoden für die Automatisierung Ihrer Bereitstellungen mit CloudFormation AWS.	
Laden Sie die erforderliche Software herunter.	DDownload die folgende Software zusammen mit den erforderlichen Versionen und Patches von der Oracle-Website: • Java JDK8 • WebLogic Oracle-Server 12c • Oracle BI 12c	Migrationsarchitekt, Datenbankingenieur, Anwendungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Installationsskripten vor.	Erstellen Sie Softwareinstallationsskripts, die eine unbeaufsichtigte Installation ausführen. Diese Skripts vereinfachen die Automatisierung der Bereitstellung. Weitere Informationen finden Sie unter OBIEE 12c: Wie führe ich eine Installation im Hintergrund durch? auf der Oracle Support-Website. Sie benötigen ein Oracle Support-Konto, um die Dokumentation einsehen zu können.	Migrationsarchitekt, Datenbankingenieur, Anwendungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon EBS-gestütztes Linux-AMI für Ihre Web- und Anwendungsstufen.	1. Stellen Sie EC2 Amazon-Instances für Ihre Web- und Anwendungsstufen bereit und konfigurieren Sie sie. Stellen Sie sicher, dass die Instances die Voraussetzungen für die Ausführung der folgenden Komponenten erfüllen: • Einrichtung der Oracle-Betriebssystemumgebung • Benutzerkonto für das Oracle-Betriebssystem eingerichtet • Installation der Java-Software 2. Erstellen Sie Amazon Machine Images (AMIs) der Instances und speichern Sie Kopien für die future Verwendung. Anweisungen finden Sie unter Erstellen eines Amazon EBS-gestützten Linux-AMI im EC2 Amazon-Benutzerhandbuch für Linux-Instances.	Migrationsarchitekt, Datenbankingenieur, Anwendungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie Ihre AWS-Infrastruktur mithilfe von CloudFormation.	Stellen Sie Ihre Web- und Anwendungsebenen von Oracle BI 12c in Modulen bereit, indem Sie die von Ihnen erstellten CloudFormation Vorlagen verwenden. Anweisungen finden Sie unter Erste Schritte mit AWS CloudFormation im CloudFormation AWS-Benutzerhandbuch.	Cloud-Infrastrukturarchitekt, Lösungsarchitekt, Anwendungsarchitekt

Migrieren Sie Oracle BI 12c mithilfe einer Neuinstallation zu AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die erforderliche Software bereit.	Stellen Sie die erforderliche Software an einem Ort bereit, auf den die EC2 Amazon-Instances zugreifen können. Sie könnten die Software beispielsweise in Amazon S3 oder einer anderen EC2 Amazon-Instance bereitstellen, auf die Ihre Web- und Anwendungsserver zugreifen können.	Migrationsarchitekt, Oracle BI-Architekt, Cloud-Infrastrukturarchitekt, Lösungsarchitekt, Anwendungsarchitekt
Bereiten Sie Ihre Repository-Datenbank für die Installation von Oracle BI 12c vor.	Erstellen Sie Oracle BI 12c-Schemas, indem Sie das Oracle Repository Creation Utility (RCU) für eine neue Amazon RDS for Oracle	Cloud-Infrastrukturarchitekt, Lösungsarchitekt, Anwendungsarchitekt, Migrationsarchitekt, Oracle BI-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Oracle-Datenbank-Instance ausführen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Oracle Fusion Middleware 12c und Oracle BI 12c.	1. Beginnen Sie mit einer EC2 Amazon-Instance und installieren Sie die Oracle Fusion Middleware 12c-Infrastruktur und OBIEE 12c. Weitere Informationen finden Sie in den folgenden Abschnitten des Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence: • Das Infrastruktur-Installationsprogramm wird gestartet am BIHOST1 • Installation von Oracle Business Intelligence zur Vorbereitung einer Bereitstellung im Unternehmen **Note** Verwenden Sie Amazon EFS, um Verzeichnisse zu hosten, die von den Oracle BI 12c-Clusterknoten gemeinsam genutzt werden.	Migrationsarchitekt, Oracle BI Architect

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wenden Sie alle erforderl ichen Patches auf die Installation an. 3. Erstellen Sie AMIs die Instanzen und speichern Sie Kopien für die future Verwendung.	
Konfigurieren Sie Ihre Oracle WebLogic Server-Domain für Oracle BI 12c.	Konfigurieren Sie Ihre Oracle BI 12c-Domain als nicht geclusterte Bereitstellung. Weitere Informationen finden Sie unter Configuring the BI Domain im Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence.	Migrationsarchitekt, Oracle BI Architect
Führen Sie eine horizontale Skalierung von Oracle BI 12c aus durch.	Skalieren Sie den einzelnen Knoten horizontal auf die gewünschte Anzahl von Knoten. Weitere Informationen finden Sie unter Scaling out Oracle Business Intelligence im Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intellige nce.	Migrationsarchitekt, Oracle BI Architect

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Oracle HTTP Server 12c.	1. Installieren Sie Oracle HTTP Server 12c auf den EC2 Amazon-Instances der Oracle-Webebene. Anweisungen finden Sie unter Oracle HTTP Server 12c installieren in Oracle HTTP Server für Oracle Access Management 12c installieren und konfiguri eren. 2. Wenden Sie alle erforderl ichen Patches auf die Installation an. 3. Erstellen Sie AMIs die Instanzen und speichern Sie Kopien für die future Verwendung.	Migrationsarchitekt, Oracle BI Architect
Konfigurieren Sie Load Balancer für die SSL-Termi nierung.	1. Erstellen oder importieren Sie SSL-Zertifikate in ACM. 2. Ordnen Sie die SSL-Zerti fikate ELB zu.	Architekt der Cloud-Inf rastruktur, Migrationsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie Business Intelligence-Metadaten-Artefakte zu AWS.	1. Exportieren Sie Oracle Business Intelligence Application Archive (BAR) -Dateien aus der lokalen Oracle BI 12c-Installation. Um die BAR-Dateien zu exportieren, verwenden Sie das WebLogic Scripting Tool (WLST), um den Befehl auszuführen. exportServiceInstance 2. Importieren Sie die lokalen BAR-Dateien in die AWS Oracle BI 12c-Installation. Führen Sie den Befehl importServiceInstanceWLST aus, um die BAR-Dateien zu importieren.	Migrationsarchitekt, Oracle BI Architect

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie Aufgaben nach der Migration aus.	Gehen Sie nach dem Import der BAR-Dateien wie folgt vor: • Konfigurieren Sie alle zusätzlichen JDBC-Datenquellen. • Installieren Sie Treiber für andere Datenquellen wie PostgreSQL oder Amazon Redshift. • Konfigurieren Sie Oracle LDAP, SSL, Single Sign-On (SSO) und Security Store. WebLogic • Konfigurieren Sie die Richtlinien von AWS Identity and Access Management (IAM). • Aktivieren Sie die Nutzungsverfolgung. • Richten Sie Integrationen zu anderen Systemen ein. • Migrieren Sie alle benutzerdefinierten Skripts.	Migrationsarchitekt, Oracle BI Architect

Testen Sie die neue Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die neue Oracle BI 12c-Umgebung.	Führen Sie end-to-end Tests in der neuen Oracle BI 12c-Umgebung durch. Verwenden	Migrationsarchitekt, Lösungsarchitekt, Anwendungseigentümer, Oracle BI-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie so viel Automatisierung wie möglich. Beispiele für Testaktivitäten umfassen Folgendes: • Validierung von Dashboard s, Berichten und URLs • Benutzerakzeptanztests (UAT) • Betriebliche Abnahmetests (OAT) **Note** Führen Sie bei Bedarf zusätzliche Tests und Validierungen durch.	

Wechseln Sie zur neuen Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Trennen Sie den Datenverk ehr zur lokalen Oracle BI 12c-Umgebung.	Stoppen Sie den gesamten Datenverkehr zur lokalen Oracle BI 12c-Umgebung innerhalb des festgelegten Zeitfensters für die Umstellun g.	Migrationsarchitekt, Lösungsar chitekt, Anwendungseigentüm er, Oracle BI-Administrator
Synchronisieren Sie die neue Oracle BI 12c-Repository-Datenbank erneut mit der Quelldatenbank.	Synchronisieren Sie die Amazon RDS Oracle Oracle BI 12c-Repository-Dat	Oracle BI-Administrator, Datenbankingenieur/Administ rator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	enbank erneut mit der lokalen Datenbank. Um die Datenbanken zu synchronisieren, können Sie entweder eine Oracle Data Pump-Aktualisierung oder eine AWS DMS-Change Data Capture (CDC) verwenden.	
Stellen Sie Ihr Oracle BI 12c so URLs um, dass es auf die neue AWS-Umgebung verweist.	Aktualisieren Sie Oracle BI 12c URLs auf Ihren internen DNS-Servern, sodass sie auf die neue AWS-Installation verweisen.	Migrationsarchitekt, Lösungsarchitekt, Anwendungseigentümer, Oracle BI-Administrator
Überwachen Sie die neue Umgebung.	Überwachen Sie die neue Oracle BI 12c-Umgebung mit einem der folgenden Tools: • Amazon CloudWatch • Erkenntnisse zur Amazon-RDS-Leistung • Oracle Enterprise Manager	Oracle BI-Administrator, Datenbankingenieur/Administrator, Anwendungsadministrator
Holen Sie sich die Genehmigung für das Projekt.	Überprüfen Sie die Testergebnisse mit den Beteiligten und holen Sie die erforderlichen Genehmigungen ein, um die Migration abzuschließen.	Anwendungsinhaber, Serviceinhaber, Cloud-Infrastrukturarchitekt, Migrationsarchitekt, Oracle BI Architect

Zugehörige Ressourcen

- Verwenden des Oracle Repository Creation Utility auf RDS für Oracle (Amazon RDS-Benutzerhandbuch)

- Oracle auf Amazon RDS (Amazon RDS-Benutzerhandbuch)
- Oracle WebLogic Server 12c auf AWS (AWS-Whitepaper)
- Bereitstellung von Oracle Business Intelligence für hohe Verfügbarkeit (Oracle Help Center)
- Oracle Business Intelligence Application Archive (BAR) -Dateien (Oracle Help Center)
- So migrieren Sie OBI 12c zwischen Umgebungen (Oracle Support)

Zusätzliche Informationen

Im Folgenden finden Sie eine Liste mit bewährten Methoden für die Migration von Oracle BI 12c in die AWS-Cloud.

Repository-Datenbanken

Es hat sich bewährt, Oracle BI 12c-Datenbankschemas auf einer Amazon RDS for Oracle Oracle-Instance zu hosten. Dieser Instance-Typ bietet kosteneffiziente und anpassbare Kapazität und automatisiert gleichzeitig Verwaltungsaufgaben wie Hardwarebereitstellung, Datenbankeinrichtung, Patching und Backups.

Weitere Informationen finden Sie unter Using the Oracle Repository Creation Utility on RDS for Oracle im Amazon RDS-Benutzerhandbuch.

Web- und Anwendungsebenen

Speicheroptimierte EC2 Amazon-Instances eignen sich häufig gut für Oracle BI 12c-Server. Für welchen Instance-Typ Sie sich auch entscheiden, stellen Sie sicher, dass die von Ihnen bereitgestellten Instances die Anforderungen an die Speichernutzung Ihres Systems erfüllen. Stellen Sie außerdem sicher, dass Sie eine ausreichende Heap-Größe für WebLogic Java Virtual Machine (JVM) auf der Grundlage des verfügbaren Speichers Ihrer EC2 Amazon-Instance konfigurieren.

Lokaler Speicher

I/O spielt eine wichtige Rolle für die Gesamtleistung Ihrer Oracle BI 12c-Anwendung. Amazon Elastic Block Store (Amazon EBS) bietet verschiedene Speicherklassen, die für unterschiedliche Workload-Muster optimiert sind. Stellen Sie sicher, dass Sie einen Amazon EBS-Volumetyp wählen, der zu Ihrem Anwendungsfall passt.

Weitere Informationen zu EBS-Volumetypen finden Sie unter Amazon EBS-Funktionen in der Amazon EBS-Dokumentation.

Gemeinsamer Speicher

Eine geclusterte Oracle BI 12c-Domain benötigt gemeinsam genutzten Speicher für die folgenden Ressourcen:

- Konfigurationsdateien
- Oracle BI 12c Singleton Data Directory (SDD)
- Globaler Oracle-Cache
- Oracle BI Scheduler-Skripts
- Oracle WebLogic Server-Binärdateien

Sie können diese Anforderungen an gemeinsam genutzten Speicher erfüllen, indem Sie Amazon EFS verwenden, das ein skalierbares, vollständig verwaltetes elastisches Network File System (NFS) - Dateisystem bietet.

Feinabstimmung der Leistung von gemeinsam genutztem Speicher

Amazon EFS hat zwei Durchsatzmodi: Bereitgestellt und Bursting. Der Service verfügt außerdem über zwei Leistungsmodi: General Purpose und Max I/O.

Um die Leistung zu optimieren, testen Sie zunächst Ihre Workloads im allgemeinen Leistungsmodus und im Bereitstellungsdurchsatzmodus. Mithilfe dieser Tests können Sie feststellen, ob diese Basismodi ausreichen, um Ihre gewünschten Service Levels zu erreichen.

Weitere Informationen finden Sie unter Amazon EFS-Leistung im Amazon EFS-Benutzerhandbuch.

Verfügbarkeit und Notfallwiederherstellung

Es hat sich bewährt, Oracle BI 12c-Komponenten in mehreren Availability Zones bereitzustellen, um diese Ressourcen im Falle eines Ausfalls der Availability Zone zu schützen. Im Folgenden finden Sie eine Liste der bewährten Methoden zur Verfügbarkeit und Notfallwiederherstellung für bestimmte Oracle BI 12c-Ressourcen, die in der AWS-Cloud gehostet werden:

- Oracle BI 12c-Repository-Datenbanken: Stellen Sie eine Multi-AZ-Amazon RDS-Datenbank-Instance in Ihrer Oracle BI 12c-Repository-Datenbank bereit. In einer Multi-AZ-Bereitstellung stellt Amazon RDS automatisch ein synchrones Standby-Replikat in einer anderen AZ bereit und verwaltet es. Der Betrieb einer Oracle BI 12c-Repository-Datenbank-Instance in verschiedenen Availability Zones kann die Verfügbarkeit während der geplanten Systemwartung verbessern und Ihre Datenbanken vor Instance- und Availability Zone-Ausfällen schützen.

- Oracle BI 12c Managed Servers: Um Fehlertoleranz zu erreichen, ist es eine bewährte Methode, Oracle BI 12c-Systemkomponenten auf verwalteten Servern in einer Amazon EC2 Auto Scaling Scaling-Gruppe bereitzustellen, die so konfiguriert ist, dass sie sich über mehrere Availability Zones erstreckt. Auto Scaling ersetzt fehlerhafte Instances auf der Grundlage von Amazon EC2 Health Checks. Im Falle eines Ausfalls der Availability Zone leiten die Oracle HTTP-Server weiterhin den Datenverkehr an die verwalteten Server in der funktionierenden Availability Zone weiter. Anschließend startet Auto Scaling Instances, um mit Ihren Anforderungen an die Hostanzahl Schritt zu halten. Es wird empfohlen, die HTTP-Sitzungsstatusreplikation zu aktivieren, um sicherzustellen, dass ein reibungsloser Failover der vorhandenen Sitzungen auf die funktionierenden Managed Server erfolgt.
- Oracle BI 12c-Administrationsserver: Um sicherzustellen, dass Ihr Administrationsserver hochverfügbar ist, hosten Sie ihn in einer Amazon EC2 Auto Scaling Scaling-Gruppe, die so konfiguriert ist, dass sie sich über mehrere Availability Zones erstreckt. Stellen Sie dann die Mindest- und Maximalgröße der Gruppe auf 1 ein. Wenn ein Availability Zone-Fehler auftritt, startet Amazon EC2 Auto Scaling einen Ersatz-Administrationsserver in einer alternativen Availability Zone. Um alle ausgefallenen zugrunde liegenden Hosts innerhalb derselben Availability Zone wiederherzustellen, können Sie Amazon EC2 Auto Recovery aktivieren.
- Oracle Web Tier-Server: Es hat sich bewährt, Ihren Oracle HTTP Server mit Ihrer Oracle WebLogic Server-Domain zu verknüpfen. Für eine hohe Verfügbarkeit stellen Sie Ihren Oracle HTTP-Server in einer Amazon EC2 Auto Scaling Scaling-Gruppe bereit, die so konfiguriert ist, dass sie mehrere Availability Zones bereitstellt. Platzieren Sie den Server anschließend hinter einem ELB Elastic Load Balancer. Um zusätzlichen Schutz vor Hostausfällen zu bieten, können Sie Amazon EC2 Auto Recovery aktivieren.

Skalierbarkeit

Die Elastizität der AWS-Cloud hilft Ihnen dabei, Anwendungen entweder horizontal oder vertikal zu skalieren, um den Workload-Anforderungen gerecht zu werden.

Vertikale Skalierung

Um Ihre Anwendung vertikal zu skalieren, können Sie die Größe und den Typ der EC2 Amazon-Instances ändern, auf denen Ihre Oracle BI 12c-Komponenten ausgeführt werden. Sie müssen zu Beginn Ihrer Bereitstellung nicht zu viele Instances bereitstellen und es entstehen keine unnötigen Kosten.

Horizontale Skalierung

Amazon EC2 Auto Scaling hilft Ihnen dabei, Ihre Anwendung horizontal zu skalieren, indem verwaltete Server je nach Arbeitslastanforderungen automatisch hinzugefügt oder entfernt werden.

> **Note**
>
> Für die horizontale Skalierung mit Amazon EC2 Auto Scaling sind Skriptkenntnisse und gründliche Tests für die Implementierung erforderlich.

Backup und Wiederherstellung

Im Folgenden finden Sie eine Liste der bewährten Methoden zur Sicherung und Wiederherstellung für bestimmte Oracle BI 12c-Ressourcen, die in der AWS-Cloud gehostet werden:

- Oracle Business Intelligence-Metadaten-Repositorys: Amazon RDS erstellt und speichert automatisch Backups Ihrer Datenbank-Instances. Diese Backups werden für einen von Ihnen angegebenen Zeitraum aufbewahrt. Stellen Sie sicher, dass Sie Ihre Amazon RDS-Backupdauer und Aufbewahrungseinstellungen entsprechend Ihren Datenschutzanforderungen konfigurieren. Weitere Informationen finden Sie unter Amazon-RDS-Backup und -Wiederherstellung.
- Verwaltete Server, Administrationsserver und Web-Tier-Server: Stellen Sie sicher, dass Sie Amazon EBS-Snapshots entsprechend Ihren Datenschutz- und Aufbewahrungsanforderungen konfigurieren.
- Gemeinsamer Speicher: Sie können die Sicherung und Wiederherstellung von in Amazon EFS gespeicherten Dateien mithilfe von AWS Backup verwalten. Der AWS-Backup-Service kann auch zur zentralen Verwaltung der Sicherung und Wiederherstellung anderer Services wie Amazon EC2, Amazon EBS und Amazon RDS eingesetzt werden. Weitere Informationen finden Sie unter Was ist AWS Backup? Im AWS Backup Developer Guide.

Sicherheit und Einhaltung von Vorschriften

Im Folgenden finden Sie eine Liste mit bewährten Sicherheitsmethoden und AWS-Services, die Ihnen helfen können, Ihre Oracle BI 12c-Anwendungen in der AWS-Cloud zu schützen:

- Verschlüsselung im Ruhezustand: Amazon RDS, Amazon EFS und Amazon EBS unterstützen alle branchenübliche Verschlüsselungsalgorithmen. Sie können den AWS Key Management Service (AWS KMS) verwenden, um kryptografische Schlüssel zu erstellen und zu verwalten und deren Verwendung in allen AWS-Services und in Ihren Anwendungen zu kontrollieren. Sie können Oracle

Transparent Data Encryption (TDE) auch auf der Amazon RDS for Oracle Oracle-Datenbank-Instance konfigurieren, die Ihre Oracle BI 12c-Repository-Datenbank hostet.

- Verschlüsselung bei der Übertragung: Es hat sich bewährt, entweder das SSL- oder das TLS-Protokoll zu aktivieren, um Daten zu schützen, die zwischen den verschiedenen Ebenen Ihrer Oracle BI 12c-Installation übertragen werden. Sie können AWS Certificate Manager (ACM) verwenden, um öffentliche und private SSL- und TLS-Zertifikate für Ihre Oracle BI 12c-Ressourcen bereitzustellen, zu verwalten und bereitzustellen.
- Netzwerksicherheit: Stellen Sie sicher, dass Sie Ihre Oracle BI 12c-Ressourcen in einer Amazon VPC bereitstellen, für die die entsprechenden Zugriffskontrollen für Ihren Anwendungsfall konfiguriert sind. Konfigurieren Sie Ihre Sicherheitsgruppen so, dass eingehender und ausgehender Datenverkehr von den EC2 Amazon-Instances gefiltert wird, auf denen Ihre Installation ausgeführt wird. Stellen Sie außerdem sicher, dass Sie Network Access Control Lists (NACLs) konfigurieren, die Datenverkehr auf der Grundlage definierter Regeln zulassen oder verweigern.
- Überwachung und Protokollierung: Sie können AWS verwenden CloudTrail, um API-Aufrufe an Ihre AWS-Infrastruktur, einschließlich Ihrer Oracle BI 12c-Ressourcen, zu verfolgen. Diese Funktion ist nützlich, wenn Sie Änderungen an der Infrastruktur verfolgen oder eine Sicherheitsanalyse durchführen möchten. Sie können Amazon auch verwenden CloudWatch, um Betriebsdaten einzusehen, die Ihnen verwertbare Einblicke in die Leistung und den Zustand Ihrer Oracle BI 12c-Anwendung bieten können. Sie können auch Alarme konfigurieren und automatisierte Maßnahmen auf der Grundlage dieser Alarme ergreifen. Amazon RDS bietet zusätzliche Überwachungstools, darunter Enhanced Monitoring und Performance Insights.

Migrieren Sie einen lokalen Apache Kafka-Cluster zu Amazon MSK mithilfe von MirrorMaker

Erstellt von Han Zhang (AWS) und Tanner Pratt (AWS)

Übersicht

Dieses Muster bietet Anleitungen für die Migration eines lokalen, selbstverwalteten oder gehosteten Apache Kafka-Clusters zu Amazon Managed Streaming for Apache Kafka (Amazon MSK). Sie können dieses Muster auch verwenden, um von einem Amazon MSK-Cluster zu einem anderen zu migrieren.

Apache Kafka enthält die MirrorMaker Funktion, die Daten zwischen zwei Kafka-Clustern repliziert. MirrorMaker besteht aus einer Sammlung von Verbrauchern, die Teil einer Verbrauchergruppe sind. Die Verbraucher lesen Daten aus den Themen im Quellcluster und geben diese Daten dann an die Produzenten weiter, die die Daten in den Zielcluster schreiben.

Die Amazon MSK-Dokumentation enthält einen allgemeinen Überblick über den Prozess zur Verwendung von MirrorMaker Version 1.0 zur Migration von lokalen Kafka-Clustern zu Amazon MSK. Dieses Muster ergänzt diese Informationen durch umfassende step-by-step Anweisungen zur Verwendung von Version 2.0. MirrorMaker

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Kafka-Quellcluster, der einer der folgenden ist:
  - In einem lokalen Rechenzentrum
  - Selbstverwaltet in der Cloud
  - Gehostet von einem Partner

Einschränkungen

- Um MirrorMaker Version 2.0 verwenden zu können, muss auf dem Quellcluster Apache Kafka Version 2.4.0 oder höher ausgeführt werden. Frühere Versionen finden Sie in den Anweisungen in der Amazon MSK-Dokumentation zur Verwendung von MirrorMaker Version 1.0.

Produktversionen

- MirrorMaker Version 2.0
- Apache Kafka Version 2.4.0 oder höher. Weitere Informationen zu den Versionen von Apache Kafka, die Amazon MSK unterstützt, finden Sie unter Unterstützte Apache Kafka-Versionen.

Architektur

Quelltechnologie-Stack

- Lokaler oder selbstverwalteter Kafka-Cluster

Zieltechnologie-Stack

- Amazon-MSK-Cluster

Zielarchitektur

Das Diagramm zeigt den folgenden Prozess:

1. MirrorMaker liest die Daten aus den Themen und Nutzergruppen im Kafka-Quellcluster.
2. MirrorMaker repliziert die Daten und Verbraucherinformationen auf den Amazon MSK-Zielcluster.

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Managed Streaming for Apache Kafka (Amazon MSK) ist ein vollständig verwalteter Service, der Sie beim Erstellen und Ausführen von Anwendungen unterstützt, die Apache Kafka zur Verarbeitung von Streaming-Daten verwenden.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem

herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.

Andere Tools

- Apache Kafka ist eine Open-Source-Event-Streaming-Plattform. In diesem Muster verwenden Sie die MirrorMakerFunktion von Kafka, um die clusterübergreifende Migration durchzuführen.

Bewährte Methoden

Sie können es entweder in MirrorMaker der Quell- oder in der Zielumgebung ausführen, es wird jedoch empfohlen, es so nah wie möglich am Zielcluster auszuführen. Weitere Informationen finden Sie unter Best Practice: Consume from Remote, Produce to Local in der Apache Kafka-Dokumentation.

Epen

Erstellen Sie die VPC und den Amazon MSK-Zielcluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC.	1. Erstellen Sie eine VPC im AWS-Zielkonto. Anweisungen finden Sie unter Erstellen einer VPC. 2. Erstellen Sie drei private Subnetze in verschiedenen Availability Zones in der neuen VPC. Anweisungen finden Sie unter Erstellen eines Subnetzes. Die Verwendung verschiedener Availability Zones sorgt für hohe Verfügbarkeit und Fehlertoleranz.	AWS-Systemadministrator, DevOps Ingenieur, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Wenn Sie für die Migration des Kafka-Clusters eine öffentliche Internetverbindung verwenden, erstellen Sie öffentliche Subnetze und aktivieren Sie den öffentlichen Zugriff auf den Amazon MSK-Cluster.	
Erstellen Sie den Amazon MSK-Cluster.	Erstellen Sie einen Amazon MSK-Cluster. Anweisungen finden Sie unter Erstellen eines Clusters mit der AWS-Managementkonsole oder Erstellen eines Clusters mit der AWS-CLI. Konfigurieren Sie den Cluster so, dass er die VPC und die Subnetze verwendet, die Sie zuvor erstellt haben.	AWS-Systemadministrator, DevOps Ingenieur, Cloud-Administrator

Einrichten MirrorMaker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installiere MirrorMaker.	1. Starten Sie eine EC2 Instanz. 2. Connect zu Ihrer EC2 Instance her. 3. Laden Sie auf der EC2 Instance die neueste Kafka-Version herunter und extrahieren Sie sie. Anweisungen finden Sie unter Schnellstart (Kafka-Dokumentation). **Note** In diesem Muster installieren Sie MirrorMaker 2.0 als dedizierten MirrorMaker Cluster auf einer EC2 Amazon-Instance. Diese Option ist für Entwicklungsumgebungen akzeptabel und ist der in diesem Muster verwendete Ansatz. Weitere Informationen zu anderen Bereitstellungsoptionen für MirrorMaker 2.0 finden Sie im Abschnitt Zusätzliche	AWS-Systemadministrator, Cloud-Administrator, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Informationen dieses Musters.	
Geben Sie Informationen zum Kafka-Cluster an.	Erstellen Sie im `bin` Installationsordner des Kafka-Clients eine mm2.properties-Datei und konfigurieren Sie sie für Ihren Kafka-Quellcluster. Anweisungen finden Sie unter Einen dedizierten MirrorMaker Cluster ausführen (Kafka-Dokumentation).	AWS-Systemadministrator, Cloud-Administrator, DevOps Ingenieur
Fangen Sie an MirrorMaker.	Geben Sie den folgenden Befehl ein, um die Datei mm2.properties zu starten MirrorMaker und zu übergeben. `$ ./bin/connect-mirror-maker.sh mm2.properties`	AWS-Systemadministrator, Cloud-Administrator, DevOps Ingenieur
Überwachen Sie den Fortschritt.	Überprüfen Sie den Fortschritt, indem Sie die Verzögerung zwischen dem letzten Offset für jedes Thema und dem aktuellen Offset für das jeweilige Thema überprüfen, das aufwändig MirrorMaker ist. Eine Anleitung dazu finden Sie in der Kafka-Dokumentation unter Monitoring Geo-Replication.	AWS-Systemadministrator, Cloud-Administrator, DevOps Ingenieur

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stoppen Sie die Verbrauch eranwendungen.	Stoppen Sie alle Verbrauch eranwendungen, die Daten aus dem Quellcluster verbrauchen.	App-Developer
Starten Sie die Verbrauch eranwendungen.	Ändern Sie die Bootstrap-Konfiguration der Anwendung so, dass sie auf den Zielclust er verweist. Beginnen Sie dann mit der Nutzung auf dem Zielcluster.	App-Developer
Stoppen Sie die Produzenten auf dem Quellcluster.	Wenn die Verbrauch eranwendungen erfolgreich auf dem Zielcluster arbeiten, beenden Sie die Producer auf dem Quellcluster.	App-Developer
Starten Sie die Producers auf dem Zielcluster.	Ändern Sie die Konfiguration der Bootstrap-Server des Herstellers und verweisen Sie auf den Zielcluster. Warten Sie MirrorMaker , bis die Spiegelung aller Daten aus dem Quellcluster abgeschlossen ist, bevor Sie die Producer starten.	App-Developer
Stopp MirrorMaker.	Halten Sie an, nachdem die Produzenten zum Zielcluster gewechselt sind MirrorMaker.	AWS-Systemadministrator, Cloud-Administrator, DevOps Ingenieur

Zugehörige Ressourcen

AWS-Ressourcen

- Migrieren von Clustern mit MirrorMaker (Amazon MSK-Dokumentation)
- Amazon MSK-Migrationslabore (AWS-Workshop-Studio)

Sonstige Ressourcen

- MirrorMaker 2.0 (Verbesserungsvorschläge für Apache Kafka)
- Georeplikation: Clusterübergreifende Datenspiegelung (Apache Kafka-Dokumentation)

Zusätzliche Informationen

Dieses Muster läuft MirrorMaker 2.0 als dedizierter MirrorMaker Cluster auf Amazon EC2. Diese Option ist für Entwicklungsumgebungen akzeptabel. Obwohl es in diesem Muster nicht behandelt wird, können Sie MirrorMaker 2.0 auch in einem Kafka Connect-Cluster ausführen. Diese Bereitstellungsoption verwendet ein Framework innerhalb des Kafka-Ökosystems, das die Skalierung und Wartung verbessert. Sie stellen den Connector in einem Kafka Connect-Cluster mit der zugehörigen Konfiguration bereit, um die Anwendung auszuführen. Der Connector kann für Entwicklungs- oder Testzwecke im eigenständigen Modus oder für die Produktion im verteilten Modus ausgeführt werden. Weitere Informationen finden Sie unter MirrorMaker In einem Connect-Cluster ausführen (Apache Kafka-Dokumentation). Weitere Informationen zu anderen MirrorMaker 2.0-Bereitstellungsoptionen finden Sie unter Exemplarische Vorgehensweise: Running MirrorMaker 2.0 (Kafka-Dokumentation).

Migrieren Sie einen ELK-Stack zu Elastic Cloud auf AWS

Erstellt von Battulga Purevragchaa (AWS), Uday Reddy und Antony Prasad Thevaraj (AWS)

Übersicht

Elastic bietet seit vielen Jahren Dienstleistungen an, wobei Benutzer und Kunden Elastic in der Regel selbst vor Ort verwalten. Elastic Cloud, der verwaltete Elasticsearch-Service, bietet eine Möglichkeit, den Elastic Stack (ELK Stack) und Lösungen für Unternehmenssuche, Observability und Sicherheit zu nutzen. Sie können mit Apps wie Logs, Metrics, APM (Application Performance Monitoring) und SIEM (Security Information and Event Management) auf Elastic-Lösungen zugreifen. Sie können integrierte Funktionen wie maschinelles Lernen, Index-Lifecycle-Management und Kibana Lens (für Drag-and-Drop-Visualisierungen) verwenden.

Wenn Sie von selbstverwaltetem Elasticsearch zu Elastic Cloud wechseln, kümmert sich der Elasticsearch-Service um Folgendes:

- Bereitstellung und Verwaltung der zugrunde liegenden Infrastruktur
- Elasticsearch-Cluster erstellen und verwalten
- Cluster nach oben und unten skalieren
- Upgrades, Patches und Erstellen von Snapshots

So haben Sie mehr Zeit, sich auf die Lösung anderer Herausforderungen zu konzentrieren.

Dieses Muster definiert, wie Elasticsearch 7.13 vor Ort zu Elasticsearch auf Elastic Cloud auf Amazon Web Services (AWS) migriert wird. Andere Versionen erfordern möglicherweise geringfügige Änderungen an den in diesem Muster beschriebenen Prozessen. Weitere Informationen erhalten Sie von Ihrem Elastic-Ansprechpartner.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit Zugriff auf Amazon Simple Storage Service (Amazon S3) für Snapshots
- Ein sicherer privater Link mit ausreichend hoher Bandbreite zum Kopieren von Snapshot-Datendateien nach Amazon S3
- Amazon S3 Transfer Acceleration

- Elastic Snapshot-Richtlinien, um sicherzustellen, dass die Datenaufnahme regelmäßig archiviert wird, entweder in einem ausreichend großen lokalen Datenspeicher oder in einem Remotespeicher (Amazon S3)

Bevor Sie mit der Migration beginnen, müssen Sie wissen, wie umfangreich Ihre Snapshots und die Lebenszyklusrichtlinien für die zugehörigen Indizes vor Ort sind. Weitere Informationen erhalten Sie bei Elastic.

Rollen und Fähigkeiten

Für den Migrationsprozess sind außerdem die in der folgenden Tabelle beschriebenen Rollen und Fachkenntnisse erforderlich.

Rolle	Fachwissen	Verantwortlichkeiten
App-Unterstützung	Vertrautheit mit Elastic Cloud und Elastic vor Ort	Alle Aufgaben im Zusammenhang mit Elastic
Systemadministrator oder DBA	Umfassende Kenntnisse der lokalen Elastic-Umgebung und ihrer Konfiguration	Die Fähigkeit, Speicher bereitzustellen, die AWS-Befehlszeilenschnittstelle (AWS CLI) zu installieren und zu verwenden und alle Datenquellen zu identifizieren, die Elastic vor Ort versorgen
Netzwerkadministrator	Kenntnisse der Netzwerkkonnektivität, Sicherheit und Leistung zwischen lokalen und AWS-Netzwerken	Einrichtung von Netzwerkverbindungen von lokalen Standorten zu Amazon S3 mit Kenntnis der Verbindungsbandbreite

Einschränkungen

- Elasticsearch auf Elastic Cloud ist nur in unterstützten AWS-Regionen verfügbar (September 2021).

Produktversionen

- Elasticsearch 7.13

Architektur

Quelltechnologie-Stack

Lokales Elasticsearch 7.13 oder höher:

- Cluster-Snapshots
- Schnappschüsse indizieren
- Beats-Konfiguration

Architektur der Quelltechnologie

Das folgende Diagramm zeigt eine typische lokale Architektur mit unterschiedlichen Aufnahmemethoden, Knotentypen und Kibana. Die verschiedenen Knotentypen spiegeln die Elasticsearch-Cluster-, Authentifizierungs- und Visualisierungsrollen wider.

1. Aufnahme von Beats zu Logstash
2. Aufnahme von Beats in die Apache Kafka-Messaging-Warteschlange
3. Aufnahme von Filebeat nach Logstash
4. Aufnahme aus der Apache Kafka-Messaging-Warteschlange nach Logstash
5. Aufnahme von Logstash in einen Elasticsearch-Cluster
6. Elasticsearch-Cluster
7. Authentifizierungs- und Benachrichtigungsknoten
8. Kibana- und Blob-Knoten

Zieltechnologie-Stack

Elastic Cloud wird auf Ihrem SaaS-Konto (Software as a Service) in mehreren AWS-Regionen mit clusterübergreifender Replikation bereitgestellt.

- Cluster-Snapshots

- Index-Snapshots
- Beats-Konfigurationen
- Elastische Cloud
- Network Load Balancer
- Amazon Route 53
- Amazon S3

Zielarchitektur

Die verwaltete Elastic Cloud-Infrastruktur ist:

- Hochverfügbar, in mehreren Availability Zones und mehreren AWS-Regionen präsent.
- Region ist ausfalltolerant, da Daten (Indizes und Snapshots) mithilfe der Cluster-übergreifenden Replikation (CCR) von Elastic Cloud repliziert werden
- Archivierung, da Snapshots in Amazon S3 archiviert werden
- Netzwerkpartitionstolerant durch eine Kombination aus Network Load Balancers und Route 53
- Datenaufnahme, die von Elastic APM, Beats, Logstash stammt (aber nicht darauf beschränkt ist)

Migrationsschritte auf hoher Ebene

Elastic hat eine eigene präskriptive Methode für die Migration von lokalen Elastic Clustern zu Elastic Cloud entwickelt. Die Elastic-Methodik ist direkt auf die AWS-Migrationsleitlinien und Best Practices abgestimmt und ergänzt diese, darunter das Well-Architected Framework und das AWS Migration Acceleration Program (MAP). In der Regel sind die drei AWS-Migrationsphasen die folgenden:

- Bewerten
- Mobilisieren
- Migrieren und modernisieren

Elastic folgt ähnlichen Migrationsphasen mit ergänzender Terminologie:

- Initiieren

- Plan
- Implementieren
- Liefern
- Schließen

Elastic verwendet die Elastic Implementation Methodology, um die Bereitstellung von Projektergebnissen zu erleichtern. Dies ist von Haus aus inklusiv, um sicherzustellen, dass Elastic, die Beratungsteams und die Kundenteams klar zusammenarbeiten, um gemeinsam die angestrebten Ergebnisse zu erzielen.

Die Elastic-Methode kombiniert traditionelle Wasserfall-Phasen mit Scrum innerhalb der Implementierungsphase. Konfigurationen der technischen Anforderungen werden iterativ auf kollaborative Weise bereitgestellt, wobei das Risiko minimiert wird.

Tools

AWS-Services

- Amazon Route 53 — Amazon Route 53 ist ein hochverfügbarer und skalierbarer Domain Name System (DNS) -Webservice. Sie können Route 53 zum Durchführen von drei wesentlichen Aufgaben in beliebiger Kombination verwenden: Domänenregistrierung, DNS-Routing und Zustandsprüfung.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen. Dieses Muster verwendet einen S3-Bucket und Amazon S3 Transfer Acceleration.
- Elastic Load Balancing — Elastic Load Balancing verteilt Ihren eingehenden Traffic automatisch auf mehrere Ziele wie EC2 Instances, Container und IP-Adressen in einer oder mehreren Availability Zones.

Andere Tools

- Beats — Beats versendet Daten von Logstash oder Elasticsearch
- Elastic Cloud — Elastic Cloud ist ein verwalteter Dienst für das Hosten von Elasticsearch.

- Elasticsearch — Elasticsearch ist eine Such- und Analyse-Engine, die den Elastic Stack verwendet, um Ihre Daten für skalierbare Such- und Analysezwecke zentral zu speichern. Dieses Muster verwendet auch die Erstellung von Snapshots und die clusterübergreifende Replikation.
- Logstash — Logstash ist eine serverseitige Datenverarbeitungspipeline, die Daten aus mehreren Quellen aufnimmt, transformiert und dann an Ihren Datenspeicher sendet.

Epen

Bereiten Sie die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Server, auf denen die lokale Elastic-Lösung ausgeführt wird.	Vergewissern Sie sich, dass die Elastic-Migration unterstützt wird.	Besitzer der App
Machen Sie sich mit der lokalen Serverkonfiguration vertraut.	Um die Serverkonfiguration zu verstehen, die für die erfolgreiche Ausführung von Workloads vor Ort erforderlich ist, sollten Sie den Platzbedarf der Serverhardware, die Netzwerkkonfiguration und die Speichereigenschaften ermitteln, die derzeit verwendet werden	App-Unterstützung
Sammeln Sie Benutzer- und App-Kontoinformationen.	Identifizieren Sie die Benutzernamen und App-Namen, die von der lokalen Elastic-Umgebung verwendet werden.	Systemadministrator, App-Support
Dokumentieren Sie die Konfiguration von Beats und Data Shipper.	Um die Konfigurationen zu dokumentieren, schauen Sie sich die vorhandenen Datenquellen und Datenquel	App-Unterstützung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	len an. Weitere Informationen finden Sie in der Elastic-D okumentation.	
Ermitteln Sie die Geschwind igkeit und das Datenvolumen.	Legen Sie eine Ausgangsb asis dafür fest, wie viele Daten der Cluster verarbeitet.	Systemadministrator, App-Support
Dokumentieren Sie RPO- und RTO-Szenarien.	Dokumentieren Sie Szenarien mit Recovery Point Objective (RPO) und Recovery Time Objective (RTO) in Form von Ausfällen und Service Level Agreements (). SLAs	App-Besitzer, Systemadm inistrator, App-Support
Ermitteln Sie die optimalen Einstellungen für den Snapshot-Lebenszyklus.	Definieren Sie, wie oft Daten während und nach der Migration mithilfe von Elastic-Snapshots gesichert werden müssen.	App-Besitzer, Systemadm inistrator, App-Support
Definieren Sie die Leistungs erwartungen nach der Migration.	Generieren Sie Messwerte zur aktuellen und zu erwartend en Bildschirmaktualisierung, zu Abfragelaufzeiten und zum Verhalten der Benutzero berfläche.	Systemadministrator, App-Support
Dokumentieren Sie die Anforderungen an Internetz ugriff, Transport, Bandbreite und Verfügbarkeit.	Stellen Sie die Geschwind igkeit, Latenz und Stabilität der Internetverbindungen für das Kopieren von Snapshots nach Amazon S3 fest.	Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Dokumentieren Sie die aktuellen Kosten der lokalen Laufzeit für Elastic.	Stellen Sie sicher, dass die Größe der AWS-Zielu mgebung so konzipiert ist, dass sie sowohl leistungsstark als auch kostengünstig ist.	DBA, Systemadministrator, App-Support
Identifizieren Sie die Authentif izierungs- und Autorisie rungsanforderungen.	Die Sicherheitsfunktionen von Elastic Stack bieten integrier te Realms wie Lightweight Directory Access Protocol (LDAP), Security Assertion Markup Language (SAML) und OpenID Connect (OIDC).	DBA, Systemadministrator, Anwendungsunterstützung
Verstehen Sie die spezifisc hen regulatorischen Anforderu ngen je nach geografischem Standort.	Stellen Sie sicher, dass Daten gemäß Ihren Anforderungen und allen relevanten nationale n Anforderungen exportiert und verschlüsselt werden.	DBA, Systemadministrator, App-Support

Implementieren Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie den Staging-B ereich auf Amazon S3 vor.	Um Snapshots auf Amazon S3 zu erhalten, erstellen Sie einen S3-Bucket und eine temporäre AWS Identity and Access Management (IAM) -Rolle mit vollem Zugriff auf Ihren neu erstellten Bucket. Weitere Informationen finden Sie unter Eine Rolle erstellen , um Berechtigungen an einen IAM-Benutzer zu delegiere	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	n. Verwenden Sie den AWS Security Token Service, um temporäre Sicherheitsnachweise anzufordern. Bewahren Sie die Zugriffsschlüssel-ID, den geheimen Zugriffsschlüssel und das Sitzungstoken sicher auf. Aktivieren Sie Amazon S3 Transfer Acceleration für den Bucket.	
Installieren Sie AWS CLI und das Amazon S3 S3-Plugin vor Ort.	Führen Sie auf jedem Elasticsearch-Knoten den folgenden Befehl aus. `sudo bin/elasticsearch-plugin install repository-s3` Starten Sie dann den Knoten neu.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie den Amazon S3 S3-Client-Zugriff.	Fügen Sie die zuvor erstellten Schlüssel hinzu, indem Sie die folgenden Befehle ausführen.
	`elasticsearch-keystore add s3.client.default.access_key`
	`elasticsearch-keystore add s3.client.default.secret_key`
	`elasticsearch-keystore add s3.client.default.session_token`
		AWS-Administrator

Registrieren Sie ein Snapshot-Repository für Elastic-Daten	Verwenden Sie die Kibana Dev Tools, um dem lokalen lokalen Cluster mitzuteilen, in welchen Remote-S3-Bucket geschrieben werden soll.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Snapshot-Richtlinie.	Um das Snapshot-Lebenszyklusmanagement zu konfigurieren, wählen Sie auf der Registerkarte Kibana-Richtlinien die Option SLM-Richtlinie aus und definieren Sie, welche Zeiten, Datenströme oder Indizes enthalten sein sollen und welche Namen verwendet werden sollen. Konfigurieren Sie eine Richtlinie, die häufig Snapshots erstellt. Snapshots sind inkrementell und nutzen den Speicherplatz effizient. Passen Sie Ihre Entscheidung bei der Eignungsbeurteilung an. Eine Richtlinie kann auch eine Aufbewahrungsrichtlinie festlegen und Snapshots automatisch löschen, wenn sie nicht mehr benötigt werden.	Unterstützung für Apps
Stellen Sie sicher, dass Snapshots funktionieren.	Führen Sie in Kibana Dev Tools den folgenden Befehl aus. `GET _snapshot/<your_repo_name>/_all`	AWS-Administrator, Anwendungssupport,

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie einen neuen Cluster auf Elastic Cloud bereit.	Melden Sie sich bei Elastic an und wählen Sie einen Cluster für „Observability, Search oder Security“ aus, der sich aus Ihren Geschäftsergebnissen im Readiness Assessment ergibt.	AWS-Administrator, Anwendungssupport
Richten Sie den Zugriff auf den Cluster-Schlüsselspeicher ein.	Der neue Cluster benötigt Zugriff auf den S3-Bucket, in dem die Snapshots gespeicherte werden. Wählen Sie in der Elasticsearch Service Console Sicherheit und geben Sie die Zugriffs- und geheimen IAM-Schlüssel ein, die Sie zuvor erstellt haben.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den von Elastic Cloud gehosteten Cluster für den Zugriff auf Amazon S3.	Richten Sie einen neuen Cluster-Zugriff auf das zuvor erstellte Snapshot-Repository in Amazon S3 ein. Gehen Sie mit Kibana wie folgt vor: 1. Wählen Sie Stack Management, Snapshot-Einstellungen, RegisterR epo. 2. Geben Sie im Feld Alias den Namen des Repositor ys ein. 3. Wählen Sie als S3-Client name die Option Secondary aus. 4. Fügen Sie den S3-Bucket , den Sie zuvor erstellt haben, dem Repository hinzu. 5. Wählen Sie Snapshot komprimieren. 6. Behalten Sie für die Verschlüsselungsei nstellungen die Standardw erte bei.	AWS-Administrator, Anwendungssupport
Überprüfen Sie das neue Amazon S3 S3-Repository.	Stellen Sie sicher, dass Sie auf Ihr neues Repository zugreifen können, das im Elastic Cloud-Cluster gehostet wird.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Initialisieren Sie den Elasticsearch-Servicecluster.	Initialisieren Sie in der Elasticsearch Service Console den Elasticsearch-Servicecluster aus dem S3-Snapshot.
	
	Führen Sie die folgenden Befehle als POST aus.
	
	`*/_close?expand_wildcards=all`
	
	`/_snapshot/<your-repo-name>/  <your-snapshot-name>/_restore`
	
	`*/_open?expand_wildcards=all`
		App-Unterstützung

Schließen Sie die Migration ab

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die Snapshot-Wiederherstellung erfolgreich war.	Führen Sie mit den Kibana Dev Tools den folgenden Befehl aus. `GET _cat/indices`	App-Unterstützung
Stellen Sie die Aufnahmeleistungen erneut bereit.	Connect die Endpunkte für Beats und Logstash mit dem neuen Elasticsearch-Serviceendpunkt.	Unterstützung für Apps

Testen Sie die Cluster-Umgebung und bereinigen Sie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Cluster-Umgebung.	Nachdem die lokale Elastic-Cluster-Umgebung zu AWS migriert wurde, können Sie eine Verbindung zu ihr herstellen und Ihre eigenen UAT-Tools (User Acceptance Testing) verwenden, um die neue Umgebung zu validieren.	Unterstützung für Apps
Säubere die Ressourcen.	Nachdem Sie überprüft haben, dass der Cluster erfolgreich migriert wurde, entfernen Sie den S3-Bucket und die für die Migration verwendete IAM-Rolle.	AWS-Administrator

Zugehörige Ressourcen

Elastische Referenzen

- Elastische Cloud
- Verwaltetes Elasticsearch und Kibana auf AWS
- Elastische Unternehmenssuche
- Elastische Integrationen
- Elastische Beobachtbarkeit
- Elastische Sicherheit
- Beats
- Elastisches APM
- Wechseln Sie zum Index-Lifecycle-Management
- Elastische Abonnements
- Kontaktieren Sie Elastic

Blogbeiträge von Elastic

- So migrieren Sie von selbstverwaltetem Elasticsearch zu Elastic Cloud on AWS (Blogbeitrag)
- Migration zu Elastic Cloud (Blogbeitrag)

Elastische Dokumentation

- Tutorial: Automatisieren Sie Backups mit SLM
- ILM: Den Index-Lebenszyklus verwalten
- Logstash
- Clusterübergreifende Replikation (CCR)
- Pipelines aufnehmen
- Elasticsearch-API-Anfragen ausführen
- Snapshot-Aufbewahrung

Elastic-Video und Webinar

- Elastische Cloud-Migration
- Elastic Cloud: Warum migrieren Kunden (Webinar)

AWS-Referenzen

- Elastic Cloud auf dem AWS Marketplace
- AWS-Befehlszeilenschnittstelle
- AWS Direct Connect
- AWS Migration Acceleration Program
- Network Load Balancers
- Regionen und Availability Zones
- Amazon Route 53
- Amazon Simple Storage Service
- Amazon S3 Transfer Acceleration
- VPN-Verbindungen
- Well-Architected Framework

Zusätzliche Informationen

Wenn Sie planen, komplexe Workloads zu migrieren, wenden Sie sich an Elastic Consulting Services. Wenn Sie grundlegende Fragen zu Konfigurationen und Services haben, wenden Sie sich an das Elastic Support-Team.

Migrieren Sie Daten mithilfe AWS Cloud von Starburst auf die

Erstellt von Antony Prasad Thevaraj (AWS), Shaun Van Staden und Suresh Veeragoni (AWS)

Übersicht

Starburst hilft Ihnen dabei, Ihre Datenmigration zu Amazon Web Services (AWS) zu beschleunigen, indem es eine Abfrage-Engine für Unternehmen bereitstellt, die bestehende Datenquellen in einem einzigen Zugriffspunkt zusammenführt. Sie können Analysen für mehrere Datenquellen durchführen, um wertvolle Erkenntnisse zu gewinnen, bevor Sie Migrationspläne fertigstellen. Ohne die business-as-usual Analytik zu unterbrechen, können Sie die Daten mithilfe der Starburst-Engine oder einer speziellen ETL-Anwendung (Extrahieren, Transformieren und Laden) migrieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Eine virtuelle private Cloud (VPC)
- Ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster
- Eine Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppe
- Eine Liste der aktuellen System-Workloads, die migriert werden müssen
- Netzwerkkonnektivität von AWS zu Ihrer lokalen Umgebung

Architektur

Referenzarchitektur

Das folgende Architekturdiagramm auf hoher Ebene zeigt den typischen Einsatz von Starburst Enterprise in: AWS Cloud

1. Der Starburst Enterprise-Cluster läuft in Ihrem. AWS-Konto
2. Ein Benutzer authentifiziert sich mithilfe des Lightweight Directory Access Protocol (LDAP) oder Open Authorization (OAuth) und interagiert direkt mit dem Starburst-Cluster.
3. Starburst kann eine Verbindung zu verschiedenen AWS Datenquellen herstellen, z. B. AWS Glue Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon

RDS) und Amazon Redshift. Starburst bietet föderierte Abfragefunktionen für Datenquellen in der AWS Cloud, vor Ort oder in anderen Cloud-Umgebungen.

4. Sie starten Starburst Enterprise in einem Amazon EKS-Cluster mithilfe von Helm-Diagrammen.
5. Starburst Enterprise verwendet Amazon EC2 Auto Scaling Scaling-Gruppen und Amazon EC2 Spot-Instances, um die Infrastruktur zu optimieren.
6. Starburst Enterprise stellt eine direkte Verbindung zu Ihren vorhandenen lokalen Datenquellen her, um Daten in Echtzeit zu lesen. Wenn Sie eine bestehende Starburst Enterprise-Bereitstellung in dieser Umgebung haben, können Sie außerdem Ihren neuen Starburst-Cluster im direkt mit diesem vorhandenen Cluster verbinden. AWS Cloud

Beachten Sie bitte Folgendes:

- Starburst ist keine Datenvirtualisierungsplattform. Es handelt sich um eine SQL-basierte MPP-Abfrage-Engine (Massively Parallel Processing), die die Grundlage einer umfassenden Data-Mesh-Strategie für Analysen bildet.
- Wenn Starburst im Rahmen einer Migration bereitgestellt wird, ist es direkt mit der vorhandenen lokalen Infrastruktur verbunden.
- Starburst bietet mehrere integrierte Unternehmens- und Open-Source-Konnektoren, die die Konnektivität zu einer Vielzahl von Altsystemen erleichtern. Eine vollständige Liste der Konnektoren und ihrer Funktionen finden Sie unter Konnektoren im Starburst Enterprise-Benutzerhandbuch.
- Starburst kann Daten in Echtzeit aus lokalen Datenquellen abfragen. Dies verhindert Unterbrechungen des regulären Geschäftsbetriebs während der Datenmigration.
- Wenn Sie von einer bestehenden lokalen Starburst Enterprise-Bereitstellung migrieren, können Sie einen speziellen Konnektor, Starburst Stargate, verwenden, um Ihren Starburst Enterprise-Cluster direkt mit Ihrem lokalen Cluster zu verbinden. AWS Dies bietet zusätzliche Leistungsvorteile, wenn Geschäftsanwender und Datenanalysten Abfragen aus der Umgebung in Ihre lokale Umgebung zusammenführen. AWS Cloud

Allgemeiner Überblick über die Prozesse

Mit Starburst können Sie Datenmigrationsprojekte beschleunigen, da Starburst Einblicke in all Ihre Daten ermöglicht, bevor Sie sie migrieren. Die folgende Abbildung zeigt den typischen Prozess für die Datenmigration mithilfe von Starburst.

Rollen

Die folgenden Rollen sind in der Regel erforderlich, um eine Migration mit Starburst abzuschließen:

- Cloud-Administrator — Verantwortlich für die Bereitstellung von Cloud-Ressourcen für die Ausführung der Starburst Enterprise-Anwendung
- Starburst-Administrator — Verantwortlich für die Installation, Konfiguration, Verwaltung und Unterstützung der Starburst-Anwendung
- Dateningenieur — Verantwortlich für:
  - Migration der Altdaten in die Cloud
  - Erstellung semantischer Ansichten zur Unterstützung von Analysen
- Lösungs- oder Systemeigentümer — Verantwortlich für die Implementierung der Gesamtlösung

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Mit Amazon Elastic Kubernetes Service (Amazon EKS) können Sie Kubernetes ausführen, AWS ohne dass Sie Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten müssen.

Andere Tools

- Helm — Helm ist ein Paketmanager für Kubernetes, der Sie bei der Installation und Verwaltung von Anwendungen auf Ihrem Kubernetes-Cluster unterstützt.
- Starburst Enterprise — Starburst Enterprise ist eine SQL-basierte MPP-Abfrage-Engine (Massively Parallel Processing), die die Grundlage einer umfassenden Data-Mesh-Strategie für Analysen bildet.
- Starburst Stargate — Starburst Stargate verknüpft Kataloge und Datenquellen in einer Starburst Enterprise-Umgebung, z. B. einen Cluster in einem lokalen Rechenzentrum, mit den Katalogen und

Datenquellen in einer anderen Starburst Enterprise-Umgebung, z. B. einem Cluster in der. AWS Cloud

Epen

Beurteilen Sie die Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren und priorisieren Sie Ihre Daten.	Identifizieren Sie die Daten, die Sie verschieben möchten. Große, lokale Altsysteme können neben Daten, die Sie migrieren möchten, auch Daten enthalten, die Sie aus Compliance-Gründen nicht verschieben möchten oder die nicht verschoben werden können. Wenn Sie mit einem Dateninventar beginnen, können Sie Priorität en setzen, auf welche Daten Sie zuerst abzielen sollten. Weitere Informationen finden Sie unter Erste Schritte mit der automatisierten Portfolio erkennung.	Dateningenieur, DBA
Erkunden, inventarisieren und sichern Sie Ihre Daten.	Überprüfen Sie die Qualität, Quantität und Relevanz der Daten für Ihren Anwendung sfall. Sichern oder erstellen Sie nach Bedarf einen Snapshot der Daten und stellen Sie die Zielumgebung für die Daten fertig.	Dateningenieur, DBA

Richten Sie die Starburst Enterprise-Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Starburst Enterprise in der AWS Cloud.	Richten Sie Starburst Enterprise in einem verwaltet en Amazon EKS-Cluster ein, während die Daten katalogisiert werden. Weitere Informationen finden Sie unter Deployment with Kubernete s in der Starburst Enterpris e-Referenzdokumentation. Dies ermöglicht business-as-usual Analysen während der Datenmigration.	AWS-Administrator, App-Entwi ckler
Connect Starburst mit den Datenquellen.	Nachdem Sie die Daten identifiziert und Starburst Enterprise eingerichtet haben, verbinden Sie Starburst mit den Datenquellen. Starburst liest Daten direkt aus der Datenquelle als SQL-Abfrage. Weitere Informationen finden Sie in der Starburst Enterpris e-Referenzdokumentation.	AWS-Administrator, App-Entwi ckler

Migrieren Sie die Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und betreiben Sie die ETL-Pipelines.	Beginnen Sie mit dem Datenmigrationsprozess. Diese Aktivität kann gleichzei tig mit der business-as-	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	usual Analyse erfolgen. Für die Migration können Sie ein Drittanbieterprodukt oder Starburst verwenden . Starburst ist in der Lage, Daten aus verschiedenen Quellen sowohl zu lesen als auch zu schreiben. Weitere Informationen finden Sie in der Starburst Enterprise-Referenzdokumentation.	
Validieren Sie die Daten.	Nachdem die Daten migriert wurden, validieren Sie die Daten, um sicherzustellen, dass alle erforderlichen Daten verschoben wurden und intakt sind.	Dateningenieur, DevOps Ingenieur

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schneide die Daten ab.	Nach Abschluss der Datenmigration und -validierung können Sie die Daten überarbeiten. Dies beinhaltet das Ändern der Datenverbindungslinks in Starburst. Anstatt auf die lokalen Quellen zu verweisen, verweisen Sie auf die neuen Cloud-Quellen und aktualisieren die semantischen Ansichten. Weitere Informationen finden	Dateningenieur, Cutover-Leiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie unter Connectors in der Starburst Enterprise-Referenzdokumentation.	
Für Benutzer bereitstellen.	Datenkonsumenten beginnen, mit den migrierten Datenquellen zu arbeiten. Dieser Prozess ist für die Analytics-Endbenutzer unsichtbar.	Leiter der Umstellung, Dateningenieur

Zugehörige Ressourcen

AWS Marketplace

- Starburst-Galaxie
- Starburst Enterprise
- Starburst-Daten JumpStart
- Starburst Enterprise mit Graviton

Starburst-Dokumentation

- Starburst Enterprise-Benutzerhandbuch
- Referenzdokumentation zu Starburst Enterprise

Andere Dokumentation AWS

- Beginnen Sie mit der automatisierten Portfolioerkennung (AWS Prescriptive Guidance)
- Optimierung der Kosten und Leistung der Cloud-Infrastruktur mit Starburst on AWS(Blogbeitrag)AWS

Optimieren Sie die ETL-Erfassung der Eingabedateigröße auf AWS

Erstellt von Apoorva Patrikar (AWS)

Übersicht

Dieses Muster zeigt Ihnen, wie Sie den Aufnahmeschritt des ETL-Prozesses (Extrahieren, Transformieren und Laden) für Big Data- und Apache Spark-Workloads auf AWS Glue optimieren können, indem Sie die Dateigröße vor der Verarbeitung Ihrer Daten optimieren. Verwenden Sie dieses Muster, um das Problem mit kleinen Dateien zu verhindern oder zu lösen. Dies ist der Fall, wenn eine große Anzahl kleiner Dateien die Datenverarbeitung aufgrund der Gesamtgröße der Dateien verlangsamt. Beispielsweise können Hunderte von Dateien, die jeweils nur einige hundert Kilobyte groß sind, die Datenverarbeitungsgeschwindigkeit für Ihre AWS Glue Glue-Jobs erheblich verlangsamen. Dies liegt daran, dass AWS Glue interne Listenfunktionen auf Amazon Simple Storage Service (Amazon S3) ausführen muss und YARN (Yet Another Resource Negotiator) eine große Menge an Metadaten speichern muss. Um die Datenverarbeitungsgeschwindigkeit zu verbessern, können Sie mithilfe von Gruppierung Ihre ETL-Aufgaben in die Lage versetzen, eine Gruppe von Eingabedateien in eine einzige In-Memory-Partition zu lesen. Die Partition gruppiert automatisch kleinere Dateien zusammen. Alternativ können Sie benutzerdefinierten Code verwenden, um Ihren vorhandenen Dateien Batch-Logik hinzuzufügen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein oder mehrere AWS-Klebejobs
- Eine oder mehrere Big-Data- oder Apache Spark-Workloads
- Einen S3-Bucket

Architektur

Das folgende Muster zeigt, wie Daten in verschiedenen Formaten von einem AWS Glue Glue-Job verarbeitet und dann in einem S3-Bucket gespeichert werden, um einen Überblick über die Leistung zu erhalten.

Das Diagramm zeigt den folgenden Workflow:

1. **Note**

   Ein AWS Glue Glue-Job konvertiert kleine Dateien im CSV-, JSON- und Parquet-Format in dynamische Frames. : Die Größe der Eingabedatei hat den größten Einfluss auf die Leistung des AWS Glue Glue-Jobs.

2. Der AWS Glue Glue-Job führt interne Listenfunktionen in einem S3-Bucket aus.

Tools

- AWS Glue ist ein vollständig verwalteter ETL-Service. Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Epen

Verwenden Sie Gruppierung, um die ETL-Aufnahme beim Lesen zu optimieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie die Gruppengröße an.	Wenn Sie mehr als 50.000 Dateien haben, erfolgt die Gruppierung standardm äßig. Sie können die Gruppierung jedoch auch für weniger als 50.000 Dateien verwenden, indem Sie die Gruppengröße im `connectio n0ptions` Parameter angeben. Der `connectio n0ptions` Parameter ist in der `create_dynamic_fra`	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`me.from_options` Methode enthalten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schreiben Sie den Gruppierungscode.	Verwenden Sie die `create_dynamic_frame` Methode, um einen dynamischen Frame zu erstellen. Zum Beispiel: `S3bucket_node1 = glueContext.create_dynamic_frame.from_options(format_options={"multiline": False}, connection_type="s3", format="json", connection_options={ "paths": ["s3://bucket/prefix/file.json"], "recurse": True, "groupFiles": 'inPartition', "groupSize": 1048576 }, transformation_ctx="S3bucket_node1",)` **Note** Wird verwendet `groupFiles` , um Dateien in einer Amazon S3 S3-Partitionsgruppe zu	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	gruppieren. Wird verwendet`groupSize` , um die Zielgröße der Gruppe festzuleg en, die im Speicher gelesen werden soll. Geben Sie `groupSize` in Byte an (1048576 = 1 MB).	
Fügen Sie den Code zum Workflow hinzu.	Fügen Sie den Gruppieru ngscode zu Ihrem Job-Workf low in AWS Glue hinzu.	Dateningenieur

Verwenden Sie benutzerdefinierte Logik, um die ETL-Erfassung zu optimieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie die Sprache und die Verarbeitungsplattform.	Wählen Sie die Skriptsprache und die Verarbeitungsplatt form, die auf Ihren Anwendung sfall zugeschnitten sind.	Cloud-Architekt
Schreiben Sie den Code.	Schreiben Sie die benutzerd efinierte Logik, um Ihre Dateien zu stapeln.	Cloud-Architekt
Fügen Sie den Code zum Workflow hinzu.	Fügen Sie den Code zu Ihrem Job-Workflow in AWS Glue hinzu. Dadurch kann Ihre benutzerdefinierte Logik bei jeder Ausführung des Jobs angewendet werden.	Dateningenieur

Neupartitionierung beim Schreiben von Daten nach der Transformation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie Konsummuster.	Finden Sie heraus, wie nachgelagerte Anwendungen die von Ihnen geschriebenen Daten verwenden werden. Wenn sie beispielsweise täglich Daten abfragen und Sie nur Daten pro Region partitionieren oder sehr kleine Ausgabedateien haben, z. B. 2,5 KB pro Datei, ist dies nicht optimal für die Nutzung.	DBA
Daten vor dem Schreiben neu partitionieren.	Neupartitionierung auf der Grundlage von Verknüpfungen oder Abfragen während der Verarbeitung (basierend auf der Verarbeitungslogik) und nach der Verarbeitung (basierend auf dem Verbrauch). Zum Beispiel eine Neupartitionierung auf der Grundlage der Bytegröße, wie `.repartition(100000)` , oder eine Neupartitionierung auf der Grundlage von Spalten, wie. `.repartition("column_name")`	Dateningenieur

Zugehörige Ressourcen

- Eingabedateien in größeren Gruppen lesen
- Überwachung von AWS Glue

- Überwachung von AWS Glue mithilfe von CloudWatch Amazon-Metriken
- Auftragsüberwachung und Debugging
- Erste Schritte mit serverlosem ETL auf AWS Glue

Zusätzliche Informationen

Ermitteln der Dateigröße

Es gibt keine einfache Methode, um festzustellen, ob eine Datei zu groß oder zu klein ist. Die Auswirkung der Dateigröße auf die Verarbeitungsleistung hängt von der Konfiguration Ihres Clusters ab. In Core Hadoop empfehlen wir, Dateien mit einer Größe von 128 MB oder 256 MB zu verwenden, um die Blockgröße optimal zu nutzen.

Für die meisten Textdatei-Workloads auf AWS Glue empfehlen wir eine Dateigröße zwischen 100 MB und 1 GB für einen 5-10 DPU-Cluster. Um die beste Größe der Eingabedateien zu ermitteln, überwachen Sie den Vorverarbeitungsbereich Ihres AWS Glue Glue-Auftrags und überprüfen Sie dann die CPU-Auslastung und die Speicherauslastung des Auftrags.

Zusätzliche Überlegungen

Wenn die Leistung in den frühen ETL-Phasen einen Engpass darstellt, sollten Sie die Datendateien vor der Verarbeitung gruppieren oder zusammenführen. Wenn Sie die vollständige Kontrolle über den Dateigenerierungsprozess haben, kann es noch effizienter sein, Datenpunkte auf dem Quellsystem selbst zu aggregieren, bevor die Rohdaten an AWS gesendet werden.

Orchestrieren Sie eine ETL-Pipeline mit Validierung, Transformation und Partitionierung mithilfe von AWS Step Functions

Erstellt von Sandip Gangapadhyay (AWS)

Übersicht

Dieses Muster beschreibt, wie Sie eine serverlose ETL-Pipeline (Extrahieren, Transformieren und Laden) erstellen, um einen großen CSV-Datensatz zur Leistungs- und Kostenoptimierung zu validieren, zu transformieren, zu komprimieren und zu partitionieren. Die Pipeline wird von AWS Step Functions orchestriert und umfasst Funktionen zur Fehlerbehandlung, zur automatischen Wiederholung und zur Benutzerbenachrichtigung.

Wenn eine CSV-Datei in einen Bucket-Quellordner von Amazon Simple Storage Service (Amazon S3) hochgeladen wird, beginnt die ETL-Pipeline zu laufen. Die Pipeline validiert den Inhalt und das Schema der CSV-Quelldatei, wandelt die CSV-Datei in ein komprimiertes Apache Parquet-Format um, partitioniert den Datensatz nach Jahr, Monat und Tag und speichert ihn in einem separaten Ordner, damit Analysetools ihn verarbeiten können.

Der Code, der dieses Muster automatisiert GitHub, ist im Repository ETL-Pipeline mit AWS Step Functions verfügbar.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Die AWS-Befehlszeilenschnittstelle (AWS CLI) wurde mit Ihrem AWS-Konto installiert und konfiguriert, sodass Sie AWS-Ressourcen erstellen können, indem Sie einen CloudFormation AWS-Stack bereitstellen. AWS CLI Version 2 wird empfohlen. Installationsanweisungen finden Sie unter Installation, Aktualisierung und Deinstallation von AWS CLI Version 2 in der AWS-CLI-Dokumentation. Anweisungen zur AWS-CLI-Konfiguration finden Sie unter Einstellungen für Konfiguration und Anmeldeinformationsdatei in der AWS-CLI-Dokumentation.
- Ein Amazon-S3-Bucket

- Ein CSV-Datensatz mit dem richtigen Schema. (Das in diesem Muster enthaltene Code-Repository enthält eine CSV-Beispieldatei mit dem richtigen Schema und Datentyp, die Sie verwenden können.)
- Ein Webbrowser, der für die Verwendung mit der AWS-Managementkonsole unterstützt wird. (Sehen Sie sich die Liste der unterstützten Browser an.)
- Zugriff auf die AWS Glue Glue-Konsole.
- Zugriff auf die AWS Step Functions Functions-Konsole.

Einschränkungen

- In AWS Step Functions beträgt die Höchstgrenze für die Aufbewahrung von Verlaufsprotokollen 90 Tage. Weitere Informationen finden Sie unter Kontingente und Kontingente für Standard-Workflows in der AWS Step Functions Functions-Dokumentation.

Produktversionen

- Python 3.11 für AWS Lambda
- AWS Glue, Version 2.0

Architektur

Der in der Abbildung dargestellte Arbeitsablauf besteht aus diesen grundlegenden Schritten:

1. Der Benutzer lädt eine CSV-Datei in den Quellordner in Amazon S3 hoch.
2. Ein Amazon S3 S3-Benachrichtigungsereignis initiiert eine AWS Lambda Lambda-Funktion, die die Step Functions Functions-Zustandsmaschine startet.
3. Die Lambda-Funktion validiert das Schema und den Datentyp der CSV-Rohdatei.
4. Abhängig von den Validierungsergebnissen:
    a. Wenn die Überprüfung der Quelldatei erfolgreich ist, wird die Datei zur weiteren Verarbeitung in den Stage-Ordner verschoben.
    b. Schlägt die Überprüfung fehl, wird die Datei in den Fehlerordner verschoben und eine Fehlerbenachrichtigung wird über Amazon Simple Notification Service (Amazon SNS) gesendet.

5. Ein AWS Glue Glue-Crawler erstellt das Schema der Rohdatei aus dem Stage-Ordner in Amazon S3.
6. Ein AWS Glue Glue-Job transformiert, komprimiert und partitioniert die Rohdatei in das Parquet-Format.
7. Der AWS Glue Glue-Job verschiebt die Datei auch in den Transformationsordner in Amazon S3.
8. Der AWS Glue Glue-Crawler erstellt das Schema aus der transformierten Datei. Das resultierende Schema kann von jedem Analysejob verwendet werden. Sie können Amazon Athena auch verwenden, um Ad-hoc-Abfragen auszuführen.
9. Wenn die Pipeline ohne Fehler abgeschlossen wird, wird die Schemadatei in den Archivordner verschoben. Wenn Fehler auftreten, wird die Datei stattdessen in den Fehlerordner verschoben.
10. Amazon SNS sendet eine Benachrichtigung, die auf Erfolg oder Misserfolg basierend auf dem Status der Pipeline-Fertigstellung hinweist.

Alle in diesem Muster verwendeten AWS-Ressourcen sind serverlos. Es müssen keine Server verwaltet werden.

Tools

AWS-Services

- AWS Glue — AWS Glue ist ein vollständig verwalteter ETL-Service, der es Kunden erleichtert, ihre Daten für Analysen vorzubereiten und zu laden.
- AWS Step Functions — AWS Step Functions ist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen. In der grafischen Konsole von AWS Step Functions sehen Sie den Workflow Ihrer Anwendung als eine Reihe von ereignisgesteuerten Schritten.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice, der branchenführende Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) ist ein hochverfügbarer, langlebiger, sicherer und vollständig verwalteter Pub/Sub-Messaging-Service, mit dem Sie Microservices, verteilte Systeme und serverlose Anwendungen entkoppeln können.
- AWS Lambda — AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitzustellen oder zu verwalten. AWS Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.

Code

Der Code für dieses Muster ist im Repository ETL-Pipeline mit AWS Step Functions verfügbar. GitHub Das Code-Repository enthält die folgenden Dateien und Ordner:

- `template.yml`— CloudFormation AWS-Vorlage für die Erstellung der ETL-Pipeline mit AWS Step Functions.
- `parameter.json`— Enthält alle Parameter und Parameterwerte. Sie aktualisieren diese Datei, um Parameterwerte zu ändern, wie im Abschnitt Epics beschrieben.
- `myLayer/python`Ordner — Enthält Python-Pakete, die zur Erstellung der erforderlichen AWS-Lambda-Schicht für dieses Projekt benötigt werden.
- `lambda`Ordner — Enthält die folgenden Lambda-Funktionen:
  - `move_file.py`— Verschiebt den Quelldatensatz in den Archiv-, Transformations- oder Fehlerordner.
  - `check_crawler.py`— Überprüft den Status des AWS Glue Glue-Crawlers so oft, wie von der `RETRYLIMIT` Umgebungsvariablen konfiguriert, bevor er eine Fehlermeldung sendet.
  - `start_crawler.py`— Startet den AWS Glue Glue-Crawler.
  - `start_step_function.py`— Startet AWS Step Functions.
  - `start_codebuild.py`— Startet das CodeBuild AWS-Projekt.
  - `validation.py`— Validiert den Eingabe-Rohdatensatz.
  - `s3object.py`— Erzeugt die erforderliche Verzeichnisstruktur innerhalb des S3-Buckets.
  - `notification.py`— Sendet Erfolgs- oder Fehlerbenachrichtigungen am Ende der Pipeline.

Um den Beispielcode zu verwenden, folgen Sie den Anweisungen im Abschnitt Epics.

Epen

Bereiten Sie die Quelldateien vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Beispielcode-Repository.	1. Öffnen Sie die ETL-Pipeline mit dem AWS Step Functions Functions-Repository.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie auf der Haupt-Repository-Seite über der Dateiliste die Option Code aus und kopieren Sie die unter Clone with HTTPS aufgeführte URL. 3. Ändern Sie Ihr Arbeitsverzeichnis in das Verzeichnis, in dem Sie die Beispieldateien speichern möchten. 4. Geben Sie an einem Terminal oder einer Befehlszeile den folgenden Befehl ein: `git clone <repoURL>` wo `<repoURL>` bezieht sich auf die URL, die Sie in Schritt 2 kopiert haben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Parameterwerte.	Bearbeiten Sie in Ihrer lokalen Kopie des Repositorys die `parameter.json` Datei und aktualisieren Sie die Standardparameterwerte wie folgt: • `pS3BucketName` – Der Name des S3-Buckets zum Speichern der Datensätze. Die Vorlage erstellt diesen Bucket für Sie. Der Bucket-Name muss global eindeutig sein. • `pSourceFolder` – Der Name des Ordners im S3-Bucket, der zum Hochladen der CSV-Quell datei verwendet wird. • `pStageFolder` – Der Name des Ordners im S3-Bucket, der während des Vorgangs als Staging-B ereich verwendet wird. • `pTransformFolder` – Der Name des Ordners im S3-Bucket, der zum Speichern transformierter und partition ierter Datensätze verwendet wird. • `pErrorFolder` – Der Ordner im S3-Bucket, in den die CSV-Quelldatei	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	verschoben wird, wenn sie nicht validiert werden kann. • `pArchiveFolder` – Der Name des Ordners im S3-Bucket, der zum Archivieren der CSV-Quelldatei verwendet wird. • `pEmailforNotification` – Eine gültige E-Mail-Adresse für den Empfang von Erfolgs- und Fehlerbenachrichtigungen. • `pPrefix`– Eine Präfixzeichenfolge, die im Namen des AWS Glue Glue-Crawlers verwendet wird. • `pDatasetSchema` – Das Datensatz-Schema, anhand dessen die Quelldatei validiert wird. Das Python-Paket Cerberus wird für die Validierung von Quelldatensätzen verwendet. Weitere Informationen finden Sie auf der Cerberus-Website.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Quellcode in den S3-Bucket hoch.	Bevor Sie die CloudFormation Vorlage bereitstellen, die die ETL-Pipeline automatisiert, müssen Sie die Quelldate ien für die CloudFormation Vorlage verpacken und in einen S3-Bucket hochladen . Führen Sie dazu den folgenden AWS-CLI-Befehl mit Ihrem vorkonfigurierten Profil aus: `aws cloudformation package --template-file template.yml --s3-bucket <bucket_name> --output-template-file packaged.template --profile <profile_name>` Wobei: • `<bucket_name>` ist der Name eines vorhanden en S3-Buckets in der AWS-Region, in der Sie den Stack bereitstellen möchten. Dieser Bucket wird verwendet, um das Quellcodepaket für die CloudFormation Vorlage zu speichern. • `<profile_name>` ist ein gültiges AWS-CLI-Profil, das Sie bei der Einrichtung	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	von AWS CLI vorkonfiguriert haben.	

Erstellen Sie den -Stack

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation Vorlage bereit.	Führen Sie den folgenden AWS-CLI-Befehl aus, um die CloudFormation Vorlage bereitzustellen: `aws cloudformation deploy --stack-name <stack_name> --template-file packaged.template --parameter-overrides file://parameter.json --capabilities CAPABILITY_IAM --profile <profile_name>` Wobei: • `<stack_name>` ist ein eindeutiger Bezeichner für den CloudFormation Stack. • `<profile-name>` ist Ihr vorkonfiguriertes AWS-CLI-Profil.	Developer
Überprüfen Sie den Fortschritt.	Überprüfen Sie auf der CloudFormation AWS-Konsole den Fortschritt der Stack-Entwicklung. Wenn der Status	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	lautet`CREATE_COMPLETE` , wurde der Stack erfolgreich bereitgestellt.	
Notieren Sie sich den Namen der AWS Glue Glue-Datenbank.	Auf der Registerkarte Ausgaben für den Stack wird der Name der AWS Glue Glue-Datenbank angezeigt. Der Schlüsselname ist`GlueDBOutput` .	Developer

Testen Sie die Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die ETL-Pipeline.	1. Navigieren Sie zum Quellordner (oder dem Ordnernamen`source`, den Sie in der `parameter.json` Datei festgelegt haben) im S3-Bucket. 2. Laden Sie eine CSV-Beispieldatei in diesen Ordner hoch. (Das Code-Repository enthält eine Beispieldatei namens`Sample_Bank_Transaction_Raw_Dataset.csv` , die Sie verwenden können.) Durch das Hochladen der Datei wird die ETL-Pipeline über Step Functions gestartet. 3. Überprüfen Sie in der Step Functions Functions	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	-Konsole den Status der ETL-Pipeline.	
Suchen Sie nach dem partitionierten Datensatz.	Wenn die ETL-Pipeline abgeschlossen ist, stellen Sie sicher, dass der partitionierte Datensatz im Amazon S3 S3-Transformationsordner (oder dem Ordnernam `entransform` , den Sie in der `parameter.json` Datei festgelegt haben) verfügbar ist.	Developer
Suchen Sie nach der partitionierten AWS Glue Glue-Datenbank.	1. Wählen Sie in der AWS Glue Glue-Konsole die vom Stack erstellte AWS Glue Glue-Datenbank aus (dies ist die Datenbank, die Sie im vorherigen Epic notiert haben). 2. Stellen Sie sicher, dass die partitionierte Tabelle im AWS Glue Glue-Datenkatalog verfügbar ist.	Developer
Führen Sie Abfragen aus.	(Optional) Verwenden Sie Amazon Athena, um Ad-hoc-Abfragen in der partitionierten und transformierten Datenbank auszuführen. Anweisungen finden Sie in der AWS-Dokumentation unter Ausführen von SQL-Abfragen mit Amazon Athena.	Datenbank-Analyst

Fehlerbehebung

Problem	Lösung
AWS Identity and Access Management (IAM) -Berechtigungen für den AWS Glue Glue-Job und den Crawler	Wenn Sie den AWS Glue Glue-Job oder den Crawler weiter anpassen, stellen Sie sicher, dass Sie die entsprechenden IAM-Berechtigungen in der vom AWS Glue Glue-Job verwendeten IAM-Rolle gewähren oder AWS Lake Formation Datenberechtigungen gewähren. Weitere Informationen finden Sie in der AWS-Dokumentation.

Zugehörige Ressourcen

AWS-Servicedokumentation

- AWS Step Functions
- AWS Glue
- AWS Lambda
- Amazon S3
- Amazon SNS

Zusätzliche Informationen

Das folgende Diagramm zeigt den AWS Step Functions Functions-Workflow für eine erfolgreiche ETL-Pipeline im Bereich Step Functions Inspector.

Das folgende Diagramm zeigt den AWS Step Functions Functions-Workflow für eine ETL-Pipeline, die aufgrund eines Eingabevalidierungsfehlers fehlschlägt, im Bereich Step Functions Inspector.

Führen Sie erweiterte Analysen mit Amazon Redshift ML durch

Erstellt von Po Hong (AWS) und Chyanna Antonio (AWS)

Übersicht

In der Amazon Web Services (AWS) -Cloud können Sie Amazon Redshift Machine Learning (Amazon Redshift ML) verwenden, um ML-Analysen für Daten durchzuführen, die entweder in einem Amazon Redshift Redshift-Cluster oder in Amazon Simple Storage Service (Amazon S3) gespeichert sind. Amazon Redshift ML unterstützt überwachtes Lernen, das in der Regel für erweiterte Analysen verwendet wird. Zu den Anwendungsfällen für Amazon Redshift ML gehören Umsatzprognosen, Erkennung von Kreditkartenbetrug und Prognosen zum Customer Lifetime Value (CLV) oder zur Kundenabwanderung.

Amazon Redshift ML macht es Datenbankbenutzern leicht, ML-Modelle mithilfe von Standard-SQL-Befehlen zu erstellen, zu trainieren und bereitzustellen. Amazon Redshift ML verwendet Amazon SageMaker Autopilot, um anhand Ihrer Daten automatisch die besten ML-Modelle für die Klassifizierung oder Regression zu trainieren und zu optimieren, während Sie die Kontrolle und Transparenz behalten.

Alle Interaktionen zwischen Amazon Redshift, Amazon S3 und Amazon SageMaker werden abstrahiert und automatisiert. Nachdem das ML-Modell trainiert und bereitgestellt wurde, ist es als benutzerdefinierte Funktion (UDF) in Amazon Redshift verfügbar und kann in SQL-Abfragen verwendet werden.

Dieses Muster ergänzt die Lernprogramme Erstellen, Trainieren und Bereitstellen von ML-Modellen in Amazon Redshift mithilfe von SQL mit Amazon Redshift ML aus dem AWS-Blog und das SageMaker Tutorial Erstellen, Trainieren und Bereitstellen eines ML-Modells mit Amazon aus dem Getting Started Resource Center.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Bestehende Daten in einer Amazon Redshift Redshift-Tabelle

Fähigkeiten

- Vertrautheit mit den von Amazon Redshift ML verwendeten Begriffen und Konzepten, einschließlich maschinellem Lernen, Training und Prognose. Weitere Informationen dazu finden Sie unter Training ML-Modelle in der Dokumentation zu Amazon Machine Learning (Amazon ML).
- Erfahrung mit der Benutzereinrichtung von Amazon Redshift, der Zugriffsverwaltung und der Standard-SQL-Syntax. Weitere Informationen dazu finden Sie unter Erste Schritte mit Amazon Redshift in der Amazon Redshift Redshift-Dokumentation.
- Wissen und Erfahrung mit Amazon S3 und AWS Identity and Access Management (IAM).
- Erfahrung mit der Ausführung von Befehlen in der AWS-Befehlszeilenschnittstelle (AWS CLI) ist ebenfalls von Vorteil, aber nicht erforderlich.

Einschränkungen

- Der Amazon Redshift Redshift-Cluster und der S3-Bucket müssen sich in derselben AWS-Region befinden.
- Der Ansatz dieses Musters unterstützt nur Modelle des überwachten Lernens wie Regression, binäre Klassifizierung und Mehrklassenklassifizierung.

Architektur

In den folgenden Schritten wird erklärt, wie Amazon Redshift ML beim Erstellen SageMaker , Trainieren und Bereitstellen eines ML-Modells zusammenarbeitet:

1. Amazon Redshift exportiert Trainingsdaten in einen S3-Bucket.
2. SageMaker Autopilot verarbeitet die Trainingsdaten automatisch vor.
3. Nachdem die `CREATE MODEL` Anweisung aufgerufen wurde, verwendet Amazon Redshift ML sie SageMaker für das Training.
4. SageMaker Autopilot sucht nach dem ML-Algorithmus und den optimalen Hyperparametern, die die Bewertungsmetriken optimieren, und empfiehlt diese.
5. Amazon Redshift ML registriert das Ausgabe-ML-Modell als SQL-Funktion im Amazon Redshift Redshift-Cluster.
6. Die Funktion des ML-Modells kann in einer SQL-Anweisung verwendet werden.

Technologie-Stack

- Amazon Redshift
- SageMaker
- Amazon S3

Tools

- Amazon Redshift — Amazon Redshift ist ein vollständig verwalteter Data-Warehousing-Service auf Unternehmensebene im Petabyte-Bereich.
- Amazon Redshift ML — Amazon Redshift Machine Learning (Amazon Redshift ML) ist ein robuster, cloudbasierter Service, der es Analysten und Datenwissenschaftlern aller Qualifikationsstufen leicht macht, ML-Technologie zu nutzen.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist Speicher für das Internet.
- Amazon SageMaker — SageMaker ist ein vollständig verwalteter ML-Service.
- Amazon SageMaker Autopilot — SageMaker Autopilot ist ein Funktionsumfang, der wichtige Aufgaben eines automatischen maschinellen Lernprozesses (AutoML) automatisiert.

Code

Sie können ein überwachtes ML-Modell in Amazon Redshift erstellen, indem Sie den folgenden Code verwenden:

```
“CREATE MODEL customer_churn_auto_model
FROM (SELECT state,
             account_length,
             area_code,
             total_charge/account_length AS average_daily_spend,
             cust_serv_calls/account_length AS average_daily_cases,
             churn
      FROM customer_activity
      WHERE  record_date < '2020-01-01'
     )
TARGET churn
FUNCTION ml_fn_customer_churn_auto
IAM_ROLE 'arn:aws:iam::XXXXXXXXXXXX:role/Redshift-ML'
SETTINGS (
  S3_BUCKET 'your-bucket'
);”)
```

> **Note**
>
> Der `SELECT` Status kann sich auf reguläre Amazon Redshift-Tabellen, externe Amazon Redshift Spectrum-Tabellen oder auf beide beziehen.

Epen

Bereiten Sie einen Trainings- und Testdatensatz vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie einen Trainings- und Testdatensatz vor.	Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die SageMaker Amazon-Konsole. Folgen Sie den Anweisungen im Tutorial Ein Modell für maschinelles Lernen erstellen, trainieren und bereitstellen, um eine .csv- oder Apache Parquet-Datei zu erstellen, die eine Labelspalte (betreutes Training) und keinen Header enthält. **Note** Wir empfehlen, dass Sie den Rohdatensatz mischen und in einen Trainingssatz für das Training des Modells (70 Prozent) und einen Testsatz für die Leistungsbewertung	Data Scientist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	des Modells (30 Prozent) aufteilen.	

Bereiten Sie den Technologie-Stack vor und konfigurieren Sie ihn

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und konfigurieren Sie einen Amazon Redshift Redshift-Cluster.	Erstellen Sie auf der Amazon Redshift Redshift-Konsole einen Cluster gemäß Ihren Anforderungen. Weitere Informationen dazu finden Sie unter Create a cluster in der Amazon Redshift Redshift-Dokumentation. **Important** Amazon Redshift Redshift-Cluster müssen zusammen mit dem `SQL_PREVIEW` Maintenance Track erstellt werden. Weitere Informationen zu Vorschau-Tracks finden Sie unter Cluster-Wartungsspuren auswählen in der Amazon Redshift Redshift-Dokumentation.	DBA, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket zum Speichern von Trainings daten und Modellartefakten.	Erstellen Sie auf der Amazon S3 S3-Konsole einen S3-Bucket für die Trainings- und Testdaten. Weitere Informati onen zum Erstellen eines S3-Buckets finden Sie unter Erstellen eines S3-Buckets über AWS Quick Starts. **Important** Stellen Sie sicher, dass sich Ihr Amazon Redshift Redshift-Cluster und Ihr S3-Bucket in derselben Region befinden.	DBA, Cloud-Architekt
Erstellen Sie eine IAM-Richt linie und fügen Sie sie dem Amazon Redshift Redshift-Cluster hinzu.	Erstellen Sie eine IAM-Richtlinie, um dem Amazon Redshift Redshift-Cluster den Zugriff auf Amazon S3 SageMaker zu ermöglichen. Anweisungen und Schritte finden Sie unter Cluster-S etup für die Verwendung von Amazon Redshift ML in der Amazon Redshift Redshift-Dokumentation.	DBA, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erlauben Sie Amazon Redshift Redshift-Benutzern und -Gruppen den Zugriff auf Schemas und Tabellen.	Erteilen Sie Berechtigungen, um Benutzern und Gruppen in Amazon Redshift den Zugriff auf interne und externe Schemas und Tabellen zu ermöglichen. Schritte und Anweisungen finden Sie unter Berechtigungen und Besitz verwalten in der Amazon Redshift Redshift-Dokumentation.	DBA

Erstellen und trainieren Sie das ML-Modell in Amazon Redshift

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und trainieren Sie das ML-Modell in Amazon Redshift.	Erstellen und trainieren Sie Ihr ML-Modell in Amazon Redshift ML. Weitere Informationen finden Sie in der `CREATE MODEL` Erklärung in der Amazon Redshift Redshift-Dokumentation.	Entwickler, Datenwissenschaftler

Batch-Inferenz und Vorhersage in Amazon Redshift durchführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Inferenz mithilfe der generierten ML-Modellfunktion durch.	Weitere Informationen zur Durchführung von Inferenzen mithilfe der generierten ML-Modellfunktion finden Sie unter Vorhersage in der	Datenwissenschaftler, Business Intelligence-Benutzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon Redshift Redshift-Dokumentation.	

Zugehörige Ressourcen

Bereiten Sie einen Trainings- und Testdatensatz vor

- Aufbau, Schulung und Bereitstellung eines Modells für maschinelles Lernen mit Amazon SageMaker

Bereiten Sie den Technologie-Stack vor und konfigurieren Sie ihn

- Einen Amazon Redshift Redshift-Cluster erstellen
- Auswahl von Amazon Redshift Redshift-Cluster-Wartungsplänen
- Erstellen eines S3-Buckets
- Einrichtung eines Amazon Redshift-Clusters für die Verwendung von Amazon Redshift ML
- Verwaltung von Berechtigungen und Eigentum in Amazon Redshift

Erstellen und trainieren Sie das ML-Modell in Amazon Redshift

- CREATE MODEL-Anweisung in Amazon Redshift

Batch-Inferenz und Vorhersage in Amazon Redshift durchführen

- Prognose in Amazon Redshift

Sonstige Ressourcen

- Erste Schritte mit Amazon Redshift ML
- Erstellen, Trainieren und Bereitstellen von ML-Modellen in Amazon Redshift mithilfe von SQL mit Amazon Redshift ML

- Amazon Redshift Redshift-Partner
- AWS-Kompetenzpartner für maschinelles Lernen

Abfragen von Amazon DynamoDB-Tabellen mit SQL mithilfe von Amazon Athena

Erstellt von Gavin Perrie (AWS), Ajit Ambike (AWS) und Brad Yates (AWS)

Übersicht

Wenn Ihre Daten andere Quellen als Amazon Simple Storage Service (Amazon S3) enthalten, können Sie Verbundabfragen verwenden, um auf diese relationalen, nicht-relationalen, Objekt- oder benutzerdefinierten Datenquellen zuzugreifen. Dieses Muster zeigt, wie der föderierte Abfragezugriff über Amazon Athena auf Amazon DynamoDB mithilfe eines SQL-Datenquellen-Connectors konfiguriert wird.

Mit diesem Muster können Sie Folgendes tun:

- Fragen Sie DynamoDB-Tabellen mithilfe von SQL ab.
- Führen Sie föderierte SQL-Abfragen in Athena aus und verknüpfen Sie DynamoDB-Tabellen mit anderen unterstützten Datenquellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine DynamoDB-Tabelle.
- Eine Athena-Arbeitsgruppe, die die Athena-Engine Version 2 verwenden soll. Anweisungen finden Sie in der Athena-Dokumentation.
- Ein S3-Bucket, in dem die `AthenaDynamoDBConnector` AWS Lambda Funktion die Daten weitergeben kann. Der S3-Bucket und die Lambda-Funktion müssen sich in derselben AWS-Region befinden.

Wenn Sie zum ersten Mal auf Athena zugreifen, benötigen Sie einen zusätzlichen S3-Bucket, den Sie als Speicherort für Abfrageergebnisse verwenden können. Anweisungen finden Sie in der Athena-Dokumentation.

Einschränkungen

- Schreiboperationen wie INSERT INTO werden nicht unterstützt.

Versionen der Produkte

- Athena Query Federation veröffentlicht am GitHub

Architektur

Zielarchitektur

Das folgende Diagramm zeigt den Verbindungsfluss, nachdem das Muster eingerichtet wurde. Der Benutzer stellt eine Verbindung zu Amazon Athena her, um die Anfrage bereitzustellen. Athena übergibt die Abfrage und das Ziel an die Lambda-Funktion des DynamoDB-Datenquellenkonnektors, die die Daten abruft und an Athena zurückgibt. Wenn große Datenmengen zurückgegeben werden, speichert Athena die temporären Ergebnisse im Spill-Bucket, bevor der gesamte Datensatz verpackt und zurückgegeben wird.

Tools

AWS-Services

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon Simple Storage Service (Amazon S3) analysieren können. Dieses Muster verwendet Amazon Athena DynamoDB Connector, ein Tool, das mit dem Amazon Athena Query Federation SDK erstellt und als AWS Lambda Anwendung über das installiert wird. AWS Serverless Application Repository
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code-Repository

Der Code für dieses Muster ist im GitHub Athena Query Federation Repository verfügbar.

Epen

DynamoDB-Datenquellenconnector einrichten und testen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die AthenaDynamoDBConnector Anwendung bereit.	Gehen Sie zur Bereitstellung AthenaDynamo DBConnecter wie folgt vor: 1. Melden Sie sich bei der AWS Management Console an und wählen Sie die aus AWS-Region , die Sie für die DynamoDB-Tabelle und den Spill-Bucket verwenden . 2. Öffnen Sie das Serverless Application Repository unter https://console.aws.amazon.com/serverlessrepo/. 3. Wählen Sie im Navigationsbereich die Option Verfügbare Anwendungen aus. 4. Aktivieren Sie für den AWS Identity and Access Management (IAM-) Zugriff unter der Suchleiste das Kontrollkästchen Apps anzeigen, die benutzerdefinierte IAM-Rollen oder Ressourcenrichtlinien erstellen.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Suchen Sie nach Amazon Athena Federation AthenaDynamoDBConnector, wählen Sie sie aus und stellen Sie sicher, dass es sich bei dem aufgeführten Autor um Amazon Athena Federation handelt. 6. Geben Sie in den Anwendungseinstellungen die folgenden Werte ein: • SpillBucket– Ort, an den die Funktion Daten übertragen kann. • AthenaCatalogName– Der Name der Lambda-Funktion, die erstellt wird. Der Name wird auch als Datenquellenname in Athena verwendet. 7. Aktivieren Sie das Kontrollkästchen, um die Erstellung von IAM-Rollen und -Richtlinien zu bestätigen. 8. Wählen Sie Bereitstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Datenquelle für Athena.	Gehen Sie wie folgt vor, um die Datenquelle zu erstellen: 1. Öffnen Sie die Athena-Konsole unter https://console.aws.amazon.com/athena/. 2. Erweitern Sie den Navigationsbereich und wählen Sie Datenquellen aus. 3. Klicken Sie auf Create data source. 4. Wählen Sie Amazon DynamoDB. 5. Geben Sie den Namen der Datenquelle ein. 6. Wählen Sie die Lambda-Funktion aus, die Sie erstellt haben. 7. Überprüfen Sie die Details und wählen Sie Datenquelle erstellen aus.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie Athena, um die DynamoDB-Tabelle abzufragen.	Gehen Sie wie folgt vor, um die DynamoDB-Tabelle abzufragen: 1. Erweitern Sie auf der Athena-Konsole den Navigationsbereich und wählen Sie Query-Editor aus. 2. Wählen Sie in der Dropdownliste Datenquelle die Datenquelle aus, die Sie erstellt haben. 3. Vergewissern Sie sich, dass die DynamoDB-Tabellen unter Tabellen aufgeführt sind. 4. Führen Sie die Abfrage aus.	App-Developer

Fehlerbehebung

Problem	Lösung
Die Abfrage schlägt fehl mit. *`GENERIC_INTERNAL_ERROR: The bucket is in this region: <region>`*	Stellen Sie sicher, dass der Athena Spill Bucket und die Lambda-Funktion in derselben Datei erstellt wurden. AWS-Region
Die neu erstellte Datenquelle ist auf der Athena-Konsole nicht sichtbar.	Athena-Datenkataloge sind regional. Stellen Sie sicher, dass der in der Region eingesetzt `AthenaDynamoDBConnector` wurde, in der Sie Athena verwenden möchten.
Sie können die Abfrage nicht für die neu erstellte Datenquelle ausführen.	Vergewissern Sie sich, dass der Speicherort für das Abfrageergebnis festgelegt wurde.

Zugehörige Ressourcen

- Amazon Athena DynamoDB-Konnektor
- Amazon Athena Verbundabfrage

Mit Athena auf Amazon DynamoDB-Tabellen zugreifen, diese abfragen und verbinden

Erstellt von Moinul Al-Mamun (AWS)

Übersicht

Dieses Muster zeigt Ihnen, wie Sie mithilfe des Amazon Athena DynamoDB-Connectors eine Verbindung zwischen Amazon Athena und Amazon DynamoDB einrichten. Der Connector verwendet eine AWS-Lambda-Funktion, um die Daten in DynamoDB abzufragen. Sie müssen keinen Code schreiben, um die Verbindung einzurichten. Nachdem die Verbindung hergestellt wurde, können Sie schnell auf DynamoDB-Tabellen zugreifen und diese analysieren, indem Sie Athena Federated Query verwenden, um SQL-Befehle von Athena auszuführen. Sie können auch eine oder mehrere DynamoDB-Tabellen miteinander oder mit anderen Datenquellen wie Amazon Redshift oder Amazon Aurora verbinden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit Berechtigungen zur Verwaltung von DynamoDB-Tabellen, Athena-Datenquellen, Lambda und AWS Identity and Access Management (IAM) -Rollen
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket, in dem Athena Abfrageergebnisse speichern kann
- Ein S3-Bucket, in dem der Athena DynamoDB Connector die Daten kurzfristig speichern kann
- Eine AWS-Region, die Athena Engine Version 2 unterstützt
- IAM-Berechtigungen für den Zugriff auf Athena und die erforderlichen S3-Buckets
- Amazon Athena DynamoDB Connector, installiert

Einschränkungen

Das Abfragen von DynamoDB-Tabellen ist kostenpflichtig. Tabellengrößen, die einige Gigabyte (GBs) überschreiten, können hohe Kosten verursachen. Wir empfehlen, dass Sie die Kosten berücksichtigen, bevor Sie einen vollständigen Tabellen-SCAN-Vorgang durchführen. Weitere Informationen finden Sie unter Amazon DynamoDB – Preise. Um die Kosten zu senken und eine hohe Leistung zu erzielen, empfehlen wir, in Ihrer Abfrage immer LIMIT zu verwenden (z.

B.`SELECT * FROM table1 LIMIT 10`). Bevor Sie eine JOIN- oder GROUP BY-Abfrage in einer Produktionsumgebung ausführen, sollten Sie außerdem die Größe Ihrer Tabellen berücksichtigen. Wenn Ihre Tabellen zu groß sind, ziehen Sie alternative Optionen in Betracht, z. B. die Migration der Tabelle zu Amazon S3.

Architektur

Das folgende Diagramm zeigt, wie ein Benutzer eine SQL-Abfrage für eine DynamoDB-Tabelle von Athena aus ausführen kann.

Das Diagramm zeigt den folgenden Workflow:

1. Um eine DynamoDB-Tabelle abzufragen, führt ein Benutzer eine SQL-Abfrage von Athena aus.
2. Athena initiiert eine Lambda-Funktion.
3. Die Lambda-Funktion fragt die angeforderten Daten in der DynamoDB-Tabelle ab.
4. DynamoDB gibt die angeforderten Daten an die Lambda-Funktion zurück. Anschließend überträgt die Funktion die Abfrageergebnisse über Athena an den Benutzer.
5. Die Lambda-Funktion speichert Daten im S3-Bucket.

Technologie-Stack

- Amazon Athena
- Amazon-DynamoDB
- Amazon S3
- AWS Lambda

Tools

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon S3 analysieren können.
- Amazon Athena DynamoDB Connector ist ein AWS-Tool, mit dem Athena mithilfe von SQL-Abfragen eine Verbindung mit DynamoDB herstellen und auf Ihre Tabellen zugreifen kann.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.

- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.

Epen

DynamoDB-Beispieltabellen erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die erste Beispieltabelle.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die DynamoDB-Konsole. 2. Wählen Sie Create table (Tabelle erstellen) aus. 3. Geben Sie als Tabellenname dydbtable1 ein. 4. Geben Sie als Partitionsschlüssel ein. PK1 5. Geben Sie als Sortierschlüssel ein SK1. 6. Wählen Sie im Bereich Tabelleneinstellungen die Option Einstellungen anpassen aus. 7. Wählen Sie im Abschnitt Tabellenklasse die Option DynamoDB Standard aus. 8. Wählen Sie im Abschnitt Lese-/Schreibkapazitätseinstellungen für den Kapazitätsmodus die Option On-Demand aus.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	9. Wählen Sie im Abschnitt Verschlüsselung im Ruhezustand die Option Owned by Amazon DynamoDB aus. 10. Wählen Sie Create table (Tabelle erstellen) aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie Beispieldaten in die erste Tabelle ein.	1. Öffnen Sie die DynamoDB-Konsole.
	2. Wählen Sie im Navigationsbereich Tabelle und dann Ihre Tabelle in der Spalte Name aus.
	3. Wählen Sie Aktionen und dann Element erstellen aus.
	4. Wählen Sie JSON-Ansicht.
	5. Deaktivieren Sie in der Titelleiste des Attributs-Editors die Option DynamoDB-JSON anzeigen.
	6. Geben Sie im Attribut-Editor nacheinander die folgenden Beispieldaten ein:
	
	`{ "PK1": "1234", "SK1": "info", "Salary": "5000" }`
	
	`{ "PK1": "1235", "SK1": "info", "Salary": "5200" }`
		Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die zweite Beispieltabelle.	1. Öffnen Sie die DynamoDB-Konsole. 2. Wählen Sie Create table aus. 3. Geben Sie als Tabellenname dydbtable2 ein. 4. Geben Sie für Partition key (Partitionsschlüssel) den Wert PK2 ein. 5. Geben Sie als Sortierschlüssel ein. SK2 6. Wählen Sie im Bereich Tabelleneinstellungen die Option Einstellungen anpassen aus. 7. Wählen Sie im Abschnitt Tabellenklasse die Option DynamoDB Standard aus. 8. Wählen Sie im Abschnitt Lese-/Schreibkapazitätseinstellungen für den Kapazitätsmodus die Option On-Demand aus. 9. Wählen Sie im Abschnitt Verschlüsselung im Ruhezustand die Option Owned by Amazon DynamoDB aus. 10. Wählen Sie Create table (Tabelle erstellen) aus.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie Beispieldaten in die zweite Tabelle ein.	1. Öffnen Sie die DynamoDB-Konsole.
	2. Wählen Sie im Navigationsbereich Tabelle und dann Ihre Tabelle in der Spalte Name aus.
	3. Wählen Sie Aktionen und dann Element erstellen aus.
	4. Deaktivieren Sie in der Titelleiste des Attributs-Editors die Option DynamoDB-JSON anzeigen.
	5. Geben Sie im Attribut-Editor nacheinander die folgenden Beispieldaten ein:
	`{ "PK2": "1234", "SK2": "bonus", "Bonus": "500" }`
	`{ "PK2": "1235", "SK2": "bonus", "Bonus": "1000" }`
		Developer

Erstellen Sie eine Datenquelle in Athena für DynamoDB

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie den Datenquellenkonnektor ein.	Erstellen Sie eine Datenquelle für DynamoDB und anschließend eine Lambda-Funktion, um eine Verbindung zu dieser Datenquelle herzustellen. 1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Athena-Konsole. 2. Wählen Sie im Navigationsbereich Datenquellen und dann Datenquelle erstellen aus. 3. Wählen Sie die Amazon DynamoDB DynamoDB-Datenquelle und dann Weiter. 4. Geben Sie im Abschnitt Datenquellendetails als Datenquellenname TestDynamoDB ein. 5. Wählen Sie im Abschnitt Verbindungsdetails eine Lambda-Funktion aus, die bereits bereitgestellt wurde, oder wählen Sie Lambda-Funktion erstellen, wenn Sie keine Lambda-Funktion für dieses Muster verwenden können. Hinweis: Weitere Informati	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	onen zum Erstellen einer Lambda-Funktion finden Sie unter Getting started with Lambda im Lambda Developer Guide. 6. (Optional) Wenn Sie die Funktion „Lambda erstellen “ wählen, müssen Sie die CloudFormation AWS-Vorlage konfigurieren, die in der Java-Anwendung enthalten ist, bevor Sie diesen Stack bereitstellen. Die Vorlage umfasst ApplicationName, SpillBucket AthenaCatalogName, und andere Anwendungseinstellungen. Hinweis: Nachdem Sie diese Java-basierte Anwendung bereitgestellt haben, erstellt der Stack eine Lambda-Funktion, die es Athena ermöglicht, mit DynamoDB zu kommunizieren. Dadurch können Sie über SQL-Befehle auf Ihre Tabellen zugreifen. 7. Stellen Sie Ihre Lambda-Funktion bereit. 8. Wählen Sie Weiter aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die Lambda-Funktion auf den S3-Spill-Bucket zugreifen kann.	1. Öffnen Sie die Lambda-Konsole. 2. Wählen Sie im Navigationsbereich Funktionen und dann die Funktion aus, die Sie zuvor erstellt haben. 3. Wählen Sie die Registerkarte Konfiguration aus. 4. Wählen Sie im linken Bereich die Option Umgebungsvariablen aus, und vergewissern Sie sich dann, dass der Wert für den Schlüssel lautet `spill_bucket` . 5. Wählen Sie im linken Bereich Berechtigungen und dann im Abschnitt Ausführungsrolle die angehängte IAM-Rolle aus. Hinweis: Sie werden zu der IAM-Rolle weitergeleitet, die Ihrer Lambda-Funktion in der IAM-Konsole zugeordnet ist. 6. Vergewissern Sie sich, dass Sie Schreibberechtigungen für den Bucket haben. `spill_bucket` Wenn Sie auf Fehler stoßen, finden Sie im Abschnitt	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Zusätzliche Informationen in diesem Muster eine Anleitung.	

Greifen Sie von Athena aus auf DynamoDB-Tabellen zu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fragen Sie die DynamoDB-Tabellen ab.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Athena-Konsole. 2. Wählen Sie im Navigationsbereich Datenquellen und dann Datenquelle erstellen aus. 3. Wählen Sie im Navigationsbereich die Option Query Editor (Abfrage-Editor) aus. 4. Wählen Sie auf der Registerkarte Editor im Bereich Daten für Datenquelle Ihre Datenquelle aus. 5. Als Datenbank wählen Sie Ihre Datenbank aus. 6. Geben Sie für Abfrage 1 die folgende Abfrage ein: `SELECT * FROM dydbtable1 t1;` 7. Wählen Sie Ausführen aus, und überprüfen Sie dann die Ausgabe in der Tabelle.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Geben Sie für Abfrage 2 die folgende Abfrage ein: `SELECT * FROM dydbtable2 t2;` 9. Wählen Sie Ausführen aus, und überprüfen Sie dann die Ausgabe in der Tabelle.	
Verbinden Sie die beiden DynamoDB-Tabellen.	DynamoDB ist ein NoSQL-Datenspeicher und unterstützt den SQL-Join-Vorgang nicht. Folglich müssen Sie einen Join-Vorgang für zwei DynamoDB-Tabellen ausführen: 1. Wählen Sie das Plussymbol, um eine weitere Abfrage zu erstellen. 2. Geben Sie für Abfrage 3 die folgende Abfrage ein: `SELECT pk1, salary, bonus FROM dydbtable1 t1 JOIN dydbtable2 t2 ON t1.pk1 = t2.pk2;`	Developer

Zugehörige Ressourcen

- Amazon Athena DynamoDB-Konnektor (AWS Labs)
- Abfragen beliebiger Datenquellen mit der neuen Verbundabfrage von Amazon Athena (AWS Big Data Blog)

- Versionsreferenz der Athena-Engine (Athena-Benutzerhandbuch)
- Vereinfachen Sie die Datenextraktion und -analyse mit Amazon DynamoDB mithilfe von AWS Glue und Amazon Athena (AWS-Datenbank-Blog)

Zusätzliche Informationen

Wenn Sie in Athena eine Abfrage mit `spill_bucket` im `{bucket_name}/folder_name/` Format ausführen, erhalten Sie möglicherweise die folgende Fehlermeldung:

```
"GENERIC_USER_ERROR: Encountered an exception[java.lang.RuntimeException] from your
 LambdaFunction[arn:aws:lambda:us-east-1:xxxxxx:function:testdynamodb] executed in
 context[retrieving meta-data] with message[You do NOT own the spill bucket with the
 name: s3://amzn-s3-demo-bucket/athena_dynamodb_spill_data/]
This query ran against the "default" database, unless qualified by the query. Please
 post the error message on our forum  or contact customer support with Query Id:
 [query-id]"
```

Um diesen Fehler zu beheben, aktualisieren Sie die Umgebungsvariable der Lambda-Funktion `spill_bucket` auf `{bucket_name_only}` und aktualisieren Sie dann die folgende Lambda-IAM-Richtlinie für den Bucket-Schreibzugriff:

```
{
             "Action": [
                 "s3:GetObject",
                 "s3:ListBucket",
                 "s3:GetBucketLocation",
                 "s3:GetObjectVersion",
                 "s3:PutObject",
                 "s3:PutObjectAcl",
                 "s3:GetLifecycleConfiguration",
                 "s3:PutLifecycleConfiguration",
                 "s3:DeleteObject"
             ],
             "Resource": [
                 "arn:aws:s3:::spill_bucket",
                 "arn:aws:s3:::spill_bucket/*"
             ],
             "Effect": "Allow"
         }
```

Alternativ können Sie den Athena-Datenquellenconnector, den Sie zuvor erstellt haben, entfernen und ihn neu erstellen, indem Sie nur `{bucket_name}` für verwenden. `spill_bucket`

Richten Sie einen nutzbaren Mindestdatenraum für die gemeinsame Nutzung von Daten zwischen Organisationen ein

Erstellt von Ramy Hcini (Think-IT), Ismail Abdellaoui (Think-IT), Malte Gasseling (Think-IT), Jorge Hernandez Suarez (AWS) und Michael Miller (AWS)

Übersicht

Datenräume sind föderierte Netzwerke für den Datenaustausch mit Vertrauen und Kontrolle über die eigenen Daten als Kernprinzipien. Sie ermöglichen es Unternehmen, Daten in großem Umfang zu teilen, auszutauschen und zusammenzuarbeiten, indem sie eine kostengünstige und technologieunabhängige Lösung bieten.

Datenräume haben das Potenzial, die Bemühungen für eine nachhaltige future erheblich voranzutreiben, indem datengesteuerte Problemlösungen mit einem end-to-end Ansatz eingesetzt werden, der alle relevanten Interessengruppen einbezieht.

Dieses Muster führt Sie durch das Beispiel, wie zwei Unternehmen die Datenraum-Technologie auf Amazon Web Services (AWS) nutzen können, um ihre Strategie zur Reduzierung der CO2-Emissionen voranzutreiben. In diesem Szenario liefert Unternehmen X Daten zu den CO2-Emissionen, die Unternehmen Y verbraucht. Im Abschnitt Zusätzliche Informationen finden Sie die folgenden Einzelheiten zur Datenraumspezifikation:

- Teilnehmer
- Geschäftsszenario
- Behörde für den Datenraum
- Komponenten des Datenraums
- Dienste für den Datenraum
- Daten, die ausgetauscht werden sollen
- Datenmodell
- Tractus-X EDC-Anschluss

Das Muster umfasst Schritte für Folgendes:

- Bereitstellung der Infrastruktur, die für einen Basisdatenraum erforderlich ist, auf dem zwei Teilnehmer laufen AWS.

- Sicherer Austausch von Daten zur Kohlenstoffemissionsintensität mithilfe der Konnektoren.

Dieses Muster stellt einen Kubernetes-Cluster bereit, der Datenraum-Konnektoren und deren Dienste über Amazon Elastic Kubernetes Service (Amazon EKS) hostet.

Die Steuerungsebene und die Datenebene von Eclipse Dataspace Components (EDC) werden beide auf Amazon EKS bereitgestellt. Das offizielle Tractus-X Helm-Diagramm stellt PostgreSQL- und Vault-Dienste als Abhängigkeiten bereit. HashiCorp

Darüber hinaus wird der Identitätsdienst auf Amazon Elastic Compute Cloud (Amazon EC2) bereitgestellt, um ein reales Szenario mit einem Minimum Viable Data Space (MVDS) zu replizieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein Aktiv AWS-Konto zur Bereitstellung der Infrastruktur in der von Ihnen ausgewählten AWS-Region
- Ein AWS Identity and Access Management (IAM-) Benutzer mit Zugriff auf Amazon S3, der vorübergehend als technischer Benutzer verwendet wird (Der EDC-Connector unterstützt derzeit nicht die Verwendung von Rollen. Wir empfehlen, dass Sie einen IAM-Benutzer speziell für diese Demo erstellen und diesem Benutzer eingeschränkte Berechtigungen zuweisen.)
- AWS Command Line Interface (AWS CLI) in der von Ihnen ausgewählten Version installiert und konfiguriert AWS-Region
- AWS Sicherheitsanmeldedaten
- eksctl auf Ihrer Workstation
- Git auf deiner Workstation
- kubectl
- Helm
- Postbote
- Ein AWS Certificate Manager (ACM) SSL/TLS-Zertifikat
- Ein DNS-Name, der auf einen Application Load Balancer verweist (der DNS-Name muss durch das ACM-Zertifikat abgedeckt sein)
- HashiCorp Tresor (Informationen AWS Secrets Manager zur Verwaltung von Geheimnissen finden Sie im Abschnitt Zusätzliche Informationen.)

Produktversionen

- AWS CLI Version 2+
- Postman-Sammlung v2.1

Einschränkungen

- Konnektorauswahl – Diese Bereitstellung verwendet einen EDC-basierten Konnektor. Achten Sie jedoch darauf, die Stärken und Funktionen der EDC - und FIWARE True-Konnektoren zu berücksichtigen, um eine fundierte Entscheidung zu treffen, die den spezifischen Anforderungen der Implementierung entspricht.
- Aufbau des EDC-Konnektors – Die gewählte Bereitstellungslösung basiert auf der Tractus-X EDC Connector Helm-Übersicht, einer etablierten und ausführlich getesteten Implementierungsoption. Die Entscheidung, dieses Diagramm zu verwenden, basiert auf seiner allgemeinen Verwendung und der Aufnahme wesentlicher Erweiterungen in der bereitgestellten Version. PostgreSQL und HashiCorp Vault sind zwar Standardkomponenten, Sie haben jedoch die Flexibilität, Ihren eigenen Connector-Build bei Bedarf anzupassen.
- Zugriff auf private Cluster – Der Zugriff auf den bereitgestellten EKS-Cluster ist auf private Kanäle beschränkt. Die Interaktion mit dem Cluster erfolgt ausschließlich mithilfe von `kubectl` und IAM. Der öffentliche Zugriff auf die Clusterressourcen kann mithilfe von Load Balancern und Domainnamen ermöglicht werden. Diese müssen selektiv implementiert werden, um bestimmte Dienste einem breiteren Netzwerk zugänglich zu machen. Wir empfehlen jedoch nicht, öffentlichen Zugriff zu gewähren.
- Sicherheitsfokus – Der Schwerpunkt liegt auf der Abstraktion von Sicherheitskonfigurationen anhand von Standardspezifikationen, sodass Sie sich auf die Schritte konzentrieren können, die beim Datenaustausch mit dem EDC-Konnektor erforderlich sind. Die Standardsicherheitseinstellungen werden zwar beibehalten, es ist jedoch unerlässlich, die sichere Kommunikation zu aktivieren, bevor Sie den Cluster dem öffentlichen Netzwerk zugänglich machen. Diese Vorsichtsmaßnahme gewährleistet eine solide Grundlage für eine sichere Datenverarbeitung.
- Infrastrukturkosten – Eine Schätzung der Infrastrukturkosten finden Sie unter. AWS -Preisrechner Eine einfache Berechnung zeigt, dass die Kosten für die bereitgestellte Infrastruktur bis zu 162,92 USD pro Monat betragen können.

Architektur

Die MVDS-Architektur umfasst zwei virtuelle private Clouds (VPCs), eine für den Identitätsdienst Dynamic Attribute Provisioning System (DAPS) und eine für Amazon EKS.

DAPS-Architektur

Das folgende Diagramm zeigt, wie DAPS auf EC2 Instances ausgeführt wird, die von einer Auto Scaling Scaling-Gruppe gesteuert werden. Ein Application Load Balancer und eine Routing-Tabelle machen die DAPS-Server verfügbar. Amazon Elastic File System (Amazon EFS) synchronisiert die Daten zwischen den DAPS-Instances.

Amazon EKS-Architektur

Datenräume sind als technologieunabhängige Lösungen konzipiert, und es gibt mehrere Implementierungen. Dieses Muster verwendet einen Amazon EKS-Cluster, um die technischen Komponenten des Datenraums bereitzustellen. Das folgende Diagramm zeigt die Bereitstellung des EKS-Clusters. Worker-Knoten werden in privaten Subnetzen installiert. Die Kubernetes-Pods greifen auf die Amazon Relational Database Service (Amazon RDS) for PostgreSQL-Instance zu, die sich ebenfalls in den privaten Subnetzen befindet. Die Kubernetes-Pods speichern gemeinsam genutzte Daten in Amazon S3.

Tools

AWS Dienste

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend AWS-Konten zu verwalten.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Elastic File System (Amazon EFS) hilft Ihnen bei der Erstellung und Konfiguration gemeinsam genutzter Dateisysteme in der AWS Cloud.
- Mit Amazon Elastic Kubernetes Service (Amazon EKS) können Sie Kubernetes ausführen, AWS ohne dass Sie Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten müssen.

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Datenverkehr auf EC2 Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen.

Andere Tools

- eksctl ist ein Befehlszeilenprogramm zum Erstellen und Verwalten von Kubernetes-Clustern auf Amazon EKS.
- Git ist ein verteiltes Open-Source-Versionskontrollsystem.
- HashiCorp Vault bietet sicheren Speicher mit kontrolliertem Zugriff auf Anmeldeinformationen und andere vertrauliche Informationen.
- Helm ist ein Open-Source-Paketmanager für Kubernetes, der Sie bei der Installation und Verwaltung von Anwendungen auf Ihrem Kubernetes-Cluster unterstützt.
- kubectl ist eine Befehlszeilenschnittstelle, mit der Sie Befehle für Kubernetes-Cluster ausführen können.
- Postman ist eine API-Plattform.

Code-Repository

Die Kubernetes-Konfigurations-YAML-Dateien und Python-Skripte für dieses Muster sind im Repository verfügbar. GitHub aws-patterns-edc Das Muster verwendet auch das Tractus-X EDC-Repository.

Bewährte Methoden

Amazon EKS und Isolierung der Infrastrukturen der Teilnehmer

Namespaces in Kubernetes trennen nach diesem Muster die Infrastruktur des Anbieters von Unternehmen X von der Infrastruktur des Verbrauchers von Unternehmen Y ab. Weitere Informationen finden Sie in den EKS Best Practices Guides.

In einer realistischeren Situation hätte jeder Teilnehmer einen separaten Kubernetes-Cluster, der in seinem eigenen Cluster läuft. AWS-Konto Die gemeinsame Infrastruktur (DAPS in diesem Muster) wäre für die Teilnehmer des Datenraums zugänglich und gleichzeitig vollständig von den Infrastrukturen der Teilnehmer getrennt.

Epen

Richten Sie die Umgebung ein und stellen Sie einen EKS-Cluster und -Instanzen bereit EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Führen Sie den folgenden Befehl aus, um das Repository auf Ihre Workstation zu klonen: `git clone https://github.com/Think-iT-Labs/aws-patterns-edc` Die Workstation muss Zugriff auf Ihre haben AWS-Konto.	DevOps Ingenieur
Stellen Sie den Kubernetes-Cluster bereit und richten Sie Namespaces ein.	Um einen vereinfachten Standard-EKS-Cluster in Ihrem Konto bereitzustellen, führen Sie den folgenden `eksctl` Befehl auf der Workstation aus, auf der Sie das Repo geklont haben: `eksctl create cluster` Der Befehl erstellt die VPC sowie private und öffentliche Subnetze, die sich über drei verschiedene Availability Zones erstrecken. Nachdem die Netzwerkschicht erstellt wurde, erstellt der Befehl zwei `m5.large` EC2 Instanzen	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	innerhalb einer Auto Scaling Scaling-Gruppe.
	
	Weitere Informationen und Beispielausgaben finden Sie im eksctl-Handbuch.
	
	Nachdem Sie den privaten Cluster bereitgestellt haben, fügen Sie den neuen EKS-Cluster zu Ihrer lokalen Kubernetes-Konfiguration hinzu, indem Sie den folgenden Befehl ausführen:
	
	`aws eks update-kubeconfig --name <EKS CLUSTER NAME> --region <AWS REGION>`
	
	Dieses Muster verwendet den `eu-west-1` AWS-Region , um alle Befehle auszuführen. Sie können jedoch dieselben Befehle in Ihrer bevorzugten Version ausführen AWS-Region.
	
	Führen Sie den folgenden Befehl aus, um zu überprüfen, ob Ihre EKS-Knoten ausgeführt werden und sich im Bereitschaftszustand befinden:
	
	`kubectl get nodes`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie die Namespaces ein.	Führen Sie die folgenden Befehle aus, um Namespaces für den Anbieter und den Verbraucher zu erstellen:
	`kubectl create ns provider`
	`kubectl create ns consumer`
	In diesem Muster ist es wichtig, `provider` und `consumer` als Namespaces zu verwenden, damit sie den Konfigurationen in den nächsten Schritten entsprechen.
		DevOps Ingenieur

Stellen Sie den Identitätsdienst bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie DAPS bereit, indem Sie AWS CloudFormation	Um die Verwaltung von DAPS-Vorgängen zu vereinfachen, ist der DAPS-Server auf Instanzen installiert. EC2 Verwenden Sie die Vorlage, um DAPS zu installieren.AWS CloudFormation Sie benötigen das ACM-Zertifikat und den DNS-Namen aus dem Abschnitt Voraussetzungen. Die Vorlage stellt Folgendes bereit und konfiguriert es:	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Application Load Balancer • Auto Scaling-Gruppe • EC2 Instanzen, die mit Benutzerdaten konfiguriert sind, um alle erforderlichen Pakete zu installieren • IAM-Rollen • DAPS Sie können die AWS CloudFormation Vorlage bereitstellen, indem Sie sich bei der AWS CloudFormation Konsole anmelden AWS Management Console und diese verwenden. Sie können die Vorlage auch mithilfe eines AWS CLI Befehls wie dem folgenden bereitstellen: `aws cloudformation create-stack --stack-name daps \ --template-body file://aws-patterns-edc/cloudformation.yml --parameters \ ParameterKey=CertificateARN,ParameterValue=<ACM Certificate ARN> \ ParameterKey=DNSName,ParameterValue=<DNS name> \ ParameterKey=InstanceType,Paramete`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`rValue=<EC2 instance type> \ ParameterKey=EnvironmentName,ParameterValue=<Environment Name> --capabilities CAPABILITY_NAMED_IAM` Der Name der Umgebung ist Ihre eigene Wahl. Wir empfehlen, einen aussagekräftigen Begriff zu verwenden `DapsInfrastructure`, z. B. weil er sich in den AWS Ressourcen-Tags wiederfindet. Für dieses Muster `t3.small` ist es groß genug, um den DAPS-Workflow auszuführen, der über drei Docker-Container verfügt. Die Vorlage stellt die EC2 Instanzen in privaten Subnetzen bereit. Das bedeutet, dass auf die Instanzen nicht direkt über SSH (Secure Shell) aus dem Internet zugegriffen werden kann. Die Instanzen werden mit der erforderlichen IAM-Rolle und dem AWS Systems Manager Agenten ausgestattet, um den Zugriff auf die laufenden Instanzen über	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	den Session Manager zu ermöglichen, eine Funktion von. AWS Systems Manager
	
	Wir empfehlen die Verwendung von Session Manager für den Zugriff. Alternativ könnten Sie einen Bastion-Host bereitstellen, der den SSH-Zugriff aus dem Internet ermöglicht. Wenn Sie den Bastion-Host-Ansatz verwenden, kann es noch einige Minuten dauern, bis die EC2 Instanz ausgeführt wird.
	
	Nachdem die AWS CloudFormation Vorlage erfolgreich bereitgestellt wurde, verweisen Sie den DNS-Namen auf Ihren Application Load Balancer Balancer-DNS-Namen. Führen Sie zur Bestätigung den folgenden Befehl aus:
	
	`dig <DNS NAME>`
	
	Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:
	
	`; <<>> DiG 9.16.1-Ubuntu <<>> edc-pattern.think-it.io`
	`;; global options: +cmd`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42344 ;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1 ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 65494 ;; QUESTION SECTION: ;edc-pattern.think- it.io. IN A ;; ANSWER SECTION: edc-pattern.think- it.io. 276 IN CNAME daps- alb-iap9zmwy3kn8-13287 73120.eu-west-1.el b.amazonaws.com. daps-alb-iap9zmwy3k n8-1328773120.eu-w est-1.elb.amazonaw s.com. 36 IN A 52.208.240.129 daps-alb-iap9zmwy3kn8 -1328773120.eu-wes t-1.elb.amazonaws. com. 36 IN A 52.210.15 5.124	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Registrieren Sie die Konnektoren der Teilnehmer für den DAPS-Dienst.	Registrieren Sie die Teilnehmer von einer der für DAPS bereitgestellten EC2 Instanzen aus:
	1. Führen Sie das verfügbare Skript auf der EC2 Instanz aus, indem Sie den Root-Benutzer verwenden:
	`cd /srv/mvds/omejdn-daps`
	2. Registrieren Sie den Anbieter:
	`bash scripts/register_connector.sh <provider_name>`
	3. Registrieren Sie den Verbraucher:
	`bash scripts/register_connector.sh <consumer_name>`
	Die Wahl der Namen hat keinen Einfluss auf die nächsten Schritte. Wir empfehlen, entweder `provider` und `consumer` oder `companyx` und zu verwenden`companyy`.
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Die Registrierungsbefehle konfigurieren den DAPS-Dienst außerdem automatisch mit den erforderlichen Informationen, die aus den erstellten Zertifikaten und Schlüsseln abgerufen werden. Sammeln Sie Informationen, die Sie für spätere Installationsschritte benötigen, während Sie bei einem DAPS-Server angemeldet sind: 1. Von `omejdn-daps/config/clients.yml` get the `client id` für den Anbieter und den Verbraucher. Die `client id` Werte sind lange Zeichenketten mit Hexadezimalziffern. 2. Kopieren Sie aus dem `omejdn-daps/keys` Verzeichnis den Inhalt der Dateien`consumer.cert` , `consumer.key provider.cert` , und`provider.key` . Wir empfehlen, den Text zu kopieren und in Dateien mit ähnlichem Namen `daps-` auf Ihrer Workstation mit dem Präfix „A“ einzufügen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie sollten den Client IDs für den Anbieter und den Verbraucher haben und vier Dateien in Ihrem Arbeitsverzeichnis auf Ihrer Workstation haben: • Der Name der Quelldatei `consumer.cert` wird zum Namen der Workstation-Datei `daps-consumer.cert`. • Der Name der Quelldatei `consumer.key` wird zum Namen der Arbeitsstationsdatei `daps-consumer.key`. • Der Name der Quelldatei `provider.cert` wird zum Namen der Arbeitsstationsdatei `daps-provider.cert`. • Der Name der Quelldatei `provider.key` wird zum Namen der Arbeitsstationsdatei `daps-provider.key`.	

Stellen Sie die Konnektoren der Teilnehmer bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Tractus-X EDC-Repository und	Für den Build des Tractus-X EDC-Connectors müssen die	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

verwenden Sie die Version 0.4.1.	Dienste PostgreSQL (Asset Database) und HashiCorp Vault (Secrets Managemen t) bereitgestellt und verfügbar sein.
	
	Es gibt viele verschiedene Versionen von Tractus-X EDC Helm-Charts. Dieses Muster spezifiziert Version 0.4.1, da es den DAPS-Server verwendet.
	
	Die neuesten Versionen verwenden Managed Identity Wallet (MIW) mit einer verteilte n Implementierung des Identitätsdienstes.
	
	Klonen Sie auf der Workstati on, auf der Sie die beiden Kubernetes-Namespa ces erstellt haben, das tractusx-edc-Repository und checken Sie den Branch aus. `release/0.4.1`
	
	`git clone https://g ithub.com/eclipse- tractusx/tractusx-edc`
	
	`cd tractusx-edc`
	
	`git checkout release/0 .4.1`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie das Tractus-X EDC Helm-Diagramm.	Ändern Sie die Konfiguration der Tractus-X-Helm-Diagrammvorlage, damit beide Konnektoren miteinander interagieren können. Dazu würden Sie den Namespace zum DNS-Namen des Dienstes hinzufügen, sodass er von anderen Diensten im Cluster aufgelöst werden kann. Diese Änderungen sollten an der `charts/tractusx-connector/templates/_helpers.tpl` Datei vorgenommen werden. Dieses Muster bietet eine endgültige modifizierte Version dieser Datei, die Sie verwenden können. Kopieren Sie es und fügen Sie es in den `daps` Abschnitt der Datei ein`charts/tractusx-connector/templates/_helpers.tpl` . Stellen Sie sicher, dass Sie alle DAPS-Abhängigkeiten kommentieren in`charts/tractusx-connector/Chart.yaml` : `dependencies:`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> # IDS Dynamic Attribute Provisioning Service (IAM)
	  # - name: daps
	  # version: 0.0.1
	  # repository: "file://./subcharts/omejdn"
	  # alias: daps
	  # condition: install.daps</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie die Konnektoren für die Verwendung von PostgreSQL auf Amazon RDS.	(Optional) Die Amazon Relational Database Service (Amazon RDS) -Instance ist in diesem Muster nicht erforderlich. Wir empfehlen jedoch dringend, Amazon RDS oder Amazon Aurora zu verwenden, da sie Funktione n wie Hochverfügbarkeit sowie Sicherung und Wiederher stellung bieten.
	
	Gehen Sie wie folgt vor, um PostgreSQL auf Kubernete s durch Amazon RDS zu ersetzen:
	
	1. Stellen Sie die Amazon RDS for PostgreSQL PostgreSQL-Instance bereit.
	2. Kommentieren `Chart.yam l` Sie den `PostgreSQL` Abschnitt in.
	3. In `provider_ values.yml` und `consumer_values.ym l` konfigurieren Sie den `postgresql` Abschnitt wie folgt:
	
	`postgresql:`
	`auth:`
	`database: edc`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>password: <RDS PASSWORD>
	username: <RDS Username>
	jdbcUrl: jdbc:postgresql://<RDS DNS NAME>:5432/edc
	username: <RDS Username>
	password: <RDS PASSWORD>
	primary:
	persistence:
	enabled: false
	readReplicas:
	persistence:
	enabled: false</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren und implement ieren Sie den Provider-Connector und seine Dienste.	Gehen Sie wie folgt vor, um den Provider-Connector und seine Dienste zu konfiguri eren: 1. Führen Sie den folgenden Befehl aus, um die `provider_edc.yaml` Datei aus dem `edc_helm_configs` Verzeichnis in den aktuellen Helm-Chart-Ordner herunterzuladen: `wget -q https://raw.githubusercontent.com/Think-iT-Labs/aws-patterns-edc/main/edc_helm_configs/provider_edc.yaml> -P charts/tractusx-connector/` 2. Ersetzen Sie die folgenden Variablen (ebenfalls in der Datei markiert) durch ihre Werte: • `CLIENT_ID` – Die vom DAPS generierte ID. Die `CLIENT_ID` sollte sich `/srv/mvds/omejdn-daps/config/clients.yml/config/clients.yml` auf dem DAPS-Server befinden. Es sollte eine	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Folge von Hexadezim alzeichen sein. • `DAPS_URL`– Die URL des DAPS-Servers. Er sollte den DNS-Namen `https://{DNS name}` verwenden, den Sie bei der Ausführung der AWS CloudFormation Vorlage eingerichtet haben. • `VAULT_TOKEN` – Das Token, das für die Vault-Autorisierung verwendet werden soll. Wählen Sie einen beliebigen Wert. • `vault.fullnameOverride` – `vault-provider` . • `vault.hashicorp.url` – `http://vault-provider:8200/` . Bei den vorherigen Werten wird davon ausgegangen, dass der Bereitstellungsname und der Namespace-Name Provider sind. 3. Verwenden Sie die folgenden Befehle, um das Helm-Diagramm von Ihrer Workstation aus auszuführen:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`cd charts/tractusx-connector`
	
	`helm dependency build`
	
	`helm upgrade --install provider ./ -f provider_edc.yaml -n provider`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie das Zertifikat und die Schlüssel zum Provider-Tresor hinzu.	Um Verwirrung zu vermeiden , sollten Sie die folgenden Zertifikate außerhalb des `tractusx-edc/charts` Verzeichnisses erstellen.
	
	Führen Sie beispielsweise den folgenden Befehl aus, um zu Ihrem Home-Verzeichnis zu wechseln:
	
	`cd ~`
	
	Sie müssen jetzt die vom Anbieter benötigten Geheimnisse zum Tresor hinzufügen.
	
	Die Namen der Geheimnis se im Tresor entsprechen den Werten der Schlüssel im `secretNames:` Abschnitt der `provider_edc.yml` Datei. Standardmäßig sind sie wie folgt konfiguriert:
	
	`secretNames:`
	`transferP roxyTokenSignerPri vateKey: transfer- proxy-token-signer- private-key`
	`transferP roxyTokenSignerPub licKey: transfer- proxy-token-signer- public-key`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>transferP
	roxyTokenEncryptio
	nAesKey: transfer-
	proxy-token-encryp
	tion-aes-key
	dapsPriva
	teKey: daps-private-
	key
	dapsPubli
	cKey: daps-public-key</pre>
	Zunächst werden ein AES-Schlüssel (Advanced Encryption Standard), ein privater Schlüssel, ein öffentlicher Schlüssel und ein selbstsigniertes Zertifikat generiert. Diese werden anschließend als Geheimnisse zum Tresor hinzugefügt.
	Außerdem sollte dieses Verzeichnis die `daps-provider.key` Dateien `daps-provider.cert` und enthalten, die Sie vom DAPS-Server kopiert haben.
	1. Führen Sie die folgenden Befehle aus:
	<pre># generate a private
	key
	openssl ecparam -name
	prime256v1 -genkey
	-noout -out provider-
	private-key.pem</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>```
	# generate correspon
	ding public key
	openssl ec -in
	 provider-private-k
	ey.pem -pubout -out
	 provider-public-ke
	y.pem
	# create a self-sign
	ed certificate
	openssl req -new -
	x509 -key provider-
	private-key.pem -out
	 provider-cert.pem -
	days 360
	# generate aes key
	openssl rand -base64
	 32 > provider-
	aes.key
	``</pre>	

	2. Bevor Sie die Geheimnis se zum Tresor hinzufüge n, konvertieren Sie sie von mehreren Zeilen in einzelne Zeilen, indem Sie die Zeilenumbrüche durch Folgendes ersetzen: \n
	<pre>```
	cat provider-private-
	key.pem | sed 's/$/\
	\\\n/'|tr -d '\\n' >
	 provider-private-k
	ey.pem.line
	cat provider-public-
	key.pem | sed 's/$/\
	\\\n/'|tr -d '\\n' >
	 provider-public-ke
	y.pem.line
	cat provider-cert.pem
	 | sed 's/$/\\\\
	n/'|tr -d '\\n' >
	``</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
 provider-cert.pem.
line
cat provider-aes.key
 | sed 's/$/\\\\
n/'|tr -d '\\n' >
 provider-aes.key.l
ine

## The following block
 is for daps certifica
te and key
openssl x509 -in
 daps-provider.cert -
outform PEM | sed 's/
$/\\\\n/'|tr -d '\\n'
 > daps-provider.cert
.line
cat daps-provider.key
 | sed 's/$/\\\\n/'|
tr -d '\\n' > daps-
provider.key.line
```

3. Führen Sie die folgenden Befehle aus, um die Geheimnisse zu formatier en, die dem Tresor hinzugefügt werden:

```
JSONFORMAT='{"cont
ent": "%s"}'
#create a single line
 in JSON format
printf "${JSONFO
RMAT}\\n" "`cat
 provider-private-
key.pem.line`" >
 provider-private-k
ey.json
printf "${JSONFO
RMAT}\\n" "`cat
 provider-public-
```

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	key.pem.line`" > provider-public-key.json printf "${JSONFORMAT}\\n" "`cat provider-cert.pem.line`" > provider-cert.json printf "${JSONFORMAT}\\n" "`cat provider-aes.key.line`" > provider-aes.json  printf "${JSONFORMAT}\\n" "`cat daps-provider.key.line`" > daps-provider.key.json printf "${JSONFORMAT}\\n" "`cat daps-provider.cert.line`" > daps-provider.cert.json Die Geheimnisse liegen jetzt im JSON-Format vor und können dem Tresor hinzugefügt werden. 4. Führen Sie den folgenden Befehl aus, um den Pod-Namen für den Tresor abzurufen: kubectl get pods -n provider|egrep "vault|NAME"	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Der Pod-Name wird ähnlich sein wie`"vault-provider-0"` . Dieser Name wird verwendet , wenn eine Portweiterleitung zum Tresor erstellt wird. Mit der Portweiterleitung können Sie auf den Tresor zugreifen, um den geheimen Schlüssel hinzuzufügen. Sie sollten dies von einer Workstation aus ausführen, für die AWS-Anmeldeinformationen konfiguriert sind. 5. Um auf den Tresor zuzugreifen, verwenden Sie, `kubectl` um eine Portweiterleitung zu konfigurieren: `kubectl port-forward <VAULT_POD_NAME> 8200:8200 -n provider` Sie sollten jetzt über Ihren Browser oder die CLI auf den Tresor zugreifen können. Browser 1. Navigieren Sie im Browser zu http://127.0.0.1:8200, wo der von Ihnen konfigurierte	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Port Forward verwendet wird. 2. Melden Sie sich mit dem Token an, das Sie zuvor konfiguri ert haben`provider_ edc.yml` . Erstellen Sie in der Secrets-Engine drei Geheimnisse. Jedes Geheimnis hat einen `Path for this secret` Wert, bei dem es sich um den Geheimnamen handelt, der in der folgenden Liste aufgeführt ist. Innerhalb des `secret data` Abschnitt s wird der Name des Schlüssels `content` und der Wert ist die einzelne Textzeile aus der jeweiligen Datei benannt`.line`. 3. Die geheimen Namen stammen aus dem `secretNames` Abschnitt in der `provider_ edc.yml` Datei. 4. Erstellen Sie die folgenden Geheimnisse: • Secret `transfer-proxy-token-signer-private-key` mit dem Namen der Datei	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`provider-private-key.pem.line` • `transfer-proxy-token-signer-public-key` Geheim mit dem Dateinamen `provider-cert.pem.line` • `transfer-proxy-token-encryption-aes-key` Geheim mit dem Dateinamen `provider-aes.key.line` • `daps-private-key`Geheim mit dem Dateinamen `daps-provider.key.line` • `daps-public-key`Geheim mit dem Dateinamen `daps-provider.cert.line` Vault-CLI Die CLI verwendet auch den Port Forward, den Sie konfiguriert haben. 1. Installieren Sie Vault CLI auf Ihrer Workstation, indem Sie den Anweisungen in der HashiCorp Vault-Dokumentation folgen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	2. Um sich mit dem Token, das Sie eingerichtet haben, beim Tresor anzumelde nprovider_edc.yml , führen Sie den folgenden Befehl aus:
	`vault login -address= http://127.0.0.1:8 200`
	Mit dem richtigen Token sollte die Meldung angezeigt werden `"Success! You are now authenticated."`
	3. Führen Sie den folgenden Code aus, um die Secrets mithilfe der zuvor erstellte n Dateien im JSON-Format zu erstellen:
	`vault kv put -address= http://127.0.0.1:8 200 secret/transfer- proxy-token-signer-p rivate-key @provider -private-key.json vault kv put - address=http://12 7.0.0.1:8200 secret/ transfer-proxy-token -signer-public-key @provider-cert.json vault kv put -address= http://127.0.0.1:8 200 secret/transfer- proxy-token-encrypti`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	on-aes-key @provider -aes.json vault kv put -address= http://127.0.0.1:8 200 secret/daps- private-key @daps-pro vider.key.json vault kv put - address=http://12 7.0.0.1:8200 secret/ daps-public-key @daps-provider.cer t.json	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren und implementieren Sie den Consumer-Connector und seine Dienste.	Die Schritte zur Konfiguration und Bereitstellung des Consumer ähneln denen, die Sie für den Anbieter ausgeführt haben: 1. Führen Sie die folgenden Befehle `consumer_edc.yaml` aus, um sie aus dem aws-patterns-edcRepository in den Ordner `tractusx-edc/charts/tractusx-connector` zu kopieren: ``` cd tractusx-edc wget -q https://raw.githubusercontent.com/Think-iT-Labs/aws-patterns-edc/main/edc_helm_configs/consumer_edc.yaml -P charts/tractusx-connector/ ``` 2. Aktualisieren Sie die folgenden Variablen mit ihren tatsächlichen Werten: • `CONSUMER_CLIENT_ID` – Die von DAPS generierte ID. Die `CONSUMER_CLIENT_ID` sollte sich `config/clients.yml` auf dem DAPS-Server befinden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	• `DAPS_URL`– Dieselbe DAPS-URL, die Sie für den Anbieter verwendet haben.
	• `VAULT_TOKEN` – Das Token, das für die Vault-Autorisierung verwendet werden soll. Wählen Sie einen beliebigen Wert.
	• `vault.fullnameOverride` – `vault-consumer`
	• `vault.hashicorp.url` – `http://vault-provider:8200/`
	
	Bei den vorherigen Werten wird davon ausgegangen, dass der Bereitstellungsname und der Namespace-Name `consumer`
	3. Verwenden Sie die folgenden Befehle, um das Helm-Diagramm auszuführen:
	
	`cd charts/tractusx-connector`
	
	`helm upgrade --install consumer ./ -f consumer_edc.yaml -n consumer`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie das Zertifikat und die Schlüssel zum Verbrauch ertresor hinzu.	Aus Sicherheitsgründen empfehlen wir, die Zertifika te und Schlüssel für jeden Datenraum-Teilnehmer neu zu generieren. Dieses Muster generiert Zertifikate und Schlüssel für den Verbraucher neu. Die Schritte sind denen für den Anbieter sehr ähnlich. Sie können die geheimen Namen in der `consumer_edc.yml` Datei überprüfen. Die Namen der Geheimnis se im Tresor entsprechen den Werten der Schlüssel im `secretNames:` Abschnitt von`consumer_edc.yml file`. Standardmäßig sind sie wie folgt konfiguriert: `secretNames: transferProxyTokenSignerPrivateKey: transfer-proxy-token-signer-private-key transferProxyTokenSignerPublicKey: transfer-proxy-token-signer-public-key transferProxyTokenEncryptionAesKey: transfer-`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>proxy-token-encryption-aes-key
	  dapsPrivateKey: daps-private-key
	  dapsPublicKey: daps-public-key</pre>
	Die `daps-consumer.key` Dateien `daps-consumer.cert` und, die Sie vom DAPS-Server kopiert haben, sollten bereits in diesem Verzeichnis vorhanden sein.
	1. Führen Sie die folgenden Befehle aus:
	<pre># generate a private key
	openssl ecparam -name prime256v1 -genkey -noout -out consumer-private-key.pem
	# generate corresponding public key
	openssl ec -in consumer-private-key.pem -pubout -out consumer-public-key.pem
	# create a self-signed certificate
	openssl req -new -x509 -key consumer-private-key.pem -out consumer-cert.pem -days 360
	# generate aes key</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`openssl rand -base64 32 > consumer-aes.key`
	2. Bearbeiten Sie die Dateien manuell, um Zeilenumbrüche durch sie zu ersetzen\n, oder verwenden Sie drei Befehle, die den folgenden ähneln:
	`cat consumer-private-key.pem | sed 's/$/\\\n/'|tr -d '\\n' > consumer-private-key.pem.line`
	`cat consumer-public-key.pem | sed 's/$/\\\n/'|tr -d '\\n' > consumer-public-key.pem.line`
	`cat consumer-cert.pem | sed 's/$/\\\\n/'|tr -d '\\n' > consumer-cert.pem.line`
	`cat consumer-aes.key | sed 's/$/\\\\n/'|tr -d '\\n' > consumer-aes.key.line`
	`cat daps-consumer.cert | sed 's/$/\\\\n/'|tr -d '\\n' > daps-consumer.cert.line`
	`cat daps-consumer.key | sed 's/$/\\\\n/'|tr -d '\\n' > daps-consumer.key.line`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	3. Führen Sie die folgenden Befehle aus, um die Geheimnisse zu formatier en, die zu Vault hinzugefügt werden:
	
	`JSONFORMAT='{"cont ent": "%s"}'`
	
	`#create a single line in JSON format`
	
	`printf "${JSONFO RMAT}\\n" "`cat consumer-private- key.pem.line`" > consumer-private-k ey.json`
	`printf "${JSONFO RMAT}\\n" "`cat consumer-public- key.pem.line`" > consumer-public-ke y.json`
	`printf "${JSONFO RMAT}\\n" "`cat consumer-cert.pem. line`" > consumer- cert.json`
	`printf "${JSONFO RMAT}\\n" "`cat consumer-aes.key.l ine`" > consumer- aes.json`
	
	`printf "${JSONFO RMAT}\\n" "`cat daps- consumer.key.line`" > daps-consumer.key. json`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`printf "${JSONFO RMAT}\\n" "`cat daps-consumer.cert.line`" > daps-consumer.cert .json`
	
	Die Geheimnisse liegen jetzt im JSON-Format vor und können dem Tresor hinzugefügt werden.
	
	4. Führen Sie den folgenden Befehl aus, um den Pod-Namen für den Consumer-Tresor abzurufen:
	
	`kubectl get pods -n consumer | egrep "vault|NAME"`
	
	Der Pod-Name wird ähnlich sein wie`"vault-consumer-0"` . Dieser Name wird verwendet , wenn eine Portweiterleitung zum Tresor erstellt wird. Mit der Portweiterleitung können Sie auf den Tresor zugreifen, um den geheimen Schlüssel hinzuzufügen. Sie sollten dies von einer Workstation aus ausführen, für die AWS Anmeldeinformationen konfiguriert sind.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Um auf den Tresor zuzugreifen, verwenden Sie, `kubectl` um eine Portweiterleitung zu konfigurieren: `kubectl port-forward <VAULT_POD_NAME> 8201:8200 -n consumer` Der lokale Port ist diesmal 8201, sodass Sie Portweiterleitungen sowohl für den Hersteller als auch für den Verbraucher einrichten können. Browser Sie können Ihren Browser verwenden, um eine Verbindung zu http://localhost:8201/ herzustellen, um auf den Verbraucher-Tresor zuzugreifen und die Secrets mit Namen und Inhalt wie beschrieben zu erstellen. Die Geheimnisse und Dateien, die den Inhalt enthalten, sind die folgenden: • `transfer-proxy-token-signer-private-key` Geheim mit dem Dateinamen `consumer-`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`private-key.pem.line`
	• `transfer-proxy-token-signer-public-key` Geheim mit dem Dateinamen `consumer-cert.pem.line`
	• `transfer-proxy-token-encryption-aes-key` Geheim mit dem Dateinamen `consumer-aes.key.line`
	
	Vault-CLI
	
	Mit der Vault-CLI können Sie die folgenden Befehle ausführen, um sich beim Tresor anzumelden und die Secrets zu erstellen:
	
	1. Melden Sie sich mit dem Token, das Sie darin konfiguriert haben, beim Tresor an`consumer_edc.yml` :
	
	`vault login -address=http://127.0.0.1:8201`
	
	Mit dem richtigen Token sollte die Meldung angezeigt werden	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`"Success! You are now authenticated."`
	2. Führen Sie den folgenden Code aus, um die Secrets mithilfe der zuvor erstellten Dateien im JSON-Format zu erstellen:
	`vault kv put -address=http://127.0.0.1:8201 secret/transfer-proxy-token-signer-private-key @consumer-private-key.json`
	`vault kv put -address=http://127.0.0.1:8201 secret/transfer-proxy-token-signer-public-key @consumer-cert.json`
	`vault kv put -address=http://127.0.0.1:8201 secret/transfer-proxy-token-encryption-aes-key @consumer-aes.json`
	`vault kv put -address=http://127.0.0.1:8201 secret/daps-private-key @daps-consumer.key.json`
	`vault kv put -address=http://127.0.0.1:8201 secret/daps-public-key @daps-consumer.cert.json`	

Richten Sie einen HTTP-Client ein, um mit der Management-API der Konnektoren zu interagieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie die Portweiterleitung ein.	1. Führen Sie die folgenden Befehle aus, um den Status der Pods zu überprüfen:
	`kubectl get pods -n provider`
	`kubectl get pods -n consumer`
	2. Um sicherzustellen, dass die Kubernetes-Bereitstellungen erfolgreich waren, sehen Sie sich die Protokolle der Kubernetes-Pods für Anbieter und Verbraucher an, indem Sie die folgenden Befehle ausführen:
	`kubectl logs -n provider <producer control plane pod name>`
	`kubectl logs -n consumer <consumer control plane pod name>`
	Der Cluster ist privat und nicht öffentlich zugänglich. Um mit den Konnektoren zu interagieren, verwenden Sie die Kubernetes-Port-Forwarding-Funktion, um den von Ihrem Computer
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	generierten Datenverkehr an die Connector-Steuerebene weiterzuleiten.
	
	1. Leiten Sie auf dem ersten Terminal die Anfragen des Verbrauchers über Port 8300 an die Management-API weiter:
	
	`kubectl port-forward deployment/consumer-tractusx-connector-controlplane 8300:8081 -n consumer`
	
	2. Leiten Sie auf dem zweiten Terminal die Anfragen des Anbieters über Port 8400 an die Management-API weiter:
	
	`kubectl port-forward deployment/provider-tractusx-connector-controlplane 8400:8081 -n provider`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie S3-Buckets für den Anbieter und den Verbraucher.	Der EDC-Connector verwendet derzeit keine temporären AWS-Anmel deinformationen, wie sie beispielsweise bei der Übernahme einer Rolle bereitgestellt werden. Der EDC unterstützt nur die Verwendung einer Kombinati on aus IAM-Zugriffsschlüs sel-ID und geheimer Zugriffss chlüssel-ID. Für spätere Schritte sind zwei S3-Buckets erforderl ich. Ein S3-Bucket wird zum Speichern von Daten verwendet, die vom Anbieter zur Verfügung gestellt werden. Der andere S3-Bucket ist für Daten vorgesehen, die vom Verbraucher empfangen werden. Der IAM-Benutzer sollte nur die Berechtigung haben, Objekte in den beiden benannten Buckets zu lesen und zu schreiben. Eine Zugangsschlüssel-ID und ein geheimes Zugriffss chlüsselpaar müssen erstellt und sicher aufbewahrt werden. Nach der Außerbetriebnahme	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dieses MVDS sollte der IAM-Benutzer gelöscht werden. Der folgende Code ist ein Beispiel für eine IAM-Richtlinie für den Benutzer: `{ "Version": "2012-10-17", "Statement": [{ "Sid": "Stmt1708699805237", "Action": ["s3:GetObject", "s3:GetObjectVersion", "s3:ListAllMyBuckets", "s3:ListBucket", "s3:ListBucketMultipartUploads", "s3:ListBucketVersions", "s3:PutObject"], "Effect": "Allow", "Resource": ["arn:aws:s3:::<S3 Provider Bucket>", "arn:aws:s3:::<S3 Consumer Bucket>", "arn:aws:s3:::<S3 Provider Bucket>/*",`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"arn:aws: s3:::<S3 Consumer Bucket>/*"] }] }	
Richten Sie Postman so ein, dass es mit dem Konnektor interagiert.	Sie können jetzt über Ihre EC2 Instanz mit den Konnektoren interagieren. Verwenden Sie Postman als HTTP-Client und stellen Sie Postman-Sammlungen sowohl für den Provider- als auch für den Consumer-Connector bereit. Importieren Sie die Sammlungen aus dem `aws-pattern-edc` Repository in Ihre Postman-Instanz. Dieses Muster verwendet Postman-Sammlungsvariablen, um Eingaben für Ihre Anfragen bereitzustellen.	App-Entwickler, Dateningenieur

Stellen Sie über den Konnektor Daten zum CO2-Fußabdruck von Unternehmen X bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Daten zur CO2-Emissionsintensität für die gemeinsame Nutzung vor.	Zunächst müssen Sie entscheiden, welche Datenmenge gemeinsam genutzt werden soll. Die Daten von Unternehmen X stellen den CO2-Fußab	Dateningenieur, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	druck seiner Fahrzeugflotte dar. Das Gewicht ist das Bruttofahrzeuggewicht (GVW) in Tonnen, und die Emissionen werden gemäß der (WTW) - Messung in Gramm CO2 pro Tonnenkilometer (g CO2 e/ t-km) angegeben: Wheel-to-Well • Fahrzeugtyp: Van; Gewicht: < 3,5; Emissionen: 800 • Fahrzeugtyp: Stadtlaster; Gewicht: 3,5—7,5; Emissionen: 315 • Fahrzeugtyp: Mittlerer Nutzfahrzeug (MGV); Gewicht: 7,5—20; Emissionen: 195 • Fahrzeugtyp: Schwerlastwagen (Lkw); Gewicht: > 20; Emissionen: 115 Die Beispieldaten befinden sich in der `carbon_emissions_data.json` Datei im `aws-patterns-edc` Repository. Unternehmen X verwendet Amazon S3 zum Speichern von Objekten. Erstellen Sie den S3-Bucket und speichern	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Sie dort das Beispield atenobjekt. Die folgenden Befehle erstellen einen S3-Bucket mit Standards icherheitseinstellungen. Wir empfehlen dringend, sich mit den bewährten Sicherheitsmethoden für Amazon S3 vertraut zu machen.
	
	`aws s3api create-bucket --bucket <BUCKET_NAME> --region <AWS_REGION>`
	`# You need to add '--create-bucket-configuration LocationConstraint=<AWS_REGION>' if you want to create # the bucket outside of us-east-1 region`
	
	`aws s3api put-object --bucket <BUCKET_NAME> \`
	`--key <S3 OBJECT NAME> \`
	`--body <PATH OF THE FILE TO UPLOAD>`
	
	Der S3-Bucket-Name sollte weltweit eindeutig sein. Weitere Informationen zu Benennungsregeln finden Sie in der AWS-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Registrieren Sie das Datenobjekt mithilfe von Postman beim Connector des Anbieters.	Ein EDC-Connector-Datenobjekt enthält den Namen der Daten und ihren Speicherort. In diesem Fall zeigt das EDC-Connector-Datenobjekt auf das erstellte Objekt im S3-Bucket: • Konnektor: Anbieter • Anfrage: Asset erstellen • Sammlungsvariablen: Aktualisieren`ASSET_NAME`. Wählen Sie einen aussagekräftigen Namen, der das Asset repräsentiert. • Hauptteil der Anfrage: Aktualisieren Sie den Hauptteil der Anfrage mit dem S3-Bucket, den Sie für den Anbieter erstellt haben. `"dataAddress": { "edc:type": "AmazonS3", "name": "Vehicle Carbon Footprint", "bucketName": "<REPLACE WITH THE SOURCE BUCKET NAME>", "keyName": "<REPLACE WITH YOUR OBJECT NAME>", "region": "<REPLACE WITH THE BUCKET REGION>",`	App-Entwickler, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"accessKeyId": "<REPLACE WITH YOUR ACCESS KEY ID>", "secretAccessKey": "<REPLACE WITH SECRET ACCESS KEY>" }</pre> • Antwort: Eine erfolgreiche Anfrage gibt die Erstellungszeit und die Asset-ID des neu erstellten Assets zurück. <pre>{ "@id": "c89aa31c-ec4c-44ed-9e8c-1647f19d7583" }</pre> • Sammlungsvariable ASSET_ID: Aktualisieren Sie die Sammlungsvariable Postman `ASSET_ID` mit der ID, die nach der Erstellung automatisch vom EDC-Connector generiert wurde.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Definieren Sie die Nutzungsrichtlinie für das Asset.	Ein EDC-Datenbestand muss klaren Nutzungsrichtlinien zugeordnet sein. Erstellen Sie zunächst die Richtliniendefinition im Provider-Connector.
	
	Die Richtlinie von Unternehmen X besteht darin, den Teilnehmern des Datenraums die Nutzung der Daten zum CO2-Fußabdruck zu ermöglichen.
	
	• Hauptteil der Anfrage:
	  • Anschluss: Anbieter
	  • Anfrage: Richtlinie erstellen
	  • Sammlungsvariablen: Aktualisieren Sie die `Policy Name` Variable mit dem Namen der Richtlinie.
	• Antwort: Bei einer erfolgreichen Anfrage werden die Uhrzeit der Erstellung und die Richtlinien-ID der neu erstellten Richtlinie zurückgegeben. Aktualisieren Sie die Sammlungsvariable `POLICY_ID` mit der ID der Richtlinie, die vom EDC-Connector nach der Erstellung generiert wurde.
		App-Entwickler, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie ein EDC-Vertr agsangebot für das Asset und dessen Nutzungsrichtlinien.	Damit andere Teilnehme r Zugriff auf Ihre Daten beantragen können, bieten Sie diesen in einem Vertrag an, der die Nutzungsbedingungen und Berechtigungen festlegt: • Konnektor: Anbieter • Anfrage: Vertragsdefinition erstellen • Sammlungsvariablen : Aktualisieren Sie die `Contract Name` Variable mit einem Namen für das Vertragsangebot oder die Vertragsdefinition.	App-Entwickler, Dateninge nieur

Entdecken Sie die Vorteile und erzielen Sie eine Einigung über die definierten Verträge

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fordern Sie den von Unternehmen X gemeinsam genutzten Datenkatalog an.	Als Datenkonsument im Datenraum muss Unternehm en Y zunächst herausfinden, welche Daten von anderen Teilnehmern gemeinsam genutzt werden. In dieser Grundkonfiguration können Sie dazu den Consumer-Connector bitten, den Katalog der verfügbar en Ressourcen direkt vom	App-Entwickler, Dateninge nieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Provider-Connector anzuforderrn. • Konnektor: Consumer • Anfrage: Katalog anfordern • Antwort: Alle verfügbaren Datenbestände des Anbieters zusammen mit den beigefügten Nutzungsrichtlinien. Suchen Sie als Datenverbraucher nach dem Vertrag, für den Sie sich interessieren, und aktualisieren Sie die folgenden Erfassungsvariablen entsprechend. • `CONTRACT_OFFER_ID` – Die ID des Vertragsangebots, das der Verbraucher aushandeln möchte • `ASSET_ID`– Die ID des Vermögenswerts, den der Verbraucher aushandeln möchte • `PROVIDER_CLIENT_ID` – Die ID des Provider-Connectors, mit dem verhandelt werden soll	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initiieren Sie eine Vertragsverhandlung für die Daten zur CO2-Emissionsintensität von Unternehmen X.	Nachdem Sie nun den Vermögenswert identifiziert haben, den Sie nutzen möchten, leiten Sie einen Vertragsverhandlungsprozess zwischen dem Verbraucher und dem Anbieter ein. • Konnektor: Verbraucher • Anfrage: Vertragsverhandlung • Sammlungsvariablen: Aktualisieren Sie die `CONSUMER_CLIENT_ID` Variable mit der ID des Consumer-Connectors, mit dem Sie verhandeln möchten. Der Vorgang kann einige Zeit dauern, bis der Status VERIFIED erreicht wird. Mithilfe der `Get Negotiation` Anfrage können Sie den Status der Vertragsverhandlung und die entsprechende Vereinbarungs-ID überprüfen.	App-Entwickler, Dateningenieur

Verbrauchen Sie die Daten mithilfe der Vertragsvereinbarung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verbrauchen Sie Daten von HTTP-Endpunkten.	(Option 1) Um die HTTP-Datenebene für die Nutzung von Daten im Datenraum zu verwenden, können Sie webhook.site verwenden, um einen HTTP-Server zu emulieren und den Übertragungsprozess im Consumer-Connector zu initiieren: • Konnektor: Verbraucher • Anfrage: Vertragsverhandlung • Sammlungsvariablen: Aktualisieren Sie die `Contract Agreement ID` Variable mit der ID der Vertragsvereinbarung, die vom EDC-Connector generiert wurde. • Hauptteil der Anfrage: Aktualisieren Sie den Hauptteil der Anfrage und geben Sie HTTP `dataDestination` neben dem Webhook folgende URL an: `{ "dataDestination": { "type": "HttpProxy"`	App-Entwickler, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> },
	    "privateP
	roperties": {
	      "receiver
	HttpEndpoint":
	 "<WEBHOOK URL>"
	    }
	}</pre>
	Der Connector sendet die zum Herunterladen der Datei erforderlichen Informationen direkt an die Webhook-URL.
	
	Die empfangene Nutzlast ähnelt der folgenden:
	
	<pre>{
	  "id": "dcc90391
	-3819-4b54-b401-1a
	005a029b78",
	  "endpoint":
	 "http://consumer-t
	ractusx-connector-
	dataplane.consumer
	:8081/api/public",
	  "authKey":
	 "Authorization",
	  "authCode": "<AUTH
	 CODE YOU RECEIVE IN
	 THE ENDPOINT>",
	  "properties": {
	    "https://
	w3id.org/edc/v0.0.
	1/ns/cid": "vehicle-
	carbon-footprint-c
	ontract:4563abf7-5
	dc7-4c28-bc3d-97f4
	5e32edac:b073669b-</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>db20-4c83-82df-46b
	583c4c062"
	  }
	}</pre>
	Verwenden Sie die empfangenen Anmeldeinformationen, um das S3-Asset abzurufen, das vom Anbieter gemeinsam genutzt wurde.
	
	In diesem letzten Schritt müssen Sie die Anfrage an die Consumer-Datenebene senden (Ports ordnungsgemäß weiterleiten), wie in der Payload (`endpoint`) angegeben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Daten aus S3-Buckets direkt konsumieren.	(Option 2) Verwenden Sie die Amazon S3 S3-Integration mit dem EDC-Connector und verweisen Sie direkt auf den S3-Bucket in der Verbrauch erinfrastruktur als Ziel: • Hauptteil der Anfrage: Aktualisieren Sie den Hauptteil der Anfrage, um den S3-Bucket als DataDestination anzugeben. Dies sollte der S3-Bucket sein, den Sie zuvor zum Speichern von Daten erstellt haben, die vom Verbraucher empfangen wurden. `{ "dataDestination": { "type": "AmazonS3", "bucketName": "{{ REPLACE WITH THE DESTINATION BUCKET NAME }}", "keyName": "{{ REPLACE WITH YOUR OBJECT NAME }}", "region": "{{ REPLACE WITH THE BUCKET REGION }}", "accessKeyId": "{{ REPLACE WITH YOUR ACCESS KEY ID }}",`	Dateningenieur, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"secretAc
	cessKey": "{{ REPLACE
	WITH SECRET ACCESS
	KEY }}"
	}
	}
	}</pre>	

Fehlerbehebung

Problem	Lösung
Der Konnektor könnte ein Problem mit dem PEM-Format des Zertifikats aufwerfen.	Verketten Sie den Inhalt jeder Datei zu einer einzigen Zeile, indem Sie Folgendes hinzufüge n. \n

Zugehörige Ressourcen

- DSSC
- Aufbau von Datenräumen für Anwendungsfälle im Bereich Nachhaltigkeit (AWS Prescriptive Guidance Guidance-Strategie von Think-IT)
- AWS für Datenräume
- Tractus-X-Dokumentation
- DAPS
- Aktivierung der gemeinsamen Nutzung von Daten über Datenräume und AWS (Blogbeitrag)

Zusätzliche Informationen

Spezifikationen für den Datenraum

Teilnehmer

Teilnehmer	Beschreibung des Unternehmens	Schwerpunkt des Unternehmens
Firma X	Betreibt eine Fahrzeugflotte in ganz Europa und Südamerika, um verschiedene Güter zu transportieren.	Zielt darauf ab, datengestützte Entscheidungen zu treffen, um die Intensität seines CO2-Fußabdrucks zu reduzieren.
Firma Y	Eine Umweltregulierungsbehörde	Setzt Umweltvorschriften und -richtlinien durch, die darauf abzielen, die Umweltauswirkungen von Unternehmen und Branchen, einschließlich der Intensität der CO2-Emissionen, zu überwachen und zu mindern.

Geschäftsszenario

Unternehmen X nutzt Datenraumtechnologie, um Daten zum CO2-Fußabdruck an einen Compliance-Auditor, Unternehmen Y, weiterzugeben, um die Umweltauswirkungen der Logistikaktivitäten von Unternehmen X zu bewerten und zu berücksichtigen.

Behörde für den Datenraum

Die Data Space Authority ist ein Konsortium der Organisationen, die für den Datenraum zuständig sind. In diesem Muster bilden sowohl Unternehmen X als auch Unternehmen Y das Leitungsorgan und stellen eine föderierte Datenschutzbehörde dar.

Komponenten des Datenraums

Komponente	Gewählte Implementierung	Zusätzliche Informationen
Protokoll für den Austausch von Datensätzen	Dataspace-Protokoll, Version 0.8	• JSON-LD • Datenkatalog-Vokabular (DCAT)

Anschluss für den Datenraum	Tractus-X EDC-Anschluss Version 0.4.1	• EDC-Erweiterungen
Richtlinien für den Datenaustausch	Standard-USE-Richtlinie	• Öffnen Sie die Sprache für digitale Rechte (ODRL)

Dienste im Bereich Datenraum

Service	Implementierung	Zusätzliche Informationen
Identitätsdienst	Dynamisches Attributbereitstellungssystem (DAPS)	„Ein Dynamic Attribute Provisioning System (DAPS) hat die Absicht, bestimmte Eigenschaften von Organisationen und Konnektoren zu ermitteln. Daher müssen Dritte letzteren nicht vertrauen, vorausgesetzt, sie vertrauen den DAPS-Assertionen.“ — DAPS Um sich auf die Logik des Connectors zu konzentrieren, wird der Datenraum mithilfe von Docker Compose auf einem EC2 Amazon-Computer bereitgestellt.
Discovery Service	Verbundkatalog von Gaia-X	„Der Federated Catalogue stellt eine indexierte Sammlung von Gaia-X-Selbstbeschreibungen dar, die es ermöglichen, Anbieter und deren Serviceangebote zu finden und auszuwählen. Bei den Selbstbeschreibungen handelt es sich um Informati

		onen, die von den Teilnehme rn über sich selbst und ihre Dienstleistungen in Form von Eigenschaften und Ansprüche n bereitgestellt werden.“ — Kickstarter für das Gaia-X-Ök osystem

Daten, die ausgetauscht werden sollen

Datenbestände	Beschreibung	Format
Daten zu den CO2-Emiss ionen	Intensitätswerte für verschied ene Fahrzeugtypen in der angegebenen Region (Europa und Südamerika) aus der gesamten Fahrzeugflotte	JSON-Datei

Datenmodell

```
{
  "region": "string",
  "vehicles": [
// Each vehicle type has its Gross Vehicle Weight (GVW) category and its emission
 intensity in grams of CO2 per Tonne-Kilometer (g CO2 e/t-km) according to the "Well-
to-Wheel" (WTW) measurement.
    {
      "type": "string",
      "gross_vehicle_weight": "string",
      "emission_intensity": {
        "CO2": "number",
        "unit": "string"
      }
    }
  ]
}
```

Tractus-X EDC-Anschluss

Die Dokumentation der einzelnen Tractus-X EDC-Parameter finden Sie in der Datei mit den Originalwerten.

In der folgenden Tabelle sind alle Dienste zusammen mit ihren entsprechenden exponierten Ports und Endpunkten als Referenz aufgeführt.

Name des Dienstes	Port und Pfad
Steuerebene	• Verwaltung: – Port: 8081 Pfad: `/management` • Steuerung – Port: 8083 Pfad: `/control` • Protokoll-Port: 8084 Pfad: `/api/v1/dsp` • Metriken – Port: 9090 Pfad: `/metrics` • Beobachtbarkeit – Port: 8085 Pfad: `/observability`
Datenebene	Standard – Port: 8080 Pfad: `/api` public – Port: 8081 Pfad: `/api/dataplane/control` proxy – Port: 8186 Pfad: `/proxy` Metriken – Port: 9090 Pfad: `/metrics` Beobachtbarkeit – Port: 8085 Pfad: `/observability`
Vault	Anschluss: 8200
PostgreSQL	Hafen: 5432

Manager verwenden AWS Secrets Manager

Es ist möglich, Secrets Manager anstelle von HashiCorp Vault als Secrets Manager zu verwenden. Dazu müssen Sie die AWS Secrets Manager EDC-Erweiterung verwenden oder erstellen.

Sie sind für die Erstellung und Pflege Ihres eigenen Images verantwortlich, da Tractus-X keine Unterstützung für Secrets Manager bietet.

Um dies zu erreichen, müssen Sie die Build-Gradle-Dateien sowohl der Steuerungsebene als auch der Datenebene des Konnektors ändern, indem Sie Ihre AWS Secrets Manager EDC-Erweiterung eingeben (ein Beispiel finden Sie in diesem Maven-Artefakt) und dann das Docker-Image erstellen, verwalten und referenzieren.

Weitere Informationen zum Refactoring des Docker-Images des Tractus-X-Connectors finden Sie unter Refactor Tractus-X EDC Helm-Diagramme.

Der Einfachheit halber vermeiden wir es, das Connector-Image nach diesem Muster neu zu erstellen, und verwenden Vault. HashiCorp

Richten Sie eine sprachspezifische Sortierung für Amazon Redshift Redshift-Abfrageergebnisse mithilfe einer skalaren Python-UDF ein

Erstellt von Ethan Stark (AWS)

Übersicht

Dieses Muster enthält Schritte und Beispielcode für die Verwendung einer skalaren Python-UDF (benutzerdefinierte Funktion) zur Einrichtung einer sprachlichen Sortierung ohne Berücksichtigung der Groß- und Kleinschreibung für Amazon Redshift Redshift-Abfrageergebnisse. Es ist notwendig, eine skalare Python-UDF zu verwenden, da Amazon Redshift Ergebnisse auf der Grundlage der binären UTF-8-Reihenfolge zurückgibt und keine sprachspezifische Sortierung unterstützt. Eine Python-UDF ist Nicht-SQL-Verarbeitungscode, der auf einem Python 2.7-Programm basiert und in einem Data Warehouse ausgeführt wird. Sie können Python-UDF-Code mit einer SQL-Anweisung in einer einzigen Abfrage ausführen. Weitere Informationen finden Sie im Blogbeitrag Einführung UDFs in Python in Amazon Redshift AWS Big Data.

Die Beispieldaten in diesem Muster basieren zu Demonstrationszwecken auf dem türkischen Alphabet. Die skalare Python-UDF in diesem Muster ist so konzipiert, dass die Standardabfrageergebnisse von Amazon Redshift der sprachlichen Reihenfolge der Zeichen in der türkischen Sprache entsprechen. Weitere Informationen finden Sie im Beispiel in türkischer Sprache im Abschnitt Zusätzliche Informationen dieses Musters. Sie können die skalare Python-UDF in diesem Muster für andere Sprachen ändern.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Amazon Redshift Redshift-Cluster mit einer Datenbank, einem Schema und Tabellen
- Amazon Redshift Redshift-Benutzer mit CREATE TABLE- und CREATE FUNCTION-Berechtigungen
- Python 2.7 oder höher

Einschränkungen

Bei der sprachlichen Sortierung, die von den Abfragen in diesem Muster verwendet wird, wird nicht zwischen Groß- und Kleinschreibung unterschieden.

Architektur

Technologie-Stack

- Amazon Redshift
- Python-UDF

Tools

AWS-Services

- Amazon Redshift ist ein verwalteter Data-Warehouse-Service im Petabyte-Bereich in der AWS-Cloud. Amazon Redshift ist in Ihren Data Lake integriert, sodass Sie Ihre Daten nutzen können, um neue Erkenntnisse für Ihr Unternehmen und Ihre Kunden zu gewinnen.

Andere Tools

- Benutzerdefinierte Funktionen von Python (UDFs) sind Funktionen, die Sie in Python schreiben und dann in SQL-Anweisungen aufrufen können.

Epen

Entwickeln Sie Code, um Abfrageergebnisse in sprachlicher Reihenfolge zu sortieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine Tabelle für Ihre Beispieldaten.	Verwenden Sie die folgenden SQL-Anweisungen, um eine Tabelle in Amazon Redshift zu erstellen und Ihre Beispieldaten in die Tabelle einzufügen:
	`CREATE TABLE my_table (first_name varchar(30));`
	`INSERT INTO my_table (first_name)`
		Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	``
	VALUES
	    ('ali'),
	    ('Ali'),
	    ('ırmak'),
	    ('IRMAK'),
	    ('irem'),
	    ('İREM'),
	    ('oğuz'),
	    ('OĞUZ'),
	    ('ömer'),
	    ('ÖMER'),
	    ('sedat'),
	    ('SEDAT'),
	    ('şule'),
	``	

	Note Die Vornamen in den Beispieldaten enthalten Sonderzeichen aus dem türkischen Alphabet. Weitere Informationen zu den Überlegungen zur türkischen Sprache für dieses Beispiel finden Sie unter Beispiel für eine türkische Sprache im Abschnitt Zusätzliche Informationen dieses Musters.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Standards ortierung der Beispieldaten.	Führen Sie die folgende Abfrage aus, um die Standardsortierung Ihrer Beispieldaten in Amazon Redshift zu sehen:
	`SELECT first_name FROM my_table ORDER BY first_name;`
	Die Abfrage gibt die Liste der Vornamen aus der Tabelle zurück, die Sie zuvor erstellt haben:
	`first_name`
	`---------------`
	`Ali`
	`IRMAK`
	`OĞUZ`
	`SEDAT`
	`ali`
	`irem`
	`oğuz`
	`sedat`
	`ÖMER`
	`ömer`
	`İREM`
	`ırmak`
	`ŞULE`
	`şule`
	Die Abfrageergebnisse sind nicht in der richtigen Reihenfol ge, da die standardmäßige binäre UTF-8-Reihenfolge die sprachliche Reihenfolge
		Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der türkischen Sonderzeichen nicht berücksichtigt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine skalare Python-UDF.	Verwenden Sie den folgenden SQL-Code, um eine skalare Python-UDF zu erstellen: `CREATE OR REPLACE FUNCTION collate_sort (value varchar) RETURNS varchar IMMUTABLE AS $$ def sort_str(val): import string dictionary = { 'I': 'ı', 'ı': 'h~', 'İ': 'i', 'Ş': 's~', 'ş': 's~', 'Ğ': 'g~', 'ğ': 'g~', 'Ü': 'u~', 'ü': 'u~', 'Ö': 'o~', 'ö': 'o~', 'Ç': 'c~', 'ç': 'c~' } for key, value in dictionary.items(): val = val.replace(key, value) return val.lower()`	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`    return sort_str( value)`
	
	`$$ LANGUAGE plpythonu;`	

Fragen Sie die Beispieldaten ab.	Führen Sie die folgende SQL-Abfrage aus, um die Beispieldaten mithilfe der Python-UDF abzufragen:
	
	`SELECT first_name FROM my_table ORDER BY collate_order(first_name);`
	
	Die Abfrage gibt jetzt die Beispieldaten in türkischer Sprachreihenfolge zurück:
	
	`first_name`
	`---------------`
	`ali`
	`Ali`
	`ırmak`
	`IRMAK`
	`irem`
	`İREM`
	`oğuz`
	`OĞUZ`
	`ömer`
	`Ömer`
	`sedat`
	`SEDAT`
	`şule`
	`ŞULE`
		Dateningenieur

Zugehörige Ressourcen

- ORDER BY-Klausel (Amazon Redshift Redshift-Dokumentation)
- Erstellen einer skalaren Python-UDF (Amazon Redshift Redshift-Dokumentation)

Zusätzliche Informationen

Beispiel in türkischer Sprache

Amazon Redshift gibt Abfrageergebnisse zurück, die auf der binären UTF-8-Sortierreihenfolge basieren, nicht auf der sprachspezifischen Sortierreihenfolge. Das heißt, wenn Sie eine Amazon Redshift Redshift-Tabelle abfragen, die türkische Zeichen enthält, werden die Abfrageergebnisse nicht nach der sprachlichen Reihenfolge der türkischen Sprache sortiert. Die türkische Sprache enthält sechs Sonderzeichen (ç, ı, ğ, ö, ş und ü), die im lateinischen Alphabet nicht vorkommen. Diese Sonderzeichen werden am Ende einer sortierten Ergebnismenge platziert, die auf der binären UTF-8-Reihenfolge basiert, wie die folgende Tabelle zeigt.

Binäre UTF-8-Reihenfolge	Türkische sprachliche Reihenfolge
a	a
b	b
c	c
d	ç (*)
e	d
f	e
g	f
h	g
i	ğ (*)
j	h
k	ı (*)

l	i
m	j
n	k
o	l
p	m
r	n
S	o
t	ö (*)
u	p
V	r
y	S
z	ş (*)
ç (*)	t
ğ (*)	u
ı (*)	ü (*)
ö (*)	V
ş (*)	y
ü (*)	z

> **Note**
>
> Das Sternchen (*) steht für ein Sonderzeichen in der türkischen Sprache.

Wie die obige Tabelle zeigt, steht das Sonderzeichen ç in der türkischen Sprachreihenfolge zwischen c und d, in der binären UTF-8-Reihenfolge jedoch hinter z Die skalare Python-UDF in diesem Muster verwendet das folgende Zeichenersetzungswörterbuch, um die türkischen Sonderzeichen durch entsprechende lateinische äquivalente Zeichen zu ersetzen.

Türkisches Sonderzeichen	Entsprechendes lateinisches Zeichen
ç	c~
ı	h~
ğ	g~
ö	o~
ş	s~
ü	u~

> **Note**
>
> An das Ende der lateinischen Zeichen, die die entsprechenden türkischen Sonderzeichen ersetzen, wird eine Tilde (~) angehängt.

Ändern Sie eine skalare Python-UDF-Funktion

Verwenden Sie den folgenden SQL-Code, um die skalare Python-UDF-Funktion anhand dieses Musters so zu ändern, dass die Funktion einen Locate-Parameter akzeptiert und ein Wörterbuch mit mehreren Transaktionen unterstützt:

```
CREATE OR REPLACE FUNCTION collate_sort (value varchar, locale varchar)
RETURNS varchar
IMMUTABLE
AS
$$
    def sort_str(val):
       import string
       # Turkish Dictionary
       if locale == 'tr-TR':
```

```
            dictionary = {
               'I': 'ı',
               'ı': 'h~',
               'İ': 'i',
               'Ş': 's~',
               'ş': 's~',
               'Ğ': 'g~',
               'ğ': 'g~',
               'Ü': 'u~',
               'ü': 'u~',
               'Ö': 'o~',
               'ö': 'o~',
               'Ç': 'c~',
               'ç': 'c~'
        }
        # German Dictionary
        if locale == 'de-DE':
            dictionary = {
               ....
               ....
        }

        for key, value in dictionary.items():
            val = val.replace(key, value)

        return val.lower()

    return sort_str(value)

$$ LANGUAGE plpythonu;
```

Der folgende Beispielcode zeigt, wie die modifizierte Python-UDF abgefragt wird:

```
SELECT first_name FROM my_table ORDER BY collate_order(first_name, 'tr-TR');
```

Abonnieren Sie eine Lambda-Funktion für Ereignisbenachrichtigungen von S3-Buckets in verschiedenen AWS-Regionen

Erstellt von Suresh Konathala, Andrew Preston und Arindom Sarkar

Übersicht

Amazon Simple Storage Service (Amazon S3) Event Notifications veröffentlicht Benachrichtigungen für bestimmte Ereignisse in Ihrem S3-Bucket (z. B. Ereignisse, die durch Objekte erstellt wurden, Objekte entfernt oder Objekte wiederhergestellt). Sie können eine AWS Lambda Lambda-Funktion verwenden, um diese Benachrichtigungen gemäß den Anforderungen Ihrer Anwendung zu verarbeiten. Die Lambda-Funktion kann jedoch Benachrichtigungen von S3-Buckets, die in verschiedenen AWS-Regionen gehostet werden, nicht direkt abonnieren.

Der Ansatz dieses Musters stellt ein Fanout-Szenario zur Verarbeitung von Amazon S3 S3-Benachrichtigungen aus regionsübergreifenden S3-Buckets mithilfe eines Amazon Simple Notification Service (Amazon SNS) -Themas für jede Region bereit. Diese regionalen SNS-Themen senden die Amazon S3 S3-Ereignisbenachrichtigungen an eine Amazon Simple Queue Service (Amazon SQS) -Warteschlange in einer zentralen Region, die auch Ihre Lambda-Funktion enthält. Die Lambda-Funktion abonniert diese SQS-Warteschlange und verarbeitet die Ereignisbenachrichtigungen gemäß den Anforderungen Ihres Unternehmens.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Bestehende S3-Buckets in mehreren Regionen, einschließlich einer zentralen Region zum Hosten der Amazon SQS SQS-Warteschlange und der Lambda-Funktion.
- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert. Weitere Informationen dazu finden Sie unter Installation, Aktualisierung und Deinstallation der AWS-CLI in der AWS-CLI-Dokumentation.
- Vertrautheit mit dem Fanout-Szenario in Amazon SNS. Weitere Informationen dazu finden Sie unter Allgemeine Amazon SNS SNS-Szenarien in der Amazon SNS SNS-Dokumentation.

Architektur

Das folgende Diagramm zeigt die Architektur für den Ansatz dieses Musters.

Das Diagramm zeigt den folgenden Workflow:

1. Amazon S3 sendet Ereignisbenachrichtigungen über S3-Buckets (z. B. erstelltes, entferntes Objekt oder wiederhergestelltes Objekt) an ein SNS-Thema in derselben Region.
2. Das SNS-Thema veröffentlicht das Ereignis in einer SQS-Warteschlange in der Zentralregion.
3. Die SQS-Warteschlange ist als Ereignisquelle für Ihre Lambda-Funktion konfiguriert und puffert die Ereignisnachrichten für die Lambda-Funktion.
4. Die Lambda-Funktion fragt die SQS-Warteschlange nach Nachrichten ab und verarbeitet die Amazon S3 S3-Ereignisbenachrichtigungen gemäß den Anforderungen Ihrer Anwendung.

Technologie-Stack

- Lambda
- Amazon SNS
- Amazon SQS
- Amazon S3

Tools

- AWS CLI — Die AWS-Befehlszeilenschnittstelle (AWS CLI) ist ein Open-Source-Tool für die Interaktion mit AWS-Services über Befehle in Ihrer Befehlszeilen-Shell. Mit minimaler Konfiguration können Sie AWS-CLI-Befehle, die Funktionen implementieren, die denen entsprechen, die von der browserbasierten AWS-Managementkonsole bereitgestellt werden, von einer Befehlszeile aus ausführen.
- AWS CloudFormation — AWS CloudFormation hilft Ihnen dabei, Ihre AWS-Ressourcen zu modellieren und einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus zu verwalten. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben und sie zusammen als Stapel zu starten und zu konfigurieren, anstatt Ressourcen einzeln zu verwalten. Sie können Stacks für mehrere AWS-Konten und AWS-Regionen verwalten und bereitstellen.

- AWS Lambda — AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.
- Amazon SQS — Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können. Amazon SQS unterstützt sowohl Standard- als auch FIFO-Warteschlangen.

Epen

Erstellen Sie die SQS-Warteschlange und die Lambda-Funktion in Ihrer zentralen Region

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine SQS-Warteschlange mit einem Lambda-Trigger.	Melden Sie sich bei der AWS-Managementkonsole an und verwenden Sie die Anweisungen aus dem Tutorial Using Lambda with Amazon SQS in der AWS Lambda-Dokumentation, um die folgenden Ressourcen in Ihrer zentralen Region zu erstellen: • Eine Lambda-Ausführungsrolle • Eine Lambda-Funktion zur Verarbeitung der Amazon S3 S3-Ereignisse • Eine SQS-Warteschlange	AWS DevOps, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Stellen Sie sicher, dass Sie die SQS-Warteschlange als Ereignisquelle für Ihre Lambda-Funktion konfigurieren.	

Erstellen Sie ein SNS-Thema und richten Sie Ereignisbenachrichtigungen für die S3-Buckets in jeder erforderlichen Region ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein SNS-Thema , um Amazon S3 S3-Ereign isbenachrichtigungen zu erhalten.	Erstellen Sie ein SNS-Thema in einer Region, von der Sie Amazon S3 S3-Ereign isbenachrichtigungen erhalten möchten. Weitere Informati onen dazu finden Sie unter dem Thema Creating an SNS in der Amazon SNS SNS-Dokumentation. **Important** Stellen Sie sicher, dass Sie den Amazon-Ressourcennamen (ARN) Ihres SNS-Themas aufzeichnen.	AWS DevOps, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Abonnieren Sie das SNS-Thema für die zentrale SQS-Warteschlange.	Abonnieren Sie Ihr SNS-Thema für die SQS-Warte schlange, die von Ihrer zentralen Region gehostet wird. Weitere Informationen dazu finden Sie unter dem Thema Abonnieren eines SNS in der Amazon SNS SNS-Dokumentation.	AWS DevOps, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Zugriffsrichtlinie des SNS-Themas.	1. Öffnen Sie die Amazon SNS SNS-Konsole, wählen Sie Themen und dann das SNS-Thema aus, das Sie zuvor erstellt haben. 2. Wählen Sie Bearbeiten und erweitern Sie dann den Abschnitt Zugriffsrichtlinie — optional. 3. Fügen Sie Ihrem SNS-Thema die folgende Zugriffsrichtlinie bei, um die `sns:publish` Erlaubnis für Amazon S3 zu gewähren, und wählen Sie dann Speichern aus: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "0", "Effect": "Allow", "Principal": { "Service": "s3.amazonaws.com" }, "Action": "sns:Publish", "Resource": "arn:aws:sns:us-west-2::s3Events-SNSTopic-us-west-2" } ]`	AWS DevOps, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>}</pre>	
Richten Sie Benachric htigungen für jeden S3-Bucket in der Region ein.	Richten Sie Ereignisb enachrichtigungen für jeden S3-Bucket in der Region ein. Weitere Informationen dazu finden Sie unter Aktivieren und Konfigurieren von Ereignisb enachrichtigungen mithilfe der Amazon S3 S3-Konsole in der Amazon S3 S3-Dokume ntation. **Note** Wählen Sie im Abschnitt Ziel die Option SNS-Thema aus und geben Sie den ARN des SNS-Themas an, das Sie zuvor erstellt haben.	AWS DevOps, Cloud-Architekt
Wiederholen Sie dieses Epos für alle erforderlichen Regionen.	**Important** Wiederholen Sie die Aufgaben in diesem Epos für jede Region, aus der Sie Amazon S3 S3-Ereign isbenachrichtigung en erhalten möchten, einschließlich Ihrer zentralen Region.	AWS DevOps, Cloud-Architekt

Zugehörige Ressourcen

- Konfiguration einer Zugriffsrichtlinie (Amazon SQS SQS-Dokumentation)
- Konfiguration einer SQS-Warteschlange als Ereignisquelle (AWS Lambda Lambda-Dokumentation)
- Konfiguration einer SQS-Warteschlange zur Initiierung einer Lambda-Funktion (Amazon SQS SQS-Dokumentation)
- AWS::Lambda::Function Ressource (CloudFormation AWS-Dokumentation)

Drei AWS Glue ETL-Auftragstypen für die Konvertierung von Daten in Apache Parquet

Erstellt von Adnan Alvee (AWS), Karthikeyan Ramachandran (AWS) und Nith Govindasivan (AWS)

Übersicht

In der Amazon Web Services (AWS) Cloud ist AWS Glue ein vollständig verwalteter Service zum Extrahieren, Transformieren und Laden (ETL). Mit AWS Glue können Sie Ihre Daten kostengünstig kategorisieren, bereinigen, anreichern und zuverlässig zwischen verschiedenen Datenspeichern und Datenströmen verschieben.

Dieses Muster bietet verschiedene Auftragstypen in AWS Glue und verwendet drei verschiedene Skripts, um die Erstellung von ETL-Jobs zu demonstrieren.

Sie können AWS Glue verwenden, um ETL-Jobs in einer Python-Shell-Umgebung zu schreiben. Sie können auch Batch- und Streaming-ETL-Jobs mithilfe von Python (PySpark) oder Scala in einer verwalteten Apache Spark-Umgebung erstellen. Um Ihnen den Einstieg in die Erstellung von ETL-Jobs zu erleichtern, konzentriert sich dieses Muster auf Batch-ETL-Jobs mit Python-Shell und Scala. PySpark Python-Shell-Jobs sind für Workloads gedacht, die weniger Rechenleistung benötigen. Die verwaltete Apache Spark-Umgebung ist für Workloads gedacht, die eine hohe Rechenleistung erfordern.

Apache Parquet wurde entwickelt, um effiziente Komprimierungs- und Kodierungsschemata zu unterstützen. Es kann Ihre Analytics-Workloads beschleunigen, da es Daten spaltenweise speichert. Durch die Konvertierung von Daten in Parquet können Sie auf längere Sicht Speicherplatz, Kosten und Zeit sparen. Weitere Informationen zu Parquet finden Sie im Blogbeitrag Apache Parquet: How to be a hero with the open-source columnar data format.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Rolle AWS Identity and Access Management (IAM) (Wenn Sie noch keine Rolle haben, lesen Sie den Abschnitt Zusätzliche Informationen.)

Architektur

Zieltechnologie-Stack

- AWS Glue
- Amazon Simple Storage Service (Amazon-S3)
- Apache Parquet

Automatisierung und Skalierung

- AWS Glue Glue-Workflows unterstützen die vollständige Automatisierung einer ETL-Pipeline.
- Sie können die Anzahl der Datenverarbeitungseinheiten (DPUs) oder Workertypen ändern, um sie horizontal und vertikal zu skalieren.

Tools

AWS-Services

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Glue ist ein vollständig verwalteter ETL-Service zum Kategorisieren, Bereinigen, Anreichern und Verschieben Ihrer Daten zwischen verschiedenen Datenspeichern und Datenströmen.

Andere Tools

- Apache Parquet ist ein spaltenorientiertes Open-Source-Datendateiformat, das zum Speichern und Abrufen entwickelt wurde.

Konfiguration

Verwenden Sie die folgenden Einstellungen für die Konfiguration der Rechenleistung von AWS Glue ETL. Um die Kosten zu senken, sollten Sie die minimalen Einstellungen verwenden, wenn Sie den Workload ausführen, der in diesem Muster bereitgestellt wird.

- Python-Shell — Sie können 1 DPU verwenden, um 16 GB Speicher zu nutzen, oder 0,0625 DPU, um 1 GB Speicher zu nutzen. Dieses Muster verwendet 0,0625 DPU, was die Standardeinstellung in der AWS Glue Glue-Konsole ist.
- Python oder Scala für Spark — Wenn Sie die Spark-bezogenen Jobtypen in der Konsole auswählen, verwendet AWS Glue standardmäßig 10 Worker und den G.1X-Workertyp. Bei

diesem Muster werden zwei Worker verwendet, was der zulässigen Mindestanzahl entspricht. Der Standard-Worker-Typ ist ausreichend und kostengünstig.

In der folgenden Tabelle sind die verschiedenen AWS Glue Glue-Worker-Typen für die Apache Spark-Umgebung aufgeführt. Da ein Python-Shell-Job die Apache Spark-Umgebung nicht zum Ausführen von Python verwendet, ist er nicht in der Tabelle enthalten.

	Standard	G.1X	G.2X
vCPU	4	4	8
Arbeitsspeicher	16 GB	16 GB	32 GB
Festplattenkapazität	50 GB	64 GB	128 GB
Testamentsvollstrecker pro Arbeiter	2	1	1

Code

Den Code, der in diesem Muster verwendet wird, einschließlich der IAM-Rolle und der Parameterkonfiguration, finden Sie im Abschnitt Zusätzliche Informationen.

Epen

Laden Sie die Daten hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Daten in einen neuen oder vorhandenen S3-Bucket hoch.	Erstellen oder verwenden Sie einen vorhandenen S3-Bucket in Ihrem Konto. Laden Sie die Datei sample_data.csv aus dem Bereich Anlagen hoch und notieren Sie sich den S3-Bucket und den Speicherort des Präfixes.	Allgemeines AWS

Den AWS Glue Glue-Job erstellen und ausführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den AWS Glue Glue-Job.	Fügen Sie im ETL-Bereich der AWS Glue Glue-Konsole einen AWS Glue Glue-Job hinzu. Wählen Sie den entsprechenden Jobtyp, die AWS Glue Glue-Version und den entsprechenden DPU-/Worker-Typ und die Anzahl der Worker aus. Einzelheiten finden Sie im Abschnitt Konfiguration.	Entwickler, Cloud oder Daten
Ändern Sie die Eingabe- und Ausgabeorte.	Kopieren Sie den Code, der Ihrem AWS Glue Glue-Job entspricht, und ändern Sie den Eingabe- und Ausgabeort, den Sie im Abschnitt Daten hochladen notiert haben.	Entwickler, Cloud oder Daten
Konfigurieren Sie die Parameter.	Sie können die im Abschnitt Zusätzliche Informationen bereitgestellten Codefragmente verwenden, um Parameter für Ihren ETL-Job festzulegen. AWS Glue verwendet intern vier Argumentnamen: • `--conf` • `--debug` • `--mode` • `--JOB_NAME`	Entwickler, Cloud oder Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Der `--JOB_NAME` Parameter muss explizit in der AWS Glue Glue-Konsole eingegeben werden. Wählen Sie Jobs, Job bearbeiten, Sicherheitskonfiguration, Skriptbibliotheken und Jobparameter (optional). Geben Sie `--JOB_NAME` den Schlüssel ein und geben Sie einen Wert ein. Sie können diesen Parameter auch über die AWS-Befehlszeilenschnittstelle (AWS CLI) oder die AWS Glue Glue-API festlegen. Der `--JOB_NAME` Parameter wird von Spark verwendet und wird in einem Python-Shell-Umgebungsjob nicht benötigt. Sie müssen `--` vor jedem Parameter einen Namen hinzufügen, sonst funktioniert der Code nicht. Für die Codefragmente müssen die Standortparameter beispielsweise mit und aufgerufen werden. `--input_loc --output_loc`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den ETL-Job aus.	Führen Sie Ihren Job aus und überprüfen Sie die Ausgabe. Beachten Sie, wie viel Speicherplatz gegenüber der Originaldatei reduziert wurde.	Entwickler, Cloud oder Daten

Zugehörige Ressourcen

Referenzen

- Apache Spark
- AWS Glue: So funktioniert's
- Preise für AWS Glue

Tutorials und Videos

- Was ist AWS Glue?

Zusätzliche Informationen

IAM role (IAM-Rolle)

Wenn Sie die AWS Glue Glue-Jobs erstellen, können Sie entweder eine vorhandene IAM-Rolle mit den im folgenden Codeausschnitt angegebenen Berechtigungen oder eine neue Rolle verwenden.

Verwenden Sie den folgenden YAML-Code, um eine neue Rolle zu erstellen.

```
# (c) 2022 Amazon Web Services, Inc. or its affiliates. All Rights Reserved. This AWS
 Content is provided subject to the terms of the AWS Customer
# Agreement available at https://aws.amazon.com/agreement/ or other written agreement
 between Customer and Amazon Web Services, Inc.

AWSTemplateFormatVersion: "2010-09-09"

Description: This template will setup IAM role for AWS Glue service.
```

```
Resources:
  rGlueRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              Service:
                - "glue.amazonaws.com"
            Action:
              - "sts:AssumeRole"
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole
      Policies:
        - PolicyName: !Sub "${AWS::StackName}-s3-limited-read-write-inline-policy"
          PolicyDocument:
            Version: "2012-10-17"
            Statement:
              - Effect: Allow
                Action:
                  - "s3:PutObject"
                  - "s3:GetObject"
                Resource: "arn:aws:s3:::*/*"
      Tags:
        - Key  : "Name"
          Value : !Sub "${AWS::StackName}"

Outputs:
  oGlueRoleName:
    Description: AWS Glue IAM role
    Value:
      Ref: rGlueRole
    Export:
      Name: !Join [ ":", [ !Ref "AWS::StackName", rGlueRole ] ]
```

AWS Glue Python-Shell

Der Python-Code verwendet die Pandas und PyArrow Bibliotheken, um Daten in Parquet zu konvertieren. Die Pandas-Bibliothek ist bereits verfügbar. Die PyArrow Bibliothek wird heruntergeladen, wenn Sie das Pattern ausführen, da es sich um eine einmalige Ausführung handelt.

Sie können Raddateien verwenden, um sie in eine Bibliothek PyArrow zu konvertieren und die Datei als Bibliothekspaket bereitzustellen. Weitere Informationen zum Verpacken von Raddateien finden Sie unter Bereitstellen einer eigenen Python-Bibliothek.

Python-Shell-Parameter von AWS Glue

```
from awsglue.utils import getResolvedOptions

args = getResolvedOptions(sys.argv, ["input_loc", "output_loc"])
```

Python-Shellcode von AWS Glue

```
from io import BytesIO
import pandas as pd
import boto3
import os
import io
import site
from importlib import reload
from setuptools.command import easy_install
install_path = os.environ['GLUE_INSTALLATION']
easy_install.main( ["--install-dir", install_path, "pyarrow"] )
reload(site)
import pyarrow


input_loc = "s3://bucket-name/prefix/sample_data.csv"
output_loc = "s3://bucket-name/prefix/"


input_bucket = input_loc.split('/', 1)[0]
object_key = input_loc.split('/', 1)[1]


output_loc_bucket = output_loc.split('/', 1)[0]
output_loc_prefix = output_loc.split('/', 1)[1]


s3 = boto3.client('s3')
obj = s3.get_object(Bucket=input_bucket, Key=object_key)
df = pd.read_csv(io.BytesIO(obj['Body'].read()))
```

```
parquet_buffer = BytesIO()
s3_resource = boto3.resource('s3')
df.to_parquet(parquet_buffer, index=False)
s3_resource.Object(output_loc_bucket, output_loc_prefix +  'data' +
 '.parquet').put(Body=parquet_buffer.getvalue())
```

AWS Glue Spark-Auftrag mit Python

Um einen AWS Glue Spark-Auftragstyp mit Python zu verwenden, wählen Sie Spark als Auftragstyp. Wählen Sie Spark 3.1, Python 3 mit verbesserter Jobstartzeit (Glue Version 3.0) als AWS Glue Glue-Version.

Python-Parameter von AWS Glue

```
from awsglue.utils import getResolvedOptions

args = getResolvedOptions(sys.argv, ["JOB_NAME", "input_loc", "output_loc"])
```

AWS Glue Spark-Job mit Python-Code

```
import sys
from pyspark.context import SparkContext
from awsglue.context import GlueContext
from awsglue.transforms import *
from awsglue.dynamicframe import DynamicFrame
from awsglue.utils import getResolvedOptions
from awsglue.job import Job


sc = SparkContext()
glueContext = GlueContext(sc)
spark = glueContext.spark_session
job = Job(glueContext)

input_loc = "s3://bucket-name/prefix/sample_data.csv"
output_loc = "s3://bucket-name/prefix/"

inputDyf = glueContext.create_dynamic_frame_from_options(\
    connection_type = "s3", \
    connection_options = {
        "paths": [input_loc]}, \
    format = "csv",
```

```
    format_options={
        "withHeader": True,
        "separator": ","
    })


outputDF = glueContext.write_dynamic_frame.from_options(\
    frame = inputDyf, \
    connection_type = "s3", \
    connection_options = {"path": output_loc \
        }, format = "parquet")
```

Verwenden Sie für eine große Anzahl komprimierter großer Dateien (z. B. 1.000 Dateien mit einer Größe von jeweils etwa 3 MB) den `compressionType` Parameter mit dem `recurse` Parameter, um alle Dateien zu lesen, die innerhalb des Präfixes verfügbar sind, wie im folgenden Code gezeigt.

```
input_loc = "bucket-name/prefix/"
output_loc = "bucket-name/prefix/"

inputDyf = glueContext.create_dynamic_frame_from_options(
                    connection_type = "s3",
                    connection_options = {"paths": [input_loc],
                                          "compressionType":"gzip","recurse" :"True",
                                          },
                    format = "csv",
                    format_options={"withHeader": True,"separator": ","}
                    )
```

Verwenden Sie für eine große Anzahl komprimierter kleiner Dateien (z. B. 1.000 Dateien mit jeweils etwa 133 KB) den `groupFiles` Parameter zusammen mit den `recurse` Parametern `compressionType` und. Der `groupFiles` Parameter gruppiert kleine Dateien in mehrere große Dateien, und der `groupSize` Parameter steuert die Gruppierung auf die angegebene Größe in Byte (z. B. 1 MB). Der folgende Codeausschnitt bietet ein Beispiel für die Verwendung dieser Parameter im Code.

```
input_loc = "bucket-name/prefix/"
output_loc = "bucket-name/prefix/"

inputDyf = glueContext.create_dynamic_frame_from_options(
                    connection_type = "s3",
                    connection_options = {"paths": [input_loc],
```

```
                                          "compressionType":"gzip","recurse" :"True",
                                           "groupFiles" :"inPartition",
 "groupSize" :"1048576",
                                          },
                    format = "csv",
                    format_options={"withHeader": True,"separator": ","}
                    )
```

Ohne Änderung der Worker-Knoten ermöglichen diese Einstellungen dem AWS Glue Glue-Job, mehrere Dateien (groß oder klein, mit oder ohne Komprimierung) zu lesen und sie im Parquet-Format auf das Ziel zu schreiben.

AWS Glue Spark-Auftrag mit Scala

Um einen AWS Glue Spark-Auftragstyp mit Scala zu verwenden, wählen Sie Spark als Auftragstyp und Sprache als Scala. Wählen Sie Spark 3.1, Scala 2 mit verbesserter Jobstartzeit (Glue Version 3.0) als AWS Glue Glue-Version. Um Speicherplatz zu sparen, verwendet das folgende Beispiel für AWS Glue mit Scala die `applyMapping` Funktion auch zum Konvertieren von Datentypen.

AWS Glue Scala-Parameter

```
import com.amazonaws.services.glue.util.GlueArgParser val args =
 GlueArgParser.getResolvedOptions(sysArgs, Seq("JOB_NAME", "inputLoc",
 "outputLoc").toArray)
```

AWS Glue Spark-Job mit Scala-Code

```
import com.amazonaws.services.glue.GlueContext
import com.amazonaws.services.glue.MappingSpec
import com.amazonaws.services.glue.DynamicFrame
import com.amazonaws.services.glue.errors.CallSite
import com.amazonaws.services.glue.util.GlueArgParser
import com.amazonaws.services.glue.util.Job
import com.amazonaws.services.glue.util.JsonOptions
import org.apache.spark.SparkContext
import scala.collection.JavaConverters._


object GlueScalaApp {
  def main(sysArgs: Array[String]) {

    @transient val spark: SparkContext = SparkContext.getOrCreate()
```

```
    val glueContext: GlueContext = new GlueContext(spark)

    val inputLoc = "s3://bucket-name/prefix/sample_data.csv"
    val outputLoc = "s3://bucket-name/prefix/"

    val readCSV = glueContext.getSource("csv", JsonOptions(Map("paths" ->
 Set(inputLoc)))).getDynamicFrame()

    val applyMapping = readCSV.applyMapping(mappings = Seq(("_c0", "string", "date",
 "string"), ("_c1", "string", "sales", "long"),
    ("_c2", "string", "profit", "double")), caseSensitive = false)

    val formatPartition = applyMapping.toDF().coalesce(1)

    val dynamicFrame = DynamicFrame(formatPartition, glueContext)

    val dataSink = glueContext.getSinkWithFormat(
        connectionType = "s3",
        options = JsonOptions(Map("path" -> outputLoc )),
        transformationContext = "dataSink", format =
 "parquet").writeDynamicFrame(dynamicFrame)
  }
}
```

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Visualisieren Sie Amazon Redshift Redshift-Prüfprotokolle mit Amazon Athena und Amazon QuickSight

Erstellt von Sanket Sirsikar (AWS) und Gopal Krishna Bhatia (AWS)

Übersicht

Sicherheit ist ein integraler Bestandteil des Datenbankbetriebs in der Amazon Web Services (AWS) Cloud. Ihr Unternehmen sollte sicherstellen, dass es die Aktivitäten und Verbindungen der Datenbankbenutzer überwacht, um potenzielle Sicherheitsvorfälle und -risiken zu erkennen. Dieses Muster hilft Ihnen dabei, Ihre Datenbanken zu Sicherheits- und Fehlerbehebungszwecken zu überwachen. Dieser Vorgang wird als Datenbank-Auditing bezeichnet.

Dieses Muster stellt ein SQL-Skript bereit, das die Erstellung einer Amazon Athena Athena-Tabelle und Ansichten für ein Berichts-Dashboard in Amazon automatisiert QuickSight , das Sie bei der Prüfung von Amazon Redshift Redshift-Protokollen unterstützt. Dadurch wird sichergestellt, dass Benutzer, die für die Überwachung der Datenbankaktivitäten verantwortlich sind, bequemen Zugriff auf Datensicherheitsfunktionen haben.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein vorhandener Amazon Redshift Redshift-Cluster. Weitere Informationen dazu finden Sie unter Erstellen eines Amazon Redshift Redshift-Clusters in der Amazon Redshift Redshift-Dokumentation.
- Zugriff auf eine bestehende Athena-Arbeitsgruppe. Weitere Informationen finden Sie in der Amazon Athena Athena-Dokumentation unter So funktionieren Arbeitsgruppen.
- Ein vorhandener Quell-Bucket von Amazon Simple Storage Service (Amazon S3) mit den erforderlichen AWS Identity and Access Management (IAM) -Berechtigungen. Weitere Informationen finden Sie unter Bucket-Berechtigungen für die Amazon Redshift Redshift-Audit-Protokollierung unter Datenbank-Audit-Protokollierung in der Amazon Redshift Redshift-Dokumentation.

Architektur

Technologie-Stack

- Athena
- Amazon Redshift
- Amazon S3
- QuickSight

Tools

- Amazon Athena — Athena ist ein interaktiver Abfrageservice, der es einfach macht, Daten in Amazon S3 mit Standard-SQL zu analysieren.
- Amazon QuickSight — QuickSight ist ein skalierbarer, serverloser, einbettbarer, auf maschinellem Lernen basierender Business Intelligence (BI) -Service.
- Amazon Redshift — Amazon Redshift ist ein vollständig verwalteter Data-Warehousing-Service auf Unternehmensebene im Petabyte-Bereich.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Speicher für das Internet.

Epen

Den Amazon Redshift Redshift-Cluster konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie die Auditprot okollierung für den Amazon Redshift Redshift-Cluster.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon Redshift Redshift-Konsole, wählen Sie CLUSTERS und dann den Cluster aus, für den Sie die Protokollierung aktivieren möchten. 2. Wählen Sie die Registerk arte Eigenschaften und aktivieren Sie dann die	DBA, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Überwachung, indem Sie den Anweisungen unter Auditing mithilfe der Konsole konfigurieren in der Amazon Redshift Redshift-Dokumentation folgen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie die Protokollierung in der Amazon Redshift Redshift-Cluster-Parametergruppe.	Sie können die Prüfung von Verbindungsprotokollen, Benutzerprotokollen und Benutzeraktivitätsprotokollen gleichzeitig aktivieren, indem Sie die AWS-Managementkonsole, die Amazon Redshift Redshift-API-Referenz oder die AWS-Befehlszeilenschnittstelle (AWS CLI) verwenden. Für die Prüfung von Benutzeraktivitätsprotokollen müssen Sie den `enable_user_activity_logging` Datenbankparameter aktivieren. Wenn Sie nur die Audit-Logging-Funktion, aber nicht den zugehörigen Parameter aktivieren, protokolliert das Datenbank-Audit die Protokollinformationen für die Verbindungs- und Benutzerprotokolle, nicht aber für die Benutzeraktivitätsprotokolle. Der `enable_user_activity_logging` Parameter ist standardmäßig nicht aktiviert, aber Sie können ihn aktivieren, indem Sie ihn von `false` zu ändern`true`.	DBA, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Important Sie müssen eine neue Cluster-Parameterg ruppe mit aktiviert em `user_acti vity_logging` Parameter erstellen und sie an Ihren Amazon Redshift Redshift-Cluster anhängen. Weitere Informationen dazu finden Sie unter Einen Cluster modifizieren in der Amazon Redshift Redshift-Dokumenta tion. Weitere Informationen zu dieser Aufgabe finden Sie unter Amazon Redshift Redshift-Parametergruppen und Konfiguration der Überwachung mithilfe der Konsole in der Amazon Redshift Redshift-Dokumenta tion.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie S3-Bucket -Berechtigungen für die Amazon Redshift Redshift-Cluster-Protokollierung.	Wenn Sie die Protokollierung aktivieren, sammelt Amazon Redshift Protokollierungsinformationen und lädt sie in Protokolldateien hoch, die in einem S3-Bucket gespeichert sind. Sie können einen vorhandenen S3-Bucket verwenden oder einen neuen Bucket erstellen. **Important** Stellen Sie sicher, dass Amazon Redshift über die erforderlichen IAM-Berechtigungen für den Zugriff auf den S3-Bucket verfügt. Weitere Informationen dazu finden Sie unter Bucket-Berechtigungen für die Amazon Redshift Redshift-Audit-Protokollierung von Database Audit Logging in der Amazon Redshift Redshift-Dokumentation.	DBA, Dateningenieur

Erstellen Sie die Athena-Tabelle und die Athena-Ansichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Athena-Tabelle und die Ansichten, um Amazon Redshift Redshift-Audit-Protokolldaten aus dem S3-Bucket abzufragen.	Öffnen Sie die Amazon Athena Athena-Konsole und verwenden Sie die DDL-Abfrage (Data Definition Language) aus dem `AuditLogging.sql` SQL-Skript (angehängt), um die Tabelle und die Ansichten für Benutzeraktivitätsprotokolle, Benutzerprotokolle und Verbindungsprotokolle zu erstellen. Weitere Informationen und Anweisungen finden Sie im Tutorial Tabellen erstellen und Abfragen ausführen aus dem Amazon Athena Workshop.	Dateningenieur

Richten Sie die Protokollüberwachung im QuickSight Dashboard ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein QuickSight Dashboard mit Athena als Datenquelle.	Öffnen Sie die QuickSight Amazon-Konsole und erstellen Sie ein QuickSight Dashboard, indem Sie den Anweisungen im Tutorial Visualize QuickSight with Athena aus dem Amazon Athena Workshop folgen.	DBA, Dateningenieur

Zugehörige Ressourcen

- Erstellen Sie Tabellen und führen Sie Abfragen in Athena aus
- Visualisieren QuickSight mit Athena

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Visualisieren Sie IAM-Anmeldedaten für alle AWS-Konten mithilfe von Amazon QuickSight

Erstellt von Parag Nagwekar (AWS) und Arun Chandapillai (AWS)

Übersicht

> **Warning**
>
> IAM-Benutzer verfügen über langfristige Anmeldeinformationen, was ein Sicherheitsrisiko darstellt. Um dieses Risiko zu minimieren, empfehlen wir, diesen Benutzern nur die Berechtigungen zu gewähren, die sie für die Ausführung der Aufgabe benötigen, und diese Benutzer zu entfernen, wenn sie nicht mehr benötigt werden.

Sie können die Anmeldeinformationen von AWS Identity and Access Management (IAM) verwenden, um die Sicherheits-, Prüf- und Compliance-Anforderungen Ihres Unternehmens zu erfüllen. Anmeldedatenberichte enthalten eine Liste aller Benutzer in Ihren AWS-Konten und zeigen den Status ihrer Anmeldeinformationen, wie Passwörter, Zugriffsschlüssel und Geräte mit Multi-Faktor-Authentifizierung (MFA). Sie können Anmeldeinformationsberichte für mehrere AWS-Konten verwenden, die von AWS Organizations verwaltet werden.

Dieses Muster enthält Schritte und Code, mit denen Sie mithilfe von QuickSight Amazon-Dashboards IAM-Anmeldeinformationen für alle AWS-Konten in Ihrer Organisation erstellen und teilen können. Sie können die Dashboards mit Stakeholdern in Ihrer Organisation teilen. Die Berichte können Ihrem Unternehmen dabei helfen, die folgenden gezielten Geschäftsergebnisse zu erzielen:

- Identifizieren Sie Sicherheitsvorfälle im Zusammenhang mit IAM-Benutzern
- Verfolgen Sie die Migration von IAM-Benutzern zur Single Sign-On (SSO) -Authentifizierung in Echtzeit
- AWS-Regionen verfolgen, auf die IAM-Benutzer zugreifen
- Bleiben Sie konform
- Teilen Sie Informationen mit anderen Interessengruppen

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Organisation mit Mitgliedskonten
- Eine IAM-Rolle mit Berechtigungen für den Zugriff auf Konten in Organizations
- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 2, installiert und konfiguriert
- Ein Abonnement für die Amazon QuickSight Enterprise Edition

Architektur

Technologie-Stack

- Amazon Athena
- Amazon EventBridge
- Amazon QuickSight
- Amazon Simple Storage Service (Amazon-S3)
- AWS Glue
- AWS Identity and Access Management (IAM)
- AWS Lambda
- AWS Organizations

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur für die Einrichtung eines Workflows, der IAM-Anmeldedaten von mehreren AWS-Konten erfasst.

1. EventBridge ruft täglich eine Lambda-Funktion auf.
2. Die Lambda-Funktion übernimmt in jedem AWS-Konto im gesamten Unternehmen eine IAM-Rolle. Anschließend erstellt die Funktion den Bericht mit den IAM-Anmeldeinformationen und speichert die Berichtsdaten in einem zentralen S3-Bucket. Sie müssen die Verschlüsselung aktivieren und den öffentlichen Zugriff auf den S3-Bucket deaktivieren.

3. Ein AWS Glue Glue-Crawler crawlt den S3-Bucket täglich und aktualisiert die Athena-Tabelle entsprechend.
4. QuickSight importiert und analysiert die Daten aus dem Anmeldedatenbericht und erstellt ein Dashboard, das von Stakeholdern visualisiert und mit ihnen geteilt werden kann.

Tools

AWS-Services

- Amazon Athena ist ein interaktiver Abfrageservice, der es einfach macht, Daten in Amazon S3 mithilfe von Standard-SQL zu analysieren.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel Lambda-Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen AWS-Konten.
- Amazon QuickSight ist ein Business Intelligence (BI) -Service auf Cloud-Ebene, mit dem Sie Ihre Daten in einem einzigen Dashboard visualisieren, analysieren und melden können.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.

Code

Der Code für dieses Muster ist im GitHub getiamcredsreport-allaccounts-orgRepository verfügbar. Sie können den Code aus diesem Repository verwenden, um Berichte über IAM-Anmeldeinformationen für alle AWS-Konten in Organizations zu erstellen und diese an einem zentralen Ort zu speichern.

Epen

Richten Sie die Infrastruktur ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Amazon QuickSight Enterprise Edition ein.	1. Aktivieren Sie die Amazon QuickSight Enterprise Edition in Ihrem AWS-Konto . Weitere Informationen finden Sie QuickSight in der QuickSight Dokumentation unter Benutzerzugriff innerhalb von Amazon verwalten. 2. Um Dashboard-Berechtigungen zu gewähren, rufen Sie den Amazon-Ressourcennamen (ARN) der QuickSight Benutzer ab.	AWS-Administrator DevOps, AWS, Cloud-Administrator, Cloud-Architekt
Integrieren Sie Amazon QuickSight mit Amazon S3 und Athena.	Sie müssen sich für die Verwendung von Amazon S3 und Athena autorisierenQuickSight , bevor Sie den CloudFormation AWS-Stack bereitstellen.	AWS-Administrator DevOps, AWS, Cloud-Administrator, Cloud-Architekt

Stellen Sie die Infrastruktur bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	1. Klonen Sie das GitHub getiamcredsreport-allaccounts-orgRepository auf Ihren lokalen Computer,	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	indem Sie den folgenden Befehl ausführen: `git clone https://github.com/aws-samples/getiamcredsreport-allaccounts-org`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Infrastruktur bereit.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudFormation -Konsole. 2. Wählen Sie im Navigationsbereich Stack erstellen und dann Mit neuen Ressourcen (Standard) aus. 3. Wählen Sie auf der Seite Ressourcen identifizieren die Option Weiter aus. 4. Wählen Sie auf der Seite Vorlage angeben für Vorlagenquelle die Option Vorlagendatei hochladen aus. 5. Wählen Sie Datei auswählen, wählen Sie die `Cloudformation-createcredrepo.yaml` Datei aus Ihrem geklonten GitHub Repository aus und klicken Sie dann auf Weiter. 6. Aktualisieren Sie `IAMRoleName` unter Parameter Ihre IAM-Rolle. Dies sollte die IAM-Rolle sein, die Lambda in jedem Konto der Organisation übernehmen soll. Diese Rolle erstellt den Anmeldeinformationsbericht. Hinweis: Die Rolle muss in diesem	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Schritt der Stack-Ers tellung nicht in allen Konten vorhanden sein. 7. Aktualisieren Sie unter Parameter `S3BucketN ame` mit dem Namen des S3-Buckets, in dem Lambda die Anmeldein formationen für alle Konten speichern kann. 8. Geben Sie als Stack-Name Ihren Stack-Namen ein. 9. Wählen Sie Absenden aus. 10. Notieren Sie sich den Rollennamen der Lambda-Funktion.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Berechtigungsrichtlinie.	Erstellen Sie eine IAM-Richtlinie für jedes AWS-Konto in Ihrer Organisation mit den folgenden Berechtigungen: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "iam:GenerateCredentialReport", "iam:GetCredentialReport" ], "Resource": "*" } ] }`	AWS DevOps, Cloud-Administrator, Cloud-Architekt, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine IAM-Rolle mit einer Vertrauensrichtlinie.	1. Erstellen Sie eine IAM-Rolle für die AWS-Konten und fügen Sie die Berechtigungsrichtlinie hinzu, die Sie im vorherigen Schritt erstellt haben.
	2. Fügen Sie der IAM-Rolle die folgende Vertrauensrichtlinie hinzu:
	
	`{ "Version":"2012-10-17", "Statement":[ { "Effect": "Allow", "Principal":{ "AWS":[ "arn:aws:iam::<MasterAccountID>:role/<LambdaRole>" ] }, "Action": "sts:AssumeRole" } ] }`
	
	Important
	`arn:aws:iam::<MasterAccountID>:role/`
		Cloud-Administrator, Cloud-Architekt, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`<LambdaRole>` Ersetzen Sie es durch den ARN der Lambda-Rolle, den Sie zuvor notiert haben. **Note** Organizations verwenden in der Regel Automatisierung, um IAM-Rollen für ihre AWS-Konten zu erstellen. Wir empfehlen Ihnen, diese Automatisierung zu verwenden, sofern verfügbar. Alternativ können Sie das `CreateRoleforOrg.py` Skript aus dem Code-Repository verwenden. Das Skript erfordert eine bestehende Administratorrolle oder eine andere IAM-Rolle, die berechtigt ist, eine IAM-Richtlinie und -Rolle in jedem AWS-Konto zu erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Amazon QuickSight , um die Daten zu visualisieren.	1. Melden Sie sich QuickSight mit Ihren Zugangsdaten an. 2. Erstellen Sie mithilfe von Athena einen Datensatz (mithilfe der `iamcredreportdb` Datenbank und der `“cfn_iamcredreport”` Tabelle), und aktualisieren Sie den Datensatz anschließend automatisch. 3. Erstellen Sie eine Analyse in QuickSight. 4. Erstellen Sie ein QuickSight Dashboard.	AWS DevOps, Cloud-Administrator, Cloud-Architekt, Dateningenieur

Zusätzliche Informationen

Zusätzliche Überlegungen

Berücksichtigen Sie dabei Folgendes:

- Nachdem Sie die Infrastruktur bereitgestellt haben, können Sie warten, CloudFormation bis die Berichte in Amazon S3 erstellt und von Athena analysiert wurden, bis Lambda und AWS Glue gemäß ihren Zeitplänen ausgeführt werden. Alternativ können Sie Lambda manuell ausführen, um die Berichte in Amazon S3 abzurufen, und dann den AWS Glue Glue-Crawler ausführen, um die Athena-Tabelle abzurufen, die aus den Daten erstellt wurde.
- QuickSight ist ein leistungsstarkes Tool zur Analyse und Visualisierung von Daten auf der Grundlage Ihrer Geschäftsanforderungen. Sie können Parameter verwenden QuickSight , um Widget-Daten auf der Grundlage von Datenfeldern zu steuern, die Sie auswählen. Sie können eine QuickSight Analyse auch verwenden, um Parameter (z. B. Konto-, Datum- und Benutzerfelder wie `partition_0``partition_1`, und `user` bzw.) aus Ihrem Datensatz zu erstellen, um Steuerelemente für die Parameter für Konto, Datum und Benutzer hinzuzufügen.

- Informationen zum Erstellen eigener QuickSight Dashboards finden Sie unter QuickSight Workshops auf der AWS Workshop Studio-Website.
- QuickSight Beispiel-Dashboards finden Sie im GitHub getiamcredsreport-allaccounts-orgCode-Repository.

Gezielte Geschäftsergebnisse

Sie können dieses Muster verwenden, um die folgenden gezielten Geschäftsergebnisse zu erzielen:

- Identifizieren Sie Sicherheitsvorfälle im Zusammenhang mit IAM-Benutzern — Untersuchen Sie jeden Benutzer in jedem AWS-Konto in Ihrem Unternehmen über eine zentrale Oberfläche. Sie können den Trend der zuletzt aufgerufenen einzelnen AWS-Regionen eines IAM-Benutzers und der von ihm genutzten Services verfolgen.
- Verfolgen Sie die Migration von IAM-Benutzern zur SSO-Authentifizierung in Echtzeit — Mithilfe von SSO können sich Benutzer einmal mit einem einzigen Berechtigungsnachweis anmelden und auf mehrere AWS-Konten und -Anwendungen zugreifen. Wenn Sie planen, Ihre IAM-Benutzer zu SSO zu migrieren, kann Ihnen dieses Muster dabei helfen, zu SSO zu wechseln und die gesamte Nutzung der IAM-Benutzeranmeldedaten (z. B. Zugriff auf die AWS-Managementkonsole oder Verwendung von Zugriffsschlüsseln) über alle AWS-Konten hinweg zu verfolgen.
- AWS-Regionen nachverfolgen, auf die IAM-Benutzer zugreifen — Sie können den Zugriff von IAM-Benutzern auf Regionen für verschiedene Zwecke steuern, z. B. für Datenhoheit und Kostenkontrolle. Sie können auch die Nutzung von Regionen durch jeden IAM-Benutzer verfolgen.
- Bleiben Sie konform — Wenn Sie dem Prinzip der geringsten Rechte folgen, können Sie nur die spezifischen IAM-Berechtigungen gewähren, die für die Ausführung einer bestimmten Aufgabe erforderlich sind. Außerdem können Sie den Zugriff auf AWS-Services, die AWS-Managementkonsole und die langfristige Nutzung von Anmeldeinformationen verfolgen.
- Informationen mit anderen Beteiligten teilen — Sie können kuratierte Dashboards mit anderen Beteiligten teilen, ohne ihnen Zugriff auf IAM-Anmeldedaten oder AWS-Konten zu gewähren.

Mehr Muster

- Authentifizieren Sie bestehende Benutzer von React-Anwendungen mithilfe von Amazon Cognito und AWS Amplify UI
- Automatisches Extrahieren von Inhalten aus PDF-Dateien mit Amazon Textract
- Erstellen Sie ein Kaltstart-Prognosemodell, indem Sie DeepAR für Zeitreihen in Amazon SageMaker AI Studio Lab verwenden
- Erstellen Sie mit dem AWS Cost Explorer detaillierte Kosten- und Nutzungsberichte für Amazon EMR-Cluster
- Erstellen Sie detaillierte Kosten- und Nutzungsberichte für Amazon RDS und Amazon Aurora
- Erstellen Sie mit dem AWS Cost Explorer detaillierte Kosten- und Nutzungsberichte für AWS Glue-Jobs
- Stellen Sie einen AWS Glue Glue-Job mit einer AWS CodePipeline CI/CD-Pipeline bereit
- Betten Sie ein QuickSight Amazon-Dashboard in eine lokale Angular-Anwendung ein
- Stellen Sie sicher, dass ein Amazon Redshift Redshift-Cluster bei der Erstellung verschlüsselt ist
- Stellen Sie sicher, dass die Verschlüsselung für Amazon EMR-Daten im Ruhezustand beim Start aktiviert ist
- Schätzung der Speicherkosten für eine Amazon DynamoDB-Tabelle
- Führen Sie Amazon Redshift SQL-Abfragen mithilfe von Terraform aus
- Extrahieren und Abfragen von AWS IoT SiteWise Metadatenattributen in einem Data Lake
- Generieren Sie Dateneinblicke mithilfe von AWS Mainframe Modernization und Amazon Q in QuickSight
- Generieren Sie Einblicke in Db2 z/OS-Daten mithilfe von Amazon AWS Mainframe Modernization Q in QuickSight
- Geben Sie SageMaker Notebook-Instances temporären Zugriff auf ein CodeCommit Repository in einem anderen AWS-Konto
- Identifizieren und benachrichtigen Sie, wenn Amazon Data Firehose-Ressourcen nicht mit einem AWS KMS Schlüssel verschlüsselt sind
- Importieren Sie die psycopg2-Bibliothek, AWS Lambda um mit Ihrer PostgreSQL-Datenbank zu interagieren
- Erfassung und Analyse von AWS-Sicherheitsprotokollen in Microsoft Sentinel
- Migrieren Sie Amazon RDS for Oracle zu Amazon RDS for PostgreSQL im SSL-Modus mithilfe von AWS DMS

- Migrieren Sie eine Oracle-Datenbank mithilfe von GoldenGate Oracle-Flatfile-Adaptern zu Amazon RDS for Oracle
- Migrieren Sie eine Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon Redshift
- Migrieren Sie Daten mithilfe DistCp von AWS PrivateLink für Amazon S3 von einer lokalen Hadoop-Umgebung zu Amazon S3
- Migrieren Sie von Couchbase Server zu Couchbase Capella auf AWS
- Migrieren Sie lokale Cloudera-Workloads zur Cloudera Data Platform auf AWS
- Überwachen Sie Amazon EMR-Cluster beim Start auf Verschlüsselung während der Übertragung
- Multi-AZ-Failover für EMR-Cluster mithilfe von Application Recovery Controller verwalten
- Automatisieren Sie blaue/grüne Bereitstellungen globaler Amazon Aurora Aurora-Datenbanken mithilfe von IaC-Prinzipien
- Bereitstellen von AWS Service Catalog Produkten auf der Grundlage von AWS CloudFormation Vorlagen mithilfe von GitHub Aktionen
- Führen Sie Komponententests für Python-ETL-Jobs AWS Glue mithilfe des Pytest-Frameworks aus
- Richten Sie ein Grafana-Monitoring-Dashboard für AWS ein ParallelCluster
- Daten aus einem Amazon Redshift Redshift-Cluster kontenübergreifend nach Amazon S3 entladen
- Stellen Sie sicher, dass für neue Amazon Redshift Redshift-Cluster SSL-Endpunkte erforderlich sind
- Stellen Sie sicher, dass neue Amazon Redshift Redshift-Cluster in einer VPC gestartet werden
- Visualisieren Sie KI/ML-Modellergebnisse mit Flask und AWS Elastic Beanstalk

Datenverarbeitung

Themen

- Container und Microservices
- Serverless
- Netzwerk
- Bereitstellung von Inhalten

Container und Microservices

Themen

- Greifen Sie von einem Amazon EKS-Container aus auf eine Amazon Neptune-Datenbank zu
- Greifen Sie mithilfe von AWS PrivateLink und einem Network Load Balancer privat auf Container-Anwendungen auf Amazon ECS zu
- Greifen Sie privat auf Container-Anwendungen auf Amazon ECS zu, indem Sie AWS Fargate PrivateLink, AWS und einen Network Load Balancer verwenden
- Greifen Sie mit AWS PrivateLink und einem Network Load Balancer privat auf Container-Anwendungen auf Amazon EKS zu
- Aktivieren Sie mTLS in AWS App Mesh mithilfe von AWS Private CA auf Amazon EKS
- Automatisieren Sie Backups für Amazon RDS for PostgreSQL PostgreSQL-DB-Instances mithilfe von AWS Batch
- Automatisieren Sie die Bereitstellung von Node Termination Handler in Amazon EKS mithilfe einer CI/CD-Pipeline
- Automatisches Erstellen und Bereitstellen einer Java-Anwendung auf Amazon EKS mithilfe einer CI/CD-Pipeline
- Erstellen Sie eine Amazon ECS-Aufgabendefinition und mounten Sie mithilfe von Amazon EFS ein Dateisystem auf EC2 Instances
- Stellen Sie Lambda-Funktionen mit Container-Images bereit
- Bereitstellen von Java-Microservices auf Amazon ECS mithilfe von AWS Fargate
- Stellen Sie Kubernetes-Ressourcen und -Pakete mithilfe von Amazon EKS und einem Helm-Chart-Repository in Amazon S3 bereit
- Stellen Sie einen Beispiel-Java-Microservice auf Amazon EKS bereit und machen Sie den Microservice mithilfe eines Application Load Balancer verfügbar
- Stellen Sie mithilfe von AWS Copilot eine geclusterte Anwendung in Amazon ECS bereit
- Stellen Sie eine GRPC-basierte Anwendung auf einem Amazon EKS-Cluster bereit und greifen Sie mit einem Application Load Balancer darauf zu
- Bereitstellen und Debuggen von Amazon EKS-Clustern
- Container mithilfe von Elastic Beanstalk bereitstellen
- Generieren Sie eine statische ausgehende IP-Adresse mithilfe einer Lambda-Funktion, Amazon VPC und einer serverlosen Architektur

- Automatische Identifizierung doppelter Container-Images bei der Migration zu einem Amazon ECR-Repository
- Installieren Sie SSM Agent mithilfe von Kubernetes auf Amazon EKS-Worker-Knoten DaemonSet
- Installieren Sie den SSM-Agent und den CloudWatch Agenten auf Amazon EKS-Worker-Knoten mit preBootstrapCommands
- Migrieren Sie NGINX Ingress Controller, wenn Sie den Amazon EKS Auto Mode aktivieren
- Migrieren Sie Ihre Container-Workloads von Azure Red Hat OpenShift (ARO) zu Red Hat OpenShift Service in AWS (ROSA)
- Optimieren Sie die von AWS App2Container generierten Docker-Images
- Platzieren Sie Kubernetes-Pods auf Amazon EKS mithilfe von Knotenaffinität, Taints und Toleranzen
- Replizieren Sie gefilterte Amazon ECR-Container-Images über Konten oder Regionen hinweg
- Datenbankanmeldedaten rotieren, ohne Container neu zu starten
- Führen Sie Amazon ECS-Aufgaben auf Amazon WorkSpaces mit Amazon ECS Anywhere aus
- Führen Sie einen ASP.NET Core-Web-API-Docker-Container auf einer Amazon EC2 Linux-Instance aus
- Mithilfe von AWS Fargate können Sie nachrichtengesteuerte Workloads in großem Umfang ausführen
- Führen Sie statusbehaftete Workloads mit persistentem Datenspeicher aus, indem Sie Amazon EFS auf Amazon EKS mit AWS Fargate verwenden
- Richten Sie ereignisgesteuertes Auto Scaling in Amazon EKS mithilfe von Amazon EKS Pod Identity und KEDA ein
- Optimieren Sie PostgreSQL-Bereitstellungen auf Amazon EKS mithilfe von PGO
- Vereinfachen Sie die Anwendungsauthentifizierung mit gegenseitigem TLS in Amazon ECS mithilfe von Application Load Balancer
- Mehr Muster

Greifen Sie von einem Amazon EKS-Container aus auf eine Amazon Neptune-Datenbank zu

Erstellt von Ramakrishnan Palaninathan (AWS)

Übersicht

Dieses Muster stellt eine Verbindung zwischen Amazon Neptune, einer vollständig verwalteten Graphdatenbank, und Amazon Elastic Kubernetes Service (Amazon EKS), einem Container-Orchestrierungsservice, her, um auf eine Neptune-Datenbank zuzugreifen. Neptune-DB-Cluster sind auf eine virtuelle private Cloud (VPC) beschränkt. AWS Aus diesem Grund erfordert der Zugriff auf Neptune eine sorgfältige Konfiguration der VPC, um Konnektivität zu ermöglichen.

Im Gegensatz zu Amazon Relational Database Service (Amazon RDS) für PostgreSQL ist Neptune nicht auf typische Datenbankzugriffsanmeldeinformationen angewiesen. Stattdessen verwendet es AWS Identity and Access Management (IAM) -Rollen für die Authentifizierung. Um von Amazon EKS aus eine Verbindung zu Neptune herzustellen, muss daher eine IAM-Rolle mit den erforderlichen Berechtigungen für den Zugriff auf Neptune eingerichtet werden.

Darüber hinaus sind Neptune-Endpoints nur innerhalb der VPC zugänglich, in der sich der Cluster befindet. Das bedeutet, dass Sie Netzwerkeinstellungen konfigurieren müssen, um die Kommunikation zwischen Amazon EKS und Neptune zu erleichtern. Abhängig von Ihren spezifischen Anforderungen und Netzwerkpräferenzen gibt es verschiedene Ansätze zur Konfiguration der VPC, um eine nahtlose Konnektivität zwischen Neptune und Amazon EKS zu ermöglichen. Jede Methode bietet unterschiedliche Vorteile und Überlegungen, sodass Sie Ihre Datenbankarchitektur flexibel an die Anforderungen Ihrer Anwendung anpassen können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Installieren Sie die neueste Version von kubectl (siehe Anweisungen). Um deine Version zu überprüfen, führe folgenden Befehl aus:

```
kubectl version --short
```

- Installieren Sie die neueste Version von eksctl (siehe Anweisungen). Um deine Version zu überprüfen, führe folgenden Befehl aus:

```
eksctl info
```

- Installieren Sie die neueste Version von AWS Command Line Interface (AWS CLI) Version 2 (siehe Anweisungen). Um Ihre Version zu überprüfen, führen Sie folgenden Befehl aus:

```
aws --version
```

- Erstellen Sie einen Neptune-DB-Cluster (siehe Anweisungen). Stellen Sie sicher, dass die Kommunikation zwischen der VPC des Clusters und Amazon EKS über VPC-Peering oder eine andere Methode hergestellt AWS Transit Gatewaywird. Stellen Sie außerdem sicher, dass der Status des Clusters „verfügbar“ lautet und dass es für die Sicherheitsgruppe eine Regel für eingehenden Datenverkehr auf Port 8182 gibt.
- Konfigurieren Sie einen IAM OpenID Connect (OIDC) -Anbieter auf einem vorhandenen Amazon EKS-Cluster (siehe Anweisungen).

Produktversionen

- Amazon EKS 1,27
- Version 1.3.0.0 der Amazon Neptune Neptune-Engine (15.11.2023)

Architektur

Das folgende Diagramm zeigt die Verbindung zwischen Kubernetes-Pods in einem Amazon EKS-Cluster und Neptune, um Zugriff auf eine Neptune-Datenbank zu ermöglichen.

Automatisierung und Skalierung

Sie können den Amazon EKS Horizontal Pod Autoscaler verwenden, um diese Lösung zu skalieren.

Tools

Services

- Mit Amazon Elastic Kubernetes Service (Amazon EKS) können Sie Kubernetes ausführen, AWS ohne dass Sie Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten müssen.

- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Amazon Neptune ist ein Graphdatenbank-Service, mit dem Sie Anwendungen erstellen und ausführen können, die mit stark verbundenen Datensätzen arbeiten.

Bewährte Methoden

Bewährte Methoden finden Sie unter Identity and Access Management in den Amazon EKS Best Practices Guides.

Epen

Festlegen von Umgebungsvariablen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Clusterkontext.	Bevor Sie mit Ihrem Amazon EKS-Cluster mithilfe von Helm oder anderen Befehlszeilentools interagieren, müssen Sie Umgebungsvariablen definieren, die die Details Ihres Clusters kapseln. Diese Variablen werden in nachfolgenden Befehlen verwendet, um sicherzustellen, dass sie auf den richtigen Cluster und die richtigen Ressourcen abzielen. Stellen Sie zunächst sicher, dass Sie im richtigen Clusterkontext arbeiten. Dadurch wird sichergestellt, dass alle nachfolgenden Befehle an den vorgesehenen Kubernetes-Cluster gesendet	AWS-Administrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	werden. Führen Sie den folgenden Befehl aus, um den aktuellen Kontext zu überprüfen. `kubectl config current-context`	
Definieren Sie die `CLUSTER_NAME` Variable.	Definieren Sie die `CLUSTER_NAME` Umgebungsvariable für Ihren Amazon EKS-Cluster. Ersetzen Sie im folgenden Befehl den Beispielwert `us-west-2` durch den AWS-Region für Ihren Cluster korrekten Wert. Ersetzen Sie den Beispielwert `eks-workshop` durch Ihren vorhandenen Clusternamen. `export CLUSTER_NAME=$(aws eks describe-cluster --region us-west-2 --name eks-workshop --query "cluster.name" --output text)`	AWS-Administrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ausgabe validieren.	Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die Variablen richtig gesetzt wurden. `echo $CLUSTER_NAME` Stellen Sie sicher, dass die Ausgabe dieses Befehls mit der Eingabe übereinstimmt, die Sie im vorherigen Schritt angegeben haben.	AWS-Administrator, Cloud-Administrator

Erstellen Sie eine IAM-Rolle und verknüpfen Sie sie mit Kubernetes

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ein -Service-Konto aktualisieren	Sie verwenden IAM-Rollen für Dienstkonten, um Ihre Kubernetes-Servicekonten IAM-Rollen zuzuordnen, um ein detailliertes Berechtigungsmanagement für Ihre Anwendungen zu ermöglichen, die auf Amazon EKS ausgeführt werden. Sie können eksctl verwenden, um eine IAM-Rolle zu erstellen und einem bestimmten Kubernetes-Servicekonto in Ihrem Amazon EKS-Cluster zuzuordnen. Die AWS verwaltete Richtlinie `NeptuneFu`	AWS-Administrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`llAccess` ermöglicht Schreib- und Lesezugriff auf Ihren angegebenen Neptune-Cluster. **Important** Bevor Sie diese Befehle ausführen können, muss Ihrem Cluster ein OIDC-Endpunkt zugeordnet sein. Erstellen Sie ein Dienstkonto, das Sie einer AWS verwalteten Richtlinie mit dem Namen zuordnen möchten. `NeptuneFullAccess` `eksctl create iamserviceaccount --name eks-neptune-sa --namespace default --cluster $CLUSTER_NAME --attach-policy-arn arn:aws:iam::aws:policy/NeptuneFullAccess --approve --override-existing-serviceaccounts` wo `eks-neptune-sa` ist der Name des Dienstkontos, das Sie erstellen möchten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Nach Abschluss zeigt dieser Befehl die folgende Antwort an: `2024-02-07 01:12:39 [#] created serviceaccount "default/eks-neptune-sa"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie sicher, dass das Konto ordnungsgemäß eingerichtet ist.	Stellen Sie sicher, dass das `eks-neptune-sa` Dienstkonto im Standard-Namespace in Ihrem Cluster korrekt eingerichtet ist.
	`kubectl get sa eks-neptune-sa -o yaml`
	Die Ausgabe sollte in etwa wie folgt aussehen:
	`apiVersion: v1`
	`kind: ServiceAccount`
	`metadata:`
	`  annotations:`
	`  eks.amazonaws.com/role-arn: arn:aws:iam::123456789123:role/eksctl-eks-workshop-addon-iamserviceaccount-d-Role1-Q35yKgdQOlmM`
	`  creationTimestamp: "2024-02-07T01:12:39Z"`
	`  labels:`
	`  app.kubernetes.io/managed-by: eksctl`
	`  name: eks-neptune-sa`
	`  namespace: default`
	`  resourceVersion: "5174750"`
	`  uid: cd6ba2f7-a0f5-40e1-a6f4-4081e0042316`
		AWS-Administrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Konnektivität.	Stellen Sie einen Beispiel-Pod bereit, der aufgerufen wurde, `pod-util` und überprüfen Sie die Konnektivität mit Neptune.
	
	`apiVersion: v1`
	`kind: Pod`
	`metadata:`
	`  name: pod-util`
	`  namespace: default`
	`spec:`
	`  serviceAccountName: eks-neptune-sa`
	`  containers:`
	`  - name: pod-util`
	`  image: public.ecr.aws/patrickc/troubleshoot-util`
	`  command:`
	`  - sleep`
	`  - "3600"`
	`  imagePullPolicy: IfNotPresent`
	
	`kubectl apply -f pod-util.yaml`
	
	`kubectl exec --stdin --tty pod-util -- /bin/bash`
	`bash-5.1# curl -X POST -d '{"gremlin":"g.V().limit(1)"}' https://db-neptune-1.cluster-xxxxxxxxxxxx.us-west-2.neptune.amazonaws.com:8182/gremlin`
		AWS-Administrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`{"requestId":"a4964f2d-12b1-4ed3-8a14-eff511431a0e","status":{"message":"","code":200,"attributes":{"@type":"g:Map","@value":[]},"result":{"data":{"@type":"g:List","@value":[]},"meta":{"@type":"g:Map","@value":[]}}}`
	`bash-5.1# exit`
	`exit`	

Überprüfen Sie die Verbindungsaktivität

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie die IAM-Datenbankauthentifizierung.	Standardmäßig ist die IAM-Datenbankauthentifizierung deaktiviert, wenn Sie einen Neptune-DB-Cluster erstellen. Sie können die IAM-Datenbankauthentifizierung aktivieren oder deaktivieren, indem Sie den verwenden. AWS Management Console Folgen Sie den Schritten in der AWS Dokumentation, um die IAM-Datenbankauthentifizierung in Neptune zu aktivieren.	AWS-Administrator, Cloud-Administrator
Überprüfen Sie die Verbindungen.	In diesem Schritt interagieren Sie mit dem `pod-util`	AWS-Administrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Container, der sich bereits im Ausführungsstatus befindet, um awscurl zu installieren und die Verbindung zu überprüfen.
	
	1. Führen Sie den folgenden Befehl aus, um den Pod zu finden.
	
	`kubectl get pods`
	
	Die Ausgabe sollte in etwa wie folgt aussehen:
	
	`NAME READY STATUS RESTARTS AGE pod-util 1/1 Running 0 50m`
	
	2. Führen Sie den folgenden Befehl aus, um awscurl zu installieren.
	
	`kubectl exec --stdin --tty pod-util -- /bin/bash bash-5.1# pip3 install awscurl Installing collected packages: idna, configparser, configargparse, charset-normalizer, certifi, requests, awscurl Successfully installed awscurl-0.32 certifi-2024.2.2 charset-normalizer-3.3.2 configargparse-1.7 configpar`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ser-6.0.0 idna-3.6 requests-2.31.0 bash-5.1# awscurl https://db-neptune -1.cluster-xxxxxxx xxxxx.us-west-2.ne ptune.amazonaws.co m:8182/status -- region us-west-2 -- service neptune-db {"status":"healthy ","startTime":"Thu Feb 08 01:22:14 UTC 2024","dbEngineVer sion":"1.3.0.0.R1" ,"role":"writer"," dfeQueryEngine":"v iaQueryHint","grem lin":{"version":"t inkerpop-3.6.4"}," sparql":{"version" :"sparql-1.1"},"op encypher":{"versio n":"Neptune-9.0.20 190305-1.0"},"labM ode":{"ObjectIndex ":"disabled","Read WriteConflictDetec tion":"enabled"}," features":{"SlowQu eryLogs":"disabled ","ResultCache":{" status":"disabled" },"IAMAuthenticati on":"enabled","Str eams":"disabled"," AuditLog":"disable d"},"settings":{"c lusterQueryTimeout InMs":"120000","Sl	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`owQueryLogsThresho ld":"5000"}}`	

Fehlerbehebung

Problem	Lösung
Ich kann nicht auf die Neptun-Datenbank zugreifen.	Überprüfen Sie die IAM-Richtlinie, die mit dem Dienstkonto verknüpft ist. Stellen Sie sicher, dass sie die erforderlichen Aktionen (z. B.`neptune:Connec,neptune:Desc ribeDBInstances`) für die Operationen, die Sie ausführen möchten, zulässt.

Zugehörige Ressourcen

- Kubernetes-Workloads Zugriff auf die AWS Nutzung von Kubernetes-Servicekonten gewähren (Amazon EKS-Dokumentation)
- IAM-Rollen für Dienstkonten (Amazon EKS-Dokumentation)
- Einen neuen Neptune-DB-Cluster erstellen (Amazon Neptune Neptune-Dokumentation)

Greifen Sie mithilfe von AWS PrivateLink und einem Network Load Balancer privat auf Container-Anwendungen auf Amazon ECS zu

Erstellt von Kirankumar Chandrashekar (AWS)

Übersicht

Dieses Muster beschreibt, wie Sie eine Docker-Container-Anwendung privat auf Amazon Elastic Container Service (Amazon ECS) hinter einem Network Load Balancer hosten und mithilfe von AWS auf die Anwendung zugreifen. PrivateLink Sie können dann ein privates Netzwerk verwenden, um sicher auf Dienste in der Amazon Web Services (AWS) Cloud zuzugreifen. Amazon Relational Database Service (Amazon RDS) hostet die relationale Datenbank für die Anwendung, die auf Amazon ECS mit hoher Verfügbarkeit (HA) ausgeführt wird. Amazon Elastic File System (Amazon EFS) wird verwendet, wenn die Anwendung persistenten Speicher benötigt.

Der Amazon ECS-Service, auf dem die Docker-Anwendungen ausgeführt werden, mit einem Network Load Balancer am Frontend kann mit einem Virtual Private Cloud (VPC) -Endpunkt für den Zugriff über AWS verknüpft werden. PrivateLink Dieser VPC-Endpunktdienst kann dann mit anderen gemeinsam genutzt werden, VPCs indem deren VPC-Endpunkte verwendet werden.

Sie können auch AWS Fargate anstelle einer Amazon EC2 Auto Scaling Scaling-Gruppe verwenden. Weitere Informationen finden Sie unter Privaten Zugriff auf Containeranwendungen auf Amazon ECS mithilfe von AWS Fargate PrivateLink, AWS und einem Network Load Balancer.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 2, installiert und konfiguriert unter Linux, macOS oder Windows
- Docker, installiert und konfiguriert unter Linux, MacOS oder Windows
- Eine Anwendung, die auf Docker läuft

Architektur

Technologie-Stack

- Amazon CloudWatch
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon EC2 Auto Scaling
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon ECS
- Amazon RDS
- Amazon Simple Storage Service (Amazon-S3)
- AWS Lambda
- AWS PrivateLink
- AWS Secrets Manager
- Application Load Balancer
- Network Load Balancer
- VPC

Automatisierung und Skalierung

- Sie können AWS verwenden CloudFormation, um dieses Muster mithilfe von Infrastructure as Code zu erstellen.

Tools

- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud.
- Amazon EC2 Auto Scaling — Amazon EC2 Auto Scaling hilft Ihnen sicherzustellen, dass Ihnen die richtige Anzahl von EC2 Amazon-Instances zur Verfügung steht, um die Last für Ihre Anwendung zu bewältigen.
- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der es einfach macht, Container in einem Cluster auszuführen, zu stoppen und zu verwalten.
- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter AWS-Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.

- Amazon EFS — Amazon Elastic File System (Amazon EFS) bietet ein einfaches, skalierbares, vollständig verwaltetes elastisches NFS-Dateisystem zur Verwendung mit AWS-Cloud-Services und lokalen Ressourcen.
- AWS Lambda — Lambda ist ein Rechenservice zum Ausführen von Code ohne Bereitstellung oder Verwaltung von Servern.
- Amazon RDS — Amazon Relational Database Service (Amazon RDS) ist ein Webservice, der die Einrichtung, den Betrieb und die Skalierung einer relationalen Datenbank in der AWS-Cloud erleichtert.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Speicher für das Internet. Der Service ist darauf ausgelegt, Cloud Computing für Entwickler zu erleichtern.
- AWS Secrets Manager — Secrets Manager hilft Ihnen dabei, hartcodierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, zu ersetzen, indem es einen API-Aufruf an Secrets Manager bereitstellt, um das Geheimnis programmgesteuert abzurufen.
- Amazon VPC — Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten.
- Elastic Load Balancing — Elastic Load Balancing verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele, wie EC2 Amazon-Instances, Container und IP-Adressen, in mehreren Availability Zones.
- Docker — Docker hilft Entwicklern dabei, jede Anwendung als leichten, portablen und autarken Container zu packen, zu versenden und auszuführen.

Epen

Netzwerkkomponenten erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon VPC-Konsole. Wählen Sie Create VPC und dann VPC and more aus.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Geben Sie einen Namen für Ihre VPC ein und wählen Sie einen geeigneten CIDR-Blockbereich aus. 3. Geben Sie zwei Availabil ity Zones, zwei öffentlic he Subnetze und vier private Subnetze an. Zwei private Subnetze sind für Amazon ECS-Aufgaben und zwei private Subnetze für Amazon RDS-Daten banken vorgesehen. 4. Geben Sie ein NAT-Gatew ay für jede Availability Zone an. 5. Wählen Sie VPC erstellen aus.	

Erstellen Sie die Load Balancer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Network Load Balancer.	1. Öffnen Sie die EC2 Amazon-Konsole und wählen Sie die AWS-Regio n aus, die Ihre VPC enthält. 2. Wählen Sie unter Load Balancing die Option Load Balancers und dann Create Load Balancer aus.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie Network Load Balancer und dann Create aus. 4. Konfigurieren Sie auf der Seite Load Balancer konfigurieren Ihren Network Load Balancer und Listener. Wichtig: Stellen Sie sicher, dass Sie das Schema Ihres Network Load Balancers als Intern auswählen. 5. Wählen Sie die entsprechenden Sicherheitseinstellungen aus, konfigurieren Sie eine Sicherheitsgruppe und eine Zielgruppe. Wählen Sie im Abschnitt Routing konfigurieren Instance oder IP als Zieltyp aus. Stellen Sie sicher, dass Sie kein Ziel registrieren. 6. Wenn Sie alle Einstellungen konfiguriert haben, wählen Sie Weiter: Überprüfen und dann Erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Application Load Balancer.	1. Wählen Sie auf der EC2 Amazon-Konsole dieselbe Region aus, in der sich Ihre VPC befindet. 2. Wählen Sie unter Load Balancing die Option Load Balancers und dann Create Load Balancer aus. 3. Wählen Sie Application Load Balancer und dann Create aus. 4. **Important** Konfigurieren Sie Ihren Application Load Balancer und seinen Listener. Stellen Sie sicher, dass Sie das Schema Ihres Application Load Balancers als Intern wählen. 5. Wählen Sie die entsprechenden Sicherheitseinstellungen aus, konfigurieren Sie eine Sicherheitsgruppe und eine Zielgruppe. Wählen Sie im Abschnitt Routing konfigurieren Instance oder IP als Zieltyp aus. Stellen Sie sicher,	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dass Sie kein Ziel registrie ren. 6. Wenn Sie alle Einstellungen konfiguriert haben, wählen Sie Weiter: Überprüfen und dann Erstellen.	

Erstellen eines Amazon EFS-Dateisystems

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon EFS-Dateisystem.	1. Öffnen Sie die Amazon EFS-Konsole und wählen Sie Create file system aus. 2. Geben Sie im Dialogfeld Dateisystem erstellen einen Namen für Ihr Dateisyst em ein und wählen Sie Ihre VPC aus. 3. Wählen Sie Erstellen, um das Dateisystem zu erstellen. 4. Richten Sie Ihr Amazon EFS-Dateisystem ein und konfigurieren Sie es.	Cloud-Administrator
Mounten Sie Ziele für die Subnetze.	1. Kehren Sie zur Amazon EFS-Konsole zurück und wählen Sie Dateisysteme. Auf der Seite Dateisyst eme werden die Amazon EFS-Dateisysteme in Ihrem Konto angezeigt.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie das Dateisystem aus, das Sie erstellt haben, und wählen Sie Verwalten, um die Availability Zones anzuzeigen. Um ein Mount-Ziel hinzuzufügen, wählen Sie Mount-Ziel hinzufügen und fügen Sie die vier privaten Subnetze hinzu, die Sie erstellt haben.	
Stellen Sie sicher, dass die Subnetze als Ziele bereitgestellt sind.	1. Wählen Sie in der Amazon EFS-Konsole Dateisysteme aus. 2. Wählen Sie Netzwerk aus, um die Liste der vorhandenen Mount-Ziele anzuzeigen. Stellen Sie sicher, dass diese die vier Subnetze enthalten, die Sie erstellt haben.	Cloud-Administrator

Erstellen eines S3-Buckets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Öffnen Sie die Amazon S3 S3-Konsole und erstellen Sie bei Bedarf einen S3-Bucket, um die statischen Ressourcen Ihrer Anwendung zu speichern.	Cloud-Administrator

Ein Secrets Manager Manager-Geheimnis erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen AWS-KMS-Schlüssel, um das Secrets Manager Manager-Geheimnis zu verschlüsseln.	Öffnen Sie die AWS Key Management Service (AWS KMS) -Konsole und erstellen Sie einen KMS-Schlüssel.	Cloud-Administrator
Erstellen Sie ein Secrets Manager Manager-Geheimnis, um das Amazon RDS-Passwort zu speichern.	1. Öffnen Sie die AWS Secrets Manager Manager-Konsole und erstellen Sie ein neues Geheimnis, indem Sie Neues Geheimnis speichern wählen. 2. Wählen Sie den KMS-Schlüssel aus, den Sie erstellt haben, und speichern Sie Ihr neues Geheimnis.	Cloud-Administrator

Eine Amazon RDS-Instance erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine DB-Subnetzgruppe.	1. Öffnen Sie die Amazon RDS-Konsole und wählen Sie Subnetzgruppen aus. 2. Wählen Sie Create DB Subnet Group und geben Sie einen Namen und eine Beschreibung für Ihre DB-Subnetzgruppe ein. 3. Wählen Sie die VPC aus, die Sie zuvor erstellt haben, und wählen Sie die Availabil	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ity Zones und Subnetze aus. Wählen Sie die Option Erstellen aus.	
Erstellen Sie eine Amazon RDS-Instance.	Erstellen und konfigurieren Sie eine Amazon RDS-Instance in den privaten Subnetzen. Stellen Sie sicher, dass Multi-AZ für HA aktiviert ist.	Cloud-Administrator
Laden Sie Daten in die Amazon RDS-Instance.	Laden Sie die für Ihre Anwendung erforderlichen relationalen Daten in Ihre Amazon RDS-Instance. Dieser Prozess hängt von den Anforderungen Ihrer Anwendung sowie davon ab, wie Ihr Datenbankschema definiert und entworfen ist.	Cloud-Administrator, DBA

Erstellen Sie die Amazon ECS-Komponenten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen ECS-Cluster.	1. Öffnen Sie die Amazon ECS-Konsole und wählen Sie Clusters. 2. Wählen Sie Cluster erstellen und richten Sie einen ECS-Cluster gemäß Ihren erforderlichen Spezifikationen ein.	Cloud-Administrator
Erstellen Sie die Docker-Images.	Erstellen Sie die Docker-Images, indem Sie den	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anweisungen im Abschnitt Verwandte Ressourcen folgen.	
Erstellen Sie Amazon ECR-Repositorys.	1. Wählen Sie auf der Amazon ECR-Konsole Repositories aus. 2. Wählen Sie Create Repository und geben Sie einen eindeutigen Namen für Ihr Repository ein. 3. Konfigurieren Sie das Repository gemäß Ihren Spezifikationen, einschließlich AWS-KMS-Verschlüsselung, falls erforderlich.	Cloud-Administrator, DevOps Ingenieur
Authentifizieren Sie Ihren Docker-Client für das Amazon ECR-Repository.	Um Ihren Docker-Client für das Amazon ECR-Repository zu authentifizieren, führen Sie den `aws ecr get-login-password` Befehl „in der AWS-CLI aus.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Übertragen Sie die Docker-Images in das Amazon ECR-Repository.	1. Identifizieren Sie das Docker-Image, das Sie pushen möchten, und führen Sie den `docker images` Befehl in der AWS-CLI aus. 2. Kennzeichnen Sie Ihr Bild mit der Amazon ECR-Registrierung, dem Repository und der optionalen Kombination aus Image-Tagnamen. 3. Übertragen Sie das Docker-Image, indem Sie den `docker push` Befehl ausführen. 4. Wiederholen Sie diese Schritte für alle erforderlichen Bilder.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon ECS-Aufgabendefinition.	Eine Aufgabendefinition ist erforderlich, um Docker-Container in Amazon ECS auszuführen. 1. Kehren Sie zur Amazon ECS-Konsole zurück, wählen Sie Aufgabend efinitionen und dann Neue Aufgabendefinition erstellen . 2. Wählen Sie auf der Seite „Kompatibilitäten auswählen “ den Starttyp aus, den Ihre Aufgabe verwenden soll, und klicken Sie auf Nächster Schritt. **Important** Hilfe beim Einrichte n Ihrer Aufgabend efinition finden Sie unter „Eine Aufgabend efinition erstellen“ im Abschnitt Verwandte Ressourcen. Stellen Sie sicher, dass Sie die Docker-Images bereitstellen, die Sie an Amazon ECR übertragen haben.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon-ECS-Service.	Erstellen Sie einen Amazon ECS-Service mithilfe des ECS-Clusters, den Sie zuvor erstellt haben. Stellen Sie sicher, dass Sie Amazon EC2 als Starttyp und die im vorherigen Schritt erstellte Aufgabendefinition sowie die Zielgruppe des Application Load Balancer auswählen.	Cloud-Administrator

Eine Amazon EC2 Auto Scaling Scaling-Gruppe erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Startkonf iguration	Öffnen Sie die EC2 Amazon-Konsole und erstellen Sie eine Startkonfiguration. Stellen Sie sicher, dass die Benutzerd aten den Code enthalten, der es den EC2 Instances ermöglicht, dem gewünschten ECS-Cluster beizutreten. Ein Beispiel für den erforderlichen Code finden Sie im Abschnitt Verwandte Ressourcen.	Cloud-Administrator
Erstellen Sie eine Amazon EC2 Auto Scaling Scaling-G ruppe.	Kehren Sie zur EC2 Amazon-Konsole zurück und wählen Sie unter Auto Scaling die Option Auto Scaling Scaling-G ruppen aus. Richten Sie eine Amazon EC2 Auto Scaling Scaling-Gruppe ein. Stellen	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie sicher, dass Sie die privaten Subnetze auswählen und die Konfiguration starten, die Sie zuvor erstellt haben.	

AWS einrichten PrivateLink

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie den PrivateLink AWS-Endpunkt ein.	1. Erstellen Sie auf der Amazon VPC-Konsole einen PrivateLink AWS-Endpunkt. 2. Ordnen Sie diesen Endpunkt dem Network Load Balancer zu, der die auf Amazon ECS gehostete Anwendung privat für Kunden verfügbar macht. Weitere Informationen finden Sie im Abschnitt Verwandte Ressourcen.	Cloud-Administrator

Erstellen eines VPC-Endpunkts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen VPC-Endpunkt.	Erstellen Sie einen VPC-Endpunkt für den PrivateLink AWS-Endpunkt, den Sie zuvor erstellt haben. Der vollquali fizierte Domainname (FQDN)	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	des VPC-Endpunkts zeigt auf den PrivateLink AWS-Endpunkt-FQDN. Dadurch wird eine elastic network interface zum VPC-Endpunktdienst erstellt, auf die die DNS-Endpunkte zugreifen können.	

So erstellen Sie die Lambda-Funktion:

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
So erstellen Sie die Lambda-Funktion:	Erstellen Sie auf der AWS Lambda Lambda-Konsole eine Lambda-Funktion, um die IP-Adressen des Application Load Balancer als Ziele für den Network Load Balancer zu aktualisieren. Weitere Informationen dazu finden Sie im Blogbeitrag Verwenden von AWS Lambda zur Aktivierung statischer IP-Adressen für Application Load Balancers.	App-Developer

Zugehörige Ressourcen

Erstellen Sie die Load Balancer:

- Verwenden Sie einen Network Load Balancer für Amazon ECS
- Einen Network Load Balancer erstellen
- Verwenden Sie einen Application Load Balancer für Amazon ECS
- Erstellen Sie einen Application Load Balancer

Erstellen Sie ein Amazon EFS-Dateisystem:

- Erstellen Sie ein Amazon EFS-Dateisystem
- Bereitstellungsziele in Amazon EFS erstellen

Erstellen Sie einen S3-Bucket:

- Erstellen Sie einen S3-Bucket

Erstellen Sie ein Secrets Manager Manager-Geheimnis:

- Schlüssel in AWS KMS erstellen
- Erstellen Sie ein Geheimnis in AWS Secrets Manager

Erstellen Sie eine Amazon RDS-Instance:

- Eine Amazon RDS-DB-Instance erstellen

Erstellen Sie die Amazon ECS-Komponenten:

- Erstellen Sie einen Amazon ECS-Cluster
- Erstellen Sie ein Docker-Image
- Erstellen Sie ein Amazon ECR-Repository
- Authentifizieren Sie Docker mit dem Amazon ECR-Repository
- Ein Bild in ein Amazon ECR-Repository übertragen
- Amazon ECS-Aufgabendefinition erstellen
- Einen Amazon ECS-Service erstellen

Erstellen Sie eine Amazon EC2 Auto Scaling Scaling-Gruppe:

- Erstellen Sie eine Startkonfiguration
- Erstellen einer Auto-Scaling-Gruppe mithilfe einer Startkonfiguration
- Bootstrap-Container-Instances mit EC2 Amazon-Benutzerdaten

AWS einrichten PrivateLink:

- VPC-Endpunktdienste (AWS PrivateLink)

Erstellen Sie einen VPC-Endpunkt:

- Schnittstelle VPC-Endpunkte (AWS) PrivateLink

Erstellen Sie die Lambda-Funktion:

- Erstellen Sie eine Lambda-Funktion

Andere Ressourcen:

- Verwendung statischer IP-Adressen für Application Load Balancer
- Sicherer Zugriff auf Services über AWS PrivateLink

Greifen Sie privat auf Container-Anwendungen auf Amazon ECS zu, indem Sie AWS Fargate PrivateLink, AWS und einen Network Load Balancer verwenden

Erstellt von Kirankumar Chandrashekar (AWS)

Übersicht

Dieses Muster beschreibt, wie Sie eine Docker-Container-Anwendung privat in der Amazon Web Services (AWS) -Cloud hosten, indem Sie Amazon Elastic Container Service (Amazon ECS) mit einem AWS Fargate-Starttyp hinter einem Network Load Balancer verwenden und mithilfe von AWS auf die Anwendung zugreifen. PrivateLink Amazon Relational Database Service (Amazon RDS) hostet die relationale Datenbank für die Anwendung, die auf Amazon ECS mit hoher Verfügbarkeit (HA) ausgeführt wird. Sie können Amazon Elastic File System (Amazon EFS) verwenden, wenn die Anwendung persistenten Speicher benötigt.

Dieses Muster verwendet einen Fargate-Starttyp für den Amazon ECS-Service, auf dem die Docker-Anwendungen ausgeführt werden, mit einem Network Load Balancer am Frontend. Es kann dann mit einem Virtual Private Cloud (VPC) -Endpunkt für den Zugriff über AWS PrivateLink verknüpft werden. Dieser VPC-Endpunktdienst kann dann VPCs mithilfe ihrer VPC-Endpunkte mit anderen geteilt werden.

Sie können Fargate mit Amazon ECS verwenden, um Container auszuführen, ohne Server oder Cluster von Amazon Elastic Compute Cloud (Amazon EC2) -Instances verwalten zu müssen. Sie können anstelle von Fargate auch eine Amazon EC2 Auto Scaling Scaling-Gruppe verwenden. Weitere Informationen finden Sie unter Privaten Zugriff auf Containeranwendungen auf Amazon ECS mithilfe von AWS PrivateLink und einem Network Load Balancer.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 2, installiert und konfiguriert unter Linux, macOS oder Windows
- Docker, installiert und konfiguriert unter Linux, MacOS oder Windows
- Eine Anwendung, die auf Docker läuft

Architektur

Technologie-Stack

- Amazon CloudWatch
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon ECS
- Amazon EFS
- Amazon RDS
- Amazon Simple Storage Service (Amazon-S3)
- AWS Fargate
- AWS PrivateLink
- AWS Secrets Manager
- Application Load Balancer
- Network Load Balancer
- VPC

Automatisierung und Skalierung

- Sie können AWS verwenden CloudFormation, um dieses Muster mithilfe von Infrastructure as Code zu erstellen.

Tools

AWS-Services

- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter AWS-Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Stoppen und Verwalten von Containern in einem Cluster vereinfacht.
- Amazon Elastic File System (Amazon EFS) bietet ein einfaches, skalierbares, vollständig verwaltetes elastisches NFS-Dateisystem zur Verwendung mit AWS-Cloud-Services und lokalen Ressourcen.

- AWS Fargateist eine Technologie, die Sie mit Amazon ECS verwenden können, um Container auszuführen, ohne Server oder Cluster von EC2 Amazon-Instances verwalten zu müssen.
- Amazon Relational Database Service (Amazon RDS) ist ein Webservice, der die Einrichtung, den Betrieb und die Skalierung einer relationalen Datenbank in der erleichtert. AWS Cloud
- Amazon Simple Storage Service (Amazon S3) ist Speicher für das Internet. Der Service ist darauf ausgelegt, Cloud Computing für Entwickler zu erleichtern.
- Mit AWS Secrets Manager können Sie fest codierte Anmeldeinformationen im Code (einschließlich Passwörter) durch einen API-Aufruf an Secrets Manager ersetzen und das Geheimnis programmgesteuert abrufen.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele wie EC2 Instances, Container und IP-Adressen in mehreren Availability Zones.

Andere Tools

- Docker hilft Entwicklern dabei, jede Anwendung einfach als leichten, tragbaren und autarken Container zu packen, zu versenden und auszuführen.

Epen

Netzwerkkomponenten erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon VPC-Konsole. Wählen Sie Create VPC und dann VPC and more aus. 2. Geben Sie einen Namen für Ihre VPC ein und wählen	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie einen geeigneten CIDR-Blockbereich aus. 3. Geben Sie zwei Availability Zones, zwei öffentliche Subnetze und vier private Subnetze an. Zwei private Subnetze sind für Amazon ECS-Aufgaben und zwei private Subnetze für Amazon RDS-Datenbanken vorgesehen. 4. Geben Sie ein NAT-Gateway für jede Availability Zone an. 5. Wählen Sie VPC erstellen aus.	

Erstellen Sie die Load Balancer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Network Load Balancer.	1. Öffnen Sie die EC2 Amazon-Konsole und wählen Sie die AWS-Region aus, die Ihre VPC enthält. 2. Wählen Sie unter Load Balancing die Option Load Balancers und dann Create Load Balancer aus. 3. Wählen Sie Network Load Balancer und dann Create. 4. Konfigurieren Sie auf der Seite Load Balancer	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	konfigurieren Ihren Network Load Balancer und Listener. Wichtig: Stellen Sie sicher, dass Sie das Schema Ihres Network Load Balancers als Intern auswählen. 5. Wählen Sie die entsprechenden Sicherheitseinstellungen aus, konfigurieren Sie eine Sicherheitsgruppe und eine Zielgruppe. Wählen Sie im Abschnitt Routing konfigurieren IP als Zieltyp aus. Stellen Sie sicher, dass Sie kein Ziel registrieren. 6. Wenn Sie alle Einstellungen konfiguriert haben, wählen Sie Weiter: Überprüfen und dann Erstellen. Hilfe zu dieser und anderen Geschichten finden Sie im Abschnitt Verwandte Ressourcen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Application Load Balancer.	1. Wählen Sie auf der EC2 Amazon-Konsole dieselbe Region aus, in der sich Ihre VPC befindet. 2. Wählen Sie unter Load Balancing die Option Load Balancers und dann Create Load Balancer aus. 3. Wählen Sie Application Load Balancer und dann Create. 4. **Important** Konfigurieren Sie Ihren Application Load Balancer und seinen Listener. Stellen Sie sicher, dass Sie das Schema Ihres Application Load Balancers als Intern wählen. 5. Wählen Sie die entsprechenden Sicherheitseinstellungen aus, konfigurieren Sie eine Sicherheitsgruppe und eine Zielgruppe. Wählen Sie im Abschnitt Routing konfigurieren IP als Zieltyp aus. Stellen Sie sicher, dass Sie kein Ziel registrieren.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Wenn Sie alle Einstellungen konfiguriert haben, wählen Sie Weiter: Überprüfen und dann Erstellen.	

Erstellen eines Amazon EFS-Dateisystems

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon EFS-Dateisystem.	1. Öffnen Sie die Amazon EFS-Konsole und wählen Sie Create file system aus. 2. Geben Sie im Dialogfeld Dateisystem erstellen einen Namen für Ihr Dateisyst em ein und wählen Sie Ihre VPC aus. 3. Wählen Sie Erstellen, um das Dateisystem zu erstellen. 4. Richten Sie Ihr Amazon EFS-Dateisystem ein und konfigurieren Sie es.	Cloud-Administrator
Mounten Sie Ziele für die Subnetze.	1. Kehren Sie zur Amazon EFS-Konsole zurück und wählen Sie Dateisysteme. Auf der Seite Dateisyst eme werden die Amazon EFS-Dateisysteme in Ihrem Konto angezeigt. 2. Wählen Sie das Dateisyst em aus, das Sie erstellt haben, und wählen Sie	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Verwalten, um die Availabil ity Zone anzuzeigen. 3. Um ein Mount-Ziel hinzuzufügen, wählen Sie Mount-Ziel hinzufügen und fügen Sie die vier privaten Subnetze hinzu, die Sie erstellt haben.	
Stellen Sie sicher, dass die Subnetze als Ziele bereitges tellt sind.	1. Wählen Sie in der Amazon EFS-Konsole Dateisysteme aus. 2. Wählen Sie Netzwerk aus, um die Liste der vorhanden en Mount-Ziele anzuzeige n. Stellen Sie sicher, dass diese die vier Subnetze enthalten, die Sie erstellt haben.	Cloud-Administrator

Erstellen eines S3-Buckets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Öffnen Sie die Amazon S3 S3-Konsole und erstellen Sie bei Bedarf einen S3-Bucket, um die statischen Ressourcen Ihrer Anwendung zu speichern .	Cloud-Administrator

Ein Secrets Manager Manager-Geheimnis erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen AWS-KMS-Schlüssel, um das Secrets Manager Manager-Geheimnis zu verschlüsseln.	Öffnen Sie die AWS Key Management Service (AWS KMS) -Konsole und erstellen Sie einen KMS-Schlüssel.	Cloud-Administrator
Erstellen Sie ein Secrets Manager Manager-Geheimnis, um das Amazon RDS-Passwort zu speichern.	1. Öffnen Sie die AWS Secrets Manager Manager-Konsole und erstellen Sie ein neues Geheimnis, indem Sie Neues Geheimnis speichern wählen. 2. Wählen Sie den KMS-Schlüssel aus, den Sie erstellt haben, und speichern Sie Ihr neues Geheimnis.	Cloud-Administrator

Eine Amazon RDS-Instance erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine DB-Subnetzgruppe.	1. Öffnen Sie die Amazon RDS-Konsole und wählen Sie Subnetzgruppen aus. 2. Wählen Sie Create DB Subnet Group und geben Sie einen Namen und eine Beschreibung für Ihre DB-Subnetzgruppe ein. 3. Wählen Sie die VPC aus, die Sie zuvor erstellt haben, und wählen Sie die Availabil	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ity Zones und Subnetze aus. Wählen Sie die Option Erstellen aus.	
Erstellen Sie eine Amazon RDS-Instance.	Erstellen und konfigurieren Sie eine Amazon RDS-Instance in den privaten Subnetzen. Stellen Sie sicher, dass Multi-AZ für Hochverfügbarkeit (HA) aktiviert ist.	Cloud-Administrator
Laden Sie Daten in die Amazon RDS-Instance.	Laden Sie die für Ihre Anwendung erforderlichen relationalen Daten in Ihre Amazon RDS-Instance. Dieser Prozess hängt von den Anforderungen Ihrer Anwendung sowie davon ab, wie Ihr Datenbankschema definiert und entworfen ist.	DBA

Erstellen Sie die Amazon ECS-Komponenten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen ECS-Cluster.	1. Öffnen Sie die Amazon ECS-Konsole und wählen Sie Clusters. 2. Wählen Sie Cluster erstellen und richten Sie einen ECS-Cluster gemäß Ihren erforderlichen Spezifikationen ein.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Docker-Images.	Erstellen Sie die Docker-Images, indem Sie den Anweisungen in der AWS Dokumentation folgen.	Cloud-Administrator
Erstellen Sie ein Amazon-ECR-Repository.	1. Öffnen Sie die Amazon ECR-Konsole und wählen Sie Repositories. 2. Wählen Sie Create Repository und geben Sie einen eindeutigen Namen für Ihr Repository ein. 3. Konfigurieren Sie das Repository gemäß Ihren Spezifikationen, einschließlich AWS-KMS-Verschlüsselung, falls erforderlich.	Cloud-Administrator, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Übertragen Sie die Docker-Images in das Amazon ECR-Repository.	1. Identifizieren Sie das Docker-Image, das Sie pushen möchten, und führen Sie den `docker images` Befehl in der AWS-CLI aus. 2. Kennzeichnen Sie Ihr Bild mit der Amazon ECR-Registrierung, dem Repository und der optionalen Kombination aus Image-Tagnamen. 3. Übertragen Sie das Docker-Image, indem Sie den `docker push` Befehl ausführen. 4. Wiederholen Sie diese Schritte für alle erforderlichen Bilder.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon ECS-Aufgabendefinition.	Eine Aufgabendefinition ist erforderlich, um Docker-Container in Amazon ECS auszuführen. 1. Kehren Sie zur Amazon ECS-Konsole zurück, wählen Sie Aufgabend efinitionen und dann Neue Aufgabendefinition erstellen . 2. Wählen Sie auf der Seite „Kompatibilitäten auswählen “ den Starttyp aus, den Ihre Aufgabe verwenden soll, und klicken Sie auf Nächster Schritt. **Important** Hilfe beim Einrichte n Ihrer Aufgabend efinition finden Sie unter „Eine Aufgabend efinition erstellen“ im Abschnitt Verwandte Ressourcen. Stellen Sie sicher, dass Sie die Docker-Images bereitstellen, die Sie an Amazon ECR übertragen haben.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen ECS-Service und wählen Sie Fargate als Starttyp.	1. Erstellen Sie einen Amazon ECS-Service mithilfe des ECS-Clusters, den Sie zuvor erstellt haben. Stellen Sie sicher, dass Sie Fargate als Starttyp wählen. 2. Wählen Sie die im vorherigen Schritt erstellte Aufgabendefinition und wählen Sie die Zielgrupp e des Application Load Balancer aus.	Cloud-Administrator

AWS einrichten PrivateLink

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie den PrivateLink AWS-Endpunkt ein.	1. Öffnen Sie die Amazon VPC-Konsole und erstellen Sie einen AWS PrivateLink Endpunkt. 2. Ordnen Sie diesen Endpunkt dem Network Load Balancer zu, der die auf Amazon ECS gehostete Anwendung privat für Kunden verfügbar macht.	Cloud-Administrator

Erstellen eines VPC-Endpunkts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen VPC-Endpunkt.	Erstellen Sie einen VPC-Endpunkt für den PrivateLink AWS-Endpunkt, den Sie zuvor erstellt haben. Der vollquali fizierte Domainname (FQDN) des VPC-Endpunkts zeigt auf den PrivateLink AWS-Endpu nkt-FQDN. Dadurch wird eine elastic network interface zum VPC-Endpunktdienst erstellt, auf die die Domain Name Service-Endpunkte zugreifen können.	Cloud-Administrator

Legen Sie das Ziel fest

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie den Application Load Balancer als Ziel hinzu.	Folgen Sie den Anweisung en in der Dokumentation, um den Application Load Balancer als Ziel für den Network Load Balancer hinzuzufügen.AWS	App-Developer

Zugehörige Ressourcen

Erstellen Sie die Load Balancer:

- Verwenden Sie einen Network Load Balancer für Amazon ECS
- Einen Network Load Balancer erstellen
- Verwenden Sie einen Application Load Balancer für Amazon ECS

- Erstellen Sie einen Application Load Balancer

Erstellen Sie ein Amazon EFS-Dateisystem:

- Erstellen Sie ein Amazon EFS-Dateisystem
- Bereitstellungsziele in Amazon EFS erstellen

Erstellen Sie ein Secrets Manager Manager-Geheimnis:

- Schlüssel in AWS KMS erstellen
- Erstellen Sie ein Geheimnis in AWS Secrets Manager

Erstellen Sie eine Amazon RDS-Instance:

- Eine Amazon RDS-DB-Instance erstellen

Erstellen Sie die Amazon ECS-Komponenten

- Erstellen Sie ein Amazon ECR-Repository
- Authentifizieren Sie Docker mit dem Amazon ECR-Repository
- Ein Bild in ein Amazon ECR-Repository übertragen
- Amazon ECS-Aufgabendefinition erstellen
- Einen Amazon ECS-Service erstellen

Andere Ressourcen:

- Sicherer Zugriff auf Services über AWS PrivateLink

Greifen Sie mit AWS PrivateLink und einem Network Load Balancer privat auf Container-Anwendungen auf Amazon EKS zu

Erstellt von Kirankumar Chandrashekar (AWS)

Übersicht

Dieses Muster beschreibt, wie Sie eine Docker-Container-Anwendung privat auf Amazon Elastic Kubernetes Service (Amazon EKS) hinter einem Network Load Balancer hosten und mithilfe von AWS auf die Anwendung zugreifen. PrivateLink Sie können dann ein privates Netzwerk verwenden, um sicher auf Dienste in der Amazon Web Services (AWS) Cloud zuzugreifen.

Der Amazon EKS-Cluster, auf dem die Docker-Anwendungen ausgeführt werden, mit einem Network Load Balancer am Frontend kann mit einem Virtual Private Cloud (VPC) -Endpunkt für den Zugriff über AWS verknüpft werden. PrivateLink Dieser VPC-Endpunktdienst kann dann mit anderen gemeinsam genutzt werden, VPCs indem deren VPC-Endpunkte verwendet werden.

Das in diesem Muster beschriebene Setup ist eine sichere Methode, um den Anwendungszugriff zwischen VPCs AWS-Konten gemeinsam zu nutzen. Es sind keine speziellen Konnektivitäts- oder Routing-Konfigurationen erforderlich, da die Verbindung zwischen den Kunden- und Anbieterkonten auf dem globalen AWS-Backbone erfolgt und nicht über das öffentliche Internet erfolgt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Docker, installiert und konfiguriert unter Linux, MacOS oder Windows.
- Eine Anwendung, die auf Docker läuft.
- Ein aktives AWS-Konto.
- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 2, installiert und konfiguriert unter Linux, macOS oder Windows.
- Ein vorhandener Amazon EKS-Cluster mit markierten privaten Subnetzen, der für das Hosten von Anwendungen konfiguriert ist. Weitere Informationen finden Sie unter Subnet-Tagging in der Amazon EKS-Dokumentation.
- Kubectl, installiert und konfiguriert für den Zugriff auf Ressourcen in Ihrem Amazon EKS-Cluster. Weitere Informationen finden Sie unter Installation von kubectl in der Amazon EKS-Dokumentation.

Architektur

Technologie-Stack

- Amazon EKS
- AWS PrivateLink
- Network Load Balancer

Automatisierung und Skalierung

- Kubernetes-Manifeste können in einem Git-basierten Repository verfolgt und verwaltet und mithilfe von Continuous Integration and Continuous Delivery (CI/CD) in AWS bereitgestellt werden. CodePipeline
- Sie können AWS verwenden CloudFormation , um dieses Muster mithilfe von Infrastructure as Code (IaC) zu erstellen.

Tools

- AWS CLI — AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Elastic Load Balancing — Elastic Load Balancing verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele, wie Amazon Elastic Compute Cloud (Amazon EC2) - Instances, Container und IP-Adressen, in einer oder mehreren Availability Zones.

- Amazon EKS — Amazon Elastic Kubernetes Service (Amazon EKS) ist ein verwalteter Service, mit dem Sie Kubernetes auf AWS ausführen können, ohne Ihre eigene Kubernetes-Steuerebene oder Knoten installieren, betreiben und warten zu müssen.
- Amazon VPC — Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten.
- Kubectl — Kubectl ist ein Befehlszeilenprogramm zum Ausführen von Befehlen für Kubernetes-Cluster.

Epen

Stellen Sie die Kubernetes-Bereitstellungs- und Service-Manifestdateien bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Manifestdatei für die Kubernetes-Bereitstellung.	Erstellen Sie eine Bereitstellungsmanifestdatei, indem Sie die folgende Beispieldatei Ihren Anforderungen entsprechend ändern.
	`apiVersion: apps/v1`
	`kind: Deployment`
	`metadata:`
	`  name: sample-app`
	`spec:`
	`  replicas: 3`
	`  selector:`
	`  matchLabels:`
	`  app: nginx`
	`  template:`
	`  metadata:`
	`  labels:`
	`  app: nginx`
	`  spec:`
	`  containers:`
	`  - name: nginx`
	`  image: public.ecr.aws/z9d2n7e1/nginx:1.19.5`
	`  ports:`
	`  - name: http`
	`  containerPort: 80`
	Note
	Dies ist eine NGINX-Beispielkonfigurationsdatei, die mithilfe
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	des NGINX-Docker-Images bereitgestellt wird. Weitere Informationen finden Sie in der Docker-Dokumentation unter So verwenden Sie das offizielle NGINX-Docker-Image.	
Stellen Sie die Kubernetes-Bereitstellungsmanifestdatei bereit.	Führen Sie den folgenden Befehl aus, um die Bereitstellungsmanifestdatei auf Ihren Amazon EKS-Cluster anzuwenden: `kubectl apply -f <your_deployment_file_name>`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Manifestdatei des Kubernetes-Dienstes.	Erstellen Sie eine Dienstmanifestdatei, indem Sie die folgende Beispieldatei Ihren Anforderungen entsprechend ändern.
	
	`apiVersion: v1`
	`kind: Service`
	`metadata:`
	`  name: sample-service`
	`  annotations:`
	`  service.beta.kubernetes.io/aws-load-balancer-type: nlb`
	`  service.beta.kubernetes.io/aws-load-balancer-internal: "true"`
	`spec:`
	`  ports:`
	`  - port: 80`
	`  targetPort: 80`
	`  protocol: TCP`
	`  type: LoadBalancer`
	`  selector:`
	`  app: nginx`
	
	Important
	Stellen Sie sicher, dass Sie Folgendes angegeben habe`annotations`, um einen internen Network Load Balancer zu definieren:
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`service.beta.kubernetes.io/aws-load-balancer-type: nlb` `service.beta.kubernetes.io/aws-load-balancer-internal: "true"`	
Stellen Sie die Manifestdatei des Kubernetes-Dienstes bereit.	Führen Sie den folgenden Befehl aus, um die Service-Manifest-Datei auf Ihren Amazon EKS-Cluster anzuwenden: `kubectl apply -f <your_service_file_name>`	DevOps Ingenieur

Erstellen Sie die Endpunkte

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Notieren Sie sich den Namen des Network Load Balancers.	Führen Sie den folgenden Befehl aus, um den Namen des Network Load Balancer abzurufen: `kubectl get svc sample-service -o wide` Notieren Sie sich den Namen des Network Load Balancers, der für die Erstellung eines	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	PrivateLink AWS-Endpunkts erforderlich ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen PrivateLink AWS-Endpunkt.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon VPC-Konsole und erstellen Sie dann einen PrivateLink AWS-Endpunkt. Ordnen Sie diesen Endpunkt dem Network Load Balancer zu, damit die Anwendung privat für Kunden verfügbar ist. Weitere Informationen finden Sie unter VPC Endpoint Services (AWS PrivateLink) in der Amazon VPC-Dokumentation. **Important** Wenn das Verbrauchserkonto Zugriff auf die Anwendung benötigt, muss die AWS-Konto-ID des Verbrauchserkontos zur Liste der zulässigen Prinzipale für die PrivateLink AWS-Endpunktkonfiguration hinzugefügt werden. Weitere Informationen finden Sie unter Hinzufügen und Entfernen von Berechtigungen für Ihren Endpunkt-	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Service in der Amazon VPC-Dokumentation.	
Erstellen Sie einen VPC-Endpunkt.	Wählen Sie in der Amazon VPC-Konsole Endpoint Services und dann Create Endpoint Service aus. Erstellen Sie einen VPC-Endpunkt für den PrivateLink AWS-Endpunkt. Der vollqualifizierte Domainname (FQDN) des VPC-Endpunkts verweist auf den FQDN für den AWS-Endpunkt. PrivateLink Dadurch wird eine elastic network interface zum VPC-Endpunktdienst erstellt, auf die die DNS-Endpunkte zugreifen können.	Cloud-Administrator

Zugehörige Ressourcen

- Verwenden Sie das offizielle NGINX Docker-Image
- Network Load Balancing in Amazon EKS
- VPC-Endpunktdienste (AWS PrivateLink) erstellen
- Hinzufügen und Entfernen von Berechtigungen für Ihren Endpunkt-Service

Aktivieren Sie mTLS in AWS App Mesh mithilfe von AWS Private CA auf Amazon EKS

Erstellt von Omar Kahil (AWS), Emmanuel Saliu (AWS), Muhammad Shahzad (AWS) und Andy Wong (AWS)

Übersicht

Dieses Muster zeigt, wie Mutual Transport Layer Security (mTLS) auf Amazon Web Services (AWS) mithilfe von Zertifikaten von AWS Private Certificate Authority (AWS Private CA) in AWS App Mesh implementiert wird. Es verwendet die Envoy Secret Discovery Service (SDS) -API über das Secure Production Identity Framework for Everyone (SPIFFE). SPIFFE ist ein Open-Source-Projekt der Cloud Native Computing Foundation (CNCF) mit breiter Unterstützung durch die Community, das ein detailliertes und dynamisches Workload-Identitätsmanagement bietet. Verwenden Sie zur Implementierung der SPIFFE-Standards die SPIFFE-Laufzeitumgebung von SPIRE.

Die Verwendung von mTLS in App Mesh bietet eine bidirektionale Peer-Authentifizierung, da sie eine Sicherheitsebene gegenüber TLS bietet und es den Diensten im Mesh ermöglicht, den Client zu verifizieren, der die Verbindung herstellt. Der Client in der Client-Server-Beziehung stellt während des Sitzungsaushandlungsprozesses auch ein X.509-Zertifikat bereit. Der Server verwendet dieses Zertifikat, um den Client zu identifizieren und zu authentifizieren. Auf diese Weise kann überprüft werden, ob das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt wurde und ob das Zertifikat gültig ist.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster mit selbstverwalteten oder verwalteten Knotengruppen
- Auf dem Cluster bereitgestellter App Mesh Mesh-Controller mit aktiviertem SDS
- Ein privates Zertifikat von AWS Certificate Manager (ACM), das von AWS Private CA ausgestellt wurde

Einschränkungen

- SPIRE kann nicht auf AWS Fargate installiert werden, da der SPIRE-Agent als DaemonSet Kubernetes ausgeführt werden muss.

Produktversionen

- AWS App Mesh Controller-Diagramm 1.3.0 oder höher

Architektur

Das folgende Diagramm zeigt den EKS-Cluster mit App Mesh in der VPC. Der SPIRE-Server in einem Worker-Knoten kommuniziert mit den SPIRE-Agenten in anderen Worker-Knoten und mit AWS Private CA. Envoy wird für die mTLS-Kommunikation zwischen den SPIRE Agent-Worker-Knoten verwendet.

Die Abbildung zeigt die folgenden Schritte:

1. Das Zertifikat wurde ausgestellt.
2. Zertifikatssignierung und Zertifikat anfordern.

Tools

AWS-Services

- AWS Private CA — AWS Private Certificate Authority (AWS Private CA) ermöglicht die Erstellung von Hierarchien von privaten Zertifizierungsstellen (CA), einschließlich Stamm- und untergeordneter Zertifizierungsstellen CAs, ohne die Investitions- und Wartungskosten für den Betrieb einer lokalen CA.
- AWS App Mesh — AWS App Mesh ist ein Service Mesh, das die Überwachung und Steuerung von Services erleichtert. App Mesh standardisiert die Art und Weise, wie Ihre Dienste kommunizieren, und bietet Ihnen so konsistente Transparenz und Netzwerkverkehrskontrollen für jeden Service in einer Anwendung.
- Amazon EKS — Amazon Elastic Kubernetes Service (Amazon EKS) ist ein verwalteter Service, mit dem Sie Kubernetes auf AWS ausführen können, ohne Ihre eigene Kubernetes-Steuerebene oder Knoten installieren, betreiben und warten zu müssen.

Andere Tools

- Helm — Helm ist ein Paketmanager für Kubernetes, der Sie bei der Installation und Verwaltung von Anwendungen auf Ihrem Kubernetes-Cluster unterstützt. Dieses Muster verwendet Helm, um den AWS App Mesh Controller bereitzustellen.
- AWS App Mesh Controller-Diagramm — Das AWS App Mesh Controller-Diagramm wird von diesem Muster verwendet, um AWS App Mesh auf Amazon EKS zu aktivieren.

Epen

Richte die Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie App Mesh mit Amazon EKS ein.	Folgen Sie den grundlegenden Bereitstellungsschritten, die im Repository bereitgestellt werden.	DevOps Ingenieur
Installieren Sie SPIRE.	Installieren Sie SPIRE mithilfe von spire_setup.yaml auf dem EKS-Cluster.	DevOps Ingenieur
Installieren Sie das AWS Private CA-Zertifikat.	Erstellen und installieren Sie ein Zertifikat für Ihre private Root-CA, indem Sie den Anweisungen in der AWS-Dokumentation folgen.	DevOps Ingenieur
Erteilen Sie der Instanzrolle des Clusterknotens Berechtigungen.	Verwenden Sie den Code im Abschnitt Zusätzliche Informationen, um der Clusterknoten-Instanzrolle Richtlinien zuzuweisen.	DevOps Ingenieur
Fügen Sie das SPIRE-Plugin für AWS Private CA hinzu.	Verwenden Sie den Code, der sich im Abschnitt Zusätzliche Informationen befindet, um das Plugin zur SPIRE-Serverkonfiguration hinzuzufügen.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ersetzen Sie den `certificate_authority_arn` Amazon Resource Name (ARN) durch Ihren privaten CA-ARN. Der verwendete Signaturalgorithmus muss mit dem Signaturalgorithmus auf der privaten CA identisch sein. Ersetzen Sie `your_region` durch Ihre AWS-Region. Weitere Informationen zum Plugin finden Sie unter Server-Plugin: UpstreamAuthority „aws_pca“.	
Bundle.cert aktualisieren.	Nachdem Sie den SPIRE-Server erstellt haben, wird eine `spire-bundle.yaml` Datei erstellt. Ändern Sie den `bundle.crt` Wert in der `spire-bundle.yaml` Datei von der privaten Zertifizierungsstelle in das öffentliche Zertifikat.	DevOps Ingenieur

Stellen Sie die Workloads bereit und registrieren Sie sie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Registrieren Sie Knoten- und Workload-Einträge bei SPIRE.	Verwenden Sie den Code im Repository, um Knoten und Workload (Dienste) beim SPIRE-Server zu registrieren.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Mesh in App Mesh mit aktiviertem mTLS.	Erstellen Sie in App Mesh ein neues Mesh mit allen Komponenten für Ihre Microservices-Anwendung (z. B. virtueller Dienst, virtueller Router und virtuelle Knoten).	DevOps Ingenieur
Überprüfen Sie die registrierten Einträge.	Sie können die registrierten Einträge für Ihre Knoten und Workloads überprüfen, indem Sie den folgenden Befehl ausführen. `kubectl exec -n spire spire-server-0 -- /opt/spire/bin/spire-server entry show` Dadurch werden die Einträge für die SPIRE-Agenten angezeigt.	DevOps Ingenieur

Überprüfen Sie den mTLS-Verkehr

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den mTLS-Verkehr.	1. Senden Sie vom Frontend-Dienst aus einen HTTP-Header an den Back-End-Dienst und überprüfen Sie die erfolgreiche Antwort mit den Diensten, die in SPIRE registriert sind. 2. Für die gegenseitige TLS-Authentifizierung können	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Sie die `ssl.handshake` Statistik überprüfen, indem Sie den folgenden Befehl ausführen.
	`kubectl exec -it $POD -n $NAMESPACE -c envoy -- curl http://localhost:9901/stats | grep ssl.handshake`
	Nachdem Sie den vorherigen Befehl ausgeführt haben, sollten Sie die `ssl.handshake` Anzahl der Listener sehen, die dem folgenden Beispiel ähnelt:
	`listener.0.0.0.0_15000.ssl.handshake: 2`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass Zertifikate von AWS Private CA ausgestellt wurden.	Sie können anhand der Protokolle auf Ihrem SPIRE-Server überprüfen, ob die Plugins korrekt konfiguriert wurden und ob Zertifikate von Ihrer vorgelagerten privaten Zertifizierungsstelle ausgestellt wurden. Führen Sie den folgenden Befehl aus. `kubectl logs spire-server-0 -n spire` Sehen Sie sich dann die erstellten Protokolle an. Dieser Code geht davon aus, dass Ihr Server benannt ist `spire-server-0` und in Ihrem Spire-Namespace gehostet wird. Sie sollten sehen, dass die Plugins erfolgreich geladen wurden und eine Verbindung zu Ihrer privaten Upstream-CA hergestellt wurde.	DevOps Ingenieur

Zugehörige Ressourcen

- Verwendung von mTLS mit SPIFFE/SPIRE in AWS App Mesh auf Amazon EKS
- Aktivierung von mTLS in AWS App Mesh mithilfe von SPIFFE/SPIRE in einer Amazon EKS-Umgebung mit mehreren Konten
- In diesem Muster verwendete exemplarische Vorgehensweise
- Server-Plugin: UpstreamAuthority „aws_pca“
- Schnellstart für Kubernetes

Zusätzliche Informationen

Weisen Sie der Cluster-Knoten-Instanzrolle Berechtigungen zu

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ACMPCASigning",
            "Effect": "Allow",
            "Action": [
                "acm-pca:DescribeCertificateAuthority",
                "acm-pca:IssueCertificate",
                "acm-pca:GetCertificate",
                "acm:ExportCertificate"
            ],
            "Resource": "*"
        }
    ]
}
AWS Managed Policy: "AWSAppMeshEnvoyAccess"
```

Fügen Sie das SPIRE-Plugin für ACM hinzu

```
Add the SPIRE plugin for ACM
Change certificate_authority_arn to your PCA ARN. The signing algorithm used must be
 the same as the signing algorithm on the PCA. Change your_region to the appropriate
 AWS Region.
UpstreamAuthority "aws_pca" {
    plugin_data {
        region = "your_region"
        certificate_authority_arn = "arn:aws:acm-pca:...."
        signing_algorithm = "your_signing_algorithm"
    }
}
```

Automatisieren Sie Backups für Amazon RDS for PostgreSQL PostgreSQL-DB-Instances mithilfe von AWS Batch

Erstellt von Kirankumar Chandrashekar (AWS)

Übersicht

Das Sichern Ihrer PostgreSQL-Datenbanken ist eine wichtige Aufgabe und kann in der Regel mit dem Hilfsprogramm pg_dump erledigt werden, das standardmäßig den Befehl COPY verwendet, um ein Schema und einen Datendump einer PostgreSQL-Datenbank zu erstellen. Dieser Vorgang kann sich jedoch wiederholen, wenn Sie regelmäßige Backups für mehrere PostgreSQL-Datenbanken benötigen. Wenn Ihre PostgreSQL-Datenbanken in der Cloud gehostet werden, können Sie auch die automatische Backup-Funktion von Amazon Relational Database Service (Amazon RDS) für PostgreSQL nutzen. Dieses Muster beschreibt, wie regelmäßige Backups für Amazon RDS for PostgreSQL PostgreSQL-DB-Instances mithilfe des Dienstprogramms pg_dump automatisiert werden.

Hinweis: In den Anweisungen wird davon ausgegangen, dass Sie Amazon RDS verwenden. Sie können diesen Ansatz jedoch auch für PostgreSQL-Datenbanken verwenden, die außerhalb von Amazon RDS gehostet werden. Um Backups zu erstellen, muss die AWS Lambda Lambda-Funktion auf Ihre Datenbanken zugreifen können.

Ein zeitbasiertes Amazon CloudWatch Events-Ereignis initiiert eine Lambda-Funktion, die nach bestimmten Backup-Tags sucht, die auf die Metadaten der PostgreSQL-DB-Instances auf Amazon RDS angewendet wurden. Wenn die PostgreSQL-DB-Instances das Tag bkp:Automated DBDump = Active und andere erforderliche Backup-Tags haben, sendet die Lambda-Funktion einzelne Jobs für jede Datenbanksicherung an AWS Batch.

AWS Batch verarbeitet diese Jobs und lädt die Backup-Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket hoch. Dieses Muster verwendet eine Dockerfile- und eine Datei entrypoint.sh, um ein Docker-Container-Image zu erstellen, das zum Erstellen von Backups im AWS Batch Batch-Job verwendet wird. Nach Abschluss des Sicherungsvorgangs zeichnet AWS Batch die Backup-Details in einer Inventartabelle auf Amazon DynamoDB auf. Als zusätzliche Schutzmaßnahme löst ein CloudWatch Events-Ereignis eine Amazon Simple Notification Service (Amazon SNS) -Benachrichtigung aus, wenn ein Job in AWS Batch fehlschlägt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine bestehende verwaltete oder nicht verwaltete Rechenumgebung. Weitere Informationen finden Sie unter Verwaltete und nicht verwaltete Rechenumgebungen in der AWS Batch Batch-Dokumentation.
- Docker-Image der AWS-Befehlszeilenschnittstelle (CLI), Version 2, installiert und konfiguriert.
- Bestehende Amazon RDS for PostgreSQL PostgreSQL-DB-Instances.
- Ein vorhandener S3-Bucket.
- Docker, installiert und konfiguriert unter Linux, MacOS oder Windows.
- Vertrautheit mit der Programmierung in Lambda.

Architektur

Technologie-Stack

- CloudWatch Amazon-Veranstaltungen
- Amazon-DynamoDB
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon RDS
- Amazon SNS
- Amazon S3
- AWS Batch
- AWS Key Management Service (AWS KMS)
- AWS Lambda
- AWS Secrets Manager
- Docker

Tools

- Amazon CloudWatch Events — CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit.
- Amazon DynamoDB — DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der schnelle und vorhersehbare Leistung mit nahtloser Skalierbarkeit bietet.

- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter AWS-Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon RDS — Amazon Relational Database Service (Amazon RDS) ist ein Webservice, der die Einrichtung, den Betrieb und die Skalierung einer relationalen Datenbank in der AWS-Cloud erleichtert.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) ist ein verwalteter Service, der die Nachrichtenzustellung von Herausgebern an Abonnenten ermöglicht.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Speicher für das Internet.
- AWS Batch — Mit AWS Batch können Sie Batch-Computing-Workloads in der AWS-Cloud ausführen.
- AWS KMS — AWS Key Management Service (AWS KMS) ist ein verwalteter Service, mit dem Sie auf einfache Weise die zur Verschlüsselung Ihrer Daten verwendeten Verschlüsselungsschlüssel erstellen und kontrollieren können.
- AWS Lambda — Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen.
- AWS Secrets Manager — Secrets Manager hilft Ihnen dabei, hartcodierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Geheimnis programmgesteuert abzurufen.
- Docker — Docker hilft Entwicklern dabei, jede Anwendung als leichten, tragbaren und autarken Container einfach zu packen, zu versenden und auszuführen.

Auf Ihre PostgreSQL-DB-Instances auf Amazon RDS müssen Tags auf ihre Metadaten angewendet werden. Die Lambda-Funktion sucht nach Tags, um DB-Instances zu identifizieren, die gesichert werden sollten, und die folgenden Tags werden normalerweise verwendet.

Markierung	Beschreibung
bkp:Automated = Aktiv DBDump	Identifiziert eine Amazon RDS-DB-Instance als Kandidaten für Backups.
bkp: = AutomatedBackupSecret <secret_name>	Identifiziert das Secrets Manager Manager-Geheimnis, das die Amazon RDS-Anmel deinformationen enthält.

bkp: DBDump Automatisierter S3-Bucket = <s3_bucket_name>	Identifiziert den S3-Bucket, an den Backups gesendet werden sollen.
BKPDBDump: Automatisierte Frequenz BKP:Automatisierte DBDump Zeit	Identifizieren Sie die Häufigkeit und die Zeiten, zu denen Datenbanken gesichert werden sollten.
bkp:pgdumpcommand = <pgdump_command>	Identifiziert die Datenbanken, für die die Backups erstellt werden müssen.

Epen

Erstellen Sie eine Inventartabelle in DynamoDB

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Tabelle in DynamoDB.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon DynamoDB DynamoDB-Konsole und erstellen Sie eine Tabelle. Hilfe zu dieser und anderen Geschichten finden Sie im Abschnitt Verwandte Ressourcen.	Cloud-Administrator, Datenbankadministrator
Vergewissern Sie sich, dass die Tabelle erstellt wurde.	Führen Sie den Befehl `aws dynamodb describe-table --table-name <table-name> | grep TableStatus` aus. Wenn die Tabelle existiert, gibt der Befehl das `"TableStatus": "ACTIVE",` Ergebnis zurück.	Cloud-Administrator, Datenbankadministrator

Erstellen Sie ein SNS-Thema für fehlgeschlagene Auftragsereignisse in AWS Batch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein SNS-Thema.	Öffnen Sie die Amazon SNS SNS-Konsole, wählen Sie Themen und erstellen Sie ein SNS-Thema mit dem Namen. `JobFailedAlert` Abonnieren Sie das Thema mit einer aktiven E-Mail-Adresse und überprüfen Sie Ihren E-Mail-Posteingang, um die SNS-Abonnement-E-Mail von AWS Notifications zu bestätigen.	Cloud-Administrator
Erstellen Sie eine Ereignisregel für fehlgeschlagene Jobs für AWS Batch.	Öffnen Sie die CloudWatch Amazon-Konsole, wählen Sie Ereignisse und dann Regel erstellen aus. Wählen Sie Erweiterte Optionen anzeigen und anschließend Bearbeiten. Ersetzen Sie unter „Ein Muster erstellen, das Ereignisse für die Verarbeitung durch Ihre Ziele auswählt“ den vorhandenen Text durch den Code „Fehlgeschlagenes Auftragsereignis“ aus dem Abschnitt „Zusätzliche Informationen“. Dieser Code definiert eine CloudWatch Ereignisregel, die ausgelöst wird, wenn AWS Batch ein `Failed` Ereignis hat.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ziel für eine Ereignisregel hinzufügen.	Wählen Sie unter Ziele die Option Ziele hinzufügen und wählen Sie das `JobFailed Alert` SNS-Thema aus. Konfigurieren Sie die verbleibenden Details und erstellen Sie die Cloudwatch Events-Regel.	Cloud-Administrator

Erstellen Sie ein Docker-Image und übertragen Sie es in ein Amazon ECR-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon-ECR-Repository.	Öffnen Sie die Amazon ECR-Konsole und wählen Sie die AWS-Region aus, in der Sie Ihr Repository erstellen möchten. Wählen Sie Repositories und dann Create repository aus. Konfigurieren Sie das Repository gemäß Ihren Anforderungen.	Cloud-Administrator
Schreiben Sie eine Docker-Datei.	Melden Sie sich bei Docker an und verwenden Sie die „Beispieldatei Dockerfile“ und „Beispieldatei entrypoint.sh“ aus dem Abschnitt Zusätzliche Informationen, um ein Dockerfile zu erstellen.	DevOps Ingenieur
Erstellen Sie ein Docker-Image und übertragen Sie es in das Amazon ECR-Repository.	Erstellen Sie das Dockerfile in ein Docker-Image und übertragen Sie es in das Amazon ECR-Repository.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hilfe zu dieser Geschicht e finden Sie im Abschnitt Verwandte Ressourcen.	

Erstellen Sie die AWS Batch Batch-Komponenten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS Batch Batch-Auftragsdefinition.	Öffnen Sie die AWS Batch Batch-Konsole und erstellen Sie eine Auftragsdefinition , die den Uniform Resource Identifier (URI) des Amazon ECR-Repositorys als Eigenschaft `Image` enthält.	Cloud-Administrator
Konfigurieren Sie die AWS Batch Batch-Jobwarteschl ange.	Wählen Sie in der AWS Batch Batch-Konsole Job-Warte schlangen und anschließend Warteschlange erstellen aus. Erstellen Sie eine Auftragsw arteschlange, in der Jobs gespeichert werden, bis AWS Batch sie auf den Ressource n in Ihrer Rechenumgebung ausführt. Wichtig: Stellen Sie sicher, dass Sie Logik für AWS Batch schreiben, um die Backup-Details in der DynamoDB-Inventartabelle aufzuzeichnen.	Cloud-Administrator

Eine Lambda-Funktion erstellen und planen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Lambda-Funktion, um nach Tags zu suchen.	Erstellen Sie eine Lambda-Funktion, die nach Tags in Ihren PostgreSQL-DB-Instances sucht und Backup-Kandidaten identifiziert. Stellen Sie sicher, dass Ihre Lambda-Funktion das `bkp:AutomatedDBDump = Active` Tag und alle anderen erforderlichen Tags identifizieren kann. Wichtig: Die Lambda-Funktion muss auch in der Lage sein, Jobs zur AWS Batch Batch-Job warteschlange hinzuzufügen.	DevOps Ingenieur
Erstellen Sie ein zeitbasiertes Ereignis für CloudWatch Ereignisse.	Öffnen Sie die CloudWatch Amazon-Konsole und erstellen Sie ein CloudWatch Events-Ereignis, das einen Cron-Ausdruck verwendet, um Ihre Lambda-Funktion regelmäßig auszuführen. Wichtig: Alle geplanten Ereignisse verwenden die UTC-Zeitzone.	Cloud-Administrator

Testen Sie die Backup-Automatisierung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon KMS-Schlüssel.	Öffnen Sie die Amazon KMS-Konsole und erstellen Sie einen KMS-Schlüssel, der zur	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Verschlüsselung der in AWS Secrets Manager gespeicherten Amazon RDS-Anmeldeinformationen verwendet werden kann.	
Erstellen Sie ein AWS Secrets Manager Manager-Geheimnis.	Öffnen Sie die AWS Secrets Manager Manager-Konsole und speichern Sie Ihre Amazon RDS for PostgreSQL PostgreSQL-Datenbankanmeldedaten als geheim.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie den PostgreSQL-DB-Instances die erforderlichen Tags hinzu.	**Important** Öffnen Sie die Amazon RDS-Konsole und fügen Sie Tags zu den PostgreSQL-DB-Instances hinzu, die Sie automatisch sichern möchten. Sie können die Tags aus der Tabelle im Abschnitt Tools verwenden. Wenn Sie Backups von mehreren PostgreSQL-Datenbanken innerhalb derselben Amazon RDS-Instance benötigen, verwenden Sie diese `-d test:-d test1` als Wert für das `bkp:pgdumpcommand` Tag. `test` und `test1` sind Datenbanknamen. Stellen Sie sicher, dass nach dem Doppelpunkt (:) kein Leerzeichen steht.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Backup-Automatisierung.	Um die Backup-Automatisierung zu überprüfen, können Sie entweder die Lambda-Funktion aufrufen oder warten, bis der Backup-Zeitplan beginnt. Nachdem der Sicherungsvorgang abgeschlossen ist, überprüfen Sie, ob die DynamoDB-Inventartabelle einen gültigen Backup-Eintrag für Ihre PostgreSQL-DB-Instances enthält. Wenn sie übereinstimmen, ist der Backup-Automatisierungsprozess erfolgreich.	Cloud-Administrator

Zugehörige Ressourcen

Erstellen Sie eine Inventartabelle in DynamoDB

- Eine Amazon DynamoDB-Tabelle erstellen

Erstellen Sie ein SNS-Thema für fehlgeschlagene Auftragsereignisse in AWS Batch

- Ein Amazon SNS SNS-Thema erstellen
- Senden Sie SNS-Benachrichtigungen für fehlgeschlagene Auftragsereignisse in AWS Batch

Erstellen Sie ein Docker-Image und übertragen Sie es in ein Amazon ECR-Repository

- Erstellen Sie ein Amazon ECR-Repository

- Schreiben Sie eine Dockerfile, erstellen Sie ein Docker-Image und übertragen Sie es an Amazon ECR

Erstellen Sie die AWS Batch Batch-Komponenten

- Eine AWS Batch Batch-Auftragsdefinition erstellen
- Konfigurieren Sie Ihre Rechenumgebung und die AWS Batch Batch-Job-Warteschlange
- Erstellen Sie eine Auftragswarteschlange in AWS Batch

Erstellen Sie eine Lambda-Funktion

- Erstellen Sie eine Lambda-Funktion und schreiben Sie Code
- Verwenden Sie Lambda mit DynamoDB

Erstellen Sie ein Veranstaltungsereignis CloudWatch

- Erstellen Sie ein zeitbasiertes CloudWatch Veranstaltungsereignis
- Verwenden Sie Cron-Ausdrücke in Cloudwatch Events

Testen Sie die Backup-Automatisierung

- Einen Amazon KMS-Schlüssel erstellen
- Ein Secrets Manager Manager-Geheimnis erstellen
- Hinzufügen von Tags zu einer Amazon RDS-Instance

Zusätzliche Informationen

Fehlgeschlagenes Auftragsereignis:

```
{
  "detail-type": [
    "Batch Job State Change"
  ],
  "source": [
    "aws.batch"
  ],
  "detail": {
    "status": [
      "FAILED"
    ]
  }
}
```

Beispiel für eine Docker-Datei:

```
FROM alpine:latest
RUN apk --update add py-pip postgresql-client jq bash && \
pip install awscli && \
rm -rf /var/cache/apk/*
ADD entrypoint.sh /usr/bin/
RUN chmod +x /usr/bin/entrypoint.sh
ENTRYPOINT ["entrypoint.sh"]
```

Beispieldatei entrypoint.sh:

```
 #!/bin/bash
set -e
DATETIME=`date +"%Y-%m-%d_%H_%M"`
FILENAME=RDS_PostGres_dump_${RDS_INSTANCE_NAME}
FILE=${FILENAME}_${DATETIME}

aws configure --profile new-profile set role_arn arn:aws:iam::${TargetAccountId}:role/
${TargetAccountRoleName}
aws configure --profile new-profile set credential_source EcsContainer

echo "Central Account access provider IAM role is: "
aws sts get-caller-identity

echo "Target Customer Account access provider IAM role is: "
aws sts get-caller-identity --profile new-profile
```

```
securestring=$(aws secretsmanager get-secret-value --secret-id $SECRETID --output json
 --query 'SecretString' --region=$REGION --profile new-profile)

if [[ ${securestring} ]]; then
    echo "successfully accessed secrets manager and got the credentials"
    export PGPASSWORD=$(echo $securestring | jq --raw-output | jq -r '.DB_PASSWORD')
    PGSQL_USER=$(echo $securestring | jq --raw-output | jq -r '.DB_USERNAME')
    echo "Executing pg_dump for the PostGres endpoint ${PGSQL_HOST}"
    # pg_dump -h $PGSQL_HOST -U $PGSQL_USER -n dms_sample | gzip -9 -c  | aws s3 cp -
 --region=$REGION  --profile new-profile s3://$BUCKET/$FILE
    # in="-n public:-n private"
    IFS=':' list=($EXECUTE_COMMAND);
    for command in "${list[@]}";
      do
        echo $command;
        pg_dump -h $PGSQL_HOST -U $PGSQL_USER ${command} | gzip -9 -c  | aws s3 cp - --
region=$REGION --profile new-profile s3://${BUCKET}/${FILE}-${command}".sql.gz"
        echo $?;
        if  [[ $? -ne 0 ]]; then
            echo "Error occurred in database backup process. Exiting now....."
            exit 1
        else
            echo "Postgresql dump was successfully taken for the RDS endpoint
 ${PGSQL_HOST} and is uploaded to the following S3 location s3://${BUCKET}/${FILE}-
${command}.sql.gz"
            #write the details into the inventory table in central account
            echo "Writing to DynamoDB inventory table"
            aws dynamodb put-item --table-name ${RDS_POSTGRES_DUMP_INVENTORY_TABLE} --
region=$REGION --item '{ "accountId": { "S": "'"${TargetAccountId}"'" }, "dumpFileUrl":
 {"S": "'"s3://${BUCKET}/${FILE}-${command}.sql.gz"'" }, "DumpAvailableTime": {"S":
 "'"`date +"%Y-%m-%d::%H::%M::%S"` UTC"'"}}'
            echo $?
            if  [[ $? -ne 0 ]]; then
                echo "Error occurred while putting item to DynamoDb Inventory Table.
 Exiting now....."
                exit 1
            else
                echo "Successfully written to DynamoDb Inventory Table
 ${RDS_POSTGRES_DUMP_INVENTORY_TABLE}"
            fi
        fi
      done;
else
    echo "Something went wrong {$?}"
```

```
    exit 1
fi

exec "$@"
```

Automatisieren Sie die Bereitstellung von Node Termination Handler in Amazon EKS mithilfe einer CI/CD-Pipeline

Erstellt von Sandip Gangapadhyay (AWS), John Vargas (AWS), Pragtideep Singh (AWS), Sandeep Gawande (AWS) und Viyoma Sachdeva (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

In der Amazon Web Services (AWS) Cloud können Sie AWS Node Termination Handler, ein Open-Source-Projekt, verwenden, um das Herunterfahren der Amazon Elastic Compute Cloud (Amazon EC2) -Instance innerhalb von Kubernetes problemlos zu handhaben. AWS Node Termination Handler hilft sicherzustellen, dass die Kubernetes-Steuerebene angemessen auf Ereignisse reagiert, die dazu führen können, dass Ihre EC2 Instance nicht mehr verfügbar ist. Zu diesen Ereignissen gehören die folgenden:

- EC2 geplante Wartung der Instanz
- Unterbrechungen der Amazon EC2 Spot-Instance
- Auto Scaling Scaling-Gruppenskalierung
- Auto Scaling Scaling-Gruppen-Rebalancing zwischen Availability Zones
- EC2 Kündigung der Instanz über die API oder die AWS-Managementkonsole

Wenn ein Ereignis nicht behandelt wird, wird Ihr Anwendungscode möglicherweise nicht ordnungsgemäß beendet. Außerdem kann es länger dauern, bis die volle Verfügbarkeit wiederhergestellt ist, oder es wird versehentlich die Arbeit an Knoten geplant, die ausfallen. Der `aws-node-termination-handler` (NTH) kann in zwei verschiedenen Modi betrieben werden: Instance Metadata Service (IMDS) oder Queue Processor. Weitere Informationen zu den beiden Modi finden Sie in der Readme-Datei.

Dieses Muster verwendet AWS CodeCommit und automatisiert die Bereitstellung von NTH mithilfe von Queue Processor über eine CI/CD-Pipeline (Continuous Integration and Continuous Delivery).

> **Note**
>
> Wenn Sie von EKS verwaltete Knotengruppen verwenden, benötigen Sie die nicht. `aws-node-termination-handler`

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein Webbrowser, der für die Verwendung mit der AWS-Managementkonsole unterstützt wird. Sehen Sie sich die Liste der unterstützten Browser an.
- Das AWS Cloud Development Kit (AWS CDK) ist installiert.
- `kubectl`, das Kubernetes-Befehlszeilentool, installiert.
- `eksctl`, die AWS-Befehlszeilenschnittstelle (AWS CLI) für Amazon Elastic Kubernetes Service (Amazon EKS), installiert.
- Ein laufender EKS-Cluster mit Version 1.20 oder höher.
- Eine selbstverwaltete Knotengruppe, die an den EKS-Cluster angehängt ist. Führen Sie den folgenden Befehl aus, um einen Amazon EKS-Cluster mit einer selbstverwalteten Knotengruppe zu erstellen.

```
eksctl create cluster --managed=false --region <region> --name <cluster_name>
```

  Weitere Informationen dazu finden Sie in `eksctl` der eksctl-Dokumentation.
- AWS Identity and Access Management (IAM) OpenID Connect (OIDC) -Anbieter für Ihren Cluster. Weitere Informationen finden Sie unter Einen IAM-OIDC-Anbieter für Ihren Cluster erstellen.

Einschränkungen

- Sie müssen eine AWS-Region verwenden, die den Amazon EKS-Service unterstützt.

Produktversionen

- Kubernetes Version 1.20 oder höher
- `eksctl`Version 0.107.0 oder höher

- AWS CDK Version 2.27.0 oder höher

Architektur

Zieltechnologie-Stack

- Eine virtuelle private Cloud (VPC)
- Ein EKS-Cluster
- Amazon-Simple-Queue-Service (Amazon SQS)
- IAM
- Kubernetes

Zielarchitektur

Das folgende Diagramm zeigt eine allgemeine Ansicht der end-to-end Schritte, wenn die Knotenbeendigung gestartet wird.

Der im Diagramm dargestellte Arbeitsablauf besteht aus den folgenden allgemeinen Schritten:

1. Das Ereignis EC2 zum Beenden der automatischen Skalierungsinstanz wird an die SQS-Warteschlange gesendet.
2. Der NTH Pod sucht nach neuen Nachrichten in der SQS-Warteschlange.
3. Der NTH-Pod empfängt die neue Nachricht und geht wie folgt vor:
   - Sperrt den Knoten ab, sodass der neue Pod nicht auf dem Knoten ausgeführt wird.
   - Entleert den Knoten, sodass der vorhandene Pod evakuiert wird
   - Sendet ein Lifecycle-Hook-Signal an die Auto Scaling Scaling-Gruppe, sodass der Knoten beendet werden kann.

Automatisierung und Skalierung

- Der Code wird von AWS CDK verwaltet und bereitgestellt, unterstützt durch AWS CloudFormation Nested Stacks.
- Die Amazon EKS-Kontrollebene läuft über mehrere Availability Zones, um eine hohe Verfügbarkeit zu gewährleisten.

- Für die automatische Skalierung unterstützt Amazon EKS den Kubernetes Cluster Autoscaler und Karpenter.

Tools

AWS-Services

- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Komponententests ausführen und bereitstellungsbereite Artefakte erstellen können.
- AWS CodeCommit ist ein Versionskontrollservice, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodePipeline hilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.
- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen, Kubernetes auf AWS auszuführen, ohne Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten zu müssen.
- Amazon EC2 Auto Scaling hilft Ihnen dabei, die Anwendungsverfügbarkeit aufrechtzuerhalten, und ermöglicht es Ihnen, EC2 Amazon-Instances gemäß den von Ihnen definierten Bedingungen automatisch hinzuzufügen oder zu entfernen.
- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.

Andere Tools

- kubectl ist ein Kubernetes-Befehlszeilentool zum Ausführen von Befehlen für Kubernetes-Cluster. Sie können kubectl verwenden, um Anwendungen bereitzustellen, Clusterressourcen zu überprüfen und zu verwalten und Protokolle anzuzeigen.

Code

Der Code für dieses Muster ist im deploy-nth-to-eksRepo auf .com verfügbar. GitHub Das Code-Repo enthält die folgenden Dateien und Ordner.

- `nth folder`— Das Helm-Diagramm, die Wertedateien und die Skripts zum Scannen und Bereitstellen der CloudFormation AWS-Vorlage für Node Termination Handler.
- `config/config.json`— Die Konfigurationsparameterdatei für die Anwendung. Diese Datei enthält alle Parameter, die für die Bereitstellung von CDK erforderlich sind.
- `cdk`— AWS-CDK-Quellcode.
- `setup.sh`— Das Skript, das zur Bereitstellung der AWS-CDK-Anwendung verwendet wurde, um die erforderliche CI/CD-Pipeline und andere erforderliche Ressourcen zu erstellen.
- `uninstall.sh`— Das Skript, das zum Bereinigen der Ressourcen verwendet wurde.

Um den Beispielcode zu verwenden, folgen Sie den Anweisungen im Abschnitt Epics.

Bewährte Methoden

Bewährte Methoden für die Automatisierung von AWS Node Termination Handler finden Sie im Folgenden:

- EKS-Leitfäden mit bewährten Methoden
- Node Termination Handler — Konfiguration

Epen

So richten Sie Ihre Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repo.	Um das Repo mithilfe von SSH (Secure Shell) zu klonen, führen Sie den folgenden Befehl aus. `git clone git@github.com:aws-samples/deploy-nth-to-eks.git` Um das Repo mithilfe von HTTPS zu klonen, führen Sie den folgenden Befehl aus.	App-Entwickler, AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`git clone https://github.com/aws-samples/deploy-nth-to-eks.git`
	
	Beim Klonen des Repos wird ein Ordner mit dem Namen erstellt. `deploy-nth-to-eks`
	
	Wechseln Sie zu diesem Verzeichnis.
	
	`cd deploy-nth-to-eks`	

Stellen Sie die kubeconfig-Datei ein.	Geben Sie Ihre AWS-Anmeldeinformationen in Ihrem Terminal ein und bestätigen Sie, dass Sie berechtigt sind, die Cluster-Rolle zu übernehmen. Sie können den folgenden Beispielcode verwenden. `aws eks update-kubeconfig --name <Cluster_Name> --region <region>--role-arn <Role_ARN>`	AWS DevOps, DevOps Ingenieur, App-Entwickler

Stellen Sie die CI/CD-Pipeline bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Parameter ein.	Richten Sie in der `config/config.json` Datei die folgenden erforderlichen Parameter ein. • `pipelineName` : Der Name der CI/CD-Pipeline, die von AWS CDK erstellt werden soll (z. B.). `deploy-nth-to-eks-pipeline` AWS CodePipeline erstellt eine Pipeline mit diesem Namen. • `repositoryName` : Das CodeCommit AWS-Repo, das erstellt werden soll (zum Beispiel `deploy-nth-to-eks-repo`). AWS CDK erstellt dieses Repo und legt es als Quelle für die CI/CD-Pipeline fest. **Note** Diese Lösung erstellt dieses CodeCommit Repo und den Branch (im folgenden Branch-Parameter angegeben).	App-Entwickler, AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `branch`: Der Zweigname im Repo (zum Beispiel`main`). Ein Commit für diesen Branch initiiert die CI/CD-Pipeline. • `cfn_scan_script` : Der Pfad des Skripts, das verwendet wird, um die CloudFormation AWS-Vorlage nach NTH (`scan.sh`) zu scannen. Dieses Skript befindet sich in einem `nth` Ordner, der Teil des CodeCommit AWS-Repos sein wird. • `cfn_deploy_scrip t`: Der Pfad des Skripts, das zur Bereitstellung der CloudFormation AWS-Vorlage für NTH (`installAp p.sh`) verwendet wird. • `stackName` : Der Name des CloudFormation Stacks, der bereitgestellt werden soll. • `eksClusterName` : Der Name des vorhandenen EKS-Clusters. • `eksClusterRole` : Die IAM-Rolle, die für den Zugriff auf den EKS-Cluster für alle Kubernetes-API-Aufrufe verwendet wird (z. B.). `clusteradmin`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Normalerweise wird diese Rolle hinzugefügt. `aws-auth ConfigMap` • `create_cluster_role` : Um die `eksClusterRole` IAM-Rolle zu erstellen, geben Sie yes ein. Wenn Sie im `eksClusterRole` Parameter eine vorhandene Clusterrolle angeben möchten, geben Sie nein ein. • `create_iam_oidc_provider` : Geben Sie Ja ein, um den IAM-OIDC-Anbieter für Ihren Cluster zu erstellen. Wenn bereits ein IAM-OIDC-Anbieter existiert, geben Sie nein ein. Weitere Informationen finden Sie unter Einen IAM-OIDC-Anbieter für Ihren Cluster erstellen. • `AsgGroupName` : Eine durch Kommas getrennte Liste von Auto Scaling Scaling-Gruppennamen, die Teil des EKS-Clusters sind (z. B. `ASG_Group_1,ASG_Group_2`). • `region`: Der Name der AWS-Region, in der sich der Cluster befindet (z. B. `us-east-2`).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `install_cdk` : Wenn AWS CDK derzeit nicht auf dem Computer installiert ist, geben Sie Ja ein. Führen Sie den `cdk --version` Befehl aus, um zu überprüfen, ob die installierte AWS-CDK-Version 2.27.0 oder höher ist. Geben Sie in diesem Fall nein ein. Wenn Sie Ja eingeben, führt das Skript setup.sh den `sudo npm install -g cdk@2.27.0` Befehl zur Installation von AWS CDK auf dem Computer aus. Das Skript benötigt Sudo-Berechtigungen. Geben Sie daher das Kontopasswort ein, wenn Sie dazu aufgefordert werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die CI/CD-Pip eline für die Bereitstellung von NTH.	Führen Sie das Skript setup.sh aus. `./setup.sh` Das Skript stellt die AWS-CDK-Anwendung bereit, die das CodeCommit Repo mit Beispielcode, der Pipeline und CodeBuild Projekten auf der Grundlage der Benutzere ingabeparameter in `config/config.json` der Datei erstellt. Dieses Skript fragt bei der Installation von npm-Paket en mit dem Befehl sudo nach dem Passwort.	App-Entwickler, AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die CI/CD-Pipeline.	Öffnen Sie die AWS-Managementkonsole und überprüfen Sie die folgenden Ressourcen, die im Stack erstellt wurden. • CodeCommit Repo mit dem Inhalt des Ordners `nth` • CodeBuild AWS-Projektk`tcfn-scan`, das die CloudFormation Vorlage auf Sicherheitslücken scannt. • CodeBuild Projekt`Nth-Deploy` , das die CloudFormation AWS-Vorlage und die entsprechenden NTH Helm-Diagramme über die CodePipeline AWS-Pipeline bereitstellt. • Eine CodePipeline Pipeline zur Bereitstellung von NTH. Nachdem die Pipeline erfolgreich ausgeführt wurde, `aws-node-termination-handler` wird die Helm-Version im EKS-Cluster installiert. Außerdem `aws-node-termination-handler` läuft ein Pod mit dem Namen im `kube-system` Namespace im Cluster.	App-Entwickler, AWS DevOps, DevOps Ingenieur

Testen Sie die NTH-Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Simulieren Sie ein Auto Scaling-Gruppen-Scale-In-Ereignis.	Gehen Sie wie folgt vor, um ein automatisches Skalierungs-Scale-In-Ereignis zu simulieren: 1. Öffnen Sie auf der AWS-Konsole die EC2 Konsole und wählen Sie Auto Scaling Groups aus. 2. Wählen Sie die Auto Scaling Scaling-Gruppe aus, die denselben Namen wie die unter hat `config/config.json` , und klicken Sie auf Bearbeiten. 3. Verringern Sie die gewünschte Kapazität und die Mindestkapazität um 1. 4. Wählen Sie Aktualisieren.	
Überprüfen Sie die Protokolle.	Während des Scale-In-Ereignisses sperrt der NTH-Pod den entsprechenden Worker-Knoten ab und entleert ihn (die EC2 Instanz, die im Rahmen des Scale-In-Ereignisses beendet wird). Verwenden Sie den Code im Abschnitt Zusätzliche Informationen, um die Protokolle zu überprüfen.	App-Entwickler, AWS DevOps, DevOps Ingenieur

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen Sie alle AWS-Ressourcen.	Führen Sie den folgenden Befehl aus, um die nach diesem Muster erstellten Ressourcen zu bereinigen. `./uninstall.sh` Dadurch werden alle in diesem Muster erstellten Ressourcen bereinigt, indem der CloudFormation Stapel gelöscht wird.	DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Die NPM-Registrierung ist nicht richtig eingestellt.	Während der Installation dieser Lösung installiert das Skript npm install, um alle erforderlichen Pakete herunterzuladen. Wenn Sie während der Installation die Meldung „Modul kann nicht gefunden werden“ sehen, ist die npm-Registrierung möglicherweise nicht richtig eingerichtet. Führen Sie den folgenden Befehl aus, um die aktuelle Registrierungseinstellung zu sehen. `npm config get registry` Führen Sie den folgenden Befehl aus`https://registry.npmjs.org/`, um die Registrierung mit einzurichten.

Problem	Lösung
	`npm config set registry https://registry.npmjs.org`
Verzögern Sie die SQS-Nachrichtenzustellung.	Wenn Sie die SQS-Nachrichtenzustellung an den NTH Pod verzögern möchten, können Sie im Rahmen Ihrer Problembehandlung den Parameter für die Verzögerung der SQS-Zustellung anpassen. Weitere Informationen finden Sie unter Amazon SQS SQS-Verzögerungswarteschlangen.

Zugehörige Ressourcen

- Quellcode für den AWS Node Termination Handler
- EC2 Werkstatt
- AWS CodePipeline
- Amazon Elastic Kubernetes Service (Amazon EKS)
- AWS-Cloud-Entwicklungskit
- AWS CloudFormation

Zusätzliche Informationen

1. Suchen Sie den Namen des NTH-Pods.

```
kubectl get pods -n kube-system |grep aws-node-termination-handler
aws-node-termination-handler-65445555-kbqc7   1/1     Running   0          26m
kubectl get pods -n kube-system |grep aws-node-termination-handler
aws-node-termination-handler-65445555-kbqc7   1/1     Running   0          26m
```

2. Überprüfen Sie die Protokolle. Ein Beispielprotokoll sieht wie folgt aus. Es zeigt, dass der Knoten gesperrt und entleert wurde, bevor das Signal zum Abschluss des Auto Scaling Scaling-Gruppenlebenszyklus-Hooks gesendet wurde.

```
kubectl -n kube-system logs aws-node-termination-handler-65445555-kbqc7
```

```
022/07/17 20:20:43 INF Adding new event to the event store
 event={"AutoScalingGroupName":"eksctl-my-cluster-target-nodegroup-
ng-10d99c89-NodeGroup-ZME36IGAP7O1","Description":"ASG Lifecycle Termination
 event received. Instance will be interrupted at 2022-07-17 20:20:42.702
 +0000 UTC \n","EndTime":"0001-01-01T00:00:00Z","EventID":"asg-lifecycle-
term-33383831316538382d353564362d343332362d613931352d383430666165636334333564","InProgress":fal
east-2.compute.internal","NodeProcessed":false,"Pods":null,"ProviderID":"aws:///us-
east-2c/i-0409f2a9d3085b80e","StartTime":"2022-07-17T20:20:42.702Z","State":""}
2022/07/17 20:20:44 INF Requesting instance drain event-id=asg-lifecycle-
term-33383831316538382d353564362d343332362d613931352d383430666165636334333564
 instance-id=i-0409f2a9d3085b80e kind=SQS_TERMINATE node-name=ip-192-168-75-60.us-
east-2.compute.internal provider-id=aws:///us-east-2c/i-0409f2a9d3085b80e
2022/07/17 20:20:44 INF Pods on node node_name=ip-192-168-75-60.us-
east-2.compute.internal pod_names=["aws-node-qchsw","aws-node-termination-
handler-65445555-kbqc7","kube-proxy-mz5x5"]
2022/07/17 20:20:44 INF Draining the node
2022/07/17 20:20:44 ??? WARNING: ignoring DaemonSet-managed Pods: kube-system/aws-node-
qchsw, kube-system/kube-proxy-mz5x5
2022/07/17 20:20:44 INF Node successfully cordoned and drained
 node_name=ip-192-168-75-60.us-east-2.compute.internal reason="ASG Lifecycle
 Termination event received. Instance will be interrupted at 2022-07-17 20:20:42.702
 +0000 UTC \n"
2022/07/17 20:20:44 INF Completed ASG Lifecycle Hook (NTH-K8S-TERM-HOOK) for instance
 i-0409f2a9d3085b80e
```

Automatisches Erstellen und Bereitstellen einer Java-Anwendung auf Amazon EKS mithilfe einer CI/CD-Pipeline

Erstellt von MAHESH RAGHUNANDANAN (AWS), James Radtke (AWS) und Jomcy Pappachen (AWS)

Übersicht

Dieses Muster beschreibt, wie Sie eine CI/CD-Pipeline (Continuous Integration and Continuous Delivery) erstellen, die automatisch eine Java-Anwendung mit empfohlenen DevSecOps Vorgehensweisen für einen Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster auf dem erstellt und bereitstellt. AWS Cloud Dieses Muster verwendet eine Begrüßungsanwendung, die mit einem Spring Boot Java-Framework entwickelt wurde und Apache Maven verwendet.

Sie können den Ansatz dieses Musters verwenden, um den Code für eine Java-Anwendung zu erstellen, die Anwendungsartefakte als Docker-Image zu verpacken, das Image sicherheitstechnisch zu scannen und das Image als Workload-Container auf Amazon EKS hochzuladen. Der Ansatz dieses Musters ist nützlich, wenn Sie von einer eng gekoppelten monolithischen Architektur zu einer Microservices-Architektur migrieren möchten. Dieser Ansatz hilft Ihnen auch dabei, den gesamten Lebenszyklus einer Java-Anwendung zu überwachen und zu verwalten, wodurch ein höheres Maß an Automatisierung gewährleistet und Fehler oder Bugs vermieden werden können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto.
- AWS Command Line Interface (AWS CLI) Version 2, installiert und konfiguriert. Weitere Informationen dazu finden Sie AWS CLI in der AWS CLI Dokumentation unter Installation oder Aktualisierung auf die neueste Version von.

  AWS CLI Version 2 muss mit derselben AWS Identity and Access Management (IAM-) Rolle konfiguriert werden, die den Amazon EKS-Cluster erstellt, da nur diese Rolle berechtigt ist, dem weitere IAM-Rollen hinzuzufügen. `aws-auth` `ConfigMap` Informationen und Schritte zur Konfiguration AWS CLI finden Sie in der Dokumentation unter Einstellungen konfigurieren. AWS CLI
- IAM-Rollen und -Berechtigungen mit vollem Zugriff auf AWS CloudFormation. Weitere Informationen dazu finden Sie in der Dokumentation unter Steuern des Zugriffs mit IAM AWS CloudFormation .

- Ein vorhandener Amazon EKS-Cluster mit Details zum IAM-Rollennamen und zum Amazon-Ressourcennamen (ARN) der IAM-Rolle für Worker-Knoten im EKS-Cluster.
- Kubernetes Cluster Autoscaler, installiert und konfiguriert in Ihrem Amazon EKS-Cluster. Weitere Informationen finden Sie unter Skalieren von Cluster-Berechnungen mit Karpenter und Cluster Autoscaler in der Amazon EKS-Dokumentation.
- Zugriff auf Code im Repository. GitHub

> **Important**
>
> AWS Security Hub ist als Teil der AWS CloudFormation Vorlagen aktiviert, die im Code für dieses Muster enthalten sind. Standardmäßig wird Security Hub nach der Aktivierung mit einer kostenlosen 30-Tage-Testversion geliefert. Nach der Testphase fallen damit Kosten an. AWS-Service Weitere Informationen zu Preisen finden Sie unter AWS Security Hub Preise.

Produktversionen

- Helm-Version 3.4.2 oder höher
- Apache Maven Version 3.6.3 oder höher
- BridgeCrew Checkov Version 2.2 oder höher
- Aqua Security Trivy Version 0.37 oder höher

Architektur

Technologie-Stack

- AWS CodeBuild
- AWS CodeCommit

  Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen. Diese Lösung funktioniert jedoch mit jedem Git-Anbieter für Versionskontrollsysteme (VCS), z. B. GitHub oder GitLab mit minimalen Änderungen.
- Amazon CodeGuru
- AWS CodePipeline

- Amazon Elastic Container Registry (Amazon ECR)
- Amazon EKS
- Amazon EventBridge
- AWS Security Hub
- Amazon-Simple-Notification-Service (Amazon-SNS)

Zielarchitektur

Das Diagramm zeigt den folgenden Workflow:

1. Der Entwickler aktualisiert den Java-Anwendungscode im Basiszweig des CodeCommit Repositorys, wodurch eine Pull-Anfrage (PR) erstellt wird.
2. Sobald die PR eingereicht wurde, überprüft Amazon CodeGuru Reviewer den Code automatisch, analysiert ihn auf der Grundlage von Best Practices für Java und gibt dem Entwickler Empfehlungen.
3. Nachdem der PR mit dem Basiszweig zusammengeführt wurde, wird ein EventBridge Amazon-Event erstellt.
4. Das EventBridge Ereignis initiiert die CodePipeline Pipeline, die gestartet wird.
5. CodePipeline führt die CodeSecurity Scan-Phase aus (kontinuierliche Sicherheit).
6. AWS CodeBuild startet den Sicherheitsscan-Prozess, bei dem die Helm-Dateien für die Dockerfile- und Kubernetes-Bereitstellung mithilfe von Checkov gescannt werden und der Quellcode der Anwendung auf der Grundlage inkrementeller Codeänderungen gescannt wird. Der Anwendungsquellcodescan wird vom CodeGuru Reviewer Command Line Interface (CLI) - Wrapper durchgeführt.
7. Wenn die Sicherheitsscan-Phase erfolgreich ist, wird die Build-Phase (kontinuierliche Integration) eingeleitet.
8. In der CodeBuild Build-Phase erstellt das Artefakt, packt das Artefakt in ein Docker-Image, scannt das Image mithilfe von Aqua Security Trivy auf Sicherheitslücken und speichert das Image in Amazon ECR.
9. Die in Schritt 8 erkannten Sicherheitslücken werden zur weiteren Analyse durch Entwickler oder Techniker auf Security Hub hochgeladen. Security Hub bietet einen Überblick und Empfehlungen zur Behebung der Sicherheitslücken.

10 E-Mail-Benachrichtigungen über aufeinanderfolgende Phasen innerhalb der CodePipeline Pipeline werden über Amazon SNS gesendet.

11 Nachdem die Phasen der kontinuierlichen Integration abgeschlossen sind, CodePipeline beginnt die Bereitstellungsphase (kontinuierliche Bereitstellung).

12 Das Docker-Image wird mithilfe von Helm-Diagrammen als Container-Workload (Pod) in Amazon EKS bereitgestellt.

13 Der Anwendungs-Pod ist mit dem Amazon CodeGuru Profiler-Agent konfiguriert, der die Profilerstellungsdaten der Anwendung (CPU, Heap-Nutzung und Latenz) an CodeGuru Profiler sendet, sodass Entwickler das Verhalten der Anwendung besser verstehen können.

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend zu verwalten. AWS-Konten
- AWS CodeBuildist ein vollständig verwalteter Build-Service, der Ihnen hilft, Quellcode zu kompilieren, Komponententests durchzuführen und Artefakte zu erstellen, die sofort einsatzbereit sind.
- AWS CodeCommitist ein Versionskontrolldienst, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.

  Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen
- Amazon CodeGuru Profiler sammelt Laufzeitleistungsdaten aus Ihren Live-Anwendungen und gibt Empfehlungen, die Ihnen bei der Feinabstimmung Ihrer Anwendungsleistung helfen können.
- Amazon CodeGuru Reviewer verwendet Programmanalyse und maschinelles Lernen, um potenzielle Fehler zu erkennen, die für Entwickler schwer zu finden sind, und bietet Vorschläge zur Verbesserung Ihres Java- und Python-Codes.
- AWS CodePipelinehilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.

- Mit Amazon Elastic Kubernetes Service (Amazon EKS) können Sie Kubernetes ausführen, AWS ohne dass Sie Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten müssen.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, der Ihnen hilft, Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen zu verbinden, darunter AWS Lambda Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen. AWS-Konten
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Security Hubbietet einen umfassenden Überblick über Ihren Sicherheitsstatus. AWS Es hilft Ihnen auch dabei, Ihre AWS Umgebung anhand von Industriestandards und Best Practices im Bereich Sicherheit zu überprüfen.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere Dienste

- Helm ist ein Open-Source-Paketmanager für Kubernetes.
- Apache Maven ist ein Tool für die Verwaltung und Untersuchung von Softwareprojekten.
- BridgeCrew Checkov ist ein statisches Code-Analyse-Tool zum Scannen von IaC-Dateien (Infrastructure as Code) auf Fehlkonfigurationen, die zu Sicherheits- oder Compliance-Problemen führen können.
- Aqua Security Trivy ist ein umfassender Scanner für Sicherheitslücken in Container-Images, Dateisystemen und Git-Repositorys sowie für Konfigurationsprobleme.

Code

Der Code für dieses Muster ist im Repository verfügbar. GitHub aws-codepipeline-devsecops-amazoneks

Bewährte Methoden

- Dieses Muster folgt den bewährten IAM-Sicherheitsmethoden, um das Prinzip der geringsten Rechte für IAM-Entitäten in allen Phasen der Lösung anzuwenden. Wenn Sie die Lösung um zusätzliche Tools AWS-Services oder Tools von Drittanbietern erweitern möchten, empfehlen wir Ihnen, den Abschnitt zur Anwendung von Berechtigungen mit den geringsten Rechten in der IAM-Dokumentation zu lesen.
- Wenn Sie über mehrere Java-Anwendungen verfügen, empfehlen wir, für jede Anwendung separate CI/CD-Pipelines zu erstellen.
- Wenn Sie eine Monolith-Anwendung haben, empfehlen wir, die Anwendung nach Möglichkeit in Microservices aufzuteilen. Microservices sind flexibler, sie erleichtern die Bereitstellung von Anwendungen als Container und bieten einen besseren Einblick in den gesamten Aufbau und die Bereitstellung der Anwendung.

Epen

Richte die Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	Führen Sie den folgenden Befehl aus, um das Repository zu klonen. `git clone https://github.com/aws-samples/aws-codepipeline-devsecops-amazoneks`	App-Entwickler, DevOps Ingenieur
Erstellen Sie einen S3-Bucket und laden Sie den Code hoch.	1. Melden Sie sich bei der an AWS Management Console, öffnen Sie die Amazon S3 S3-Konsole und erstellen Sie dann einen S3-Bucket in AWS-Region dem Bereich, in dem Sie diese Lösung	AWS DevOps, Cloud-Administrator, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	bereitstellen möchten. Weitere Informationen finden Sie unter Bucket erstellen in der Amazon S3 S3-Dokumentation.
	2. Erstellen Sie im S3-Bucket einen Ordner mit dem Namen `code`.
	3. Navigieren Sie zu dem Ort, an dem Sie das Repository geklont haben. Führen Sie die folgenden Befehle nacheinander aus, um eine komprimierte Version des gesamten Codes mit der Erweiterung .zip (`cicdstack.zip`) zu erstellen und die ZIP-Datei zu überprüfen.
	`cd aws-codepipeline-devsecops-amazoneks`
	`python -m zipfile -c cicdstack.zip *`
	`python -m zipfile -t cicdstack.zip`
	Note
	Wenn der `python` Befehl fehlschlägt und angibt, dass Python nicht gefunden wurde, verwenden Sie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`python3` stattdessen. 4. Laden Sie die `cicdstack.zip` Datei in den Codeordner hoch, den Sie zuvor im S3-Bucket erstellt haben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen AWS CloudFormation Stack.	1. Öffnen Sie die AWS CloudFormation -Konsole und wählen Sie Create Stack (Stack erstellen) aus. 2. Wählen Sie unter Vorlage angeben die Option Eine Vorlagendatei hochladen aus, laden Sie die `cf_templates/codecommit_ecr.yaml` Datei hoch und klicken Sie dann auf Weiter. 3. Geben Sie im Feld Stackdetails angeben den Stack-Namen und anschließend die folgenden Eingabeparameterwerte ein: • `CodeCommitRepositoryBranchName` : Der Name der Filiale, in der sich Ihr Code befinden wird (die Standarde instellung ist`main`) • `CodeCommitRepositoryName` : Der Name des CodeCommitrepository zu erstellenden • `CodeCommitRepositoryS3Bucket` : Der Name des S3-Buckets, in dem Sie den Code-Ordner erstellt haben	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `CodeCommitRepositoryS3BucketObjKey` : `code/cicdstack.zip` • `ECRRepositoryName` : Der Name des zu erstellenden Amazon ECR-Repositorys 4. Wählen Sie Weiter, verwenden Sie die Standardeinstellungen für die Optionen „Stack konfigurieren“ und wählen Sie dann Weiter. 5. Überprüfen Sie im Abschnitt Überprüfen die Vorlagen- und Stack-Details und wählen Sie dann Stapel erstellen aus. Anschließend wird der Stack erstellt, einschließlich der Repositorys CodeCommit und der Amazon ECR Repositorys. 6. Notieren Sie sich die Namen der Repositorys CodeCommit und der Amazon ECR-Repositorys, die für die Einrichtung der Java CI/CD-Pipeline erforderlich sind.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die CloudFormation Stack-Bereitstellung.	1. Überprüfen Sie auf der CloudFormation Konsole unter Stacks den Status des CloudFormation Stacks, den Sie bereitgestellt haben. Der Status des Stacks sollte CREATE COMPLETE lauten. 2. Überprüfen Sie von der Konsole aus, ob die Repositorys CloudFormation und Amazon ECR bereitgestellt wurden und bereit sind.	AWS DevOps, DevOps Ingenieur
Löschen Sie den S3-Bucket.	Leeren und löschen Sie den S3-Bucket, den Sie zuvor erstellt haben. Weitere Informationen finden Sie unter Löschen eines Buckets in der Amazon S3 S3-Dokumentation.	AWS DevOps, DevOps Ingenieur

Konfigurieren Sie die Helm-Charts

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Helm-Charts Ihrer Java-Anwendung.	1. Navigieren Sie an dem Ort, an dem Sie das GitHub Repository geklont haben, zu dem Ordner`helm_charts/aws-proserve-java-greeting` . In diesem Ordner enthält	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	die `values.dev.yaml` Datei Informationen zur Konfiguration der Kubernetes-Ressourcen, die Sie für Ihre Container-Bereitstellungen in Amazon EKS ändern können. Aktualisieren Sie den Docker-Repository-Parameter, AWS-Region indem Sie Ihre AWS-Konto ID und den Namen des Amazon ECR-Repositorys angeben.
	`image:`
	`  repository:`
	`  <account-id>.dkr.ecr.<region>.amazonaws.com/<app-ecr-repo-name>`
	2. Der Servicetyp des Java-Pods ist auf eingestellt. `LoadBalancer`
	`service:`
	`  type: LoadBalancer`
	`  port: 80`
	`  targetPort: 8080`
	`  path: /hello`
	`  initialDelaySeconds: 60`
	`  periodSeconds: 30`
	Um einen anderen Dienst zu verwenden (z. B.`NodePort`), können Sie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	diesen Parameter ändern. Weitere Informationen finden Sie in der Kubernetes-Dokumentation.
	3. Sie können den Kubernetes Horizontal Pod Autoscaler aktivieren, indem Sie den Parameter auf ändern. `autoscaling enabled: true`
	`autoscaling:`
	`  enabled: true`
	`  minReplicas: 1`
	`  maxReplicas: 100`
	`  targetCPUUtilizationPercentage: 80`
	`  # targetMemoryUtilizationPercentage: 80`
	4. Sie können verschiedene Funktionen für die Kubernetes-Workloads aktivieren, indem Sie die Werte in der `values.<ENV>.yaml` Datei ändern, in der sich Ihre Entwicklungs-, Produktions-, UAT- oder QA-Umgebung `<ENV>` befindet.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie Helm-Diagramme auf Syntaxfehler.	1. Vergewissern Sie sich vom Terminal aus, dass Helm v3 auf Ihrer lokalen Workstation installiert ist, indem Sie den folgenden Befehl ausführen.
	`helm --version`
	Wenn Helm v3 nicht installiert ist, installieren Sie es.
	2. Navigieren Sie im Terminal zum Verzeichnis Helm Charts (`helm_charts/aws-proserve-java-greeting`) und führen Sie den folgenden Befehl aus.
	`helm lint . -f values.dev.yaml`
	Dadurch werden die Helm-Charts auf Syntaxfehler überprüft.
		DevOps Ingenieur

Richten Sie die Java CI/CD-Pipeline ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die CI/CD-Pipeline.	1. Öffnen Sie die AWS CloudFormation -Konsole	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und wählen Sie Create Stack (Stack erstellen) aus. 2. Wählen Sie unter Vorlage angeben die Option Eine Vorlagendatei hochladen aus, laden Sie die **`cf_templates/build_deployment.yaml`** Vorlage hoch und klicken Sie dann auf Weiter. 3. Geben Sie im Feld Stackdetails angeben den Stack-Namen und anschließend die folgenden Werte für die Eingabeparameter an: • `CodeBranchName` : Branch-Name des CodeCommit Repositorys, in dem sich Ihr Code befindet • `EKSClusterName` : Name Ihres EKS-Clusters (nicht die `EKSCluster` ID) • `EKSCodeBuildAppName` : Name der App Helm-Diagramm (`aws-proserve-java-greeting`) • `EKSWorkerNodeRoleARN` : ARN der IAM-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Rolle, die den Amazon EKS-Worker-Knoten zugewiesen ist • `EKSWorkerNodeRoleName` : Name der IAM-Rolle, die den Amazon EKS-Worker-Knoten zugewiesen ist • `EcrDockerRepository` : Name des Amazon ECR-Repositorys, in dem die Docker-Images Ihres Codes gespeichert werden • `EmailRecipient` : E-Mail-Adresse, an die Build-Benachrichtigungen gesendet werden sollen • `EnvType`: Umgebung (zum Beispiel dev, test oder prod) • `SourceRepoName` : Name des CodeCommit Repositorys, in dem sich Ihr Code befindet 4. Wählen Sie Weiter aus. Verwenden Sie die Standardeinstellungen unter Stack-Optionen konfiguri eren und wählen Sie dann Weiter. 5. Überprüfen Sie im Abschnitt Überprüfen die CloudForm	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ation Vorlagen- und Stack-Details und wählen Sie dann Weiter aus. 6. Wählen Sie Stack erstellen aus. 7. Während der CloudFormation Stack-Bereitstellung erhält der Besitzer der E-Mail-Adresse, die Sie in den Parametern angegeben haben, eine Nachricht, in der er aufgefordert wird, ein SNS-Thema zu abonnieren. Um Amazon SNS zu abonnieren, muss der Eigentümer den Link in der Nachricht auswählen. 8. Nachdem der Stack erstellt wurde, öffnen Sie die Registerkarte Outputs des Stacks und notieren Sie dann den ARN-Wert für den `EksCodeBuildkubeRoleARN` Ausgabeschlüssel. Dieser IAM-ARN-Wert wird später benötigt, wenn Sie der CodeBuild IAM-Rolle Berechtigungen zur Bereitstellung von Workloads im Amazon EKS-Cluster erteilen.	

Aktivieren Sie die Integration zwischen Security Hub und Aqua Security

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schalten Sie die Aqua Security-Integration ein.	Dieser Schritt ist erforderlich, um die von Trivy gemeldete n Ergebnisse der Docker-Image-Sicherheitslücke auf Security Hub hochzuladen. Da Security Hub Hub-Integ rationen AWS CloudForm ation nicht unterstützt werden, muss dieser Vorgang manuell durchgeführt werden. 1. Öffnen Sie die AWS Security Hub Konsole und navigieren Sie zu Integrati onen. 2. Suchen Sie nach Aqua Security und wählen Sie Aqua Security: Aqua Security aus. 3. Wählen Sie Ergebnisse akzeptieren.	AWS-Administrator, DevOps Ingenieur

Konfigurieren Sie CodeBuild die Konfiguration für die Ausführung von Helm- oder kubectl-Befehlen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
CodeBuild Erlaubt die Ausführung von Helm- oder kubectl-Befehlen im Amazon EKS-Cluster.	CodeBuild Um für die Verwendung von Helm oder `kubectl` Befehlen mit dem Amazon EKS-Cluster authentif iziert zu werden, müssen Sie die IAM-Rollen zum hinzufüge	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	n. `aws-auth ConfigMap` Fügen Sie in diesem Fall den ARN der IAM-Rolle hinzu. Dabei handelt es sich um die IAM-Rolle`EksCodeBu ildkubeRoleARN` , die für den CodeBuild Service erstellt wurde, um auf den Amazon EKS-Cluster zuzugreifen und Workloads darauf bereitzus tellen. Dies ist eine einmalige Aktivität. **Important** Das folgende Verfahren muss vor der Genehmigung der Bereitstellung abgeschlossen sein CodePipeline. 1. Öffnen Sie das `cf_templa tes/kube_aws_auth_ configmap_patch.sh` Shell-Skript in Ihrer Amazon Linux- oder macOS-Umgebung. 2. Authentifizieren Sie sich beim Amazon EKS-Cluster, indem Sie den folgenden Befehl ausführen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`aws eks --region <aws-region> update-kubeconfig --name <eks-cluster-name>`
	3. Führen Sie das Shell-Skript mit dem folgenden Befehl aus und ersetzen `<rolearn-eks-codebuild-kubectl>` Sie es durch den ARN-Wert `EksCodeBuildkubeRoleARN` , den Sie zuvor aufgezeichnet haben.
	`bash cf_templates/kube_aws_auth_configmap_patch.sh <rolearn-eks-codebuild-kubectl>`
	Der `aws_auth` `ConfigMap` ist konfiguriert und der Zugriff ist gewährt.	

Validieren Sie die CI/CD-Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die CI/CD-Pipeline automatisch initiiert wird.	1. Die CodeSecurity Scan-Phase in der Pipeline schlägt normalerweise fehl, wenn Checkov Schwachst	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ellen in den Dockerfile- oder Helm-Diagrammen entdeckt. Der Zweck dieses Beispiels besteht jedoch darin, einen Prozess zur Identifizierung potenziel ler Sicherheitslücken einzurichten, anstatt sie über die CI/CD-Pipeline zu beheben, was normalerw eise ein Prozess ist. DevSecOps In der Datei verwendet der `checkov` Befehl das `--soft-fa il` Flagbuildspec/ `buildspec_secscan .yaml` , um einen Pipeline-Ausfall zu vermeiden. `- echo -e "\n Running Dockerfile Scan" - checkov -f code/app/ Dockerfile --framewo rk dockerfile -- soft-fail --summary- position bottom - echo -e "\n Running Scan of Helm Chart files" - cp -pv helm_char ts/$EKS_CODEBUILD_ APP_NAME/values.de v.yaml helm_char ts/$EKS_CODEBUILD_ APP_NAME/values.ya ml - checkov -d helm_char ts/$EKS_CODEBUILD_`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>APP_NAME --framewo
	rk helm --soft-fail
	 --summary-position
	 bottom
	- rm -rfv helm_char
	ts/$EKS_CODEBUILD_
	APP_NAME/values.ya
	ml</pre>
	Damit die Pipeline fehlschlägt, wenn Sicherheitslücken in den Dockerfile- und Helm-Diagrammen gemeldet werden, muss die `--soft-fail` Option aus dem `checkov` Befehl entfernt werden. Entwickler oder Techniker können die Sicherheitslücken dann beheben und die Änderungen in das CodeCommit Quellcode-Repository übertragen.
	2. Ähnlich wie bei CodeSecurity Scan verwendet die Build-Phase Aqua Security Trivy, um Sicherheitslücken zu identifizieren `HIGH` und `CRITICAL` Docker-Images zu erstellen, bevor die Anwendung an Amazon ECR übertragen wird.
	<pre>- AWS_REGION=$AWS_DE
	FAULT_REGION
	 AWS_ACCOUNT_ID=$AW</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	S_ACCOUNT_ID trivy -d image --no-progress --ignore-unfixed --exit-code 0 --severity HIGH,CRITICAL --format template --template "@securityhub/asff.tpl" -o securityhub/report.asff $AWS_ACCOUNT_ID.dkr.ecr.$AWS_DEFAULT_REGION.amazonaws.com/$IMAGE_REPO_NAME:$CODEBUILD_RESOLVED_SOURCE_VERSION In diesem Beispiel schlägt die Pipeline nicht fehl, wenn Docker-Image-Schwachstellen gemeldet werden, weil der `trivy` Befehl in der `buildspec/buildspec.yml` Datei das Flag **`--exit-code 0`** mit dem Wert enthält. Damit die Pipeline ausfällt, wenn `HIGH CRTICAL` Sicherheitslücken gemeldet werden, ändern Sie den Wert `--exit-code` auf`1`. Entwickler oder Techniker können dann die Sicherheitslücken beheben und die Änderungen in das CodeCommit Quellcode-Repository übernehmen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Von Aqua Security Trivy gemeldete Docker-Image-Schwachstellen werden auf den Security Hub hochgeladen. Navigieren Sie auf der Security Hub Hub-Konsole zu Findings. Filtern Sie die Ergebnisse mit Datensatzstatus = Aktiv und Produkt = Aqua Security. Dies listet die Docker-Image-Schwachstellen in Security Hub auf. Es kann 15 Minuten bis eine Stunde dauern, bis Sicherheitslücken im Security Hub auftauchen. Weitere Informationen zum Starten der Pipeline mithilfe CodePipeline von finden Sie in der CodePipeline Dokumentation unter Eine Pipeline starten in CodePipeline, Manuelles Starten einer Pipeline und Starten einer Pipeline nach einem Zeitplan.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Genehmigen Sie die Bereitstellung.	1. Nach Abschluss der Erstellungsphase gibt es eine Genehmigungsstelle für die Bereitstellung. Der Prüfer oder ein Release-Manager sollte den Build überprüfen und ihn genehmigen, wenn alle Anforderungen erfüllt sind. Dies ist der empfohlene Ansatz für Teams, die Continuous Delivery für die Anwendungsbereitstellung verwenden. 2. Nach der Genehmigung leitet die Pipeline die Bereitstellungsphase ein. 3. Nachdem die Bereitstellungsphase erfolgreich war, enthält das CodeBuild Protokoll für diese Phase die URL der Anwendung. Verwenden Sie die URL, um zu überprüfen, ob die Anwendung bereit ist.	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Anwendungsprofilerstellung.	Nachdem die Bereitstellung abgeschlossen und der Anwendungs-Pod in Amazon EKS bereitgestellt wurde, versucht der in der Anwendung konfigurierte Amazon CodeGuru Profiler-Agent, Profilerstellungsdaten der Anwendung (CPU, Heap-Zusammenfassung, Latenz und Engpässe) an Profiler zu senden. CodeGuru Bei der ersten Bereitstellung einer Anwendung benötigt Profiler etwa 15 Minuten, um die CodeGuru Profilerstellungsdaten zu visualisieren.	AWS DevOps

Zugehörige Ressourcen

- AWS CodePipeline Dokumentation
- Bilder mit Trivy in einem AWS CodePipeline(AWS Blogbeitrag) scannen
- Verbesserung Ihrer Java-Anwendungen mit Amazon CodeGuru Profiler (AWS Blogbeitrag)
- AWS Syntax des Security Finding Format (ASFF)
- EventBridge Amazon-Ereignismuster
- Helm aufrüsten

Zusätzliche Informationen

- AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen. Diese

Lösung funktioniert auch mit jedem Git-Anbieter für Versionskontrollsysteme (VCS), z. B. GitHub oder GitLab mit minimalen Änderungen.

- CodeGuru Profiler sollte in Bezug auf die Funktionalität nicht mit dem AWS X-Ray Dienst verwechselt werden. Wir empfehlen Ihnen, CodeGuru Profiler zu verwenden, um die teuersten Codezeilen zu identifizieren, die zu Engpässen oder Sicherheitsproblemen führen könnten, und diese zu beheben, bevor sie zu einem potenziellen Risiko werden. Der X-Ray-Dienst dient der Überwachung der Anwendungsleistung.
- In diesem Muster sind die Ereignisregeln dem Standard-Event-Bus zugeordnet. Bei Bedarf können Sie das Muster erweitern, um einen benutzerdefinierten Event-Bus zu verwenden.
- Dieses Muster verwendet CodeGuru Reviewer als statisches Tool zum Testen der Anwendungssicherheit (SAST) für Anwendungscode. Sie können diese Pipeline auch für andere Tools wie SonarQube Checkmarx verwenden. Sie können die Anweisungen zur Einrichtung des Scans für jedes dieser Tools hinzufügen, `buildspec/buildspec_secscan.yaml` um die CodeGuru Scananweisungen zu ersetzen.

Erstellen Sie eine Amazon ECS-Aufgabendefinition und mounten Sie mithilfe von Amazon EFS ein Dateisystem auf EC2 Instances

Erstellt von Durga Prasad Cheepuri (AWS)

Übersicht

Dieses Muster enthält Codebeispiele und Schritte zum Erstellen einer Amazon Elastic Container Service (Amazon ECS) -Aufgabendefinition, die auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances in der Amazon Web Services (AWS) -Cloud ausgeführt wird, während Amazon Elastic File System (Amazon EFS) zum Mounten eines Dateisystems auf diesen EC2 Instances verwendet wird. Amazon ECS-Aufgaben, die Amazon EFS verwenden, mounten automatisch die Dateisysteme, die Sie in der Aufgabendefinition angeben, und stellen diese Dateisysteme den Containern der Aufgabe in allen Availability Zones in einer AWS-Region zur Verfügung.

Um Ihre Anforderungen an persistenten Speicher und gemeinsam genutzten Speicher zu erfüllen, können Sie Amazon ECS und Amazon EFS zusammen verwenden. Sie können Amazon EFS beispielsweise verwenden, um persistente Benutzerdaten und Anwendungsdaten für Ihre Anwendungen mit aktiven und Standby-ECS-Containerpaaren zu speichern, die in verschiedenen Availability Zones laufen, um eine hohe Verfügbarkeit zu gewährleisten. Sie können Amazon EFS auch verwenden, um gemeinsam genutzte Daten zu speichern, auf die parallel von ECS-Containern und verteilten Job-Workloads zugegriffen werden kann.

Um Amazon EFS mit Amazon ECS zu verwenden, können Sie einer Aufgabendefinition eine oder mehrere Volume-Definitionen hinzufügen. Eine Volume-Definition umfasst eine Amazon EFS-Dateisystem-ID, eine Zugriffspunkt-ID und eine Konfiguration für die AWS Identity and Access Management (IAM) -Autorisierung oder die Transport Layer Security (TLS) -Verschlüsselung bei der Übertragung. Sie können Containerdefinitionen innerhalb von Aufgabendefinitionen verwenden, um die Aufgabendefinitionsvolumes anzugeben, die bei der Ausführung des Containers bereitgestellt werden. Wenn eine Aufgabe ausgeführt wird, die ein Amazon EFS-Dateisystem verwendet, stellt Amazon ECS sicher, dass das Dateisystem bereitgestellt ist und für die Container verfügbar ist, die Zugriff darauf benötigen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

- Eine Virtual Private Cloud (VPC) mit einem Virtual Private Network (VPN) -Endpunkt oder einem Router
- (Empfohlen) Amazon ECS-Container-Agent 1.38.0 oder höher aus Gründen der Kompatibilität mit Amazon EFS-Zugriffspunkten und IAM-Autorisierungsfunktionen (Weitere Informationen finden Sie im AWS-Blogbeitrag Neu für Amazon EFS — IAM-Autorisierung und Zugriffspunkte.)

Einschränkungen

- Amazon ECS-Container-Agent-Versionen vor 1.35.0 unterstützen keine Amazon EFS-Dateisysteme für Aufgaben, die den EC2 Starttyp verwenden.

Architektur

Das folgende Diagramm zeigt ein Beispiel für eine Anwendung, die Amazon ECS verwendet, um eine Aufgabendefinition zu erstellen und ein Amazon EFS-Dateisystem auf EC2 Instances in ECS-Containern zu mounten.

Das Diagramm zeigt den folgenden Workflow:

1. Erstellen Sie ein Amazon EFS-Dateisystem.
2. Erstellen Sie eine Aufgabendefinition mit einem Container.
3. Konfigurieren Sie die Container-Instances für das Mounten des Amazon EFS-Dateisystems. Die Aufgabendefinition verweist auf die Volume-Mounts, sodass die Container-Instance das Amazon EFS-Dateisystem verwenden kann. ECS-Aufgaben haben Zugriff auf dasselbe Amazon EFS-Dateisystem, unabhängig davon, auf welcher Container-Instance diese Aufgaben erstellt werden.
4. Erstellen Sie einen Amazon ECS-Service mit drei Instanzen der Aufgabendefinition.

Technologie-Stack

- Amazon EC2
- Amazon ECS
- Amazon EFS

Tools

- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können Amazon verwenden EC2 , um so viele oder so wenige virtuelle Server zu starten, wie Sie benötigen, und Sie können nach oben oder unten skalieren.
- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service zum Ausführen, Stoppen und Verwalten von Containern in einem Cluster. Sie können Ihre Aufgaben und Services auf einer serverlosen Infrastruktur ausführen, die von AWS Fargate verwaltet wird. Um mehr Kontrolle über Ihre Infrastruktur zu erhalten, können Sie Ihre Aufgaben und Dienste alternativ auf einem Cluster von EC2 Instances ausführen, die Sie verwalten.
- Amazon EFS — Amazon Elastic File System (Amazon EFS) bietet ein einfaches, skalierbares, vollständig verwaltetes elastisches NFS-Dateisystem zur Verwendung mit AWS-Cloud-Services und lokalen Ressourcen.
- AWS CLI — Die AWS-Befehlszeilenschnittstelle (AWS CLI) ist ein Open-Source-Tool für die Interaktion mit AWS-Services über Befehle in Ihrer Befehlszeilen-Shell. Mit minimaler Konfiguration können Sie AWS-CLI-Befehle, die Funktionen implementieren, die denen entsprechen, die von der browserbasierten AWS-Managementkonsole bereitgestellt werden, von einer Befehlszeile aus ausführen.

Epen

Erstellen eines Amazon EFS-Dateisystems

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie mithilfe der AWS-Managementkonsole ein Amazon EFS-Dateisystem.	1. **Note** Erstellen Sie ein Amazon EFS-Dateisystem und wählen Sie die VPC aus, die Ihre Container enthält. : Wenn Sie eine andere VPC verwenden, richten	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie eine VPC-Peering-Verbindung ein. 2. Notieren Sie sich die File system ID (Dateisystem-ID).	

Erstellen Sie eine Amazon ECS-Aufgabendefinition, indem Sie entweder ein Amazon EFS-Dateisystem oder die AWS-CLI CLI

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Aufgabendefinition mit einem Amazon EFS-Dateisystem.	Erstellen Sie eine Aufgabendefinition mithilfe der neuen Amazon ECS-Konsole oder der klassischen Amazon ECS-Konsole mit den folgenden Konfigurationen: • Wenn Sie die neue Konsole verwenden, wählen Sie Amazon EC2 Instances for App environment. Wenn Sie die klassische Konsole verwenden, wählen Sie EC2als Starttyp. • Fügen Sie ein Volumen hinzu. Geben Sie einen Namen für das Volume ein, wählen Sie EFS als Volumetyp und wählen Sie dann die Dateisystem-ID, die Sie zuvor notiert haben. Wählen Sie für das Stammverzeichnis	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den Amazon EFS-Datei systempfad, den Sie auf dem Amazon ECS-Conta iner-Host hosten möchten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie mit der AWS-CLI eine Aufgabendefinition.	1. Führen Sie den folgenden Befehl aus, um eine JSON-Vorlage mit Platzhaltern für Eingabeparameter für Ihre Aufgabendefinition zu erstellen:
	`aws ecs register-task-definition --generate-cli-skeleton`
	2. Führen Sie den folgenden Befehl aus, um die Aufgabendefinition mit der JSON-Vorlage zu erstellen:
	`aws ecs register-task-definition --cli-input-json file://<path_to_your_json_file>`
	3. **Note**
	Geben Sie die Eingabeparameter in Ihre JSON-Vorlage ein, die auf der `task_definition_parameters.json` Datei (angehängt) basieren. : Weitere Informationen zu Eingabeparametern finden Sie
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	unter Aufgabendefinitionsparameter (Amazon ECS-Dokumentation) und register-task-definition(AWS CLI Command Reference).	

Zugehörige Ressourcen

- Amazon ECS-Aufgabendefinitionen
- Amazon EFS-Volumes

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Stellen Sie Lambda-Funktionen mit Container-Images bereit

Erstellt von Ram Kandaswamy (AWS)

Übersicht

AWS Lambda unterstützt Container-Images als Bereitstellungsmodell. Dieses Muster zeigt, wie Lambda-Funktionen über Container-Images bereitgestellt werden.

Lambda ist ein serverloser, ereignisgesteuerter Rechendienst, mit dem Sie Code für praktisch jede Art von Anwendung oder Backend-Service ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Mit der Container-Image-Unterstützung für Lambda-Funktionen profitieren Sie von bis zu 10 GB Speicherplatz für Ihr Anwendungsartefakt und können vertraute Container-Image-Entwicklungstools verwenden.

Das Beispiel in diesem Muster verwendet Python als zugrunde liegende Programmiersprache, aber Sie können auch andere Sprachen wie Java, Node.js oder Go verwenden. Ziehen Sie als Quelle ein Git-basiertes System wie GitHub,, oder Bitbucket in Betracht GitLab, oder verwenden Sie Amazon Simple Storage Service (Amazon S3).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Amazon Elastic Container Registry (Amazon ECR) aktiviert
- Anwendungscode
- Docker-Images mit dem Runtime-Interface-Client und der neuesten Version von Python
- Grundkenntnisse in Git

Einschränkungen

- Die maximal unterstützte Bildgröße beträgt 10 GB.
- Die maximale Laufzeit für eine Lambda-basierte Container-Bereitstellung beträgt 15 Minuten.

Architektur

Zielarchitektur

1. Sie erstellen ein Git-Repository und übertragen den Anwendungscode in das Repository.
2. Das AWS CodeBuild Projekt wird durch Commit-Änderungen ausgelöst.
3. Das CodeBuild Projekt erstellt das Docker-Image und veröffentlicht das erstellte Image in Amazon ECR.
4. Sie erstellen die Lambda-Funktion mithilfe des Images in Amazon ECR.

Automatisierung und Skalierung

Dieses Muster kann mithilfe von AWS CloudFormation AWS Cloud Development Kit (AWS CDK), oder API-Operationen aus einem SDK automatisiert werden. Lambda kann automatisch auf der Grundlage der Anzahl der Anfragen skaliert werden, und Sie können es mithilfe der Parallelitätsparameter optimieren. Weitere Informationen finden Sie in der Lambda-Dokumentation.

Tools

AWS-Services

- AWS CloudFormationMit AWS richten CloudFormationhelps Sie AWS Ressourcen ein, stellen sie schnell und konsistent bereit und verwalten sie während ihres gesamten Lebenszyklus über AWS-Konten und AWS-Regionen. Dieses Muster verwendet AWS CloudFormation Application Composer, mit dem Sie AWS CloudFormation Vorlagen visuell anzeigen und bearbeiten können.
- AWS CodeBuildist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Komponententests ausführen und bereitstellungsbereite Artefakte erstellen können.
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.

Andere Tools

- Docker ist eine Reihe von Platform-as-a-Service (PaaS) -Produkten, die Virtualisierung auf Betriebssystemebene nutzen, um Software in Containern bereitzustellen.
- GitHub, GitLab, und Bitbucket sind einige der am häufigsten verwendeten Git-basierten Quellcodeverwaltungssysteme, um Quellcodeänderungen zu verfolgen.

Bewährte Methoden

- Mache deine Funktion so effizient und klein wie möglich, um zu vermeiden, dass unnötige Dateien geladen werden.
- Bemühen Sie sich, statische Ebenen in Ihrer Docker-Dateiliste weiter oben zu platzieren, und platzieren Sie Ebenen, die sich häufiger ändern, weiter unten. Dadurch wird das Caching verbessert, was die Leistung verbessert.
- Der Image-Besitzer ist für die Aktualisierung und das Patchen des Images verantwortlich. Fügen Sie diesen Aktualisierungsrhythmus zu Ihren betrieblichen Abläufen hinzu. Weitere Informationen finden Sie in der AWS Lambda -Dokumentation.

Epen

Erstellen Sie ein Projekt in CodeBuild

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Git-Repos itory.	Erstellen Sie ein Git-Repos itory, das den Quellcode der Anwendung, das Dockerfile und die `buildspec.yaml` Datei enthält.	Developer
Erstellen Sie ein Projekt CodeBuild .	Gehen Sie wie folgt vor, um ein CodeBuild Projekt zum Erstellen des benutzerd efinierten Lambda-Images zu verwenden: 1. Melden Sie sich bei AWS Management Console https://console.aw s.amazon.com/codesuite/ codebuild/ an und öffnen Sie die CodeBuild Konsole. 2. Erstellt ein neues Projekt. Wählen Sie als Quelle das	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Git-Repository aus, das Sie erstellt haben. Informationen zu den verschiedenen Arten der Git-Repository-Integration finden Sie in der Dokumentation Arbeiten mit Verbindungen. 3. Vergewissern Sie sich, dass der privilegierte Modus aktiviert ist. Um Docker-Images zu erstellen, ist dies erforderlich. Andernfalls wird das Image nicht erfolgreich erstellt. 4. Geben Sie Werte für den Projektnamen und die Beschreibung an.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bearbeiten Sie das Dockerfile.	Das Dockerfile sollte sich im Verzeichnis der obersten Ebene befinden, in dem Sie die Anwendung entwickeln. Der Python-Code sollte sich im `src` Ordner befinden. Verwenden Sie bei der Erstellung des Images die offiziellen von Lambda unterstützten Images. Andernfalls tritt ein Bootstrap-Fehler auf, der den Packvorga ng erschwert. Einzelheiten finden Sie im Abschnitt Zusätzliche Informati onen.	Developer
Erstellen Sie ein Repository in Amazon ECR.	Erstellen Sie ein Container-Repository in Amazon ECR. Im folgenden Beispielbefehl lautet der Name des erstellten Repositorys: `cf-demo` `aws ecr create-re pository --cf-demo` Das Repository wird in der `buildspec.yaml` Datei referenziert.	AWS-Administrator, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verschieben Sie das Image zu Amazon ECR.	Sie können es verwenden CodeBuild , um den Image-Build-Prozess durchzufü hren. CodeBuild benötigt die Erlaubnis, mit Amazon ECR zu interagieren und mit S3 zu arbeiten. Im Rahmen des Prozesses wird das Docker-Im age erstellt und in die Amazon ECR-Registrierung übertrage n. Einzelheiten zur Vorlage und zum Code finden Sie im Abschnitt Zusätzliche Informati onen.	Developer
Stellen Sie sicher, dass sich das Bild im Repository befindet.	Um zu überprüfen, ob sich das Bild im Repository befindet, wählen Sie in der Amazon ECR-Konsole Repositories aus. Das Bild sollte mit Tags und den Ergebnissen eines Schwachstellenscanberichts aufgeführt werden, wenn diese Funktion in den Amazon ECR-Einstellungen aktiviert war. Weitere Informationen finden Sie in der AWS-Dokum entation.	Developer

Erstellen Sie die Lambda-Funktion, um das Image auszuführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
So erstellen Sie die Lambda-Funktion:	Wählen Sie in der Lambda-Konsole Create function und dann Container image aus. Geben Sie den Funktionsnamen und die URI für das Bild ein, das sich im Amazon ECR-Repository befindet, und wählen Sie dann Funktion erstellen. Weitere Informationen finden Sie in der AWS Lambda Lambda-Dokumentation.	App-Developer
Testen Sie die Lambda-Funktion.	Um die Funktion aufzurufen und zu testen, wählen Sie Test. Weitere Informationen finden Sie in der AWS Lambda Lambda-Dokumentation.	App-Developer

Fehlerbehebung

Problem	Lösung
Der Build ist nicht erfolgreich.	1. Überprüfen Sie, ob der privilegierte Modus für das CodeBuild Projekt aktiviert ist. 2. Stellen Sie sicher, dass die Docker-bezogenen Befehle über die erforderlichen Berechtigungen verfügen. Es wird versuchtsudo, die Befehle zu erweitern. 3. Stellen Sie sicher, dass die zugeordnete IAM-Rolle CodeBuild über eine Richtlinie mit geeigneten Aktionen für die Interaktion mit

Problem	Lösung
	Amazon ECR, Amazon S3 und CloudWatch Protokollen verfügt.

Zugehörige Ressourcen

- Basisbilder für Lambda
- Docker-Beispiel für CodeBuild
- Übergeben Sie temporäre Anmeldeinformationen

Zusätzliche Informationen

Bearbeiten Sie das Dockerfile

Der folgende Code zeigt die Befehle, die Sie im Dockerfile bearbeiten:

```
FROM public.ecr.aws/lambda/python:3.xx

# Copy function code
COPY app.py ${LAMBDA_TASK_ROOT}
COPY requirements.txt  ${LAMBDA_TASK_ROOT}

# install dependencies
RUN pip3 install --user -r requirements.txt

# Set the CMD to your handler (could also be done as a parameter override outside of
 the Dockerfile)
CMD [ "app.lambda_handler" ]
```

Verwenden Sie im `FROM` Befehl den entsprechenden Wert für die Python-Version, die von Lambda unterstützt wird (z. B. `3.12`). Dies wird das Basis-Image sein, das im öffentlichen Amazon ECR-Image-Repository verfügbar ist.

Der `COPY app.py ${LAMBDA_TASK_ROOT}` Befehl kopiert den Code in das Stammverzeichnis der Aufgabe, das von der Lambda-Funktion verwendet wird. Dieser Befehl verwendet die Umgebungsvariable, sodass wir uns keine Gedanken über den tatsächlichen Pfad machen müssen. Die auszuführende Funktion wird als Argument an den `CMD [ "app.lambda_handler" ]` Befehl übergeben.

Der `COPY requirements.txt` Befehl erfasst die für den Code erforderlichen Abhängigkeiten.

Der `RUN pip install --user -r requirements.txt` Befehl installiert die Abhängigkeiten im lokalen Benutzerverzeichnis.

Führen Sie den folgenden Befehl aus, um Ihr Image zu erstellen.

```
docker build -t <image name> .
```

Fügen Sie das Bild in Amazon ECR hinzu

Ersetzen Sie den Code im folgenden Code `aws_account_id` durch die Kontonummer und ersetzen Sie ihn, `us-east-1` wenn Sie eine andere Region verwenden. Die `buildspec` Datei verwendet die CodeBuild Buildnummer, um Image-Versionen eindeutig als Tag-Wert zu identifizieren. Sie können dies an Ihre Anforderungen anpassen.

Der benutzerdefinierte Buildspec-Code

```
phases:
  install:
    runtime-versions:
       python: 3.xx
  pre_build:
    commands:
      - python3 --version
      - pip3 install --upgrade pip
      - pip3 install --upgrade awscli
      - sudo docker info
  build:
    commands:
      - echo Build started on `date`
      - echo Building the Docker image...
      - ls
      - cd app
      - docker build -t cf-demo:$CODEBUILD_BUILD_NUMBER .
      - docker container ls
  post_build:
    commands:
      - echo Build completed on `date`
      - echo Pushing the Docker image...
      - aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin aws_account_id.dkr.ecr.us-east-1.amazonaws.com
```

```
      - docker tag cf-demo:$CODEBUILD_BUILD_NUMBER aws_account_id.dkr.ecr.us-
east-1.amazonaws.com/cf-demo:$CODEBUILD_BUILD_NUMBER
      - docker push aws_account_id.dkr.ecr.us-east-1.amazonaws.com/cf-demo:
$CODEBUILD_BUILD_NUMBER
```

Bereitstellen von Java-Microservices auf Amazon ECS mithilfe von AWS Fargate

Erstellt von Vijay Thompson (AWS) und Sandeep Bondugula (AWS)

Übersicht

Dieses Muster bietet Anleitungen für die Bereitstellung containerisierter Java-Mikroservices auf Amazon Elastic Container Service (Amazon ECS) mithilfe von AWS Fargate. Das Muster verwendet Amazon Elastic Container Registry (Amazon ECR) nicht für die Containerverwaltung. Stattdessen werden Docker-Images von einem Docker-Hub abgerufen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine bestehende Java-Microservices-Anwendung auf einem Docker-Hub
- Ein öffentliches Docker-Repository
- Ein aktives AWS-Konto
- Vertrautheit mit AWS-Services, einschließlich Amazon ECS und Fargate
- Docker-, Java- und Spring Boot-Framework
- Amazon Relational Database Service (Amazon RDS) ist betriebsbereit (optional)
- Eine virtuelle private Cloud (VPC), wenn für die Anwendung Amazon RDS erforderlich ist (optional)

Architektur

Quelltechnologie-Stack

- Java-Mikroservices (z. B. in Spring Boot implementiert) und auf Docker bereitgestellt

Quellarchitektur

Zieltechnologie-Stack

- Ein Amazon ECS-Cluster, der jeden Microservice mithilfe von Fargate hostet

- Ein VPC-Netzwerk zum Hosten des Amazon ECS-Clusters und der zugehörigen Sicherheitsgruppen
- Eine Cluster-/Aufgabendefinition für jeden Microservice, der Container mithilfe von Fargate hochfährt

Zielarchitektur

Tools

Tools

- Amazon ECS macht es überflüssig, Ihre eigene Container-Orchestrierungssoftware zu installieren und zu betreiben, einen Cluster von virtuellen Maschinen zu verwalten und zu skalieren oder Container auf diesen virtuellen Maschinen zu planen.
- Mit AWS Fargate können Sie Container ausführen, ohne Server oder Amazon Elastic Compute Cloud (Amazon EC2) -Instances verwalten zu müssen. Es wird in Verbindung mit Amazon Elastic Container Service (Amazon ECS) verwendet.
- Docker ist eine Softwareplattform, mit der Sie Anwendungen schnell erstellen, testen und bereitstellen können. Docker packt Software in standardisierte Einheiten, sogenannte Container, die alles enthalten, was die Software zum Ausführen benötigt, einschließlich Bibliotheken, Systemtools, Code und Laufzeit.

Docker-Code

Das folgende Dockerfile gibt die verwendete Version des Java Development Kit (JDK) an, in der die Java-Archivdatei (JAR) vorhanden ist, die Portnummer, die verfügbar gemacht wird, und den Einstiegspunkt für die Anwendung.

```
FROM openjdk:11
ADD target/Spring-docker.jar Spring-docker.jar
EXPOSE 8080
ENTRYPOINT ["java","-jar","Spring-docker.jar"]
```

Epen

Neue Aufgabendefinitionen erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Aufgabend efinition.	Für die Ausführung eines Docker-Containers in Amazon ECS ist eine Aufgabend efinition erforderlich. Öffnen Sie die Amazon ECS-Konso le unter https://console.a ws.amazon.com/ecs/, wählen Sie Aufgabendefinitionen und erstellen Sie dann eine neue Aufgabendefinition. Weitere Informationen finden Sie in der Amazon ECS-Dokumentation.	AWS-Systemadministrator, App-Entwickler
Wählen Sie den Starttyp.	Wählen Sie Fargate als Starttyp.	AWS-Systemadministrator, App-Entwickler
Konfigurieren Sie die Aufgabe.	Definieren Sie einen Aufgabennamen und konfiguri eren Sie die Anwendung mit der entsprechenden Menge an Aufgabenspeicher und CPU.	AWS-Systemadministrator, App-Entwickler
Definieren Sie den Container.	Geben Sie den Namen des Containers an. Geben Sie für das Image den Namen der Docker-Site, den Repositor y-Namen und den Tag-Namen des Docker-Images ein ()`docker.io/sample-repo/sample-application:sample-tag-name` . Legen Sie Speicherl	AWS-Systemadministrator, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	imits für die Anwendung und Portzuordnungen (`8080, 80`) für die zulässigen Ports fest.	
Erstellen Sie die Aufgabe.	Wenn die Aufgaben- und Containerkonfigurationen vorhanden sind, erstellen Sie die Aufgabe. Detaillierte Anweisungen finden Sie unter den Links im Abschnitt Verwandte Ressourcen.	AWS-Systemadministrator, App-Entwickler

Konfigurieren Sie den Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und konfigurieren Sie einen Cluster.	Wählen Sie als Clustertyp nur Networking aus, konfigurieren Sie den Namen und erstellen Sie dann den Cluster oder verwenden Sie einen vorhandenen Cluster, falls verfügbar. Weitere Informationen finden Sie in der Amazon ECS-Dokumentation.	AWS-Systemadministrator, App-Entwickler

Aufgabe konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Aufgabe.	Wählen Sie im Cluster die Option Neue Aufgabe ausführen aus.	AWS-Systemadministrator, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie den Starttyp.	Wählen Sie Fargate als Starttyp.	AWS-Systemadministrator, App-Entwickler
Wählen Sie Aufgabendefinition, Revision und Plattformversion.	Wählen Sie die Aufgabe, die Sie ausführen möchten, die Version der Aufgabendefinition und die Plattformversion aus.	AWS-Systemadministrator, App-Entwickler
Wählen Sie den -Cluster.	Wählen Sie den Cluster aus, von dem aus Sie die Aufgabe ausführen möchten.	AWS-Systemadministrator, App-Entwickler
Geben Sie die Anzahl der Aufgaben an.	Konfigurieren Sie die Anzahl der Aufgaben, die ausgeführt werden sollen. Wenn Sie mit zwei oder mehr Aufgaben starten, ist ein Load Balancer erforderlich, um den Datenverkehr auf die Aufgaben zu verteilen.	AWS-Systemadministrator, App-Entwickler
Geben Sie die Aufgabengruppe an.	(Optional) Geben Sie einen Aufgabengruppennamen an, um eine Gruppe verwandter Aufgaben als Aufgabengruppe zu identifizieren.	AWS-Systemadministrator, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Cluster-VPC, die Subnetze und die Sicherheitsgruppen.	Konfigurieren Sie die Cluster-VPC und die Subnetze, in denen Sie die Anwendung bereitstellen möchten. Erstellen oder aktualisieren Sie Sicherheitsgruppen (HTTP, HTTPS und Port 8080), um den Zugriff auf eingehende und ausgehende Verbindungen zu ermöglichen.	AWS-Systemadministrator, App-Entwickler
Konfigurieren Sie öffentliche IP-Einstellungen.	Aktivieren oder deaktivieren Sie die öffentliche IP, je nachdem, ob Sie eine öffentliche IP-Adresse für Fargate-Aufgaben verwenden möchten. Die empfohlene Standardoption ist Aktiviert.	AWS-Systemadministrator, App-Entwickler
Überprüfen Sie die Einstellungen und erstellen Sie die Aufgabe	Überprüfen Sie Ihre Einstellungen und wählen Sie dann Task ausführen.	AWS-Systemadministrator, App-Entwickler

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopieren Sie die Anwendungs-URL.	Wenn der Aufgabenstatus auf Wird ausgeführt aktualisiert wurde, wählen Sie die Aufgabe aus. Kopieren Sie im Bereich Netzwerk die öffentliche IP.	AWS-Systemadministrator, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie Ihre Anwendung.	Geben Sie in Ihrem Browser die öffentliche IP ein, um die Anwendung zu testen.	AWS-Systemadministrator, App-Entwickler

Zugehörige Ressourcen

- Docker-Grundlagen für Amazon ECS (Amazon ECS-Dokumentation)
- Amazon ECS auf AWS Fargate (Amazon ECS-Dokumentation)
- Eine Aufgabendefinition erstellen (Amazon ECS-Dokumentation)
- Einen Cluster erstellen (Amazon ECS-Dokumentation)
- Konfiguration grundlegender Serviceparameter (Amazon ECS-Dokumentation)
- Konfiguration eines Netzwerks (Amazon ECS-Dokumentation)
- Bereitstellung von Java-Microservices auf Amazon ECS (Blogbeitrag)

Stellen Sie Kubernetes-Ressourcen und -Pakete mithilfe von Amazon EKS und einem Helm-Chart-Repository in Amazon S3 bereit

Erstellt von Sagar Panigrahi (AWS)

Übersicht

Dieses Muster hilft Ihnen, Kubernetes-Anwendungen unabhängig von ihrer Komplexität effizient zu verwalten. Das Muster integriert Helm in Ihre bestehenden CI/CD-Pipelines (Continuous Integration and Continuous Delivery), um Anwendungen in einem Kubernetes-Cluster bereitzustellen. Helm ist ein Kubernetes-Paketmanager, der Sie bei der Verwaltung von Kubernetes-Anwendungen unterstützt. Helm-Diagramme helfen bei der Definition, Installation und Aktualisierung komplexer Kubernetes-Anwendungen. Diagramme können versioniert und in Helm-Repositorys gespeichert werden, wodurch die mittlere Wiederherstellungszeit (MTTR) bei Ausfällen verbessert wird.

Dieses Muster verwendet Amazon Elastic Kubernetes Service (Amazon EKS) für den Kubernetes-Cluster. Es verwendet Amazon Simple Storage Service (Amazon S3) als Helm-Diagramm-Repository, sodass die Diagramme zentral verwaltet und von Entwicklern im gesamten Unternehmen abgerufen werden können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS) -Konto mit einer Virtual Private Cloud (VPC)
- Ein Amazon EKS-Cluster
- Worker-Knoten, die innerhalb des Amazon EKS-Clusters eingerichtet sind und bereit sind, Workloads aufzunehmen
- Kubectl für die Konfiguration der Amazon EKS kubeconfig-Datei für den Zielcluster auf dem Client-Computer
- Zugriff auf AWS Identity and Access Management (IAM) zur Erstellung des S3-Buckets
- IAM-Zugriff (programmatischer oder Rollenzugriff) auf Amazon S3 vom Client-Computer
- Quellcodeverwaltung und eine CI/CD-Pipeline

Einschränkungen

- Derzeit wird das Aktualisieren, Löschen oder Verwalten von benutzerdefinierten Ressourcendefinitionen () CRDs nicht unterstützt.
- Wenn Sie eine Ressource verwenden, die auf eine CRD verweist, muss die CRD separat installiert werden (außerhalb des Diagramms).

Produktversionen

- Helm v3.6.3

Architektur

Zieltechnologie-Stack

- Amazon EKS
- Amazon VPC
- Amazon S3
- Verwaltung des Quellcodes
- Helm
- Kubectl

Zielarchitektur

Automatisierung und Skalierung

- AWS CloudFormation kann verwendet werden, um die Erstellung der Infrastruktur zu automatisieren. Weitere Informationen finden Sie unter Erstellen von Amazon EKS-Ressourcen mit AWS CloudFormation in der Amazon EKS-Dokumentation.
- Helm soll in Ihr vorhandenes CI/CD-Automatisierungstool integriert werden, um die Paketierung und Versionierung von Helm-Diagrammen zu automatisieren (außerhalb des Geltungsbereichs dieses Musters).
- GitVersion oder Jenkins-Build-Nummern können verwendet werden, um die Versionierung von Diagrammen zu automatisieren.

Tools

Tools

- Amazon EKS — Amazon Elastic Kubernetes Service (Amazon EKS) ist ein verwalteter Service für die Ausführung von Kubernetes auf AWS, ohne dass Sie Ihre eigene Kubernetes-Steuerebene einrichten oder verwalten müssen. Kubernetes ist ein Open-Source-System zur Automatisierung der Bereitstellung, Skalierung und Verwaltung von Anwendungen in Containern.
- Helm — Helm ist ein Paketmanager für Kubernetes, der Sie bei der Installation und Verwaltung von Anwendungen auf Ihrem Kubernetes-Cluster unterstützt.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist Speicher für das Internet. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen.
- Kubectl — Kubectl ist ein Befehlszeilenprogramm zum Ausführen von Befehlen für Kubernetes-Cluster.

Code

Der Beispielcode ist angehängt.

Epen

Helm konfigurieren und initialisieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den Helm-Client.	Verwenden Sie den folgenden Befehl, um den Helm-Client herunterzuladen und auf Ihrem lokalen System zu installieren. `sudo curl https://raw.githubusercontent.com/helm/helm/master/scripts/get-helm-3 | bash`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Helm-Installation.	Um zu überprüfen, ob Helm mit dem Kubernetes-API-Server innerhalb des Amazon EKS-Clusters kommunizieren kann, führen Sie folgenden Befehl aus. `helm version`	DevOps Ingenieur

Erstellen und installieren Sie ein Helm-Diagramm im Amazon EKS-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Helm-Diagramm für NGINX.	Führen Sie den Befehl aus, um ein Helmdiagramm mit dem Namen `my-nginx` auf dem Client-Computer zu erstellen. `helm create my-nginx`	DevOps Ingenieur
Überprüfen Sie die Struktur des Diagramms.	Um die Struktur des Diagramms zu überprüfen, führen Sie den Befehl tree aus`tree my-nginx/` .	DevOps Ingenieur
Deaktivieren Sie die Erstellung eines Dienstkontos im Diagramm.	Stellen Sie unter dem `serviceAccount` Abschnitt den `create` Schlüssel auf ein`false`. `values.yaml` Dies ist deaktiviert, da für dieses Muster kein Dienstkonto erstellt werden muss.	DevOps Ingenieur
Überprüfe (linte) das geänderte Diagramm auf syntaktische Fehler.	Führen Sie den folgenden Befehl aus, um das Diagramm vor der Installation im Zielcluster auf syntaktische Fehler zu	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	überprüfen. `helm lint my-nginx/`	
Installieren Sie das Diagramm, um Kubernetes-Ressourcen bereitzustellen.	Verwenden Sie den folgenden Befehl, um die Helm-Chart-Installation auszuführen. `helm install --name my-nginx-release --debug my-nginx/ --namespace helm-space` Das optionale `debug` Flag gibt alle Debug-Meldungen während der Installation aus. Das `namespace` Flag gibt den Namespace an, in dem der Ressourcenteil dieses Diagramms erstellt wird.	DevOps Ingenieur
Überprüfen Sie die Ressourcen im Amazon EKS-Cluster.	Verwenden Sie den folgenden Befehl, um die Ressourcen zu überprüfen, die als Teil des Helm-Diagramms im `helm-space` Namespace erstellt wurden. `kubectl get all -n helm-space`	DevOps Ingenieur

Führen Sie einen Rollback zu einer früheren Version einer Kubernetes-Anwendung durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern und aktualisieren Sie die Version.	Um das Diagramm zu ändern`values.yaml` , ändern Sie den `replicaCount` Wert in2. Aktualisieren Sie dann die bereits installierte Version, indem Sie den folgenden Befehl ausführen. `helm upgrade my-nginx-release my-nginx/ --namespace helm-space`	DevOps Ingenieur
Sehen Sie sich die Geschichte der Helm-Version an.	Führen Sie den folgenden Befehl aus, um alle Versionen für eine bestimmte Version aufzulisten, die mit Helm installiert wurden. `helm history my-nginx-release`	DevOps Ingenieur
Überprüfen Sie die Details für eine bestimmte Version.	Bevor Sie zu einer funktionierenden Version wechseln oder ein Rollback durchführen und für eine zusätzliche Überprüfungsebene vor der Installation einer Revision, sollten Sie mit dem folgenden Befehl überprüfen, welche Werte an die einzelnen Versionen übergeben wurden.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`helm get --revision=2 my-nginx-release`	
Führen Sie einen Rollback zu einer früheren Version durch.	Verwenden Sie den folgenden Befehl, um zu einer früheren Version zurückzukehren. `helm rollback my-nginx-release 1` In diesem Beispiel wird auf Version 1 zurückgesetzt.	DevOps Ingenieur

Initialisieren Sie einen S3-Bucket als Helm-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket für Helm-Charts.	Erstellen Sie einen eindeutigen S3-Bucket. Erstellen Sie im Bucket einen Ordner mit dem Namen `charts`. Das Beispiel in diesem Muster verwendet `s3://my-helm-charts/charts` als Zieldiagramm-Repository.	Cloud-Administrator
Installieren Sie das Helm-Plugin für Amazon S3.	Verwenden Sie den folgenden Befehl, um das Helm-S3-Plugin auf Ihrem Client-Computer zu installieren. `helm plugin install https://github.com/hypnoglow/helm-s3.git --version 0.10.0`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: Helm V3-Unterstützung ist mit der Plugin-Version 0.9.0 und höher verfügbar.	
Initialisieren Sie das Amazon S3 Helm-Repository.	Verwenden Sie den folgenden Befehl, um den Zielordner als Helm-Repository zu initialisieren. `helm S3 init s3://my-helm-charts/charts` Der Befehl erstellt eine `index.yaml` Datei im Ziel, um alle Diagramminformationen zu verfolgen, die an diesem Speicherort gespeichert sind.	DevOps Ingenieur
Fügen Sie das Amazon S3 S3-Repository zu Helm hinzu.	Verwenden Sie den folgenden Befehl, um das Repository auf dem Client-Computer hinzuzufügen. `helm repo add my-helm-charts s3://my-helm-charts/charts` Dieser Befehl fügt dem Ziel-Repository auf dem Helm-Client-Computer einen Alias hinzu.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Repository-Liste.	Führen `helm repo list` Sie den Befehl aus, um die Liste der Repositorys auf dem Helm-Client-Computer anzuzeigen.	DevOps Ingenieur

Package und Speichern von Diagrammen im Amazon S3 Helm-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verpacken Sie die Karte.	Führen Sie den Befehl aus, um das von Ihnen erstellte `my-nginx` Diagramm zu verpackenhelm package ./my-nginx/ . Der Befehl packt den gesamten Inhalt des `my-nginx` Diagrammordners in eine Archivdatei, die anhand der Versionsnummer benannt wird, die in der `Chart.yaml` Datei angegeben ist.	DevOps Ingenieur
Speichern Sie das Paket im Amazon S3 Helm-Repository.	Um das Paket in das Helm-Repository in Amazon S3 hochzuladen, führen Sie den folgenden Befehl aus und verwenden Sie dabei den richtigen Namen der `.tgz` Datei. `helm s3 push ./my-nginx-0.1.0.tgz my-helm-charts`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Suchen Sie nach der Helm-Karte.	Führen Sie den folgenden Befehl aus, um zu überprüfen, ob das Diagramm sowohl lokal als auch im Helm-Repository in Amazon S3 angezeigt wird. `helm search repo my-nginx`	DevOps Ingenieur

Ein Diagramm ändern, versionieren und verpacken

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern und verpacken Sie das Diagramm.	Stellen Sie in `values.yaml` den `replicaCount` Wert auf ein`1`. Verpacken Sie dann das Diagramm`helm package ./my-nginx/` , indem Sie es ausführen und diesmal die Version in `Chart.yaml` ändern`0.1.1`. Die Versionierung wird idealerweise durch Automatisierung mithilfe von Tools wie GitVersion Jenkins-Build-Nummern in einer CI/CD-Pipeline aktualisiert. Die Automatisierung der Versionsnummer ist für dieses Muster nicht vorgesehen.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Pushen Sie die neue Version in das Helm-Repository in Amazon S3.	Führen Sie den folgenden Befehl aus, um das neue Paket mit Version 0.1.1 in das `my-helm-charts` Helm-Repository in Amazon S3 zu übertragen. `helm s3 push ./my-nginx-0.1.1.tgz my-helm-charts`	DevOps Ingenieur

Suchen und installieren Sie ein Diagramm aus dem Amazon S3 Helm-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Suchen Sie nach allen Versionen des my-nginx-Diagramms.	Um alle verfügbaren Versionen eines Diagramms anzuzeigen, führen Sie den folgenden Befehl mit der Markierung aus. `--versions` `helm search repo my-nginx --versions` Ohne die Markierung zeigt Helm standardmäßig die zuletzt hochgeladene Version eines Diagramms an.	DevOps Ingenieur
Installieren Sie ein Diagramm aus dem Amazon S3 Helm-Repository.	Die Suchergebnisse der vorherigen Aufgabe zeigen die verschiedenen Versionen des `my-nginx` Diagramms.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Verwenden Sie den folgenden Befehl, um die neue Version (0.1.1) aus dem Amazon S3 Helm-Repository zu installie ren. `helm upgrade my-nginx-release my-helm-charts/my-nginx --version 0.1.1 --namespace helm-space`	

Zugehörige Ressourcen

- HELM-Dokumentation
- helm-S3-Plugin (MIT-Lizenz)
- BINÄRDATEI FÜR HELM-Cli
- Amazon EKS-Dokumentation

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Stellen Sie einen Beispiel-Java-Microservice auf Amazon EKS bereit und machen Sie den Microservice mithilfe eines Application Load Balancer verfügbar

Erstellt von Vijay Thompson (AWS) und Akkamahadevi Hiremath (AWS)

Übersicht

Dieses Muster beschreibt, wie ein Java-Microservice als containerisierte Anwendung auf Amazon Elastic Kubernetes Service (Amazon EKS) mithilfe des `eksctl` Befehlszeilenprogramms und Amazon Elastic Container Registry (Amazon ECR) bereitgestellt wird. Sie können einen Application Load Balancer für den Lastenausgleich des Anwendungsdatenverkehrs verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Die AWS-Befehlszeilenschnittstelle (AWS CLI) Version 1.7 oder höher, installiert und konfiguriert auf macOS, Linux oder Windows
- Ein laufender Docker-Daemon
- Das `eksctl` Befehlszeilenprogramm, installiert und konfiguriert auf macOS, Linux oder Windows (Weitere Informationen finden Sie unter Erste Schritte mit Amazon EKS — eksctl in der Amazon EKS-Dokumentation.)
- Das `kubectl` Befehlszeilenprogramm, installiert und konfiguriert unter macOS, Linux oder Windows (Weitere Informationen finden Sie unter Installation oder Aktualisierung von kubectl in der Amazon EKS-Dokumentation.)

Einschränkungen

- Dieses Muster deckt die Installation eines SSL-Zertifikats für den Application Load Balancer nicht ab.

Architektur

Zieltechnologie-Stack

- Amazon ECR
- Amazon EKS
- Elastic Load Balancing

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur für die Containerisierung eines Java-Microservices auf Amazon EKS.

Tools

- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen dabei, Kubernetes auf AWS auszuführen, ohne Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten zu müssen.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Elastic Load Balancing verteilt Ihren eingehenden Traffic automatisch auf mehrere Ziele, wie Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Container und IP-Adressen, in einer oder mehreren Availability Zones.
- eksctl hilft Ihnen bei der Erstellung von Clustern auf Amazon EKS.
- kubectl ermöglicht die Ausführung von Befehlen für Kubernetes-Cluster.
- Docker hilft Ihnen beim Erstellen, Testen und Bereitstellen von Anwendungen in Paketen, die als Container bezeichnet werden.

Epen

Erstellen Sie einen Amazon EKS-Cluster mithilfe von eksctl

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon-EKS-Cluster.	Um einen Amazon EKS-Cluster zu erstellen, der zwei t2.small EC2 Amazon-In	Entwickler, Systemadm inistrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	stances als Knoten verwendet , führen Sie den folgenden Befehl aus: `eksctl create cluster --name <your-cluster-name> --version <version-number> --nodes=1 --node-type=t2.small` **Note** Der Vorgang kann zwischen 15 und 20 Minuten dauern. Nachdem der Cluster erstellt wurde, wird die entsprech ende Kubernetes-Konfiguration zu Ihrer kubeconfig-Datei hinzugefü gt. Sie können die `kubeconfig` Datei mit verwenden , `kubectl` um die Anwendung in späteren Schritten bereitzustellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Amazon EKS-Cluster.	Um zu überprüfen, ob der Cluster erstellt wurde und Sie eine Verbindung zu ihm herstellen können, führen Sie den `kubectl get nodes` Befehl aus.	Entwickler, Systemadministrator

Erstellen Sie ein Amazon ECR-Repository und übertragen Sie das Docker-Image.

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon-ECR-Repository.	Folgen Sie den Anweisungen unter Privates Repository erstellen in der Amazon ECR-Dokumentation.	Entwickler, Systemadministrator
Erstellen Sie eine POM-XML-Datei.	Erstellen Sie eine `pom.xml` Datei, die auf dem POM-Beispieldateicode im Abschnitt Zusätzliche Informationen dieses Musters basiert.	Entwickler, Systemadministrator

Erstellen Sie eine Quelldatei.	Erstellen Sie anhand des folgenden `HelloWorld.java` Beispiels eine Quelldatei mit dem Namen im `src/main/java/eksExample` Pfad:
	`package eksExample;`
	`import static spark.Spark.get;`
	
	`public class HelloWorld {`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> public static void
	main(String[] args) {
	        get("/", (req,
	res) -> {
	            return
	"Hello World!";
	        });
	    }
	}</pre>
	Achten Sie darauf, die folgende Verzeichnisstruktur zu verwenden:
	<pre>### Dockerfile
	### deployment.yaml
	### ingress.yaml
	### pom.xml
	### service.yaml
	### src
	    ### main
	        ### java
	            ###
	eksExample
	                ###
	HelloWorld.java</pre>	

Erstellen Sie eine Docker-Datei.	Erstellen Sie einen auf dem Dockerfile-Beispiel *`Dockerfile`* basierenden Code im Abschnitt Zusätzliche Informationen dieses Musters.	Entwickler, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen und pushen Sie das Docker-Image.	Führen Sie in dem Verzeichnis, in dem Sie das Image erstellen, taggen und an Amazon ECR übertragen möchten, die folgenden Befehle aus: `Dockerfile`
	
	`aws ecr get-login -password --region <region>| docker login --username <username> --password-stdin <account_number>.dkr.ecr.<region>.amazonaws.com`
	`docker buildx build --platform linux/amd64 -t hello-world-java:v1 .`
	`docker tag hello-world-java:v1 <account_number>.dkr.ecr.<region>.amazonaws.com/<repository_name>:v1`
	`docker push <account_number>.dkr.ecr.<region>.amazonaws.com/<repository_name>:v1`
	
	Note
	Ändern Sie die AWS-Region, die Kontonummer und die Repository-Details in den vorherigen Befehlen. Notieren Sie sich unbedingt	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Bild-URL für die spätere Verwendung. **Important** Ein macOS-System mit einem M1-Chip hat ein Problem beim Erstellen eines Images, das mit Amazon EKS kompatibel ist, das auf einer AMD64 Plattform ausgeführt wird. Um dieses Problem zu beheben, verwenden Sie docker buildx, um ein Docker-Image zu erstellen, das auf Amazon EKS funktioniert.	

Stellen Sie die Java-Microservices bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Bereitstellungsdatei.	Erstellen Sie eine YAML-Datei, die `deployment.yaml` auf dem Code der Beispiel-Bereitstellungsdatei im Abschnitt Zusätzliche Informationen dieses Musters basiert.	Entwickler, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Verwenden Sie die Bild-URL, die Sie zuvor kopiert haben, als Pfad der Bilddatei für das Amazon ECR-Repository.	
Stellen Sie die Java-Micr oservices auf dem Amazon EKS-Cluster bereit.	Führen Sie den `kubectl apply -f deploymen t.yaml` Befehl aus, um eine Bereitstellung in Ihrem Amazon EKS-Cluster zu erstellen.	Entwickler, Systemadm inistrator
Überprüfen Sie den Status der Pods.	1. Führen Sie den `kubectl get pods` Befehl aus, um den Status der Pods zu überprüfen. 2. Warten Sie, bis sich der Status auf Bereit ändert.	Entwickler, Systemadm inistrator
Erstellen Sie einen Service.	1. Erstellen Sie eine Datei, die `service.yaml` auf dem Beispielcode der Serviceda tei im Abschnitt Zusätzlic he Informationen dieses Musters basiert. 2. Führen Sie den Befehl `kubectl apply -f service.yaml` aus.	Entwickler, Systemadm inistrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie das AWS Load Balancer Controller-Add-on.	Folgen Sie den Anweisungen unter Installation des AWS Load Balancer Controller-Add-ons in der Amazon EKS-Dokumentation. **Note** Sie müssen das Add-on installiert haben, um einen Application Load Balancer oder Network Load Balancer für einen Kubernetes-Dienst zu erstellen.	Entwickler, Systemadministrator
Erstellen Sie eine Eingangsressource.	Erstellen Sie eine YAML-Datei, die auf der `ingress.yaml` Grundlage des Beispielcodes für eine Ingress-Ressourcendatei im Abschnitt Zusätzliche Informationen dieses Musters aufgerufen wird.	Entwickler, Systemadministrator
Erstellen Sie einen Application Load Balancer.	Führen Sie den Befehl aus, um die Eingangsressource bereitzustellen und einen Application Load Balancer zu erstellen. `kubectl apply -f ingress.yaml`	Entwickler, Systemadministrator

Testen der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen und verifizieren Sie die Anwendung.	1. Führen Sie den `kubectl get ingress.networking.k8s.io/java-microservice-ingress` Befehl aus, um den DNS-Namen des Load Balancers aus dem ADDRESS-Feld abzurufen. 2. Führen Sie den `curl -v <DNS address from previous command>` Befehl auf einer EC2 Instance in derselben VPC wie Ihre Amazon EKS-Knoten aus.	Entwickler, Systemadministrator

Zugehörige Ressourcen

- Ein privates Repository erstellen (Amazon ECR-Dokumentation)
- Ein Docker-Image pushen (Amazon ECR-Dokumentation)
- Eingangscontroller (Amazon EKS-Workshop)
- Docker buildx (Docker-Dokumente)

Zusätzliche Informationen

Beispiel für eine POM-Datei

```
<?xml version="1.0" encoding="UTF-8"?>
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/xsd/
maven-4.0.0.xsd">
```

```
  <modelVersion>4.0.0</modelVersion>


  <groupId>helloWorld</groupId>
  <artifactId>helloWorld</artifactId>
  <version>1.0-SNAPSHOT</version>


  <dependencies>
    <dependency>
      <groupId>com.sparkjava</groupId><artifactId>spark-core</
artifactId><version>2.0.0</version>
    </dependency>
  </dependencies>
  <build>
    <plugins>
      <plugin>
        <groupId>org.apache.maven.plugins</groupId><artifactId>maven-jar-plugin</
artifactId><version>2.4</version>
        <configuration><finalName>eksExample</finalName><archive><manifest>
              <addClasspath>true</addClasspath><mainClass>eksExample.HelloWorld</
mainClass><classpathPrefix>dependency-jars/</classpathPrefix>
            </manifest></archive>
        </configuration>
      </plugin>
      <plugin>
        <groupId>org.apache.maven.plugins</groupId><artifactId>maven-compiler-plugin</
artifactId><version>3.1</version>
        <configuration><source>1.8</source><target>1.8</target></configuration>
      </plugin>
      <plugin>
        <groupId>org.apache.maven.plugins</groupId><artifactId>maven-assembly-plugin</
artifactId>
        <executions>
          <execution>
            <goals><goal>attached</goal></goals><phase>package</phase>
            <configuration>
              <finalName>eksExample</finalName>
              <descriptorRefs><descriptorRef>jar-with-dependencies</descriptorRef></
descriptorRefs>
              <archive><manifest><mainClass>eksExample.HelloWorld</mainClass></
manifest></archive>
            </configuration>
          </execution>
```

```
        </executions>
      </plugin>
    </plugins>
  </build>
</project>
```

Beispiel Dockerfile

```
FROM bellsoft/liberica-openjdk-alpine-musl:17

RUN apk add maven
WORKDIR /code

# Prepare by downloading dependencies
ADD pom.xml /code/pom.xml
RUN ["mvn", "dependency:resolve"]
RUN ["mvn", "verify"]

# Adding source, compile and package into a fat jar
ADD src /code/src
RUN ["mvn", "package"]

EXPOSE 4567
CMD ["java", "-jar", "target/eksExample-jar-with-dependencies.jar"]
```

Beispiel für eine Bereitstellungsdatei

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: microservice-deployment
spec:
  replicas: 2
  selector:
    matchLabels:
      app.kubernetes.io/name: java-microservice
  template:
    metadata:
      labels:
        app.kubernetes.io/name: java-microservice
    spec:
      containers:
      - name: java-microservice-container
```

```
        image: .dkr.ecr.amazonaws.com/:
        ports:
        - containerPort: 4567
```

Beispiel für eine Servicedatei

```
apiVersion: v1
kind: Service
metadata:
  name: "service-java-microservice"
spec:
  ports:
    - port: 80
      targetPort: 4567
      protocol: TCP
  type: NodePort
  selector:
    app.kubernetes.io/name: java-microservice
```

Beispiel für eine Ingress-Ressourcendatei

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: "java-microservice-ingress"
  annotations:
    kubernetes.io/ingress.class: alb
    alb.ingress.kubernetes.io/load-balancer-name: apg2
    alb.ingress.kubernetes.io/target-type: ip
  labels:
    app: java-microservice
spec:
  rules:
    - http:
        paths:
          - path: /
            pathType: Prefix
            backend:
              service:
                name: "service-java-microservice"
                port:
                  number: 80
```

Stellen Sie mithilfe von AWS Copilot eine geclusterte Anwendung in Amazon ECS bereit

Erstellt von Jean-Baptiste Guillois (AWS), Mathew George (AWS) und Thomas Scott (AWS)

Übersicht

Dieses Muster zeigt, wie Container in einem Amazon Elastic Container Service (Amazon ECS) -Cluster auf zwei Arten bereitgestellt werden können — mithilfe der Amazon Web Services (AWS) Management Console und mithilfe von AWS Copilot — um zu demonstrieren, wie AWS Copilot Bereitstellungsaufgaben vereinfacht.

Amazon ECS ist ein hoch skalierbarer, schneller Container-Management-Service, der es einfach macht, Container in einem Cluster auszuführen, zu stoppen und zu verwalten. Ihre Container sind in einer Aufgabendefinition definiert, die Sie zum Ausführen einzelner Aufgaben oder Aufgaben innerhalb eines Dienstes verwenden. Sie können Ihre Aufgaben und Services auf einer serverlosen Infrastruktur ausführen, die von AWS Fargate verwaltet wird. Für mehr Kontrolle über Ihre Infrastruktur können Sie Ihre Aufgaben und Dienste alternativ auf einem Cluster von Amazon Elastic Compute Cloud (Amazon EC2) -Instances ausführen, die Sie verwalten.

Die Befehle der Befehlszeilenschnittstelle (CLI) von AWS Copilot vereinfachen die Erstellung, Veröffentlichung und den Betrieb produktionsreifer containerisierter Anwendungen auf Amazon ECS von einer lokalen Entwicklungsumgebung aus. Die AWS Copilot CLI ist auf Entwickler-Workflows abgestimmt, die bewährte Methoden für moderne Anwendungen unterstützen: von der Verwendung von Infrastruktur als Code bis hin zur Erstellung einer Pipeline für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD), die im Namen eines Benutzers bereitgestellt wird. Sie können die AWS Copilot CLI als Teil Ihres täglichen Entwicklungs- und Testzyklus als Alternative zur AWS-Managementkonsole verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS-Befehlszeilenschnittstelle (AWS CLI), lokal installiert und konfiguriert, um Ihr AWS-Konto zu verwenden (siehe die Installations - und Konfigurationsanweisungen in der AWS-CLI-Dokumentation)
- Lokal installierter AWS Copilot (siehe Installationsanweisungen in der Amazon ECS-Dokumentation)

- Docker ist auf Ihrem lokalen Computer installiert (weitere Informationen finden Sie in der Docker-Dokumentation)

Einschränkungen

- Docker erzwingt im kostenlosen Tarif Pull-Limits von 100 Container-Images pro 6 Stunden pro IP-Adresse.

Architektur

Zieltechnologie-Stack

- AWS-Umgebung, eingerichtet mit einer Virtual Private Cloud (VPC), öffentlichen und privaten Subnetzen und Sicherheitsgruppen
- Amazon-ECS-Cluster
- Amazon ECS-Service- und Aufgabendefinition
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon-DynamoDB
- Application Load Balancer
- AWS Fargate
- Amazon Identity and Access Management (IAM)
- Amazon CloudWatch
- AWS CloudTrail

Zielarchitektur

Wenn Sie die Beispielanwendung für dieses Muster bereitstellen, werden mehrere Aufgaben erstellt und in separaten Availability Zones bereitgestellt. Jede Aufgabe speichert Daten in Amazon DynamoDB. Wenn Sie auf die Webseite für eine Aufgabe zugreifen, können Sie die Daten aller anderen Aufgaben einsehen.

Tools

AWS-Services

- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) ist ein von AWS verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist. Amazon ECR unterstützt private Container-Image-Repositories mit ressourcenbasierten Berechtigungen unter Verwendung von IAM.
- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service zum Ausführen, Stoppen und Verwalten von Containern in einem Cluster. Sie können Ihre Aufgaben und Services auf einer serverlosen Infrastruktur ausführen, die von AWS Fargate verwaltet wird. Für mehr Kontrolle über Ihre Infrastruktur können Sie Ihre Aufgaben und Dienste alternativ auf einem Cluster von Amazon Elastic Compute Cloud (Amazon EC2) -Instances ausführen, die Sie verwalten.
- AWS Copilot — AWS Copilot bietet eine Befehlszeilenschnittstelle, mit der Sie containerisierte Anwendungen auf AWS starten und verwalten können, einschließlich der Übertragung in eine Registrierung, der Erstellung einer Aufgabendefinition und der Erstellung eines Clusters.
- AWS Fargate — AWS Fargate ist eine serverlose pay-as-you-go Rechen-Engine, mit der Sie sich auf die Erstellung von Anwendungen konzentrieren können, ohne Server verwalten zu müssen. AWS Fargate ist sowohl mit Amazon ECS als auch mit Amazon Elastic Kubernetes Service (Amazon EKS) kompatibel. Wenn Sie Ihre Amazon-ECS-Aufgaben und -Services mit dem Starttyp Fargate oder einem Fargate-Kapazitätsanbieter ausführen, packen Sie Ihre Anwendung in Container, spezifizieren die CPU- und Arbeitsspeicheranforderungen, definieren Netzwerk- und IAM-Richtlinien und starten die Anwendung. Jede Fargate-Aufgabe hat ihre eigene Isolationsgrenze und teilt den zugrunde liegenden Kernel, die CPU-Ressourcen, Speicherressourcen oder die elastic network interface nicht mit einer anderen Aufgabe.
- Amazon DynamoDB — Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der schnelle und vorhersehbare Leistung mit nahtloser Skalierbarkeit bietet.
- Elastic Load Balancing (ELB) — Elastic Load Balancing verteilt Ihren eingehenden Traffic automatisch auf mehrere Ziele wie EC2 Instances, Container und IP-Adressen in einer oder mehreren Availability Zones. Es überwacht den Zustand der registrierten Ziele und leitet den Datenverkehr nur an die fehlerfreien Ziele weiter. Elastic Load Balancing skaliert Ihren Load Balancer, wenn sich der eingehende Datenverkehr im Laufe der Zeit ändert. Es kann automatisch auf die meisten Workloads skaliert werden.

Tools

- Docker-Befehlszeilenschnittstelle
- AWS-Befehlszeilenschnittstelle (AWS CLI)

- AWS Copilot-Befehlszeilenschnittstelle

Code

Der Code für die in diesem Muster verwendete Beispielanwendung ist im GitHub Cluster-Beispielanwendungs-Repository verfügbar. Folgen Sie den Anweisungen im nächsten Abschnitt, um die Beispieldateien zu verwenden.

Epen

Bereitstellen des Anwendungsstapels — Option 1 (AWS-Managementkonsole)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	Klonen Sie das Beispielcode-Repository mit dem folgenden Befehl: `git clone https://github.com/aws-samples/cluster-sample-app cluster-sample-app && cd cluster-sample-app`	App-Entwickler, AWS DevOps
Erstellen Sie Ihr Amazon ECR-Repository.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon ECR-Konsole unter https://console.aws.amazon.com/ecr/Repositorys. 2. Wählen Sie Repository erstellen aus. 3. Geben Sie als Repository-Namen ein. cluster-sample-app	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Behalten Sie für alle anderen Einstellungen die Standardwerte bei. 5. Wählen Sie Repository erstellen aus. Weitere Informationen finden Sie unter Erstellen eines privaten Repositorys in der Amazon ECR-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen, taggen und übertragen Sie Ihr Docker-Image in Ihr Amazon ECR-Repository.	1. Wählen Sie das Repository aus, das Sie gerade erstellt haben, und wählen Sie Push-Befehle anzeigen.
	2. Kopieren Sie die angezeigten Befehle und führen Sie sie lokal aus, um Ihr Docker-Image zu erstellen, zu taggen und zu pushen. Diese Befehle werden den folgenden ähneln.
	
	So authentifizieren Sie Ihren Docker-Client bei der Registrierung:
	
	`aws ecr get-login -password --region <YOUR_AWS_REGION> | docker login --username AWS --password-stdin <YOUR_AWS_ACCOUNT>.dkr.ecr.<YOUR_AWS_REGION>.amazonaws.com`
	
	Um Ihr Docker-Image zu erstellen:
	
	`docker build -t cluster-sample-app .`
	
	Um Ihr Docker-Image zu taggen:
		App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`docker tag cluster-sample-app:latest <YOUR_AWS_ACCOUNT>.dkr.ecr.<YOUR_AWS_REGION>.amazonaws.com/cluster-sample-app:latest`
	
	Um das Docker-Image in Ihr Repository zu übertragen:
	
	`docker push <YOUR_AWS_ACCOUNT>.dkr.ecr.<YOUR_AWS_REGION>.amazonaws.com/cluster-sample-app:latest`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Anwendungsstapel bereit.	1. Öffnen Sie die CloudFormation AWS-Konsole unter https://console.aws.amazon.com/cloudformation/. 2. Wählen Sie Stack erstellen aus. 3. Wählen Sie im Abschnitt Vorlage vorbereiten die Option Vorlage ist bereit aus. 4. Wählen Sie im Abschnitt Specify template (Vorlage angeben) die Option Upload a template file (Vorlagendatei hochladen) aus. 5. Wählen Sie die lokale Datei `cluster-sample-app-stack.yml`, die Sie aus dem GitHub Repository geklont haben, als CloudFormation Vorlage aus, und klicken Sie dann auf Weiter. 6. Geben Sie einen Namen für Ihren Stack ein und wählen Sie dann Weiter. 7. Behalten Sie alle Standardoptionen bei und wählen Sie dann Weiter. 8. Überprüfen Sie alle Optionen, bestätigen Sie die Erstellung von IAM-	AWS DevOps, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ressourcen und wählen Sie dann Stack erstellen aus. 9. Wenn Ihr Anwendung sstapel bereitgestellt wurde, wählen Sie die Registerk arte Ausgabe, kopieren Sie die URL und öffnen Sie sie in Ihrem Browser, um auf die Anwendung zuzugreif en. Weitere Informationen zum Bereitstellen von CloudForm ation Vorlagen finden Sie in der CloudFormation AWS-Dokumentation unter Erstellen eines Stacks.	

Bereitstellen des Anwendungsstapels — Option 2 (AWS Copilot CLI)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	Klonen Sie das Beispielcode-Repository mit dem folgenden Befehl: `git clone https://github.com/aws-samples/cluster-sample-app cluster-sample-app && cd cluster-sample-app`	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Ihr Container -Image mithilfe der AWS Copilot CLI in AWS bereit.	Stellen Sie die Anwendung in einem Schritt bereit, indem Sie den folgenden Befehl im Stammverzeichnis Ihres Projekts verwenden: `copilot init --app cluster-sample-app --name demo --type "Load Balanced Web Service" --dockerfile ./Dockerfile --port 8080 --deploy` Sie sollten dann in der Lage sein, auf die Anwendung zuzugreifen, indem Sie den als Ausgabe angegebenen DNS-Namen verwenden.	App-Entwickler, AWS DevOps

Löschen Sie die erstellten Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die über die AWS-Managementkonsole erstellten Ressourcen.	Wenn Sie Option 1 (die AWS-Managementkonsole) zur Bereitstellung des Anwendungsstapels verwendet haben, gehen Sie wie folgt vor, wenn Sie bereit sind, die von Ihnen erstellten Ressourcen zu löschen: 1. Öffnen Sie die CloudFormation Konsole unter https://	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	console.aws.amazon.com/cloudformation/. 2. Wählen Sie den Stapel aus, den Sie erstellt haben, und klicken Sie dann auf Löschen. 3. Öffnen Sie die Amazon ECR-Konsole unter https://console.aws.amazon.com/ecr/Repositorys. 4. Wählen Sie das von Ihnen erstellte Repository aus und klicken Sie dann auf Löschen.	
Löschen Sie die von AWS Copilot erstellten Ressourcen.	Wenn Sie Option 2 (die AWS Copilot CLI) zur Bereitstellung des Anwendungsstapels verwendet haben, führen Sie den folgenden Befehl im Stammverzeichnis Ihres Projekts aus, wenn Sie bereit sind, die von Ihnen erstellten Ressourcen zu löschen: `copilot app delete`	App-Entwickler, AWS DevOps

Zugehörige Ressourcen

- Installation oder Aktualisierung der neuesten Version der AWS-CLI (AWS-CLI-Dokumentation)
- Verwenden der AWS Copilot-Befehlszeilenschnittstelle (Amazon ECS-Dokumentation)
- Amazon ECS auf AWS Fargate (Amazon ECR-Dokumentation)
- Amazon ECS-Dokumentation

- Amazon ECR-Dokumentation
- CloudFormation Amazon-Dokumentation
- Docker Desktop (Docker-Dokumentation)

Stellen Sie eine GRPC-basierte Anwendung auf einem Amazon EKS-Cluster bereit und greifen Sie mit einem Application Load Balancer darauf zu

Erstellt von Kirankumar Chandrashekar (AWS) und Huy Nguyen (AWS)

Übersicht

Dieses Muster beschreibt, wie Sie eine GRPC-basierte Anwendung auf einem Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster hosten und über einen Application Load Balancer sicher darauf zugreifen.

gRPC ist ein Open-Source-RPC-Framework (Remote Procedure Call), das in jeder Umgebung ausgeführt werden kann. Sie können es für Microservice-Integrationen und Client-Server-Kommunikation verwenden. Weitere Informationen zu gRPC finden Sie im AWS-Blogbeitrag Application Load Balancer Balancer-Unterstützung für end-to-end HTTP/2 und gRPC.

Dieses Muster zeigt Ihnen, wie Sie eine GRPC-basierte Anwendung hosten, die auf Kubernetes-Pods auf Amazon EKS ausgeführt wird. Der gRPC-Client stellt über das HTTP/2-Protokoll mit einer SSL/TLS-verschlüsselten Verbindung eine Verbindung zu einem Application Load Balancer her. Der Application Load Balancer leitet den Datenverkehr an die gRPC-Anwendung weiter, die auf Amazon EKS-Pods ausgeführt wird. Die Anzahl der gRPC-Pods kann mithilfe des Kubernetes Horizontal Pod Autoscaler automatisch auf der Grundlage des Datenverkehrs skaliert werden. Die Zielgruppe des Application Load Balancers führt Integritätsprüfungen an den Amazon EKS-Knoten durch, bewertet, ob das Ziel fehlerfrei ist, und leitet den Datenverkehr nur an fehlerfreie Knoten weiter.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Docker, installiert und konfiguriert unter Linux, MacOS oder Windows.
- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 2, installiert und konfiguriert unter Linux, macOS oder Windows.
- eksctl, installiert und konfiguriert unter Linux, MacOS oder Windows.
- `kubectl`, installiert und konfiguriert für den Zugriff auf Ressourcen in Ihrem Amazon EKS-Cluster. Weitere Informationen finden Sie unter Installation oder Aktualisierung von kubectl in der Amazon EKS-Dokumentation.

- g RPCurl, installiert und konfiguriert.
- Ein neuer oder vorhandener Amazon EKS-Cluster. Weitere Informationen finden Sie unter Erste Schritte mit Amazon EKS.
- Ihr Computerterminal ist für den Zugriff auf den Amazon EKS-Cluster konfiguriert. Weitere Informationen finden Sie in der Amazon EKS-Dokumentation unter Konfiguration Ihres Computers für die Kommunikation mit Ihrem Cluster.
- AWS Load Balancer Controller, bereitgestellt im Amazon EKS-Cluster.
- Ein vorhandener DNS-Hostname mit einem gültigen SSL- oder SSL/TLS-Zertifikat. Sie können ein Zertifikat für Ihre Domain erhalten, indem Sie AWS Certificate Manager (ACM) verwenden oder ein vorhandenes Zertifikat auf ACM hochladen. Weitere Informationen zu diesen beiden Optionen finden Sie unter Anfordern eines öffentlichen Zertifikats und Importieren von Zertifikaten in AWS Certificate Manager in der ACM-Dokumentation.

Architektur

Das folgende Diagramm zeigt die durch dieses Muster implementierte Architektur.

Das folgende Diagramm zeigt einen Workflow, bei dem SSL/TLS-Verkehr von einem gRPC-Client empfangen wird, der auf einen Application Load Balancer auslagert. Der Datenverkehr wird im Klartext an den gRPC-Server weitergeleitet, da er aus einer Virtual Private Cloud (VPC) stammt.

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Elastic Load Balancing verteilt den eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Traffic auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen.
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.

- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen dabei, Kubernetes auf AWS auszuführen, ohne Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten zu müssen.

Tools

- eksctl ist ein einfaches CLI-Tool zum Erstellen von Clustern auf Amazon EKS.
- kubectl ist ein Befehlszeilenprogramm zum Ausführen von Befehlen für Kubernetes-Cluster.
- AWS Load Balancer Controller unterstützt Sie bei der Verwaltung von AWS Elastic Load Balancers für einen Kubernetes-Cluster.
- g RPCurl ist ein Befehlszeilentool, mit dem Sie mit gRPC-Diensten interagieren können.

Code-Repository

Der Code für dieses Muster ist im GitHub grpc-traffic-on-alb-to-eks-Repository verfügbar.

Epen

Erstellen Sie das Docker-Image des gRPC-Servers und übertragen Sie es auf Amazon ECR

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon-ECR-Repository.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon ECR-Konsole und erstellen Sie dann ein Amazon ECR-Repository. Weitere Informationen finden Sie unter Erstellen eines Repositorys in der Amazon ECR-Dokumentation. Stellen Sie sicher, dass Sie die URL des Amazon ECR-Repositorys aufzeichnen. Sie können auch ein Amazon ECR-Repository mit AWS	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CLI erstellen, indem Sie den folgenden Befehl ausführen: `aws ecr create-repository --repository-name helloworld-grpc`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie das Docker-Image.	1. Klonen Sie das GitHub grpc-traffic-on-alb-to-eks-Repository.
	`git clone https://github.com/aws-samples/grpc-traffic-on-alb-to-eks.git`
	2. Stellen Sie im Stammverzeichnis des Repositorys sicher, dass das Dockerfile vorhanden ist, und führen Sie dann den folgenden Befehl aus, um das Docker-Image zu erstellen:
	`docker build -t <amazon_ecr_repository_url>:<Tag> .`
	Important
	Stellen Sie sicher, dass Sie es `<amazon_ecr_repository_url>` durch die URL des Amazon ECR-Repositorys ersetzen, das Sie zuvor erstellt haben.
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Senden Sie das Docker-Image an Amazon ECR.	1. Führen Sie den folgenden Befehl aus, um sich beim Amazon ECR-Repository anzumelden:
	`aws ecr get-login -password --region us-east-1 --no-cli-auto-prompt | docker login --username AWS --password-stdin <your_aws_account_id>.dkr.ecr.us-east-1.amazonaws.com`
	2. Übertragen Sie das Docker-Image in das Amazon ECR-Repository, indem Sie den folgenden Befehl ausführen:
	`docker push <your_aws_account_id>.dkr.ecr.us-east-1.amazonaws.com/helloworld-grpc:1.0`
	Important
	Stellen Sie sicher, dass Sie es `<your_aws_account_id>` durch Ihre AWS-Konto-ID ersetzen.
		DevOps Ingenieur

Stellen Sie die Kubernetes-Manifeste im Amazon EKS-Cluster bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Werte in der Kubernetes-Manifestdatei.	1. Ändern Sie die `grpc-sample.yaml` Kubernetes-Manifestdatei im Kubernetes-Ordner des Repositorys gemäß Ihren Anforderungen. Sie müssen die Anmerkungen und den Hostnamen in der Eingangsressource ändern. Ein Beispiel für eine Ingress-Ressource finden Sie im Abschnitt Zusätzliche Informationen. Weitere Informationen zu Eingangsanmerkungen finden Sie unter Eingangsanmerkungen in der Kubernetes-Dokumentation. 2. Ändern Sie in der Kubernetes-Bereitstellungsressource die Bereitstellungsressourcen in den Uniform Resource Identifier (URI) für das Amazon ECR-Repository, in das Sie das Docker-Image übertragen haben. `image` Ein Beispiel für eine Bereitstellungsressource finden Sie im Abschnitt Zusätzliche Informationen.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Kubernetes-Manifestdatei bereit.	Stellen Sie die `grpc-sample.yaml` Datei im Amazon EKS-Cluster bereit, indem Sie den folgenden `kubectl` Befehl ausführen: `kubectl apply -f ./kubernetes/grpc-sample.yaml`	DevOps Ingenieur

Erstellen Sie den DNS-Eintrag für den FQDN des Application Load Balancers

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Notieren Sie den FQDN für den Application Load Balancer.	1. Führen Sie den folgenden `kubectl` Befehl aus, um die Kubernetes-Eingangsressource zu beschreiben, die den Application Load Balancer verwaltet: `kubectl get ingress -n grpcserver` Eine Beispielausgabe finden Sie im Abschnitt Zusätzliche Informationen. In der Ausgabe zeigt das `HOSTS` Feld den DNS-Hostnamen an, für den die SSL-Zertifikate erstellt wurden. 2. Notieren Sie den vollqualifizierten Domainnamen (FQDN) des Applicati	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	on Load Balancers aus dem `Address` Feld der Ausgabe. 3. Erstellen Sie einen DNS-Eintrag, der auf den FQDN des Application Load Balancers verweist. Wenn Ihr DNS-Anbieter Amazon Route 53 ist, können Sie einen Aliaseintrag erstellen , der auf den FQDN des Application Load Balancers verweist. Weitere Informationen zu dieser Option finden Sie unter Auswahl zwischen Alias- und Nicht-Aliasdatensätzen in der Route 53 53-Dokumentation.	

Testen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie den gRPC-Server.	Verwenden Sie gRPCurl , um den Endpunkt zu testen, indem Sie den folgenden Befehl ausführen: `grpcurl grpc.example.com:443 list grpc.reflection.v1alpha.ServerReflection helloworld.helloworld`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Ersetze es `grpc.example.com` durch deinen DNS-Namen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Testen Sie den gRPC-Server mit einem gRPC-Client.	Ersetzen Sie im `helloworld_client_ssl.py` gRPC-Beispielclient den Hostnamen von `grpc.example.com` durch den Hostnamen, der für den gRPC-Server verwendet wird.
	
	Das folgende Codebeispiel zeigt die Antwort des gRPC-Servers auf die Anfrage des Clients:
	
	`python ./app/helloworld_client_ssl.py`
	`message: "Hello to gRPC server from Client"`
	
	`message: "Thanks for talking to gRPC server!! Welcome to hello world. Received message is \"Hello to gRPC server from Client\""`
	`received: true`
	
	Dies zeigt, dass der Client mit dem Server kommunizieren kann und dass die Verbindung erfolgreich ist.
		DevOps Ingenieur

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie den DNS-Eintrag.	Entfernen Sie den DNS-Eintrag, der auf den zuvor erstellten FQDN des Application Load Balancers verweist.	Cloud-Administrator
Entfernen Sie den Load Balancer.	Wählen Sie auf der EC2 Amazon-Konsole Load Balancers und entfernen Sie dann den Load Balancer, den der Kubernetes-Controller für Ihre Eingangsressource erstellt hat.	Cloud-Administrator
Löschen Sie den Amazon EKS-Cluster.	Löschen Sie den Amazon EKS-Cluster mithilfe von `eksctl`: `eksctl delete cluster -f ./eks.yaml`	AWS DevOps

Zugehörige Ressourcen

- Network Load Balancing in Amazon EKS
- Zielgruppen für Ihre Application Load Balancer

Zusätzliche Informationen

Beispiel für eine Ingress-Ressource:

```
---
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
```

```
  annotations:
    alb.ingress.kubernetes.io/healthcheck-protocol: HTTP
    alb.ingress.kubernetes.io/ssl-redirect: "443"
    alb.ingress.kubernetes.io/backend-protocol-version: "GRPC"
    alb.ingress.kubernetes.io/listen-ports: '[{"HTTP": 80}, {"HTTPS":443}]'
    alb.ingress.kubernetes.io/scheme: internet-facing
    alb.ingress.kubernetes.io/target-type: ip
    alb.ingress.kubernetes.io/certificate-arn: arn:aws:acm:<AWS-
Region>:<AccountId>:certificate/<certificate_ID>
  labels:
    app: grpcserver
    environment: dev
  name: grpcserver
  namespace: grpcserver
spec:
  ingressClassName: alb
  rules:
  - host: grpc.example.com # <----- replace this as per your host name for which the
 SSL certtficate is available in ACM
    http:
      paths:
      - backend:
          service:
            name: grpcserver
            port:
              number: 9000
        path: /
        pathType: Prefix
```

Beispiel für eine Bereitstellungsressource:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: grpcserver
  namespace: grpcserver
spec:
  selector:
    matchLabels:
      app: grpcserver
  replicas: 1
  template:
    metadata:
```

```
      labels:
        app: grpcserver
    spec:
      containers:
      - name: grpc-demo
        image: <your_aws_account_id>.dkr.ecr.us-east-1.amazonaws.com/helloworld-
grpc:1.0   #<------- Change to the URI that the Docker image is pushed to
        imagePullPolicy: Always
        ports:
        - name: grpc-api
          containerPort: 9000
        env:
        - name: POD_IP
          valueFrom:
            fieldRef:
              fieldPath: status.podIP
      restartPolicy: Always
```

Beispielausgabe:

```
NAME             CLASS           HOSTS                          Address
 PORTS          AGE
 grpcserver      <none>      <DNS-HostName>                 <ELB-address>
 80            27d
```

Bereitstellen und Debuggen von Amazon EKS-Clustern

Erstellt von Svenja Raether (AWS) und Mathew George (AWS)

Übersicht

Container werden zu einem unverzichtbaren Bestandteil der Entwicklung cloudnativer Anwendungen. Kubernetes bietet eine effiziente Möglichkeit, Container zu verwalten und zu orchestrieren. Amazon Elastic Kubernetes Service (Amazon EKS) ist ein vollständig verwalteter, zertifizierter Kubernetes-konformer Service für den Aufbau, die Sicherung, den Betrieb und die Wartung von Kubernetes-Clustern auf Amazon Web Services (AWS). Es unterstützt die Ausführung von Pods auf AWS Fargate, um bedarfsgerecht dimensionierte Rechenkapazität bereitzustellen.

Für Entwickler und Administratoren ist es wichtig, die Debugging-Optionen für die Ausführung containerisierter Workloads zu kennen. Dieses Muster führt Sie durch die Bereitstellung und das Debuggen von Containern auf Amazon EKS mit AWS Fargate. Es umfasst das Erstellen, Bereitstellen, Zugreifen, Debuggen und Bereinigen der Amazon EKS-Workloads.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Die Rolle AWS Identity and Access Management (IAM) ist mit ausreichenden Berechtigungen konfiguriert, um Amazon EKS, IAM-Rollen und serviceverknüpfte Rollen zu erstellen und mit diesen zu interagieren
- Auf dem lokalen Computer installierte AWS-Befehlszeilenschnittstelle (AWS CLI)
- eksctl
- kubectl
- Helm

Einschränkungen

- Dieses Muster bietet Entwicklern nützliche Debugging-Methoden für Entwicklungsumgebungen. Es enthält keine bewährten Methoden für Produktionsumgebungen.
- Wenn Sie Windows ausführen, verwenden Sie Ihre betriebssystemspezifischen Befehle zum Einstellen der Umgebungsvariablen.

Verwendete Produktversionen

- AWS-CLI Version 2
- kubectl-Version innerhalb eines geringfügigen Versionsunterschieds der Amazon EKS-Kontrollebene, die Sie verwenden
- eksctl neueste Version
- Helm v3

Architektur

Technologie-Stack

- Application Load Balancer
- Amazon EKS
- AWS Fargate

Zielarchitektur

Alle im Diagramm gezeigten Ressourcen werden mithilfe von `kubectl` Befehlen `eksctl` und Befehlen bereitgestellt, die von einem lokalen Computer aus ausgegeben werden. Private Cluster müssen von einer Instance aus ausgeführt werden, die sich innerhalb der privaten VPC befindet.

Die Zielarchitektur besteht aus einem EKS-Cluster, der den Fargate-Starttyp verwendet. Dadurch wird bedarfsgerecht dimensionierte Rechenkapazität bereitgestellt, ohne dass Servertypen angegeben werden müssen. Der EKS-Cluster verfügt über eine Steuerungsebene, die zur Verwaltung der Clusterknoten und Workloads verwendet wird. Die Pods werden in privaten VPC-Subnetzen bereitgestellt, die sich über mehrere Availability Zones erstrecken. Auf die Amazon ECR Public Gallery wird verwiesen, um ein NGINX-Webserver-Image abzurufen und für die Pods des Clusters bereitzustellen.

Das Diagramm zeigt, wie Sie mithilfe von `kubectl` Befehlen auf die Amazon EKS-Steuerebene zugreifen und wie Sie mithilfe des Application Load Balancer auf die Anwendung zugreifen.

.

1. Ein lokaler Computer außerhalb der AWS-Cloud sendet Befehle an die Kubernetes-Steuerebene innerhalb einer von Amazon EKS verwalteten VPC.

2. Amazon EKS plant Pods auf der Grundlage der Selektoren im Fargate-Profil.
3. Der lokale Computer öffnet die Application Load Balancer Balancer-URL im Browser.
4. Der Application Load Balancer verteilt den Datenverkehr zwischen den Kubernetes-Pods in Fargate-Clusterknoten, die in privaten Subnetzen bereitgestellt werden, die sich über mehrere Availability Zones erstrecken.

Tools

AWS-Services

- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen, Kubernetes auf AWS auszuführen, ohne Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten zu müssen. Dieses Muster verwendet auch das Befehlszeilentool eksctl, um mit Kubernetes-Clustern auf Amazon EKS zu arbeiten.
- Mit AWS Fargate können Sie Container ausführen, ohne Server oder Amazon Elastic Compute Cloud (Amazon EC2) -Instances verwalten zu müssen. Es wird in Verbindung mit Amazon Elastic Container Service (Amazon ECS) verwendet.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Traffic auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen. Dieses Muster verwendet die AWS Load Balancer Controller-Kontrollkomponente, um den Application Load Balancer zu erstellen, wenn ein Kubernetes-Ingress bereitgestellt wird. Der Application Load Balancer verteilt den eingehenden Datenverkehr auf mehrere Ziele.

Andere Tools

- Helm ist ein Open-Source-Paketmanager für Kubernetes. In diesem Muster wird Helm verwendet, um den AWS Load Balancer Controller zu installieren.
- Kubernetes ist ein Open-Source-System zur Automatisierung der Bereitstellung, Skalierung und Verwaltung von containerisierten Anwendungen.
- NGINX ist ein leistungsstarker Web- und Reverse-Proxyserver.

Epen

Erstellen Sie einen EKS-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Dateien.	Erstellen Sie mithilfe des Codes im Abschnitt Zusätzliche Informationen die folgenden Dateien: • `clusterconfig-fargate.yaml` • `nginx-deployment.yaml` • `nginx-service.yaml` • `nginx-ingress.yaml` • `index.html`	App-Entwickler, AWS-Administrator, AWS DevOps
Legen Sie Umgebungsvariablen fest.	**Note** Wenn ein Befehl aufgrund früherer unerledigter Aufgaben fehlschlägt, warten Sie einige Sekunden, und führen Sie den Befehl dann erneut aus. Dieses Muster verwendet die AWS-Region und den Clusternamen, die in der Datei definiert sind`clusterconfig-fargate.yaml` . Legen Sie dieselben Werte wie Umgebungsvariablen fest,	App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	um in weiteren Befehlen auf sie zu verweisen.
	`export AWS_REGION="us-east-1"`
	`export CLUSTER_NAME="my-fargate"`	

Erstellen Sie einen EKS-Cluster.	Führen Sie den folgenden Befehl aus, um einen EKS-Cluster zu erstellen, der die Spezifikationen aus der `clusterconfig-fargate.yaml` Datei verwendet. `eksctl create cluster -f clusterconfig-fargate.yaml` Die Datei enthält die`ClusterConfig` , die einen neuen EKS-Cluster mit dem Namen `my-fargate-cluster` `us-east-1` Region und ein Standard-Fargate-Profil (`fp-default`) bereitstellt. Das Fargate-Standardprofil ist mit zwei Selektoren (`default`und`kube-system`) konfiguriert.	App-Entwickler, AWS DevOps, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie den erstellten Cluster.	Führen Sie den folgenden Befehl aus, um den erstellten Cluster zu überprüfen.
	`eksctl get cluster --output yaml`
	Die Ausgabe sollte wie folgt aussehen.
	`- Name: my-fargate`
	`  Owned: "True"`
	`  Region: us-east-1`
	Überprüfen Sie das erstellte Fargate-Profil mit dem`CLUSTER_NAME` .
	`eksctl get fargatepr ofile --cluster $CLUSTER_NAME --output yaml`
	Dieser Befehl zeigt Informationen zu den Ressourcen an. Sie können die Informationen verwenden, um den erstellten Cluster zu überprüfen. Die Ausgabe sollte wie folgt aussehen.
	`- name: fp-default`
	`  podExecutionRoleARN: arn:aws:iam::<YOUR-ACCOUNT-ID>:role/eksctl-my-fargate-`
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`cluster-FargatePod ExecutionRole-xxx`
	`  selectors:`
	`  - namespace: default`
	`  - namespace: kube-system`
	`  status: ACTIVE`
	`  subnets:`
	`  - subnet-aaa`
	`  - subnet-bbb`
	`  - subnet-ccc`	

Stellen Sie einen Container bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie den NGINX-Web server bereit.	Führen Sie den folgenden Befehl aus, um die NGINX-Webserver-Bereitstellung auf dem Cluster anzuwenden.
	`kubectl apply -f ./ nginx-deployment.yaml`
	Die Ausgabe sollte wie folgt aussehen.
	`deployment.apps/nginx-deployment created`
	Die Bereitstellung umfasst drei Repliken des NGINX-Images aus der Amazon ECR Public Gallery. Das Image wird im Standard-Namespace bereitgestellt und auf Port 80
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der laufenden Pods verfügbar gemacht.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Bereitstellung und die Pods.	(Optional) Überprüfen Sie die Bereitstellung. Sie können den Status Ihrer Bereitstellung mit dem folgenden Befehl überprüfen.
	`kubectl get deployment`
	Die Ausgabe sollte wie folgt aussehen.
	`NAME READY UP-TO-DATE AVAILABLE AGE nginx-deployment 3/3 3 3 7m14s`
	Ein Pod ist ein bereitstellbares Objekt in Kubernetes, das einen oder mehrere Container enthält. Führen Sie den folgenden Befehl aus, um alle Pods aufzulisten.
	`kubectl get pods`
	Die Ausgabe sollte wie folgt aussehen.
	`NAME READY STATUS RESTARTS AGE`
		App-Entwickler, AWS DevOps, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`nginx-deployment-xxxx-aaa 1/1 Running 0 94s`
	`nginx-deployment-xxxx-bbb 1/1 Running 0 94s`
	`nginx-deployment-xxxx-ccc 1/1 Running 0 94s`	

Skalieren Sie die Bereitstellung.	Verwenden Sie den folgenden Befehl, um die Bereitstellung von den drei angegebenen Replikaten `deployment.yaml` auf vier Replikate zu skalieren.
	`kubectl scale deployment nginx-deployment --replicas 4`
	Die Ausgabe sollte wie folgt aussehen.
	`deployment.apps/nginx-deployment scaled`
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Stellen Sie einen AWS Load Balancer Controller bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie Umgebungsvariablen fest.	Beschreiben Sie den CloudFormation Stack des Clusters, um Informationen über seine VPC abzurufen.	App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`aws cloudformation describe-stacks --stack-name eksctl-$CLUSTER_NAME-cluster --query "Stacks[0].Outputs[?OutputKey==\`VPC\`].OutputValue"`
	
	Die Ausgabe sollte wie folgt aussehen.
	
	`[ "vpc-<YOUR-VPC-ID>" ]`
	
	Kopieren Sie die VPC-ID und exportieren Sie sie als Umgebungsvariable.
	
	`export VPC_ID="vpc-<YOUR-VPC-ID>"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie IAM für das Cluster-Servicekonto.	Verwenden Sie das `AWS_REGION` und `CLUSTER_NAME` aus dem früheren Epic, um einen IAM Open ID Connect-Anbieter für den Cluster zu erstellen. `eksctl utils associate-iam-oidc-provider \ --region $AWS_REGION \ --cluster $CLUSTER_NAME \ --approve`	App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Laden Sie die IAM-Richtlinie herunter und erstellen Sie sie.	Laden Sie die IAM-Richtlinie für den AWS Load Balancer Controller herunter, die es ihm ermöglicht, in Ihrem Namen Anrufe APIs an AWS zu tätigen.
	`curl -o iam-policy.json https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/main/docs/install/iam_policy.json`
	Erstellen Sie die Richtlinie in Ihrem AWS-Konto mithilfe der AWS-CLI.
	`aws iam create-policy \ --policy-name AWSLoadBalancerControllerIAMPolicy \ --policy-document file://iam-policy.json`
	Die Ausgabe sollte folgender maßen aussehen.
	`{ "Policy": { "PolicyName": "AWSLoadBalancerControllerIAMPolicy", "PolicyId": "<YOUR_POLICY_ID>",`
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Arn": "arn:aws:
	iam::<YOUR-ACCOUNT
	-ID>:policy/AWSLoa
	dBalancerControlle
	rIAMPolicy",
	"Path": "/",
	"DefaultV
	ersionId": "v1",
	"Attachme
	ntCount": 0,
	"Permissi
	onsBoundaryUsageCo
	unt": 0,
	"IsAttachable":
	true,
	"CreateDate":
	"<YOUR-DATE>",
	"UpdateDate":
	"<YOUR-DATE>"
	}
	}</pre> Speichern Sie den Amazon-Ressourcennamen (ARN) der Richtlinie unter`$POLICY_ARN` .
	<pre>export POLICY_AR
	N=”arn:aws:iam::<Y
	OUR-ACCOUNT-ID>:po
	licy/AWSLoadBalanc
	erControllerIAMPol
	icy”</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie ein IAM-Servicekonto.	Erstellen Sie ein `aws-load-balancer-controller` im Namespace benanntes IAM-Dienstkonto. `kube-system` Verwenden Sie die`CLUSTER_NAME`, und`AWS_REGION`, `POLICY_ARN` die Sie zuvor konfiguriert haben.
	`eksctl create iamserviceaccount \ --cluster=$CLUSTER_NAME \ --region=$AWS_REGION \ --attach-policy-arn=$POLICY_ARN \ --namespace=kube-system \ --name=aws-load-balancer-controller \ --override-existing-serviceaccounts \ --approve`
	Überprüfen Sie die Erstellung.
	`eksctl get iamserviceaccount \ --cluster $CLUSTER_NAME \ --name aws-load-balancer-controller \ --namespace kube-system \ --output yaml`
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Die Ausgabe sollte wie folgt aussehen.
	
	`- metadata:`
	`    name: aws-load-balancer-controller`
	`    namespace: kube-system`
	`  status:`
	`    roleARN: arn:aws:iam::<YOUR-ACCOUNT-ID>:role/eksctl-my-fargate-addon-iam serviceaccount-ku-Role1-<YOUR-ROLE-ID>`
	`  wellKnownPolicies:`
	`    autoScaler: false`
	`    awsLoadBalancerController: false`
	`    certManager: false`
	`    ebsCSIController: false`
	`    efsCSIController: false`
	`    externalDNS: false`
	`    imageBuilder: false`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie den AWS Load Balancer Controller.	Aktualisieren Sie das Helm-Repository.
	`helm repo update`
	Fügen Sie das Amazon EKS-Chart-Repository zum Helm-Repo hinzu.
	`helm repo add eks https://aws.github.io/eks-charts`
	Wenden Sie die benutzerdefinierten Kubernetes-Ressourcendefinitionen (CRDs) an, die vom AWS Load Balancer Controller eks-chart im Hintergrund verwendet werden.
	`kubectl apply -k "github.com/aws/eks-charts/stable/aws-load-balancer-controller//crds?ref=master"`
	Die Ausgabe sollte wie folgt aussehen.
	`customresourcedefinition.apiextensions.k8s.io/ingressclassparams.elbv2.k8s.aws created`
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`customresourcedefinition.apiextensions.k8s.io/targetgroupbindings.elbv2.k8s.aws created`
	
	Installieren Sie das Helm-Diagramm mithilfe der Umgebungsvariablen, die Sie zuvor festgelegt haben.
	
	`helm install aws-load-balancer-controller eks/aws-load-balancer-controller \ --set clusterName=$CLUSTER_NAME \ --set serviceAccount.create=false \ --set region=$AWS_REGION \ --set vpcId=$VPC_ID \ --set serviceAccount.name=aws-load-balancer-controller \ -n kube-system`
	
	Die Ausgabe sollte wie folgt aussehen.
	
	`NAME: aws-load-balancer-controller LAST DEPLOYED: <YOUR-DATE> NAMESPACE: kube-system STATUS: deployed REVISION: 1 TEST SUITE: None NOTES:`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`AWS Load Balancer controller installed!`	

Erstellen Sie einen NGINX-Service.	Erstellen Sie einen Dienst, um die NGINX-Pods mithilfe der Datei verfügbar zu machen. `nginx-service.yaml`
	`kubectl apply -f nginx-service.yaml`
	Die Ausgabe sollte wie folgt aussehen.
	`service/nginx-service created`
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Erstellen Sie die Kubernetes-Ingress-Ressource.	Erstellen Sie einen Dienst, um den Kubernetes-NGINX-Ingress mithilfe der Datei verfügbar zu machen. `nginx-ingress.yaml`
	`kubectl apply -f nginx-ingress.yaml`
	Die Ausgabe sollte wie folgt aussehen.
	`ingress.networking.k8s.io/nginx-ingress created`
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Rufen Sie die Load Balancer-URL ab.	Verwenden Sie den folgenden Befehl, um die Eingangsinformationen abzurufen.
	`kubectl get ingress nginx-ingress`
	Die Ausgabe sollte wie folgt aussehen.
	`NAME CLASS HOSTS ADDRESS PORTS AGE`
	`nginx-ingress <none> * k8s-default-nginxing-xxx.us-east-1.elb.amazonaws.com 80 80s`
	Kopieren Sie die ADDRESS (z. B. `k8s-default-nginxing-xxx.us-east-1.elb.amazonaws.com`) aus der Ausgabe und fügen Sie sie in Ihren Browser ein, um auf die `index.html` Datei zuzugreifen.
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Debuggen Sie laufende Container

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Wählen Sie einen Pod aus.	Listet alle Pods auf und kopiert den Namen des gewünschten Pods.
	`kubectl get pods`
	Die Ausgabe sollte wie folgt aussehen.
	`NAME READY STATUS RESTARTS AGE nginx-deployment-xxxx-aaa 1/1 Running 0 55m nginx-deployment-xxxx-bbb 1/1 Running 0 55m nginx-deployment-xxxx-ccc 1/1 Running 0 55m nginx-deployment-xxxx-ddd 1/1 Running 0 42m`
	Dieser Befehl listet die vorhandenen Pods und zusätzliche Informationen auf.
	Wenn Sie an einem bestimmte n Pod interessiert sind, geben
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie den Namen des Pods, an dem Sie interessiert sind, für die `POD_NAME` Variable ein oder legen Sie ihn als Umgebungsvariable fest. Andernfalls lassen Sie diesen Parameter weg, um nach allen Ressourcen zu suchen. `export POD_NAME="nginx-deployment-<YOUR-POD-NAME>"`	
Greifen Sie auf die Protokolle zu.	Rufen Sie die Protokolle von dem Pod ab, den Sie debuggen möchten. `kubectl logs $POD_NAME`	App-Entwickler, AWS-Systemadministrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Leiten Sie den NGINX-Port weiter.	Verwenden Sie Port-Forwarding, um den Port des Pods für den Zugriff auf den NGINX-Webserver einem Port auf Ihrem lokalen Computer zuzuordnen.
	`kubectl port-forward deployment/nginx-deployment 8080:80`
	Öffnen Sie in Ihrem Browser die folgende URL.
	`http://localhost:8080`
	Der `port-forward` Befehl ermöglicht den Zugriff auf die `index.html` Datei, ohne sie über einen Load Balancer öffentlich verfügbar zu machen. Dies ist nützlich, um beim Debuggen auf die laufende Anwendung zuzugreifen. Sie können die Portweiterleitung beenden, indem Sie den Tastaturbefehl Strg+C drücken.
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie Befehle innerhalb des Pods aus.	Verwenden Sie den folgenden Befehl, um sich die aktuelle `index.html` Datei anzusehen. `kubectl exec $POD_NAME -- cat /usr/share/nginx/html/index.html` Sie können den `exec` Befehl verwenden, um jeden Befehl direkt im Pod auszuführen. Dies ist nützlich für das Debuggen laufender Anwendungen.	App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Dateien in einen Pod kopieren.	Entfernen Sie die `index.html` Standarddatei auf diesem Pod.
	`kubectl exec $POD_NAME -- rm /usr/share/nginx/html/index.html`
	Laden Sie die benutzerdefinierte lokale Datei `index.html` auf den Pod hoch.
	`kubectl cp index.html $POD_NAME:/usr/share/nginx/html/`
	Sie können den `cp` Befehl verwenden, um Dateien direkt zu einem der Pods zu ändern oder hinzuzufügen.
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Verwenden Sie Port-Forwarding, um die Änderung anzuzeigen.	Verwenden Sie die Portweiterleitung, um die Änderungen zu überprüfen, die Sie an diesem Pod vorgenommen haben.
	`kubectl port-forward pod/$POD_NAME 8080:80`
	Öffnen Sie die folgende URL in Ihrem Browser.
	`http://localhost:8080`
	Die an der `index.html` Datei vorgenommenen Änderungen sollten im Browser sichtbar sein.
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Löschen von Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Löschen Sie den Load Balancer.	Löschen Sie den Eingang.
	`kubectl delete ingress/nginx-ingress`
	Die Ausgabe sollte wie folgt aussehen.
	`ingress.networking.k8s.io "nginx-ingress" deleted`
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Löschen Sie den Service:
	`kubectl delete service/nginx-service`
	Die Ausgabe sollte wie folgt aussehen.
	`service "nginx-service" deleted`
	Löschen Sie den Load Balancer-Controller.
	`helm delete aws-load-balancer-controller -n kube-system`
	Die Ausgabe sollte wie folgt aussehen.
	`release "aws-load-balancer-controller" uninstalled`
	Löschen Sie das Dienstkonto.
	`eksctl delete iamserviceaccount --cluster $CLUSTER_NAME --namespace kube-system --name aws-load-balancer-controller`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Löschen Sie die Bereitstellung.	Verwenden Sie den folgenden Befehl, um die Bereitstellungsressourcen zu löschen.
	`kubectl delete deploy/nginx-deployment`
	Die Ausgabe sollte wie folgt aussehen.
	`deployment.apps "nginx-deployment" deleted`
		App-Entwickler, AWS DevOps, AWS-Systemadministrator

Löschen Sie den Cluster.	Löschen Sie den EKS-Cluster mithilfe des folgenden Befehls, wobei der Clustername `my-fargate` steht. `eksctl delete cluster --name $CLUSTER_NAME` Mit diesem Befehl wird der gesamte Cluster einschließlich aller zugehörigen Ressourcen gelöscht.	App-Entwickler, AWS DevOps, AWS-Systemadministrator
Löschen Sie die IAM-Richtlinie.	Löschen Sie die zuvor erstellte Richtlinie mithilfe der AWS-CLI. `aws iam delete-policy --policy-arn $POLICY_ARN`	App-Entwickler, AWS-Administrator, AWS DevOps

Fehlerbehebung

Problem	Lösung
Sie erhalten bei der Clustererstellung eine Fehlermeldung, die besagt, dass Ihre Ziel-Availability Zone nicht über genügend Kapazität verfügt, um den Cluster zu unterstützen. Sie sollten eine Meldung ähnlich der folgenden sehen. `Cannot create cluster 'my-fargate' because us-east-1e, the targeted availability zone, does not currently have sufficient capacity to support the cluster. Retry and choose from these availability zones: us-east-1a, us-east-1b, us-east-1c, us-east-1d, us-east-1f`	Erstellen Sie den Cluster erneut und verwenden Sie dabei die in der Fehlermeldung empfohlenen Availability Zones. Geben Sie in der letzten Zeile Ihrer `clusterconfig-fargate.yaml` Datei eine Liste von Availability Zones an (z. B.`availabilityZones: ["us-east-1a", "us-east-1b", "us-east-1c"]`).

Zugehörige Ressourcen

- Amazon EKS-Dokumentation
- Application Load Balancing in Amazon EKS
- Leitfäden zu bewährten Methoden von EKS
- Dokumentation zum AWS Load Balancer Controller
- eksctl-Dokumentation
- NGINX-Bild der öffentlichen Galerie von Amazon ECR
- Helm-Dokumentation
- Running Pods debuggen (Kubernetes-Dokumentation)
- Workshop zu Amazon EKS
- Fehler bei der Erstellung des EKS-Clusters

Zusätzliche Informationen

clusterconfig-fargate.yaml

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: my-fargate
  region: us-east-1

fargateProfiles:
  - name: fp-default
    selectors:
      - namespace: default
      - namespace: kube-system
```

nginx-bereitstellung.yaml

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: "nginx-deployment"
  namespace: "default"
spec:
  replicas: 3
  selector:
    matchLabels:
      app: "nginx"
  template:
    metadata:
      labels:
        app: "nginx"
    spec:
      containers:
      - name: nginx
        image: public.ecr.aws/nginx/nginx:latest
        ports:
        - containerPort: 80
```

nginx-service.yaml

```
apiVersion: v1
```

```
kind: Service
metadata:
  annotations:
    alb.ingress.kubernetes.io/target-type: ip
  name: "nginx-service"
  namespace: "default"
spec:
  ports:
  - port: 80
    targetPort: 80
    protocol: TCP
  type: NodePort
  selector:
    app: "nginx"
```

nginx-ingress.yaml

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  namespace: "default"
  name:  "nginx-ingress"
  annotations:
    kubernetes.io/ingress.class: alb
    alb.ingress.kubernetes.io/scheme: internet-facing
spec:
  rules:
    - http:
        paths:
        - path: /
          pathType: Prefix
          backend:
            service:
              name: "nginx-service"
              port:
                number: 80
```

index.html

```
<!DOCTYPE html>
<html>

<body>
```

```
    <h1>Welcome to your customized nginx!</h1>
    <p>You modified the file on this running pod</p>
</body>

</html>
```

Container mithilfe von Elastic Beanstalk bereitstellen

Erstellt von Thomas Scott (AWS) und Jean-Baptiste Guillois (AWS)

Übersicht

In der Amazon Web Services (AWS) Cloud unterstützt AWS Elastic Beanstalk Docker als verfügbare Plattform, sodass Container mit der erstellten Umgebung ausgeführt werden können. Dieses Muster zeigt, wie Container mithilfe des Elastic Beanstalk-Service bereitgestellt werden. Bei der Bereitstellung dieses Musters wird die auf der Docker-Plattform basierende Webserver-Umgebung verwendet.

Um Elastic Beanstalk für die Bereitstellung und Skalierung von Webanwendungen und Services zu verwenden, laden Sie Ihren Code hoch und die Bereitstellung erfolgt automatisch. Kapazitätsbereitstellung, Lastenausgleich, automatische Skalierung und Überwachung des Anwendungszustands sind ebenfalls enthalten. Wenn Sie Elastic Beanstalk verwenden, können Sie die volle Kontrolle über die AWS-Ressourcen übernehmen, die Elastic Beanstalk in Ihrem Namen erstellt. Für die Nutzung von Elastic Beanstalk fallen keine zusätzlichen Gebühren an. Sie zahlen nur für die AWS-Ressourcen, die zum Speichern und Ausführen Ihrer Anwendungen verwendet werden.

Dieses Muster enthält Anweisungen für die Bereitstellung mithilfe der AWS Elastic Beanstalk Command Line Interface (EB CLI) und der AWS-Managementkonsole.

Anwendungsfälle

Zu den Anwendungsfällen für Elastic Beanstalk gehören:

- Stellen Sie eine Prototypumgebung bereit, um eine Frontend-Anwendung zu demonstrieren. (Dieses Muster verwendet ein Dockerfile als Beispiel.)
- Stellen Sie eine API bereit, um API-Anfragen für eine bestimmte Domain zu bearbeiten.
- Stellen Sie eine Orchestrierungslösung mithilfe von Docker-Compose bereit (`docker-compose.yml`wird in diesem Muster nicht als praktisches Beispiel verwendet).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein AWS-Konto
- AWS EB CLI lokal installiert

- Docker ist auf einem lokalen Computer installiert

Einschränkungen

- Im kostenlosen Tarif gibt es ein Docker-Pull-Limit von 100 Pulls pro 6 Stunden pro IP-Adresse.

Architektur

Zieltechnologie-Stack

- Amazon Elastic Compute Cloud (Amazon EC2) -Instanzen
- Sicherheitsgruppe
- Application Load Balancer
- Auto Scaling-Gruppe

Zielarchitektur

Automatisierung und Skalierung

AWS Elastic Beanstalk kann automatisch auf der Grundlage der Anzahl der gestellten Anfragen skalieren. Zu den für eine Umgebung erstellten AWS-Ressourcen gehören ein Application Load Balancer, eine Auto Scaling Scaling-Gruppe und eine oder mehrere EC2 Amazon-Instances.

Der Load Balancer befindet sich vor den EC2 Amazon-Instances, die Teil der Auto Scaling Scaling-Gruppe sind. Amazon EC2 Auto Scaling startet automatisch zusätzliche EC2 Amazon-Instances, um der zunehmenden Belastung Ihrer Anwendung Rechnung zu tragen. Wenn die Auslastung Ihrer Anwendung abnimmt, stoppt Amazon EC2 Auto Scaling Instances, hält aber mindestens eine Instance am Laufen.

Automatische Skalierung löst aus

Die Auto Scaling Scaling-Gruppe in Ihrer Elastic Beanstalk Beanstalk-Umgebung verwendet zwei CloudWatch Amazon-Alarme, um Skalierungsvorgänge einzuleiten. Mit den Standardauslösern wird die Skalierung durchgeführt, wenn der durchschnittliche ausgehende Netzwerkdatenverkehr von der jeweiligen Instance innerhalb von 5 Minuten 6 MB über- oder 2 MB unterschreitet. Um Amazon EC2 Auto Scaling effektiv zu nutzen, konfigurieren Sie Trigger, die für Ihre Anwendung, Ihren Instance-Typ und Ihre Serviceanforderungen geeignet sind. Sie können die Skalierung anhand unterschiedlicher

Statistiken wie Latenz, Festplatten-I/O-Vorgänge, CPU-Auslastung und Anforderungsanzahl ausführen. Weitere Informationen finden Sie unter Auto Scaling-Trigger.

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS EB Command Line Interface (EB CLI) ist ein Befehlszeilenclient, mit dem Sie Elastic Beanstalk Beanstalk-Umgebungen erstellen, konfigurieren und verwalten können.
- Elastic Load Balancing verteilt den eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Traffic auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen.

Andere Dienste

- Docker packt Software in standardisierte Einheiten, sogenannte Container, die Bibliotheken, Systemtools, Code und Laufzeit enthalten.

Code

Der Code für dieses Muster ist im GitHub Cluster Sample Application Repository verfügbar.

Epen

Mit einem Dockerfile erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Remote-Repository.	• Führen Sie den Befehl aus, um das Repository zu klonen`git clone https://github.com/aws-samples/cluster-sample-app.git` . < /p >	App-Entwickler, AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initialisieren Sie das Elastic Beanstalk Docker-Projekt.	1. Erstellen Sie eine Datei mit dem Namen `aws.json` im Stammverzeichnis. 2. Fügen Sie der `aws.json` Datei den folgenden Code hinzu. `{ "AWSEBDockerrunVersion":"1", "Image":{ "Name":"cluster-sample-app" }, "Ports":[ { "ContainerPort":80 , "HostPort":8080 } ] }` 3. Führen Sie den Befehl `eb init -p docker` im Stammverzeichnis des Projekts aus.	App-Entwickler, AWS-Administrator, AWS DevOps
Testen Sie das Projekt lokal.	1. Führen Sie den Befehl `eb local run` im Stammverzeichnis des Projekts aus. 2. Testen Sie die Anwendung, indem Sie zu `http://localhost` navigieren.	App-Entwickler, AWS-Administrator, AWS DevOps

Mit EB CLI bereitstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den Bereitste llungsbefehl aus	1. Führen Sie den Befehl `eb create docker-sa mple-cluster-app` im Stammverzeichnis des Projekts aus.	App-Entwickler, AWS-Admin istrator, AWS DevOps
Greifen Sie auf die bereitges tellte Version zu.	Nachdem der Bereitste llungsbefehl abgeschlossen ist, greifen Sie mit dem `eb open` Befehl auf das Projekt zu.	App-Entwickler, AWS-Admin istrator, AWS DevOps

Mit der Konsole bereitstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung mithilfe des Browsers bereit.	1. Öffnen Sie die -Konsole. 2. Navigieren Sie zur Elastic Beanstalk Beanstalk-Konsole. 3. Wählen Sie Anwendung erstellen. 4. Geben Sie als Anwendung snamen Cluster-Sample-App ein. 5. Wählen Sie Docker als Plattform. 6. Wählen Sie Code hochladen. 7. Wählen Sie Ihre lokale ZIP-Datei (im Stammverz	App-Entwickler, AWS-Admin istrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eichnis des geklonten Projekts) oder eine öffentlic he Amazon Simple Storage Service (Amazon S3) -URL.	
Greifen Sie auf die bereitges tellte Version zu.	Greifen Sie nach der Bereitste llung auf die bereitgestellte Anwendung zu und wählen Sie die angegebene URL aus.	App-Entwickler, AWS-Admin istrator, AWS DevOps

Zugehörige Ressourcen

- Webserver-Umgebungen
- Installieren Sie die EB CLI auf macOS
- Manuelles Installieren der EB-CLI

Zusätzliche Informationen

Vorteile der Verwendung von Elastic Beanstalk

- Automatische Bereitstellung der Infrastruktur
- Automatische Verwaltung der zugrunde liegenden Plattform
- Automatisches Patchen und Updates zur Unterstützung der Anwendung
- Automatische Skalierung der Anwendung
- Möglichkeit, die Anzahl der Knoten anzupassen
- Möglichkeit, bei Bedarf auf die Infrastrukturkomponenten zuzugreifen
- Einfache Bereitstellung im Vergleich zu anderen Container-Bereitstellungslösungen

Generieren Sie eine statische ausgehende IP-Adresse mithilfe einer Lambda-Funktion, Amazon VPC und einer serverlosen Architektur

Erstellt von Thomas Scott (AWS)

Übersicht

Dieses Muster beschreibt, wie eine statische ausgehende IP-Adresse in der Amazon Web Services (AWS) -Cloud mithilfe einer serverlosen Architektur generiert wird. Ihr Unternehmen kann von diesem Ansatz profitieren, wenn es Dateien mithilfe des Secure File Transfer Protocol (SFTP) an eine separate Geschäftseinheit senden möchte. Das bedeutet, dass die Geschäftseinheit Zugriff auf eine IP-Adresse haben muss, über die Dateien ihre Firewall passieren können.

Der Ansatz des Musters hilft Ihnen bei der Erstellung einer AWS Lambda Lambda-Funktion, die eine Elastic IP-Adresse als ausgehende IP-Adresse verwendet. Wenn Sie die Schritte in diesem Muster befolgen, können Sie eine Lambda-Funktion und eine Virtual Private Cloud (VPC) erstellen, die ausgehenden Datenverkehr über ein Internet-Gateway mit einer statischen IP-Adresse weiterleitet. Um die statische IP-Adresse zu verwenden, fügen Sie die Lambda-Funktion der VPC und ihren Subnetzen hinzu.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS Identity and Access Management (IAM) -Berechtigungen zum Erstellen und Bereitstellen einer Lambda-Funktion sowie zum Erstellen einer VPC und ihrer Subnetze. Weitere Informationen dazu finden Sie unter Ausführungsrolle und Benutzerberechtigungen in der AWS Lambda Lambda-Dokumentation.
- Wenn Sie den Ansatz dieses Musters mithilfe von Infrastructure as Code (IaC) implementieren möchten, benötigen Sie eine integrierte Entwicklungsumgebung (IDE) wie AWS Cloud9. Weitere Informationen dazu finden Sie unter Was ist AWS Cloud9? in der AWS Cloud9 Cloud9-Dokumentation.

Architektur

Das folgende Diagramm zeigt die serverlose Architektur für dieses Muster.

Das Diagramm zeigt den folgenden Workflow:

1. Ausgehender Verkehr geht `NAT gateway 1` rein. `Public subnet 1`
2. Ausgehender Verkehr geht `NAT gateway 2` rein. `Public subnet 2`
3. Die Lambda-Funktion kann in `Private subnet 1` oder `Private subnet 2` ausgeführt werden.
4. `Private subnet 1`und leitet `Private subnet 2` den Verkehr zu den NAT-Gateways in den öffentlichen Subnetzen weiter.
5. Die NAT-Gateways senden ausgehenden Datenverkehr von den öffentlichen Subnetzen an das Internet-Gateway.
6. Ausgehende Daten werden vom Internet-Gateway zum externen Server übertragen.

Technologie-Stack

- Lambda
- Amazon Virtual Private Cloud (Amazon VPC)

Automatisierung und Skalierung

Sie können Hochverfügbarkeit (HA) sicherstellen, indem Sie zwei öffentliche und zwei private Subnetze in unterschiedlichen Availability Zones verwenden. Selbst wenn eine Availability Zone nicht mehr verfügbar ist, funktioniert die Pattern-Lösung weiterhin.

Tools

- AWS Lambda — AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.
- Amazon VPC — Amazon Virtual Private Cloud (Amazon VPC) stellt einen logisch isolierten Bereich der AWS-Cloud bereit, in dem Sie AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können. Dieses virtuelle Netzwerk entspricht weitgehend einem herkömmlichen

Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben, kann jedoch die Vorzüge der skalierbaren Infrastruktur von AWS nutzen.

Epen

Erstellen einer neuen VPC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer neuen VPC.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon VPC-Konsole und erstellen Sie dann eine VPC mit `Lambda VPC` dem Namen `10.0.0.0/25` IPv4 CIDR-Bereich. Weitere Informationen zum Erstellen einer VPC finden Sie unter Erste Schritte mit Amazon VPC in der Amazon VPC-Dokumentation.	AWS-Administrator

Erstellen Sie zwei öffentliche Subnetze

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das erste öffentliche Subnetz.	1. Wählen Sie in der Amazon VPC-Konsole Subnets und dann Create Subnet aus. 2. Geben Sie für Name Tag `public-one` ein. 3. Wählen Sie für VPC `Lambda VPC` aus.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie eine Availability Zone und zeichnen Sie sie auf. 5. Geben Sie für IPv4 CIDR-Block den Wert Subnetz erstellen ein **`10.0.0.0/28`** und wählen Sie dann Create subnet aus.	
Erstellen Sie das zweite öffentliche Subnetz.	1. Wählen Sie in der Amazon VPC-Konsole Subnets und dann Create Subnet aus. 2. Geben Sie für Name Tag `public-two` ein. 3. Wählen Sie für VPC `Lambda VPC` aus. 4. **Important** Wählen Sie eine Availability Zone und zeichnen Sie sie auf. : Sie können die Availability Zone, die das `public-one` Subnetz enthält, nicht verwenden. 5. Geben Sie für IPv4 CIDR-Block den Wert Subnetz erstellen ein `10.0.0.16/28` und wählen Sie dann Create subnet aus.	AWS-Administrator

Erstellen Sie zwei private Subnetze

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das erste private Subnetz.	1. Wählen Sie in der Amazon VPC-Konsole Subnets und dann Create Subnet aus. 2. Geben Sie für Name Tag `private-one` ein. 3. Wählen Sie für VPC `Lambda VPC` aus. 4. Wählen Sie die Availability Zone aus, die das `public-one` Subnetz enthält, das Sie zuvor erstellt haben. 5. Geben Sie als IPv4 CIDR-Block Subnetz erstellen ein `10.0.0.32/28` und wählen Sie dann Create subnet aus.	AWS-Administrator
Erstellen Sie das zweite private Subnetz.	1. Wählen Sie in der Amazon VPC-Konsole Subnets und dann Create Subnet aus. 2. Geben Sie für Name Tag `private-two` ein. 3. Wählen Sie für VPC `Lambda VPC` aus. 4. Wählen Sie dieselbe Availability Zone, die das `public-two` Subnetz enthält, das Sie zuvor erstellt haben. 5. Geben Sie für IPv4 CIDR-Block Subnetz erstellen	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ein `10.0.0.64/28` und wählen Sie dann Create subnet aus.	

Erstellen Sie zwei Elastic IP-Adressen für Ihre NAT-Gateways

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die erste Elastic IP-Adresse.	1. Wählen Sie in der Amazon VPC-Konsole Elastic IPs und dann Allocate new address aus. 2. Wählen Sie Allocate und notieren Sie die Allocation ID für Ihre neu erstellte Elastic IP-Adresse. **Note** Diese Elastic IP-Adresse wird für Ihr erstes NAT-Gateway verwendet.	AWS-Administrator
Erstellen Sie die zweite Elastic IP-Adresse.	1. Wählen Sie in der Amazon VPC-Konsole Elastic IPs und dann Allocate new address aus. 2. Wählen Sie Allocate und notieren Sie die Allocation ID für diese zweite Elastic IP-Adresse.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Diese Elastic IP-Adresse wird für Ihr zweites NAT-Gateway verwendet.	

Ein Internet-Gateway erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen eines Internet-Gateways	1. Wählen Sie in der Amazon VPC-Konsole Internet Gateways und dann Create Internet Gateway aus. 2. Geben Sie `Lambda internet gateway` den Namen ein und wählen Sie dann Internet-Gateway erstellen. Stellen Sie sicher, dass Sie die Internet-Gateway-ID notieren.	AWS-Administrator
Verbinden Sie das Internet-Gateway mit der VPC.	Wählen Sie zuerst das Internet-Gateway aus, das Sie eben erstellt haben, und anschließend Actions, Attach to VPC (Aktionen, An VPC anfügen).	AWS-Administrator

Erstellen Sie zwei NAT-Gateways

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das erste NAT-Gateway.	1. Wählen Sie auf der Amazon VPC-Konsole NAT Gateways und dann Create NAT Gateway aus. 2. Geben Sie den `nat-one` Namen des NAT-Gateways ein. 3. Wählen Sie `public-one` als Subnetz, in dem das NAT-Gateway erstellt werden soll. 4. Wählen Sie als Konnektivitätstyp die Option Öffentlich aus. 5. Wählen Sie für Elastic IP Allocation ID die erste Elastic IP-Adresse aus, die Sie zuvor erstellt haben, und verknüpfen Sie sie mit dem NAT-Gateway. 6. Wählen Sie NAT-Gateway erstellen aus.	AWS-Administrator
Erstellen Sie das zweite NAT-Gateway.	1. Wählen Sie auf der Amazon VPC-Konsole NAT Gateways und dann Create NAT Gateway aus. 2. Geben Sie den `nat-two` Namen des NAT-Gateways ein.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie `public-two` als Subnetz, in dem das NAT-Gateway erstellt werden soll. 4. Wählen Sie als Konnektivitätstyp die Option Öffentlich aus. 5. Wählen Sie für Elastic IP Allocation ID die zweite Elastic IP-Adresse aus, die Sie zuvor erstellt haben, und verknüpfen Sie sie mit dem NAT-Gateway. 6. Wählen Sie NAT-Gateway erstellen aus.	

Erstellen Sie Routentabellen für Ihre öffentlichen und privaten Subnetze

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Routing-Tabelle für das öffentliche Subnetz.	1. Wählen Sie in der Amazon VPC-Konsole Route Tables und dann Create Route Table aus. 2. Geben Sie `public-one-subnet` den Namen der Routentabelle ein und wählen Sie dann Routentabelle erstellen. 3. Wählen Sie die `public-one-subnet` Routentabelle, dann Routen bearbeite	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	n und anschließend Route hinzufügen aus. 4. Geben Sie `0.0.0.0` dies im Feld Ziel an und wählen Sie dann die Internet-Gateway-ID in der Zielliste aus. 5. Wählen Sie auf der Registerkarte Subnetzzuordnungen die Option Subnetzzuordnungen bearbeiten aus, wählen Sie das **`public-one`** Subnetz mit dem **`10.0.0.0/28`** CIDR-Bereich aus, und klicken Sie dann auf Verknüpfungen speichern. 6. Wählen Sie Save Changes.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Routing-Tabelle für das Public-Two-Subnetz.	1. Wählen Sie in der Amazon VPC-Konsole Route Tables und dann Create Route Table aus. 2. Geben Sie `public-two-subnet` den Namen der Routentabelle ein und wählen Sie dann Routentabelle erstellen. 3. Wählen Sie die `public-two-subnet` Routentabelle, dann Routen bearbeiten und anschließend Route hinzufügen aus. 4. Geben Sie `0.0.0.0` dies im Feld Ziel an und wählen Sie dann die Internet-Gateway-ID in der Zielliste aus. 5. Wählen Sie auf der Registerkarte Subnetzzuordnungen die Option Subnetzzuordnungen bearbeiten aus, wählen Sie das **`public-two`** Subnetz mit dem **`10.0.0.16/28`** CIDR-Bereich aus, und klicken Sie dann auf Verknüpfungen speichern. 6. Wählen Sie Save Changes.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Routing-Tabelle für das private One-Subnetz.	1. Wählen Sie in der Amazon VPC-Konsole Route Tables und dann Create Route Table aus. 2. Geben Sie `private-one-subnet` den Namen der Routentabelle ein und wählen Sie dann Routentabelle erstellen. 3. Wählen Sie die `private-one-subnet` Routentabelle, dann Routen bearbeiten und anschließend Route hinzufügen aus. 4. Geben Sie `0.0.0.0` dies im Feld Ziel an und wählen Sie dann das NAT-Gateway im `public-one` Subnetz in der Zielliste aus. 5. Wählen Sie auf der Registerkarte Subnetzzuordnungen die Option Subnetzzuordnungen bearbeiten aus, wählen Sie das **`private-one`** Subnetz mit dem **`10.0.0.32/28`** CIDR-Bereich aus, und klicken Sie dann auf Verknüpfungen speichern. 6. Wählen Sie Save Changes.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Routing-Tabelle für das Private-Two-Subnetz.	1. Wählen Sie in der Amazon VPC-Konsole Route Tables und dann Create Route Table aus. 2. Geben Sie `private-two-subnet` den Namen der Routentabelle ein und wählen Sie dann Routentabelle erstellen. 3. Wählen Sie die `private-two-subnet` Routentabelle, dann Routen bearbeiten und anschließend Route hinzufügen aus. 4. Geben Sie `0.0.0.0` dies im Feld Ziel an und wählen Sie dann das NAT-Gateway im `public-two` Subnetz in der Zielliste aus. 5. Wählen Sie auf der Registerkarte Subnetzzuordnungen die Option Subnetzzuordnungen bearbeiten aus, wählen Sie das **`private-two`** Subnetz mit dem **`10.0.0.64/28`** CIDR-Bereich aus, und klicken Sie dann auf Verknüpfungen speichern. 6. Wählen Sie Save Changes.	AWS-Administrator

Erstellen Sie die Lambda-Funktion, fügen Sie sie der VPC hinzu und testen Sie die Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine neue Lambda-Funktion.	1. Öffnen Sie die AWS Lambda Lambda-Konsole und wählen Sie Create function. 2. Geben Sie unter Basisinfo rmationen `Lambda test` unter Funktionsname ein und wählen Sie dann unter Runtime die Sprache Ihrer Wahl aus. 3. Wählen Sie Funktion erstellen.	AWS-Administrator
Fügen Sie die Lambda-Fu nktion zu Ihrer VPC hinzu.	1. Wählen Sie in der AWS Lambda Lambda-Konsole Funktionen und dann die Funktion aus, die Sie zuvor erstellt haben. 2. Wählen Sie Konfiguration und dann VPC aus. 3. Wählen Sie Bearbeiten und anschließend beide privaten Subnetze aus `Lambda VPC`. 4. Wählen Sie zu Testzweck en die Standardsicherheit sgruppe und dann Speichern aus.	AWS-Administrator
Schreiben Sie Code, um einen externen Service aufzurufen.	1. Schreiben Sie in der Programmiersprache Ihrer Wahl Code, um einen	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	externen Dienst aufzurufen, der Ihre IP-Adresse zurückgibt. 2. Stellen Sie sicher, dass die zurückgegebene IP-Adresse mit einer Ihrer Elastic IP-Adressen übereinstimmt.	

Zugehörige Ressourcen

- Konfigurieren einer Lambda-Funktion für den Zugriff auf Ressourcen in einer VPC

Automatische Identifizierung doppelter Container-Images bei der Migration zu einem Amazon ECR-Repository

Erstellt von Rishabh Yadav (AWS) und Rishi Singla (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Das Muster bietet eine automatisierte Lösung zur Identifizierung, ob es sich bei Bildern, die in verschiedenen Container-Repositorys gespeichert sind, um Duplikate handelt. Diese Prüfung ist nützlich, wenn Sie planen, Bilder aus anderen Container-Repositorys zu Amazon Elastic Container Registry (Amazon ECR) zu migrieren.

Für grundlegende Informationen beschreibt das Muster auch die Komponenten eines Container-Images, wie z. B. den Image-Digest, das Manifest und die Tags. Wenn Sie eine Migration zu Amazon ECR planen, entscheiden Sie sich möglicherweise dafür, Ihre Container-Images zwischen den Container-Registern zu synchronisieren, indem Sie die Digests der Images vergleichen. Bevor Sie Ihre Container-Images migrieren, müssen Sie überprüfen, ob diese Images bereits im Amazon ECR-Repository vorhanden sind, um Duplikate zu vermeiden. Es kann jedoch schwierig sein, Duplikate durch den Vergleich von Image-Digests zu erkennen, und dies kann zu Problemen in der ersten Migrationsphase führen. Dieses Muster vergleicht die Digests zweier ähnlicher Bilder, die in unterschiedlichen Container-Registern gespeichert sind, und erklärt, warum die Digests variieren, damit Sie Bilder genau vergleichen können.

Voraussetzungen und Einschränkungen

- Ein aktiver AWS-Konto
- Zugriff auf das öffentliche Amazon ECR-Register
- Vertrautheit mit den folgenden Themen: AWS-Services
  - AWS CodeCommit
  - AWS CodePipeline
  - AWS CodeBuild
  - AWS Identity and Access Management (ICH BIN)
  - Amazon Simple Storage Service (Amazon-S3)

- Konfigurierte CodeCommit Anmeldeinformationen (siehe Anweisungen)

Architektur

Container-Image-Komponenten

Das folgende Diagramm zeigt einige der Komponenten eines Container-Images. Diese Komponenten werden im Anschluss an das Diagramm beschrieben.

Begriffe und Definitionen

Die folgenden Begriffe sind in der Image Specification der Open Container Initiative (OCI) definiert.

- Registry: Ein Dienst für die Speicherung und Verwaltung von Bildern.
- Client: Ein Tool, das mit Registern kommuniziert und mit lokalen Bildern arbeitet.
- Push: Der Prozess zum Hochladen von Bildern in eine Registry.
- Pull: Der Prozess zum Herunterladen von Bildern aus einer Registry.
- Blob: Die binäre Form von Inhalten, die in einer Registry gespeichert werden und mit einem Digest adressiert werden können.
- Index: Ein Konstrukt, das mehrere Image-Manifeste für verschiedene Computerplattformen (wie x86-64 oder ARM 64-Bit) oder Medientypen identifiziert. Weitere Informationen finden Sie in der OCI Image Index Specification.
- Manifest: Ein JSON-Dokument, das ein Bild oder Artefakt definiert, das über den Endpunkt des Manifests hochgeladen wird. Ein Manifest kann mithilfe von Deskriptoren auf andere Blobs in einem Repository verweisen. Weitere Informationen finden Sie in der OCI Image Manifest Specification.
- Dateisystemebene: Systembibliotheken und andere Abhängigkeiten für ein Bild.
- Konfiguration: Ein Blob, der Artefakt-Metadaten enthält und auf den im Manifest verwiesen wird. Weitere Informationen finden Sie in der OCI-Image-Konfigurationsspezifikation.
- Objekt oder Artefakt: Ein konzeptionelles Inhaltselement, das als Blob gespeichert und einem zugehörigen Manifest mit einer Konfiguration zugeordnet ist.
- Zusammenfassung: Eine eindeutige Kennung, die aus einem kryptografischen Hash des Inhalts eines Manifests erstellt wird. Der Image-Digest hilft dabei, ein unveränderliches Container-Image eindeutig zu identifizieren. Wenn Sie ein Image mithilfe des zugehörigen Digest abrufen, laden

Sie jedes Mal dasselbe Image auf ein beliebiges Betriebssystem oder eine beliebige Architektur herunter. Weitere Informationen finden Sie in der OCI-Image-Spezifikation.

- Tag: Ein für Menschen lesbarer Manifestbezeichner. Im Vergleich zu Bildauszügen, die unveränderlich sind, sind Tags dynamisch. Ein Tag, der auf ein Bild verweist, kann sich ändern und von einem Bild zum anderen verschoben werden, obwohl der zugrunde liegende Bildauszug derselbe bleibt.

Zielarchitektur

Das folgende Diagramm zeigt die allgemeine Architektur der Lösung, die durch dieses Muster bereitgestellt wird, um doppelte Container-Images zu identifizieren, indem Bilder verglichen werden, die in Amazon ECR und privaten Repositorys gespeichert sind.

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend AWS-Konten zu verwalten.
- AWS CodeBuildist ein vollständig verwalteter Build-Service, der Ihnen hilft, Quellcode zu kompilieren, Komponententests durchzuführen und Artefakte zu erstellen, die sofort einsatzbereit sind.
- AWS CodeCommitist ein Versionskontrolldienst, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodePipelinehilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.

Kode

Der Code für dieses Muster ist im GitHub Repository verfügbar. Automatisierte Lösung zur Identifizierung doppelter Container-Images zwischen Repositorys.

Bewährte Methoden

- AWS CloudFormation bewährte Verfahren
- AWS CodePipeline bewährte Verfahren

Epen

Container-Images aus öffentlichen und privaten Amazon ECR-Repositorys abrufen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Rufen Sie ein Bild aus dem öffentlichen Amazon ECR-Repository ab.	Führen Sie im Terminal den folgenden Befehl aus, um das Bild `amazonlinux` aus dem öffentlichen Amazon ECR-Repository abzurufen.
	`$~ % docker pull public.ecr.aws/amazonlinux/amazonlinux:2018.03`
	Wenn das Bild auf Ihren lokalen Computer abgerufen wurde, sehen Sie den folgenden Pull-Digest, der den Bildindex darstellt.
	`2018.03: Pulling from amazonlinux/amazonlinux`
	`4ddc0f8d367f: Pull complete`
	`Digest: sha256:f972d24199508c52de7ad37a298bda35d8a1bd7df158149b381c03f6c6e363b5`
		App-Entwickler, AWS DevOps, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`Status: Downloaded newer image for public.ecr.aws/amazonlinux/amazonlinux:2018.03 public.ecr.aws/amazonlinux/amazonlinux:2018.03`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Pushen Sie das Bild in ein privates Amazon ECR-Repository.	1. Erstellen Sie ein privates Amazon ECR-Repository mit dem Namen `test_ecr_repository` der Region USA Ost (Nord-Virginia) (`us-east-1`).
	`$~ % aws ecr get-login-password --region us-east-1 | docker login --username AWS --password-stdin <account-id>.dkr.ecr.us-east-1.amazonaws.com`
	`Login Succeeded`
	wo `<account-id>` bezieht sich auf Ihre AWS-Konto.
	2. Markieren Sie das lokale Bild, das Sie zuvor abgerufen haben. Verwenden Sie den Wert `public.ecr.aws/amazonlinux/amazonlinux:2018.03` und übertragen Sie ihn in das private Amazon ECR-Repository.
	`$~ % docker tag public.ecr.aws/amazonlinux/amazonlinux:2018.03 <account-`
		AWS-Administrator, AWS DevOps, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>id>.dkr.ecr.us-eas
	t-1.amazonaws.com/
	test_ecr_repositor
	y:latest
	
	$~ % docker push
	 <account-id>.dkr.e
	cr.us-east-1.amazo
	naws.com/test_ecr_
	repository:latest</pre>
	Wenn Sie das Bild in das Amazon ECR-Repository übertragen, überträgt Docker das zugrunde liegende Image und nicht den Bildindex.
	<pre>The push refers to
	 repository [<account
	-id>.dkr.ecr.us-ea
	st-1.amazonaws.com/
	test_ecr_repository]
	d5655967c2c4: Pushed
	latest: digest:
	 sha256:52db9000073
	d93b9bdee6a7246a68
	c35a741aaade05a8f4
	febba0bf795cdac02
	 size: 529</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Rufen Sie dasselbe Bild aus dem privaten Amazon ECR-Repository ab.	1. Führen Sie vom Terminal aus den folgenden Befehl aus, um das Image abzurufen, das Sie zuvor in das private Amazon ECR-Repository übertragen haben.
	
	`$~ % docker pull <account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
	`latest: Pulling from test_ecr_repository`
	`Digest: sha256:52db9000073d93b9bdee6a7246a68c35a741aaade05a8f4febba0bf795cdac02`
	`Status: Image is up to date for <account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
	`<account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
	
	Der Digest für dieses Image entspricht dem Digest des Images, das Sie in das private Amazon ECR-Repository übertragen haben, und stellt das zugrunde liegende Image
		App-Entwickler, AWS DevOps, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	dar. Dieser Wert entsprich t nicht dem Bildindex, den Sie aus dem öffentlichen Repository abgerufen haben.
	2. Rufen Sie zur Überprüfung den Bildindex per Digest ab.
	
	`curl -k -H “Authoriz ation: Bearer $TOKEN” https://public.ecr .aws/v2/amazonlinu x/amazonlinux/mani fests/sha256:f972d 24199508c52de7ad37 a298bda35d8a1bd7df 158149b381c03f6c6e 363b55`
	`{ “schemaVersion”: 2, “mediaType”: “application/vnd.d ocker.distribution .manifest.list.v2+ json”, “manifests”: [ { “mediaType”: “application/vnd.d ocker.distribution .manifest.v2+json”, “size”: 529, “digest”: “sha256:52db900007 3d93b9bdee6a7246a6 8c35a741aaade05a8f 4febba0bf795cdac02 ",`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	“platform”: { “architecture”: “amd64”, “os”: “linux” } }] }	

Vergleichen Sie die Image-Manifeste

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Suchen Sie das Manifest des Bilds, das im öffentlichen Amazon ECR-Repository gespeichert ist.	Führen Sie im Terminal den folgenden Befehl aus, um das Manifest des Images `public.ecr.aws/amazonlinux/amazonlinux:2018.03` aus dem öffentlichen Amazon ECR-Repository abzurufen. $~ % docker manifest inspect public.ecr.aws/amazonlinux/amazonlinux:2018.03 { "schemaVersion": 2, "mediaType": "application/vnd.docker.distribution.manifest.list.v2+json", "manifests": [{	AWS-Administrator, AWS DevOps, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"mediaType": "application/vnd.docker.distribution.manifest.v2+json", "size": 529, "digest": "sha256:52db9000073d93b9bdee6a7246a68c35a741aaade05a8f4febba0bf795cdac02", "platform": { "architecture": "amd64", "os": "linux" } }] }	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Suchen Sie das Manifest des Images, das im privaten Amazon ECR-Repository gespeichert ist.	Führen Sie im Terminal den folgenden Befehl aus, um das Manifest des Images `<account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest` aus dem privaten Amazon ECR-Repository abzurufen.
	
	`$~ % docker manifest inspect <account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
	
	`{ "schemaVersion": 2, "mediaType": "application/vnd.docker.distribution.manifest.v2+json", "config": { "mediaType": "application/vnd.docker.container.image.v1+json", "size": 1477, "digest": "sha256:f7cee5e1af28ad4e147589c474d399b12d9b551ef4c3e11e02d982fce5eebc68" }, "layers": [ {`
		AWS DevOps, AWS-Systemadministrator, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip", "size": 62267075, "digest": "sha256:4ddc0f8d367f424871a060e2067749f32bd36a91085e714dcb159952f2d71453" }] }	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vergleichen Sie den von Docker abgerufenen Digest mit dem Manifest-Digest für das Image im privaten Amazon ECR-Repository.	Eine weitere Frage ist, warum sich der vom Befehl docker pull bereitgestellte Digest vom Digest des Manifests für das Image unterscheidet. `<account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest` Der für Docker Pull verwendete Digest stellt den Digest des Image-Manifests dar, das in einer Registrierung gespeichert ist. Dieser Digest wird als Stamm einer Hash-Kette betrachtet, da das Manifest den Hash des Inhalts enthält, der heruntergeladen und in Docker importiert wird. Die in Docker verwendete Image-ID finden Sie in diesem Manifest als. `config.digest` Dies stellt die Image-Konfiguration dar, die Docker verwendet. Man könnte also sagen, dass das Manifest der Umschlag ist und das Bild der Inhalt des Umschlags. Der Manifest-Digest unterscheidet sich immer von der Bild-ID. Ein bestimmtes Manifest sollte jedoch immer dieselbe Image-ID erzeugen. Da es sich bei	AWS DevOps, AWS-Systemadministrator, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dem Manifest-Digest um eine Hash-Kette handelt, können wir nicht garantieren, dass sie für eine bestimmte Image-ID immer dieselbe ist. In den meisten Fällen wird derselbe Digest erzeugt, obwohl Docker dies nicht garantieren kann. Der mögliche Unterschied im Manifest-Digest ist darauf zurückzuführen, dass Docker die mit gzip komprimierten Blobs nicht lokal speichert . Daher kann das Exportier en von Ebenen zu einem anderen Digest führen, obwohl der unkomprimierte Inhalt derselbe bleibt. Die Bild-ID überprüft, ob der unkomprim ierte Inhalt identisch ist. Das heißt, die Bild-ID ist jetzt eine inhaltsadressierbare Kennung (). `chainID` Um diese Informationen zu bestätigen, können Sie die Ausgabe des Befehls docker inspect in den öffentlichen und privaten Repositorys von Amazon ECR vergleichen: 1. Führen Sie den folgenden Befehl von Ihrem Terminal aus für das Bild aus, das im	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	öffentlichen Amazon ECR-Repository gespeichert ist.
	
	`$~ % docker inspect public.ecr.aws/amazonlinux/amazonlinux:2018.03`
	
	Die Ausgabe des Befehls finden Sie im Abschnitt Zusätzliche Informationen.
	2. Führen Sie den folgenden Befehl von Ihrem Terminal aus für das Bild aus, das im privaten Amazon ECR-Repository gespeichert ist.
	
	`$~ % docker inspect <account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
	
	Die Ausgabe des Befehls finden Sie im Abschnitt Zusätzliche Informationen.
	
	Die Ergebnisse bestätigen, dass beide Bilder denselben Bild-ID-Digest und Ebenen-Digest haben.
	
	ID: `f7cee5e1af28ad4e147589c474d399b12d9b551ef4c3e11e02d982fce5eebc68`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Schichten: `d5655967c 2c4e8d68f8ec7cf753 218938669e6c16ac13 24303c073c736a2e2a2` Darüber hinaus basieren die Digests auf den Bytes des Objekts, das lokal verwaltet wird (die lokale Datei ist ein Tar der Container-Image-Ebene), oder des Blobs, der an den Registrierungsserv er übertragen wird. Wenn Sie das Blob jedoch in eine Registrierung übertragen, wird das Tar komprimiert und der Digest wird in der komprimierten TAR-Datei berechnet. Daher ist der Unterschied im Docker Pull Digest-Wert auf die Komprimie rung zurückzuführen, die auf Registrierungsebene (Amazon ECR privat oder öffentlich) angewendet wird. **Note** Diese Erklärung bezieht sich speziell auf die Verwendun g eines Docker-Cl ients. Sie werden dieses Verhalten bei anderen Clients wie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	nerdctl oder Finch nicht feststellen, da sie das Bild bei Push- und Pull-Vorgängen nicht automatisch komprimieren.	

Identifizieren Sie automatisch doppelte Bilder zwischen öffentlichen und privaten Amazon ECR-Repositorys

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Klonen Sie das Github-Repository für dieses Muster in einen lokalen Ordner: `$git clone https://github.com/aws-samples/automated-solution-to-identify-duplicate-container-images-between-repositories`	AWS-Administrator, AWS DevOps
Richten Sie eine CI/CD-Pipeline ein.	Das GitHub Repository enthält eine `.yaml` Datei, die einen AWS CloudFormation Stack erstellt, in dem eine Pipeline eingerichtet werden kann. AWS CodePipeline 1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS CloudFormation Konsole.	AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Erstellen Sie einen Stapel mithilfe der `pipeline.yaml` Vorlagendatei, die sich im `code` Ordner im geklonten Repository befindet. 3. Akzeptieren oder ändern Sie die Standardwerte der Parameter. Geben Sie Werte für Folgendes an: • Stack name • `ArtifactStoreBucketName` — Ein vorhandener S3-Bucket, der zum Speichern von AWS CodePipeline Artefakten verwendet wird • `OutputBucket` — Ein vorhandener S3-Bucket, der zum Speichern der URIs für die doppelten Bilder verwendet wird • `SourceImageFile` — Eine bestehende Textdatei mit dem Name`input.txt` , die das Bild URIs aus dem öffentlichen Repository enthält, das mit dem privaten Amazon ECR-Repository verglichen wird, um Duplikate zu erkennen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Überprüfen und passen Sie die Stack-Optionen an und wählen Sie dann Submit, um die Vorlage auszuführ en. Die Pipeline wird in zwei Schritten (CodeCommit und CodeBuild, wie im Architekt urdiagramm dargestellt) eingerichtet, um Bilder im privaten Repository zu identifiz ieren, die auch im öffentlic hen Repository vorhanden sind. Die Pipeline ist mit den folgenden Ressourcen konfiguriert: • CodePipeline für die Orchestrierung der Bereitste llungspipeline. • Ein CodeCommit Repositor y zum Speichern des Bash-Skripts und der Eingabedatei. Das Bash-Skript wird verwendet, um das Container-Image IDs in den öffentlichen und privaten Repositorys zu vergleichen, um Duplikate zu finden. Diese Prüfung wird für alle Repositorys in den angegebenen AWS-Konto Repositorys in einem	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	einzigen durchgeführt. AWS-Region • Ein CodeBuild Projekt zum Aufrufen des Bash-Skripts zur Identifizierung von Bildern, die bereits im Amazon ECR-Repository vorhanden sind. • Erforderliche IAM-Rollen, um den Zugriff zu ermöglich en. • Ein S3-Bucket zum Speichern der Ausgabeda tei, die das Bild URIs enthält. • Ein weiterer S3-Bucket zum Speichern von CodePipeline Artefakten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Füllen Sie das CodeCommit Repository aus.	Gehen Sie wie folgt vor, um das CodeCommit Repository zu füllen: 1. Öffnen Sie die CodeCommit Konsole und navigieren Sie zu dem Ort, an AWS-Regio n dem Sie den CloudForm ation Stack erstellt haben. 2. Suchen Sie in der Liste nach dem Repository, das Sie mithilfe des CloudForm ation Skripts bereitgestellt haben, wählen Sie Clone URL aus und kopieren Sie dann das HTTPS-URL-Protokoll, um eine Verbindung zum Repository herzustellen. 3. Öffnen Sie eine Befehlsze ile und führen Sie den Befehl git clone mit der HTTPS-URL aus, die Sie im vorherigen Schritt kopiert haben. 4. Navigiere zum Stammverz eichnis. Erstellen Sie eine Datei mit dem Namen `input.txt` und füllen Sie diese Datei mit der öffentlic hen Amazon ECR-Image -Registry URIs , nach der Sie im privaten Amazon	AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	ECR-Repository suchen möchten.
	5. Kopieren Sie die Dateien `script.sh` und `input.txt` von Ihrer lokalen Kopie des GitHub Repositorys Automatisierte Lösung zur Identifizierung doppelter Container-Images zwischen Repositorys in das geklonte Repository. `buildspec.yml` CodeCommit
	6. Laden Sie die Dateien mit den folgenden CodeCommit Befehlen hoch:
	`git add .`
	`git commit -m “added input files”`
	`git push`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen Sie.	Um future Gebühren zu vermeiden, löschen Sie die Ressourcen, indem Sie die folgenden Schritte ausführen: 1. Navigieren Sie zu dem S3-Bucket, in dem die CodePipeline Artefakte gespeichert sind, und leeren Sie den Bucket. 2. Navigieren Sie zu dem S3-Bucket, in dem das doppelte Image gespeichert ist URIs, und leeren Sie den Bucket. 3. Navigieren Sie zur CloudFormation Konsole und löschen Sie den Stack, den Sie zum Einrichten der Pipeline erstellt haben.	AWS-Administrator

Fehlerbehebung

Problem	Lösung
Wenn Sie versuchen, ein CodeCommi t Repository über das Terminal oder die Befehlszeile zu pushen, abzurufen oder auf andere Weise mit ihm zu interagieren, werden Sie aufgefordert, einen Benutzernamen und ein Passwort einzugeben, und Sie müssen die Git-Anmeldeinformationen für Ihren IAM-Benutzer angeben.	Die häufigsten Ursachen für diesen Fehler sind die folgenden: • Auf Ihrem lokalen Computer wird ein Betriebssystem ausgeführt, das die Verwaltung von Anmeldeinformationen nicht unterstützt, oder es ist kein Programm zur Verwaltung von Anmeldeinformationen installiert.

Problem	Lösung
	• Die Git-Anmeldeinformationen für Ihren IAM-Benutzer wurden nicht in einem dieser Anmeldeinformationsverwaltungssysteme gespeichert. Je nach Ihrem Betriebssystem und der lokalen Umgebung müssen Sie möglicherweise einen Anmeldeinformationsmanager installieren, den in Ihr Betriebssystem integrierten Anmeldeinformationsmanager konfigurieren oder Ihre lokale Umgebung so anpassen, dass Anmeldeinformationen gespeichert werden. Wenn auf Ihrem Computer beispielsweise macOS ausgeführt wird, können Sie das Keychain Access-Hilfsprogramm verwenden, um Ihre Anmeldeinformationen zu speichern. Wenn Sie einen Windows-Computer nutzen, können Sie das Git-Dienstprogramm zur Verwaltung von Anmeldeinformationen (Git Credential Manager) verwenden, das zusammen mit Git für Windows installiert wird. Weitere Informationen finden Sie in der CodeCommit Dokumentation unter Einrichtung für HTTPS-Benutzer mit Git-Anmeldeinformationen und unter Credential Storage in der Git-Dokumentation.

Problem	Lösung
Wenn Sie ein Bild in das Amazon ECR-Repository übertragen, treten Fehler vom Typ HTTP 403 oder „no basic auth credentials“ auf.	Diese Fehlermeldungen können beim Befehl docker push oder docker pull auftreten, auch wenn Sie sich erfolgreich mit dem Befehl aws ecr bei Docker authentifiziert haben. get-login-password Bekannte Ursachen sind: • Sie haben sich in einer anderen Region authentifiziert. Weitere Informationen finden Sie unter Private Registry Authentication in der Amazon ECR-Dokumentation. • Sie haben sich authentifiziert, um in ein Repository zu pushen, für das Sie keine Berechtigungen haben. Weitere Informationen finden Sie unter Richtlinien für private Repositorys in der Amazon ECR-Dokumentation. • Ihr Token ist abgelaufen. Die Standardablaufzeit für Token, die Sie mithilfe dieses `GetAuthorizationToken` Vorgangs erhalten haben, beträgt 12 Stunden.

Zugehörige Ressourcen

- Automatisierte Lösung zur Identifizierung doppelter Container-Images zwischen Repositorys (GitHub Repository)
- Öffentliche Galerie Amazon ECR
- Private Bilder in Amazon ECR (Amazon ECR-Dokumentation)
- AWS::CodePipeline::Pipeline Ressource (Dokumentation)AWS CloudFormation
- Spezifikation des OCI-Bildformats

Zusätzliche Informationen

Ausgabe der Docker-Inspektion für Bilder im öffentlichen Amazon ECR-Repository

```
[
    {
        "Id":
 "sha256:f7cee5e1af28ad4e147589c474d399b12d9b551ef4c3e11e02d982fce5eebc68",
        "RepoTags": [
            "<account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest",
            "public.ecr.aws/amazonlinux/amazonlinux:2018.03"
        ],
        "RepoDigests": [
            "<account-id>.dkr.ecr.us-east-1.amazonaws.com/
test_ecr_repository@sha256:52db9000073d93b9bdee6a7246a68c35a741aaade05a8f4febba0bf795cdac02",
            "public.ecr.aws/amazonlinux/
amazonlinux@sha256:f972d24199508c52de7ad37a298bda35d8a1bd7df158149b381c03f6c6e363b5"
        ],
        "Parent": "",
        "Comment": "",
        "Created": "2023-02-23T06:20:11.575053226Z",
        "Container":
 "ec7f2fc7d2b6a382384061247ef603e7d647d65f5cd4fa397a3ccbba9278367c",
        "ContainerConfig": {
            "Hostname": "ec7f2fc7d2b6",
            "Domainname": "",
            "User": "",
            "AttachStdin": false,
            "AttachStdout": false,
            "AttachStderr": false,
            "Tty": false,
            "OpenStdin": false,
            "StdinOnce": false,
            "Env": [
                "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
            ],
            "Cmd": [
                "/bin/sh",
                "-c",
                "#(nop) ",
                "CMD [\"/bin/bash\"]"
            ],
            "Image":
 "sha256:c1bced1b5a65681e1e0e52d0a6ad17aaf76606149492ca0bf519a466ecb21e51",
            "Volumes": null,
            "WorkingDir": "",
            "Entrypoint": null,
```

```
            "OnBuild": null,
            "Labels": {}
        },
        "DockerVersion": "20.10.17",
        "Author": "",
        "Config": {
            "Hostname": "",
            "Domainname": "",
            "User": "",
            "AttachStdin": false,
            "AttachStdout": false,
            "AttachStderr": false,
            "Tty": false,
            "OpenStdin": false,
            "StdinOnce": false,
            "Env": [
                "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
            ],
            "Cmd": [
                "/bin/bash"
            ],
            "Image":
 "sha256:c1bced1b5a65681e1e0e52d0a6ad17aaf76606149492ca0bf519a466ecb21e51",
            "Volumes": null,
            "WorkingDir": "",
            "Entrypoint": null,
            "OnBuild": null,
            "Labels": null
        },
        "Architecture": "amd64",
        "Os": "linux",
        "Size": 167436755,
        "VirtualSize": 167436755,
        "GraphDriver": {
            "Data": {
                "MergedDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/merged",
                "UpperDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/diff",
                "WorkDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/work"
            },
            "Name": "overlay2"
        },
```

```
        "RootFS": {
            "Type": "layers",
            "Layers": [

 "sha256:d5655967c2c4e8d68f8ec7cf753218938669e6c16ac1324303c073c736a2e2a2"
            ]
        },
        "Metadata": {
            "LastTagTime": "2023-03-02T10:28:47.142155987Z"
        }
    }
]
```

Ausgabe der Docker-Inspektion für Bilder im privaten Amazon ECR-Repository

```
[
    {
        "Id":
 "sha256:f7cee5e1af28ad4e147589c474d399b12d9b551ef4c3e11e02d982fce5eebc68",
        "RepoTags": [
            "<account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest",
            "public.ecr.aws/amazonlinux/amazonlinux:2018.03"
        ],
        "RepoDigests": [
            "<account-id>.dkr.ecr.us-east-1.amazonaws.com/
test_ecr_repository@sha256:52db9000073d93b9bdee6a7246a68c35a741aaade05a8f4febba0bf795cdac02",
            "public.ecr.aws/amazonlinux/
amazonlinux@sha256:f972d24199508c52de7ad37a298bda35d8a1bd7df158149b381c03f6c6e363b5"
        ],
        "Parent": "",
        "Comment": "",
        "Created": "2023-02-23T06:20:11.575053226Z",
        "Container":
 "ec7f2fc7d2b6a382384061247ef603e7d647d65f5cd4fa397a3ccbba9278367c",
        "ContainerConfig": {
            "Hostname": "ec7f2fc7d2b6",
            "Domainname": "",
            "User": "",
            "AttachStdin": false,
            "AttachStdout": false,
            "AttachStderr": false,
            "Tty": false,
            "OpenStdin": false,
```

```
            "StdinOnce": false,
            "Env": [
                "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
            ],
            "Cmd": [
                "/bin/sh",
                "-c",
                "#(nop) ",
                "CMD [\"/bin/bash\"]"
            ],
            "Image":
"sha256:c1bced1b5a65681e1e0e52d0a6ad17aaf76606149492ca0bf519a466ecb21e51",
            "Volumes": null,
            "WorkingDir": "",
            "Entrypoint": null,
            "OnBuild": null,
            "Labels": {}
        },
        "DockerVersion": "20.10.17",
        "Author": "",
        "Config": {
            "Hostname": "",
            "Domainname": "",
            "User": "",
            "AttachStdin": false,
            "AttachStdout": false,
            "AttachStderr": false,
            "Tty": false,
            "OpenStdin": false,
            "StdinOnce": false,
            "Env": [
                "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
            ],
            "Cmd": [
                "/bin/bash"
            ],
            "Image":
"sha256:c1bced1b5a65681e1e0e52d0a6ad17aaf76606149492ca0bf519a466ecb21e51",
            "Volumes": null,
            "WorkingDir": "",
            "Entrypoint": null,
            "OnBuild": null,
            "Labels": null
        },
```

```
        "Architecture": "amd64",
        "Os": "linux",
        "Size": 167436755,
        "VirtualSize": 167436755,
        "GraphDriver": {
            "Data": {
                "MergedDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/merged",
                "UpperDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/diff",
                "WorkDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/work"
            },
            "Name": "overlay2"
        },
        "RootFS": {
            "Type": "layers",
            "Layers": [

 "sha256:d5655967c2c4e8d68f8ec7cf753218938669e6c16ac1324303c073c736a2e2a2"
            ]
        },
        "Metadata": {
            "LastTagTime": "2023-03-02T10:28:47.142155987Z"
        }
    }
]
```

Installieren Sie SSM Agent mithilfe von Kubernetes auf Amazon EKS-Worker-Knoten DaemonSet

Erstellt von Mahendra Revanasiddappa (AWS)

Übersicht

Hinweis, September 2021: Mit der neuesten für Amazon EKS optimierten Version wird der SSM-Agent automatisch AMIs installiert. Weitere Informationen finden Sie in den Versionshinweisen für Juni 2021 AMIs.

In Amazon Elastic Kubernetes Service (Amazon EKS) sind Worker-Knoten aufgrund von Sicherheitsrichtlinien nicht mit Secure Shell (SSH) -Schlüsselpaaren verknüpft. Dieses Muster zeigt, wie Sie den DaemonSet Kubernetes-Ressourcentyp verwenden können, um den AWS Systems Manager Agent (SSM Agent) auf allen Worker-Knoten zu installieren, anstatt ihn manuell zu installieren oder das Amazon Machine Image (AMI) für die Knoten zu ersetzen. DaemonSet verwendet einen Cron-Job auf dem Worker-Knoten, um die Installation des SSM-Agenten zu planen. Sie können dieses Muster auch verwenden, um andere Pakete auf Worker-Knoten zu installieren.

Wenn Sie Probleme im Cluster beheben, können Sie durch die Installation von SSM Agent on Demand ohne SSH-Schlüsselpaare eine SSH-Sitzung mit dem Worker-Knoten einrichten, Protokolle sammeln oder die Instanzkonfiguration überprüfen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein vorhandener Amazon EKS-Cluster mit Amazon Elastic Compute Cloud (Amazon EC2) -Worker-Knoten.
- Container-Instances sollten über die erforderlichen Berechtigungen für die Kommunikation mit dem SSM-Service verfügen. Die von AWS Identity and Access Management (IAM) verwaltete Rolle Amazon SSMManaged InstanceCore stellt die erforderlichen Berechtigungen bereit, damit der SSM-Agent auf EC2 Instances ausgeführt werden kann. Weitere Informationen finden Sie in der Dokumentation zu AWS Systems Manager.

Einschränkungen

- Dieses Muster gilt nicht für AWS Fargate, da es auf der Fargate-Plattform DaemonSets nicht unterstützt wird.

- Dieses Muster gilt nur für Linux-basierte Worker-Knoten.
- Die DaemonSet Pods werden im privilegierten Modus ausgeführt. Wenn der Amazon EKS-Cluster über einen Webhook verfügt, der Pods im privilegierten Modus blockiert, wird der SSM-Agent nicht installiert.

Architektur

Das folgende Diagramm veranschaulicht die Architektur für dieses Muster.

Tools

Tools

- kubectl ist ein Befehlszeilenprogramm, das für die Interaktion mit einem Amazon EKS-Cluster verwendet wird. Dieses Muster wird verwendet`kubectl`, um einen DaemonSet auf dem Amazon EKS-Cluster bereitzustellen, der den SSM-Agent auf allen Worker-Knoten installiert.
- Amazon EKS macht es Ihnen leicht, Kubernetes auf AWS auszuführen, ohne Ihre eigene Kubernetes-Steuerebene oder Knoten installieren, betreiben und warten zu müssen. Kubernetes ist ein Open-Source-System zur Automatisierung der Bereitstellung, Skalierung und Verwaltung von Anwendungen in Containern.
- Mit AWS Systems Manager Session Manager können Sie Ihre EC2 Instances, lokalen Instances und virtuellen Maschinen (VMs) über eine interaktive, browserbasierte Shell mit einem Klick oder über die AWS-Befehlszeilenschnittstelle (AWS CLI) verwalten.

Code

Verwenden Sie den folgenden Code, um eine DaemonSet Konfigurationsdatei zu erstellen, mit der der SSM-Agent auf dem Amazon EKS-Cluster installiert wird. Folgen Sie den Anweisungen im Abschnitt Epics.

```
cat << EOF > ssm_daemonset.yaml
apiVersion: apps/v1
kind: DaemonSet
metadata:
  labels:
    k8s-app: ssm-installer
  name: ssm-installer
```

```
  namespace: kube-system
spec:
  selector:
    matchLabels:
      k8s-app: ssm-installer
  template:
    metadata:
      labels:
        k8s-app: ssm-installer
    spec:
      containers:
      - name: sleeper
        image: busybox
        command: ['sh', '-c', 'echo I keep things running! && sleep 3600']
      initContainers:
      - image: amazonlinux
        imagePullPolicy: Always
        name: ssm
        command: ["/bin/bash"]
        args: ["-c","echo '* * * * * root yum install -y https://s3.amazonaws.com/
ec2-downloads-windows/SSMAgent/latest/linux_amd64/amazon-ssm-agent.rpm & rm -rf /etc/
cron.d/ssmstart' > /etc/cron.d/ssmstart"]
        securityContext:
          allowPrivilegeEscalation: true
        volumeMounts:
        - mountPath: /etc/cron.d
          name: cronfile
        terminationMessagePath: /dev/termination-log
        terminationMessagePolicy: File
      volumes:
      - name: cronfile
        hostPath:
          path: /etc/cron.d
          type: Directory
      dnsPolicy: ClusterFirst
      restartPolicy: Always
      schedulerName: default-scheduler
      terminationGracePeriodSeconds: 30
EOF
```

Epen

Richten Sie kubectl ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren und konfigurieren Sie kubectl für den Zugriff auf den EKS-Cluster.	Falls es noch `kubectl` nicht installiert und für den Zugriff auf den Amazon EKS-Clust er konfiguriert ist, finden Sie weitere Informationen unter Installation von kubectl in der Amazon EKS-Dokumentation.	DevOps

Stellen Sie das bereit DaemonSet

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die DaemonSet Konfigurationsdatei.	Verwenden Sie den Code im Abschnitt Code weiter oben in diesem Muster, um eine DaemonSet Konfigura tionsdatei namens zu erstellen `ssm_daemonset.yaml` , die im Amazon EKS-Cluster bereitgestellt wird. Der von gestartete Pod DaemonSet hat einen Hauptcontainer und einen `init` Container. Der Hauptcontainer hat einen `sleep` Befehl. Der `init` Container enthält einen `command` Abschnitt, der eine Cron-Job-Datei zur Installat ion des SSM-Agenten im	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Pfad erstellt. `/etc/cron.d/` Der Cron-Job wird nur einmal ausgeführt, und die von ihm erstellte Datei wird nach Abschluss des Jobs automatisch gelöscht. Wenn der Init-Container fertig ist, wartet der Hauptcontainer 60 Minuten, bevor er beendet wird. Nach 60 Minuten wird ein neuer Pod gestartet. Dieser Pod installiert den SSM-Agent, falls er fehlt, oder aktualisiert den SSM-Agenten auf die neueste Version. Bei Bedarf können Sie den `sleep` Befehl so ändern, dass der Pod einmal täglich neu gestartet oder häufiger ausgeführt wird.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den DaemonSet auf dem Amazon EKS-Cluster bereit.	Verwenden Sie den folgenden Befehl, um die DaemonSet Konfigurationsdatei, die Sie im vorherigen Schritt erstellt haben, auf dem Amazon EKS-Cluster bereitzustellen: `kubectl apply -f ssm_daemonset.yaml` Dieser Befehl erstellt einen DaemonSet , um die Pods auf Worker-Knoten auszuführen, um den SSM-Agent zu installieren.	DevOps

Zugehörige Ressourcen

- Installation von kubectl (Amazon EKS-Dokumentation)
- Session Manager einrichten (AWS Systems Manager Manager-Dokumentation)

Installieren Sie den SSM-Agent und den CloudWatch Agenten auf Amazon EKS-Worker-Knoten mit preBootstrapCommands

Erstellt von Akkamahadevi Hiremath (AWS)

Übersicht

Dieses Muster enthält Codebeispiele und Schritte zur Installation des AWS Systems Manager Agent (SSM Agent) und des Amazon-Agenten auf Amazon CloudWatch Elastic Kubernetes Service (Amazon EKS) -Worker-Knoten in der Amazon Web Services (AWS) -Cloud während der Amazon EKS-Clustererstellung. Sie können den SSM-Agent und CloudWatch den SSM-Agenten installieren, indem Sie die `preBootstrapCommands` Eigenschaft aus dem `eksctl` Konfigurationsdateischema (Weaveworks-Dokumentation) verwenden. Anschließend können Sie den SSM-Agent verwenden, um eine Verbindung zu Ihren Worker-Knoten herzustellen, ohne ein Amazon Elastic Compute Cloud (Amazon EC2) -Schlüsselpaar zu verwenden. Darüber hinaus können Sie den CloudWatch Agenten verwenden, um die Speicher- und Festplattenauslastung auf Ihren Amazon EKS-Worker-Knoten zu überwachen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Das Befehlszeilenprogramm eksctl, installiert und konfiguriert auf macOS, Linux oder Windows
- Das kubectl-Befehlszeilenprogramm, installiert und konfiguriert auf macOS, Linux oder Windows

Einschränkungen

- Wir empfehlen, das Hinzufügen von Skripten mit langer Laufzeit zur `preBootstrapCommands` Eigenschaft zu vermeiden, da dies den Knoten daran hindert, dem Amazon EKS-Cluster während der Skalierungsaktivitäten beizutreten. Wir empfehlen Ihnen, stattdessen ein benutzerdefiniertes Amazon Machine Image (AMI) zu erstellen.
- Dieses Muster gilt nur für Amazon EC2 Linux-Instances.

Architektur

Technologie-Stack

- Amazon CloudWatch
- Amazon Elastic Kubernetes Service (Amazon EKS)
- AWS Systems Manager Parameter Store

Zielarchitektur

Das folgende Diagramm zeigt ein Beispiel für einen Benutzer, der mithilfe des SSM-Agenten, der mit dem installiert wurde, eine Verbindung zu Amazon EKS-Worker-Knoten herstellt. `preBootstrapCommands`

Das Diagramm zeigt den folgenden Workflow:

1. Der Benutzer erstellt mithilfe der `eksctl` Konfigurationsdatei mit der `preBootstrapCommands` Eigenschaft, die den SSM-Agenten und CloudWatch den Agenten installiert, einen Amazon EKS-Cluster.
2. Alle neuen Instances, die dem Cluster aufgrund von Skalierungsaktivitäten später beitreten, werden mit dem vorinstallierten SSM-Agenten und -Agenten erstellt. CloudWatch
3. Der Benutzer stellt EC2 mithilfe des SSM-Agenten eine Verbindung zu Amazon her und überwacht dann mithilfe des CloudWatch Agenten die Speicher- und Festplattenauslastung.

Tools

- Amazon CloudWatch hilft Ihnen dabei, die Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie auf AWS ausführen, in Echtzeit zu überwachen.
- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen, Kubernetes auf AWS auszuführen, ohne Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten zu müssen.
- AWS Systems Manager Parameter Store bietet sicheren, hierarchischen Speicher für die Verwaltung von Konfigurationsdaten und Geheimnissen.
- AWS Systems Manager Session Manager unterstützt Sie bei der Verwaltung Ihrer EC2 Instances, lokalen Instances und virtuellen Maschinen über eine interaktive, browserbasierte Shell mit einem Klick oder über die AWS-Befehlszeilenschnittstelle (AWS CLI).
- eksctl ist ein Befehlszeilenprogramm zum Erstellen und Verwalten von Kubernetes-Clustern auf Amazon EKS.
- kubectl ist ein Befehlszeilenprogramm für die Kommunikation mit dem Cluster-API-Server.

Epen

Erstellen Sie einen Amazon EKS-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Speichern Sie die CloudWatch Agenten-Konfigurationsdatei.	Speichern Sie die CloudWatch Agentenkonfigurationsdatei im AWS Systems Manager Parameter Store in der AWS-Region, in der Sie Ihren Amazon EKS-Cluster erstellen möchten. Erstellen Sie dazu einen Parameter im AWS Systems Manager Parameter Store und notieren Sie sich den Namen des Parameters (z. B. `AmazonCloudwatch-linux`). Weitere Informationen finden Sie im Beispielcode der CloudWatch Agenten-Konfigurationsdatei im Abschnitt Zusätzliche Informationen dieses Musters.	DevOps Ingenieur
Erstellen Sie die eksctl-Konfigurationsdatei und den Cluster.	1. Erstellen Sie eine `eksctl` Konfigurationsdatei, die die Installationsschritte für den CloudWatch Agenten und den SSM-Agenten enthält. Weitere Informationen finden Sie im Beispielcode für die eksctl-Konfigurationsdatei im Abschnitt Zusätzliche Informationen dieses Musters.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Erstellen Sie einen Cluster, indem Sie den `eksctl create cluster -f cluster.yaml` Befehl ausführen.	

Stellen Sie sicher, dass der SSM-Agent und der CloudWatch SSM-Agent funktionieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie den SSM-Agenten.	Verwenden Sie SSH, um eine Verbindung zu Ihren Amazon EKS-Clusterknoten herzustellen, indem Sie eine der Methoden verwenden, die in der AWS Systems Manager Manager-Dokumentation unter Sitzung starten beschrieben werden.	AWS DevOps
Testen Sie den CloudWatch Agenten.	Verwenden Sie die CloudWatch Konsole, um den CloudWatch Agenten zu validieren: 1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudWatch -Konsole. 2. Erweitern Sie im Navigationsbereich Metriken und wählen Sie dann Alle Metriken aus. 3. Geben Sie im Suchfeld auf der Registerkarte	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Durchsuchen den Text CWAgent Metriken ein und wählen Sie dann aus, um sich die Speicher- und Festplattenmetriken anzusehen.	

Zugehörige Ressourcen

- Installation und Ausführung des CloudWatch Agenten auf Ihren Servern (CloudWatch Amazon-Dokumentation)
- Einen Systems Manager Manager-Parameter erstellen (Konsole) (AWS Systems Manager Manager-Dokumentation)
- Erstellen Sie die CloudWatch Agenten-Konfigurationsdatei (CloudWatch Amazon-Dokumentation)
- Starten einer Sitzung (AWS CLI) (AWS Systems Manager Manager-Dokumentation)
- Starten einer Sitzung (EC2 Amazon-Konsole) (AWS Systems Manager Manager-Dokumentation)

Zusätzliche Informationen

Beispiel für eine CloudWatch Agenten-Konfigurationsdatei

Im folgenden Beispiel ist der CloudWatch Agent so konfiguriert, dass er die Festplatten- und Speicherauslastung auf Amazon Linux-Instances überwacht:

```
{
    "agent": {
        "metrics_collection_interval": 60,
        "run_as_user": "cwagent"
    },
    "metrics": {
        "append_dimensions": {
            "AutoScalingGroupName": "${aws:AutoScalingGroupName}",
            "ImageId": "${aws:ImageId}",
            "InstanceId": "${aws:InstanceId}",
            "InstanceType": "${aws:InstanceType}"
        },
```

```
        "metrics_collected": {
            "disk": {
                "measurement": [
                    "used_percent"
                ],
                "metrics_collection_interval": 60,
                "resources": [
                    "*"
                ]
            },
            "mem": {
                "measurement": [
                    "mem_used_percent"
                ],
                "metrics_collection_interval": 60
            }
        }
    }
}
```

Beispiel für eine eksctl-Konfigurationsdatei

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig
metadata:
  name: test
  region: us-east-2
  version: "1.24"
managedNodeGroups:
  - name: test
    minSize: 2
    maxSize: 4
    desiredCapacity: 2
    volumeSize: 20
    instanceType: t3.medium
    preBootstrapCommands:
    - sudo yum install amazon-ssm-agent -y
    - sudo systemctl enable amazon-ssm-agent
    - sudo systemctl start amazon-ssm-agent
    - sudo yum install amazon-cloudwatch-agent -y
    - sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-
config -m ec2 -s -c ssm:AmazonCloudwatch-linux
    iam:
```

```
      attachPolicyARNs:
        - arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy
        - arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy
        - arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly
        - arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
        - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
```

Zusätzliche Codedetails

- In der letzten Zeile der `preBootstrapCommands` Eigenschaft `AmazonCloudwatch-linux` steht der Name des Parameters, der im AWS System Manager Parameter Store erstellt wurde. Sie müssen `AmazonCloudwatch-linux` in Parameter Store in derselben AWS-Region angeben, in der Sie den Amazon EKS-Cluster erstellt haben. Sie können auch einen Dateipfad angeben, wir empfehlen jedoch, Systems Manager zu verwenden, um die Automatisierung und Wiederverwendbarkeit zu vereinfachen.
- Wenn Sie `preBootstrapCommands` in der `eksctl` Konfigurationsdatei verwenden, werden in der AWS-Managementkonsole zwei Startvorlagen angezeigt. Die erste Startvorlage enthält die unter angegebenen Befehle`preBootstrapCommands`. Die zweite Vorlage enthält die in den Amazon EKS-Benutzerdaten angegebenen Befehle `preBootstrapCommands` und die standardmäßigen Amazon EKS-Benutzerdaten. Diese Daten sind erforderlich, damit die Knoten dem Cluster beitreten können. Die Auto Scaling Scaling-Gruppe der Knotengruppe verwendet diese Benutzerdaten, um neue Instances hochzufahren.
- Wenn Sie das `iam` Attribut in der `eksctl` Konfigurationsdatei verwenden, müssen Sie die standardmäßigen Amazon EKS-Richtlinien mit allen zusätzlichen Richtlinien auflisten, die in Ihren angehängten AWS Identity and Access Management (IAM) -Richtlinien erforderlich sind. Im Codeausschnitt aus dem Schritt „Eksctl-Konfigurationsdatei und Cluster erstellen“ wurden zusätzliche Richtlinien hinzugefügt, um sicherzustellen, dass der CloudWatch Agent `CloudWatchAgentServerPolicy` und `AmazonSSMMangedInstanceCore` der SSM-Agent wie erwartet funktionieren. Die`AmazonEKSWorkerNodePolicy`,`AmazonEKS_CNI_Policy`, `AmazonEC2ContainerRegistryReadOnly` Richtlinien sind verbindliche Richtlinien, die erforderlich sind, damit der Amazon EKS-Cluster ordnungsgemäß funktioniert.

Migrieren Sie NGINX Ingress Controller, wenn Sie den Amazon EKS Auto Mode aktivieren

Erstellt von Olawale Olaleye (AWS) und Shamanth Devagari (AWS)

Übersicht

Der automatische EKS-Modus für Amazon Elastic Kubernetes Service (Amazon EKS) kann den Betriebsaufwand für die Ausführung Ihrer Workloads auf Kubernetes-Clustern reduzieren. In diesem Modus können Sie auch AWS die Infrastruktur in Ihrem Namen einrichten und verwalten. Wenn Sie den EKS-Automatikmodus auf einem vorhandenen Cluster aktivieren, müssen Sie die Migration der NGINX Ingress Controller-Konfigurationen sorgfältig planen. Dies liegt daran, dass die direkte Übertragung von Network Load Balancers nicht möglich ist.

Sie können eine Blau/Grün-Bereitstellungsstrategie verwenden, um eine NGINX Ingress Controller-Instance zu migrieren, wenn Sie den EKS-Automatikmodus in einem vorhandenen Amazon EKS-Cluster aktivieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Ein Amazon EKS-Cluster, auf dem Kubernetes Version 1.29 oder höher ausgeführt wird
- Amazon EKS-Add-Ons mit Mindestversionen
- Aktuelle Version von kubectl
- Eine bestehende NGINX Ingress Controller-Instanz
- (Optional) Eine gehostete Zone in Amazon Route 53 für DNS-basierte Verkehrsverlagerung

Architektur

Eine blaue/grüne Bereitstellung ist eine Bereitstellungsstrategie, bei der Sie zwei separate, aber identische Umgebungen erstellen. Bereitstellungen in Blau/Grün ermöglichen Releases- und Rollback-Funktionen, bei denen fast keine Ausfallzeiten auftreten. Die Grundidee besteht darin, den Datenverkehr zwischen zwei identischen Umgebungen zu verlagern, in denen unterschiedliche Versionen Ihrer Anwendung ausgeführt werden.

Die folgende Abbildung zeigt die Migration von Network Load Balancers von zwei verschiedenen NGINX Ingress Controller-Instanzen, wenn der EKS-Automatikmodus aktiviert wird. Sie verwenden eine blaue/grüne Bereitstellung, um den Verkehr zwischen den beiden Network Load Balancern zu verlagern.

Der ursprüngliche Namespace ist der blaue Namespace. Hier werden der ursprüngliche NGINX Ingress Controller-Dienst und die ursprüngliche Instanz ausgeführt, bevor Sie den EKS Auto Mode aktivieren. Der ursprüngliche Dienst und die ursprüngliche Instanz stellen eine Verbindung zu einem Network Load Balancer her, dessen DNS-Name in Route 53 konfiguriert ist. Der Load AWS Balancer Controller hat diesen Network Load Balancer in der Ziel-Virtual Private Cloud (VPC) bereitgestellt.

Das Diagramm zeigt den folgenden Arbeitsablauf zum Einrichten einer Umgebung für eine blaue/grüne Bereitstellung:

1. Installieren und konfigurieren Sie eine weitere NGINX Ingress Controller-Instanz in einem anderen Namespace, einem grünen Namespace.
2. Konfigurieren Sie in Route 53 einen DNS-Namen für einen neuen Network Load Balancer.

Tools

AWS-Services

- Mit Amazon Elastic Kubernetes Service (Amazon EKS) können Sie Kubernetes ausführen, AWS ohne dass Sie Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten müssen.
- Elastic Load Balancing verteilt den eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Traffic auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk bereitzustellen. Dieses virtuelle Netzwerk entspricht einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben würden, mit den Vorteilen der Verwendung der skalierbaren Infrastruktur von AWS.

Andere Tools

- Helm ist ein Open-Source-Paketmanager für Kubernetes, der Sie bei der Installation und Verwaltung von Anwendungen auf Ihrem Kubernetes-Cluster unterstützt.
- kubectl ist eine Befehlszeilenschnittstelle, mit der Sie Befehle für Kubernetes-Cluster ausführen können.
- Der NGINX Ingress Controller verbindet Kubernetes-Apps und -Dienste mit Anforderungsbearbeitung, Authentifizierung, benutzerdefinierten Self-Service-Ressourcen und Debugging.

Epen

Überprüfen Sie die bestehende Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vergewissern Sie sich, dass die ursprüngliche NGINX Ingress Controller-Instanz betriebsbereit ist.	Geben Sie den folgenden Befehl ein, um zu überprüfen, ob die Ressourcen im `ingress-nginx` Namespace betriebsbereit sind. Wenn Sie den NGINX Ingress Controller in einem anderen Namespace bereitgestellt haben, aktualisieren Sie den Namespace-Namen in diesem Befehl. `kubectl get all -n ingress-nginx` Vergewissern Sie sich in der Ausgabe, dass sich die NGINX Ingress Controller-Pods im laufenden Zustand befinden. Im Folgenden finden Sie ein Beispiel für eine Ausgabe:	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	NAME READY STATUS RESTARTS AGE pod/ingress-nginx- admission-create-xqn9d 0/1 Completed 0 88m pod/ingress-nginx- admission-patch-lhk4j 0/1 Completed 1 88m pod/ingress-nginx- controller-68f68f859- xrz74 1/1 Running 2 (10m ago) 72m NAME TYPE CLUSTER- IP EXTERNAL-IP PORT(S) AGE service/ingress-nginx- controller LoadBalancer 10.100.67.255 k8s- ingressn-ingressn- abcdefg-12345.elb.eu- west-1.amazonaws.com 80:30330/TCP,443:3 1462/TCP 88m service/ingress- nginx-controller- admission ClusterIP 10.100.201.176 <none>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	443/TCP 88m NAME READY UP-TO-DATE AVAILABLE AGE deployment.apps/ingress-nginx-controller 1/1 1 1 88m NAME DESIRED CURRENT READY AGE replicaset.apps/ingress-nginx-controller-68f68f859 1 1 1 72m replicaset.apps/ingress-nginx-controller-d8c96cf68 0 0 0 88m NAME STATUS COMPLETIONS DURATION AGE job.batch/ingress-nginx-admission-create Complete 1/1 4s 88m job.batch/ingress-nginx-admission-patch Complete 1/1 5s 88m	

Stellen Sie einen HTTPd Beispiel-Workload bereit, um den NGINX Ingress Controller zu verwenden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Kubernetes-Ressourcen.	Geben Sie die folgenden Befehle ein, um ein Beispiel für eine Kubernetes-Bereitstellung, einen Service und einen Ingress zu erstellen:
	`kubectl create deployment demo --image=httpd --port=80`
	`kubectl expose deployment demo`
	`kubectl create ingress demo --class=nginx \ --rule nginxautomode.local.dev/=demo:80`
		DevOps Ingenieur

Überprüfen Sie die eingesetzten Ressourcen.	Geben Sie den folgenden Befehl ein, um eine Liste der bereitgestellten Ressourcen anzuzeigen: `kubectl get all,ingress` Vergewissern Sie sich in der Ausgabe, dass sich der HTTPd Beispiel-Pod im laufenden Zustand befindet. Im Folgenden finden Sie ein Beispiel für eine Ausgabe:	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	NAME READY STATUS RESTARTS AGE pod/demo-7d94f8cb4f-q68wc 1/1 Running 0 59m NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE service/demo ClusterIP 10.100.78.155 <none> 80/TCP 59m service/kubernetes ClusterIP 10.100.0.1 <none> 443/TCP 117m NAME READY UP-TO-DATE AVAILABLE AGE deployment.apps/demo 1/1 1 1 59m NAME DESIRED CURRENT READY AGE replicaset.apps/demo-7d94f8cb4f 1 1 1 59m NAME CLASS HOSTS ADDRESS	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`PORTS AGE ingress.networking.k8s.io/demo nginx nginxautomode.local.dev k8s-ingressn-ingressn-abcdefg-12345.elb.eu-west-1.amazonaws.com 80 56m`	

Bestätigen Sie, dass der Dienst erreichbar ist.	Geben Sie den folgenden Befehl ein, um zu bestätigen, dass der Dienst über den DNS-Namen des Network Load Balancer erreichbar ist:
	`curl -H "Host: nginxautomode.local.dev" http://k8s-ingressn-ingressn-abcdefg-12345.elb.eu-west-1.amazonaws.com`
	Folgendes ist die erwartete Ausgabe:
	`<html><body><h1>It works!</h1></body></html>`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

(Optional) Erstellen Sie einen DNS-Eintrag.	1. Folgen Sie den Anweisungen unter Erstellen von Einträgen mithilfe der Amazon Route 53-Konsole (Route 53-Dokumentation), um einen DNS-Eintrag für die konfigurierte Domain zu erstellen.
	2. Geben Sie den folgenden Befehl ein, um zu bestätigen, dass der Service über den konfigurierten Domainnamen erreichbar ist:
	`curl "http://nginxautomode.local.dev/?[1-5]"`
	Folgendes ist die erwartete Ausgabe:
	`<html><body><h1>It works!</h1></body></html>`
	`<html><body><h1>It works!</h1></body></html>`
	`<html><body><h1>It works!</h1></body></html>`
	`<html><body><h1>It works!</h1></body></html>`
		DevOps Ingenieur, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`<html><body><h1>It works!</h1></body></html>`	

Aktivieren Sie den automatischen EKS-Modus auf dem vorhandenen Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie den EKS-Automatikmodus.	Folgen Sie den Anweisungen unter Aktivieren des automatischen EKS-Modus auf einem vorhandenen Cluster (Amazon EKS-Dokumentation).	AWS DevOps

Installieren Sie einen neuen NGINX Ingress Controller

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie eine neue NGINX Ingress Controller-Instanz.	1. Laden Sie die Vorlage deploy.yaml herunter.
	2. Öffnen Sie die Vorlage deploy.yaml in Ihrem bevorzugten Editor.
	3. Geben Sie in dem `kind: Namespace` Abschnitt einen eindeutigen Namen für den Namespace ein, z. B.: `ingress-nginx-v2`
	`apiVersion: v1`
	`kind: Namespace`
	`metadata:`
	`  labels:`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
    app.kuber
netes.io/instance:
 ingress-nginx
    app.kuber
netes.io/name:
 ingress-nginx
  name: ingress-n
ginx-v2
```

4. Aktualisieren Sie den `namespace` Wert für jeden Abschnitt auf den neuen Namen.
5. Führen Sie im Abschnitt `kind: Deployment` folgende Schritte aus:
   a. Geben Sie einen eindeutigen Wert für ein`--controller-class` , z. `k8s.io/ingress-nginx-v2` B.
   b. Geben Sie einen eindeutigen Wert für ein`--ingress-class` , z. `nginx-v2` B.

```
apiVersion: apps/v1
kind: Deployment
  name: ingress-n
ginx-controller
  namespace: ingress-
nginx-v2
...
    spec:
      containers:
      - args:
        - /nginx-in
gress-controller
```

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
        - --publish
-service=$(POD_NAM
ESPACE)/ingress-ng
inx-controller
        - --electio
n-id=ingress-nginx-
leader
        - --control
ler-class=k8s.io/i
ngress-nginx-v2
        - --ingress-
class=nginx-v2
```

6. Geben Sie im `kind: IngressClass` Abschnitt dieselben Werte für `--controller-class` und ein`--ingress-class`, die Sie im vorherigen Abschnitt verwendet haben:

```
apiVersion: networkin
g.k8s.io/v1
kind: IngressClass
metadata:
  labels:
    app.kuber
netes.io/component:
 controller
    app.kuber
netes.io/instance:
 ingress-nginx
    app.kuber
netes.io/name:
 ingress-nginx
    app.kuber
netes.io/part-of:
 ingress-nginx
```

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>app.kuber
	netes.io/version:
	1.12.0
	name: nginx-v2
	spec:
	controller: k8s.io/
	ingress-nginx-v2</pre>	

	7. Fügen Sie im folgenden Abschnitt einen Network Load Balancer für die NGINX Ingress Controller-Instanz hinzu, `loadBalancerClass: eks.amazonaws.com/nlb` um ihn bereitzustellen:
	<pre>apiVersion: v1
	kind: Service
	metadata:
	name: ingress-n
	ginx-controller
	namespace: ingress-
	nginx-v2
	spec:
	...
	selector:
	app.kuber
	netes.io/component:
	controller
	app.kuber
	netes.io/instance:
	ingress-nginx
	app.kuber
	netes.io/name:
	ingress-nginx
	type: LoadBalancer
	loadBalancerClass:
	eks.amazonaws.com/
	nlb</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Speichern und schließen Sie die Vorlage deploy.yaml.	
Stellen Sie die neue NGINX Instance Controller-Instanz bereit.	Geben Sie den folgenden Befehl ein, um die geänderte Manifestdatei anzuwenden: `kubectl apply -f deploy.yaml`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bestätigen Sie die erfolgreiche Bereitstellung.	Geben Sie den folgenden Befehl ein, um zu überprüfen, ob die Ressourcen im `ingress-nginx-v2` Namespace betriebsbereit sind:
	`kubectl get all -n ingress-nginx-v2`
	Vergewissern Sie sich in der Ausgabe, dass sich die NGINX Ingress Controller-Pods im laufenden Zustand befinden. Im Folgenden finden Sie ein Beispiel für eine Ausgabe:
	`NAME READY STATUS RESTARTS AGE pod/ingress-nginx-admission-create-7shrj 0/1 Completed 0 24s pod/ingress-nginx-admission-patch-vkxr5 0/1 Completed 1 24s pod/ingress-nginx-controller-757bfcbc6d-4fw52 1/1 Running 0 24s`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE service/ingress-nginx-controller LoadBalancer 10.100.208.114 k8s-ingressn-ingressn-2e5e37fab6-848337cd9c9d520f.elb.eu-west-1.amazonaws.com 80:31469/TCP,443:30658/TCP 24s service/ingress-nginx-controller-admission ClusterIP 10.100.150.114 <none> 443/TCP 24s NAME READY UP-TO-DATE AVAILABLE AGE deployment.apps/ingress-nginx-controller 1/1 1 1 24s NAME DESIRED CURRENT READY AGE	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>replicaset.apps/
	ingress-nginx-co
	ntroller-757bfcbc6d
	 1 1 1
	 24s
	
	NAME
	
	 STATUS COMPLETIONS
	 DURATION AGE
	job.batch/ingress-
	nginx-admission-create
	 Complete 1/1
	 4s 24s
	job.batch/ingress-
	nginx-admission-patch
	 Complete 1/1
	 5s 24s</pre>	

Erstellen Sie einen neuen Ingress für den HTTPd Beispiel-Workload.	Geben Sie den folgenden Befehl ein, um einen neuen Ingress für den vorhandenen HTTPd Beispiel-Workload zu erstellen:
	<pre>kubectl create ingress
	 demo-new --class=n
	ginx-v2 \
	 --rule nginxauto
	mode.local.dev/=de
	mo:80</pre>
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Vergewissern Sie sich, dass der neue Ingress funktioniert.	Geben Sie den folgenden Befehl ein, um zu bestätige n, dass der neue Eingang funktioniert:
	`curl -H "Host: nginxauto mode.local.dev" k8s-ingressn-ingre ssn-2e5e37fab6-848 337cd9c9d520f.elb.eu- west-1.amazonaws.com`
	Das Folgende ist die erwartete Ausgabe:
	`<html><body><h1>It works!</h1></body></ html>`
		DevOps Ingenieur

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wechseln Sie zum neuen Namespace.	1. (Optional) Folgen Sie den Anweisungen unter Datensätze bearbeiten (Route 53-Dokumentation), um den DNS-Eintrag zu aktualisieren. 2. Wenn Sie bestätigt haben, dass die neue NGINX Ingress Controller-Instanz wie erwartet funktioniert, löschen Sie das Original.	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Löschen Sie den selbstverwalteten AWS Load Balancer Controller. Anweisungen finden Sie unter Apps aus dem veralteten ALB Ingress Controller migrieren (Amazon EKS-Dokumentation). 4. Entleeren Sie die verwalteten Knotengruppen. Anweisungen finden Sie unter Löschen und Entleeren von Knotengruppen (eksctl-Dokumentation).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfe die beiden Eingänge.	Geben Sie den folgenden Befehl ein, um die beiden Ingresses zu überprüfen, die für den HTTPd Beispiel-Workload erstellt wurden:
	`kubectl get ingress`
	Im Folgenden finden Sie ein Beispiel für eine Ausgabe:
	`NAME HOSTS ADDRESS PORTS AGE`
	`demo nginx nginxautomode.local.dev k8s-ingressn-ingressn-abcdefg-12345.elb.eu-west-1.amazonaws.com 80 95m`
	`demo-new nginx-v2 nginxautomode.local.dev k8s-ingressn-ingressn-2e5e37fab6-848337cd9c9d520f.elb.eu-west-1.amazonaws.com 80 33s`
		DevOps Ingenieur

Zugehörige Ressourcen

- Aktivieren Sie den automatischen EKS-Modus auf einem vorhandenen Cluster (Amazon EKS-Dokumentation)
- Fehlerbehebung bei Load Balancers, die vom Kubernetes Service Controller in Amazon EKS erstellt wurden (AWS re:POST Knowledge Center)
- NGINX Ingress Controller (NGINX-Dokumentation)

Migrieren Sie Ihre Container-Workloads von Azure Red Hat OpenShift (ARO) zu Red Hat OpenShift Service in AWS (ROSA)

Erstellt von Naveen Ramasamy (AWS), Gireesh Sreekantan (AWS) und Srikanth Rangavajhala (AWS)

Übersicht

Dieses Muster enthält step-by-step Anweisungen für die Migration von Container-Workloads von Azure Red Hat (ARO) nach (ROSA). OpenShift Red Hat OpenShift Service in AWS ROSA ist ein verwalteter Kubernetes-Dienst, der von Red Hat in Zusammenarbeit mit bereitgestellt wird. AWS Er unterstützt Sie bei der Bereitstellung, Verwaltung und Skalierung Ihrer containerisierten Anwendungen mithilfe der Kubernetes-Plattform und profitiert von der Expertise von Red Hat in Bezug auf Kubernetes und die Infrastruktur. AWS Cloud

Die Migration von Container-Workloads von ARO, aus anderen Clouds oder von lokalen Umgebungen zu ROSA beinhaltet die Übertragung von Anwendungen, Konfigurationen und Daten von einer Plattform auf eine andere. Dieses Muster trägt dazu bei, einen reibungslosen Übergang zu gewährleisten und gleichzeitig AWS Cloud Services, Sicherheit und Kosteneffizienz zu optimieren. Es umfasst zwei Methoden für die Migration Ihrer Workloads zu ROSA-Clustern: CI/CD und Migration Toolkit for Containers (MTC).

Dieses Muster deckt beide Methoden ab. Welche Methode Sie wählen, hängt von der Komplexität und Sicherheit Ihres Migrationsprozesses ab. Wenn Sie die volle Kontrolle über den Status Ihrer Anwendung haben und über eine Pipeline eine konsistente Einrichtung gewährleisten können, empfehlen wir Ihnen, die CI/CD-Methode zu verwenden. Wenn Ihr Anwendungsstatus jedoch Unsicherheiten, unvorhergesehene Änderungen oder ein komplexes Ökosystem beinhaltet, empfehlen wir Ihnen, MTC als zuverlässigen und kontrollierten Weg für die Migration Ihrer Anwendung und ihrer Daten auf einen neuen Cluster zu verwenden. Einen detaillierten Vergleich der beiden Methoden finden Sie im Abschnitt Zusätzliche Informationen.

Vorteile der Migration zu ROSA:

- ROSA lässt sich nahtlos AWS als systemeigener Service integrieren. Es ist leicht zugänglich über das AWS Management Console und wird über einen einzigen AWS-Konto abgerechnet. Es bietet volle Kompatibilität mit anderen Anbietern AWS-Services und bietet gemeinsamen Support sowohl AWS von RedHat als auch von RedHat.
- ROSA unterstützt Hybrid- und Multi-Cloud-Implementierungen. Es ermöglicht die konsistente Ausführung von Anwendungen in lokalen Rechenzentren und mehreren Cloud-Umgebungen.

- ROSA profitiert vom Sicherheitsfokus von Red Hat und bietet Funktionen wie rollenbasierte Zugriffskontrolle (RBAC), Image-Scanning und Schwachstellenanalysen, um eine sichere Container-Umgebung zu gewährleisten.
- ROSA wurde für die einfache Skalierung von Anwendungen entwickelt und bietet Optionen für hohe Verfügbarkeit. Dadurch können Anwendungen nach Bedarf wachsen und gleichzeitig die Zuverlässigkeit beibehalten.
- ROSA automatisiert und vereinfacht die Bereitstellung eines Kubernetes-Clusters im Vergleich zu manuellen Einrichtungs- und Verwaltungsmethoden. Dies beschleunigt den Entwicklungs- und Bereitstellungsprozess.
- ROSA profitiert von AWS Cloud Services und bietet eine nahtlose Integration mit AWS Angeboten wie Datenbankdiensten, Speicherlösungen und Sicherheitsdiensten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto.
- Berechtigungen AWS-Services , die für diese Funktion konfiguriert sind, auf die ROSA angewiesen ist, um Funktionen bereitzustellen. Weitere Informationen finden Sie in der ROSA-Dokumentation unter Voraussetzungen.
- ROSA ist auf der ROSA-Konsole aktiviert. Anweisungen finden Sie in der ROSA-Dokumentation.
- Der ROSA-Cluster wurde installiert und konfiguriert. Weitere Informationen finden Sie unter Erste Schritte mit ROSA in der ROSA-Dokumentation. Informationen zu den verschiedenen Methoden zur Einrichtung eines ROSA-Clusters finden Sie im AWS Prescriptive Guidance Guide zu ROSA-Implementierungsstrategien.
- Netzwerkkonnektivität, die vom lokalen Netzwerk AWS über das Netzwerk AWS Direct Connect(bevorzugt) oder AWS Virtual Private Network () hergestellt wird.AWS VPN
- Eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance oder ein anderer virtueller Server zur Installation von Tools wie `aws client` OpenShift CLI (`oc`) -Client, ROSA-Client und Git-Binärdatei.

Zusätzliche Voraussetzungen für die CI/CD-Methode:

- Zugriff auf den lokalen Jenkins-Server mit Berechtigungen zum Erstellen einer neuen Pipeline, zum Hinzufügen von Stages, zum Hinzufügen von OpenShift Clustern und zum Ausführen von Builds.

- Zugriff auf das Git-Repository, in dem der Quellcode der Anwendung verwaltet wird, mit der Berechtigung, einen neuen Git-Branch zu erstellen und Commits für den neuen Branch durchzuführen.

Zusätzliche Voraussetzungen für die MTC-Methode:

- Ein Amazon Simple Storage Service (Amazon S3) -Bucket, der als Replikationsrepository verwendet wird.
- Administratorzugriff auf den ARO-Quell-Cluster. Dies ist erforderlich, um die MTC-Verbindung einzurichten.

Einschränkungen

- Einige AWS-Services sind nicht in allen AWS-Regionen verfügbar. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie auf der Seite Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Architektur

ROSA bietet drei Netzwerkbereitstellungsmuster: öffentlich, privat und. AWS PrivateLink PrivateLinkermöglicht es den Teams von Red Hat Site Reliability Engineering (SRE), den Cluster mithilfe eines privaten Subnetzes zu verwalten, das mit dem PrivateLink Endpunkt des Clusters in einer vorhandenen VPC verbunden ist.

Die Wahl der PrivateLink Option bietet die sicherste Konfiguration. Aus diesem Grund empfehlen wir sie für sensible Workloads oder strenge Compliance-Anforderungen. Informationen zu den Bereitstellungsoptionen für öffentliche und private Netzwerke finden Sie in der Red OpenShift Hat-Dokumentation.

> **Important**
>
> Sie können einen PrivateLink Cluster nur bei der Installation erstellen. Sie können einen zu verwendenden Cluster PrivateLink nach der Installation nicht ändern.

Das folgende Diagramm zeigt die PrivateLink Architektur für einen ROSA-Cluster, der für die Verbindung AWS Direct Connect zu lokalen Umgebungen und ARO-Umgebungen verwendet wird.

AWS Berechtigungen für ROSA

Für AWS Berechtigungen für ROSA empfehlen wir, AWS Security Token Service (AWS STS) mit kurzlebigen, dynamischen Tokens zu verwenden. Diese Methode verwendet vordefinierte Rollen und Richtlinien mit den geringsten Rechten, um ROSA minimale Berechtigungen für den Betrieb in der ROSA-Installations- AWS-Konto, Steuerungsebene- und Rechenfunktionen zu gewähren, und unterstützt die ROSA-Funktionalität.

Neuverteilung der CI/CD-Pipeline

CI/CD pipeline redeployment is the recommended method for users who have a mature CI/CDPipeline. Wenn Sie diese Option wählen, können Sie eine beliebige DevOps Bereitstellungsstrategie verwenden, um Ihre Anwendungslast schrittweise auf Bereitstellungen auf ROSA zu verlagern.

> **Note**
>
> Dieses Muster geht von einem häufigen Anwendungsfall aus, bei dem Sie eine lokale Git-, JFrog Artifactory- und Jenkins-Pipeline haben. Dieser Ansatz erfordert, dass Sie die Netzwerkkonnektivität von Ihrem lokalen Netzwerk bis AWS hin zum Through herstellen und dass Sie den ROSA-Cluster einrichten AWS Direct Connect, bevor Sie den Anweisungen im Abschnitt Epics folgen. Einzelheiten finden Sie im Abschnitt Voraussetzungen.

Das folgende Diagramm zeigt den Arbeitsablauf für diese Methode.

MTC-Methode

Sie können das Migration Toolkit for Containers (MTC) verwenden, um Ihre containerisierten Workloads zwischen verschiedenen Kubernetes-Umgebungen zu migrieren, z. B. von ARO zu ROSA. MTC vereinfacht den Migrationsprozess, indem es mehrere wichtige Aufgaben automatisiert und ein umfassendes Framework für die Verwaltung des Migrationslebenszyklus bereitstellt.

Das folgende Diagramm zeigt den Arbeitsablauf für diese Methode.

Tools

AWS-Services

- AWS DataSyncist ein Online-Datenübertragungs- und Erkennungsdienst, mit dem Sie Dateien oder Objektdaten zu, von und zwischen AWS Speicherdiensten verschieben können.
- AWS Direct Connectverbindet Ihr internes Netzwerk über ein Standard-Ethernet-Glasfaserkabel mit einem AWS Direct Connect Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt zur Öffentlichkeit einrichten AWS-Services und dabei Internetdienstanbieter in Ihrem Netzwerkpfad umgehen.
- AWS PrivateLinkhilft Ihnen dabei, unidirektionale, private Verbindungen von Ihren virtuellen privaten Clouds (VPCs) zu Diensten außerhalb der VPC herzustellen.
- Red Hat OpenShift Service in AWS (ROSA) ist ein verwalteter Service, der OpenShift Benutzern von Red Hat dabei hilft, containerisierte Anwendungen zu erstellen, zu skalieren und zu verwalten. AWS
- AWS Security Token Service (AWS STS) hilft Ihnen dabei, temporäre Zugangsdaten mit eingeschränkten Rechten für Benutzer anzufordern.

Andere Tools

- Das Migration Toolkit for Containers (MTC) bietet eine Konsole und eine API für die Migration von containerisierten Anwendungen von ARO zu ROSA.

Bewährte Methoden

- Aus Gründen der Ausfallsicherheit und wenn Sie über Workloads zur Einhaltung der Sicherheitsbestimmungen verfügen, richten Sie einen Multi-AZ-ROSA-Cluster ein, der Folgendes verwendet: PrivateLink Weitere Informationen finden Sie in der ROSA-Dokumentation.

> **Note**
>
> PrivateLink kann nach der Installation nicht konfiguriert werden.

- Der S3-Bucket, den Sie für das Replikationsrepository verwenden, sollte nicht öffentlich sein. Verwenden Sie die entsprechenden S3-Bucket-Richtlinien, um den Zugriff einzuschränken.

- Wenn Sie sich für die MTC-Methode entscheiden, verwenden Sie die Option Stage-Migration, um das Ausfallzeitfenster während der Umstellung zu reduzieren.
- Überprüfen Sie Ihre Servicekontingenten vor und nach der Bereitstellung des ROSA-Clusters. Fordern Sie bei Bedarf eine Erhöhung des Kontingents entsprechend Ihren Anforderungen an. Weitere Informationen finden Sie in der Dokumentation zu Servicekontingenten.
- Lesen Sie die ROSA-Sicherheitsrichtlinien und implementieren Sie bewährte Sicherheitsmethoden.
- Wir empfehlen, den Standard-Clusteradministrator nach der Installation zu entfernen. Weitere Informationen finden Sie in der Red OpenShift Hat-Dokumentation.
- Verwenden Sie die automatische Skalierung von Maschinenpools, um ungenutzte Worker-Knoten im ROSA-Cluster herunterzufahren und so die Kosten zu optimieren. Weitere Informationen finden Sie im ROSA-Workshop.
- Nutzen Sie den Red Hat Cost Management Service für OpenShift Container Platform, um die Kosten für Clouds und Container besser zu verstehen und nachzuverfolgen. Weitere Informationen finden Sie im ROSA-Workshop.
- Überwachen und prüfen Sie die Infrastrukturdienste und -anwendungen des ROSA-Clusters mithilfe von AWS-Services. Weitere Informationen finden Sie im ROSA-Workshop.

Epen

Option 1: Verwenden Sie eine CI/CD-Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie den neuen ROSA-Cluster zu Jenkins hinzu.	1. Wählen Sie in der Jenkins-Konsole Manage Jenkins, Configure System aus. 2. Wählen Sie auf der Seite „Jenkins verwalten“ im Abschnitt OpenShift Plug-in die Option Neuen Cluster hinzufügen aus. 3. Geben Sie die erforderl ichen Informationen wie den Clusternamen, die API-Server-URL und Token-Inf	AWS-Administrator, AWS-Systemadministrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ormationen für die Authentif izierung bei ROSA ein.	
Fügen Sie den `oc` Client zu Ihren Jenkins-Knoten hinzu.	1. Wählen Sie in der Jenkins-Konsole Manage Jenkins, Global Tool Configuration aus. 2. Installieren Sie im Abschnitt OpenShift Client Tools die OpenShift CLI (`oc`) - Client-Version, die mit Ihrer ROSA-Cluster-Version identisch ist.	AWS-Administrator, AWS-Systemadministrator, AWS DevOps
Erstelle einen neuen Git-Branch.	Erstellen Sie einen neuen Branch in Ihrem Git-Repository für `rosa-dev`. Dieser Zweig trennt die Code- oder Konfigurationsparameteränderungen für ROSA von Ihrer bestehenden Pipeline.	AWS DevOps
Tag-Bilder für ROSA.	Verwenden Sie in Ihrer Erstellungsphase ein anderes Tag, um die Bilder zu identifizieren, die aus der ROSA-Pipeline erstellt wurden.	AWS-Administrator, AWS-Systemadministrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Pipeline.	Erstellen Sie eine neue Jenkins-Pipeline, die Ihrer bestehenden Pipeline ähnelt. Verwenden Sie für diese Pipeline den `rosa-dev` Git-Branch, den Sie zuvor erstellt haben, und stellen Sie sicher, dass die Git-Check out-, Codescan- und Build-Phasen enthalten sind, die mit Ihrer vorhandenen Pipeline identisch sind.	AWS-Administrator, AWS-Systemadministrator, AWS DevOps
Fügen Sie eine ROSA-Bere itstellungsphase hinzu.	Fügen Sie in der neuen Pipeline eine Phase hinzu, die im ROSA-Cluster bereitgestellt werden soll, und verweisen Sie auf den ROSA-Cluster, den Sie der globalen Jenkins-Konfiguration hinzugefügt haben.	AWS-Administrator, AWS DevOps, AWS-Syste madministrator
Starten Sie einen neuen Build.	Wählen Sie in Jenkins Ihre Pipeline aus und wählen Sie Jetzt erstellen oder starten Sie einen neuen Build, indem Sie eine Änderung an dem `rosa-dev` Branch in Git festschre iben.	AWS-Administrator, AWS DevOps, AWS-Syste madministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Bereitstellung.	Verwenden Sie den Befehl oc oder die ROSA-Konsole, um zu überprüfen, ob die Anwendung auf Ihrem ROSA-Zielcluster bereitgestellt wurde.	AWS-Administrator, AWS DevOps, AWS-Systemadministrator
Kopieren Sie Daten in den Zielcluster.	Kopieren Sie für statusbehaftete Workloads die Daten vom Quellcluster in den Zielcluster, indem Sie Open-Source-Dienstprogramme wie rsync verwenden AWS DataSync , oder Sie können die MTC-Methode verwenden . Weitere Informationen finden Sie in der AWS DataSync - Dokumentation.	AWS-Administrator, AWS DevOps, AWS-Systemadministrator
Testen Sie Ihre Anwendung.	1. Rufen Sie die Route-URL für Ihre Anwendung mit dem Befehl oc route oder der ROSA-Konsole ab. 2. Testen Sie Ihre Anwendung mithilfe der Route-URL.	AWS-Administrator, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überschneiden.	Wenn Ihre Tests erfolgrei ch sind, verwenden Sie die entsprechende Amazon Route 53-Richtlinie, um den Datenverkehr von der ARO-gehosteten Anwendung zur ROSA-gehosteten Anwendung zu verlagern. Wenn Sie diesen Schritt abgeschlossen haben, wird die Arbeitslast Ihrer Anwendung vollständig auf den ROSA-Cluster übertragen.	AWS-Administrator, AWS-Systemadministrator

Option 2: Verwenden Sie MTC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den MTC-Operator.	Installieren Sie den MTC-Operator sowohl auf ARO- als auch auf ROSA-Clustern: 1. Navigieren Sie in der ARO- oder ROSA-Kons ole zur OperatorHubSeite Operatoren. 2. Suchen Sie im Feld Nach Schlüsselwort filtern nach MTC, oder geben Sie es ein. 3. Wählen Sie den MTC-Operator aus, um zusätzlic he Informationen anzuzeige n.	AWS-Administrator, AWS DevOps, AWS-Syste madministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Nachdem Sie die Informationen über den Operator gelesen haben, wählen Sie Installieren.	
Konfigurieren Sie den Netzwerkverkehr zum Replikationsrepository.	Wenn Sie einen Proxyserver verwenden, konfigurieren Sie ihn so, dass Netzwerkverkehr zwischen dem Replikationsrepository und den Clustern zugelassen wird. Das Replikationsrepository ist ein Zwischenspeicherobjekt, das MTC zur Datenmigration verwendet. Die Quell- und Zielcluster müssen während der Migration Netzwerkzugriff auf das Replikationsrepository haben.	AWS-Administrator, AWS DevOps, AWS-Systemadministrator
Fügen Sie den Quellcluster zu MTC hinzu.	Fügen Sie auf der MTC-Webkonsole den ARO-Quellcluster hinzu.	AWS-Administrator, AWS DevOps, AWS-Systemadministrator
Fügen Sie Amazon S3 als Ihr Replikationsrepository hinzu.	Fügen Sie auf der MTC-Webkonsole den Amazon S3 S3-Bucket (siehe Voraussetzungen) als Replikations-Repository hinzu.	AWS-Administrator, AWS DevOps, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Migration splan.	Erstellen Sie auf der MTC-Webkonsole einen Migration splan und geben Sie als Datenübertragungstyp Kopieren an. Dadurch wird MTC angewiesen, die Daten vom Quellcluster (ARO) in den S3-Bucket und vom Bucket in den Zielcluster (ROSA) zu kopieren.	AWS-Administrator, AWS DevOps, AWS-Syste madministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den Migrationsplan aus.	Führen Sie den Migrationsplan mithilfe der Option Stage oder Cutover aus: • Wählen Sie Stage, um Daten in den Zielcluster zu kopieren, ohne Ihre Anwendung anzuhalten. Sie können Migrationen in mehreren Phasen ausführen , um die meisten Ihrer Daten vor der Übernahme migration zu kopieren. Dadurch wird die Dauer der Cutover-Migration verkürzt. • Wählen Sie Cutover, um Ihre Anwendung auf dem Quellcluster zu beenden und gleichzeitig die Ressourcen auf den Zielcluster zu verschieben. Um zu verhindern, dass die Anwendung gestoppt wird, können Sie das Kontrollk ästchen Transaktionen auf dem Quell-Cluster während der Migration anhalten deaktivieren.	AWS-Administrator, AWS DevOps, AWS-Syste madministrator

Fehlerbehebung

Problem	Lösung
Probleme mit der Verbindung	Wenn Sie Ihre Container-Workloads von ARO zu ROSA migrieren, können Verbindungsprobleme auftreten, die gelöst werden sollten, um eine erfolgreiche Migration sicherzustellen. Um diese Konnektivitätsprobleme (in dieser Tabelle aufgeführt) während der Migration zu beheben, sind eine sorgfältige Planung, Abstimmung mit Ihren Netzwerk- und Sicherheitsteams sowie gründliche Tests unerlässlich. Die Implementierung einer schrittweisen Migrationsstrategie und die Überprüfung der Konnektivität bei jedem Schritt tragen dazu bei, potenzielle Störungen zu minimieren und einen reibungslosen Übergang von ARO zu ROSA sicherzustellen.
Unterschiede in der Netzwerkkonfiguration	ARO und ROSA können unterschiedliche Netzwerkkonfigurationen aufweisen, z. B. virtuelle Netzwerkeinstellungen (VNet), Subnetze und Netzwerkrichtlinien. Stellen Sie für eine korrekte Kommunikation zwischen den Diensten sicher, dass die Netzwerkeinstellungen auf den beiden Plattformen übereinstimmen.
Sicherheitsgruppen- und Firewallregeln	ROSA und ARO haben möglicherweise unterschiedliche Standardeinstellungen für Sicherheitsgruppen und Firewalls. Stellen Sie sicher, dass Sie diese Regeln anpassen und aktualisieren, damit der erforderliche Datenverkehr zur Aufrechterhaltung der Konnektivität zwischen Containern und Diensten während der Migration gewährleistet ist.

Problem	Lösung
Änderungen der IP-Adresse und des DNS	Wenn Sie Workloads migrieren, können sich IP-Adressen und DNS-Namen ändern. Konfigurieren Sie Anwendungen neu, die auf statischen IPs oder spezifischen DNS-Namen basieren.
Zugriff auf externe Dienste	Wenn Ihre Anwendung von externen Diensten wie Datenbanken oder abhängig ist APIs, müssen Sie möglicherweise deren Verbindungseinstellungen aktualisieren, um sicherzustellen, dass sie mit den neuen Diensten von ROSA kommunizieren können.
Konfiguration von Azure Private Link	Wenn Sie Azure Private Link oder private Endpunktdienste in ARO verwenden, müssen Sie die entsprechende Funktionalität in ROSA einrichten, um die private Konnektivität zwischen Ressourcen sicherzustellen.
AWS VPN oder AWS Direct Connect einrichten	Wenn zwischen Ihrem lokalen Netzwerk und ARO bereits AWS Direct Connect Verbindungen bestehen AWS VPN oder Verbindungen bestehen, müssen Sie ähnliche Verbindungen mit ROSA herstellen, um eine unterbrechungsfreie Kommunikation mit Ihren lokalen Ressourcen zu gewährleisten.
Einstellungen für Ingress und Load Balancer	Die Konfigurationen für Ingress-Controller und Load Balancer können sich zwischen ARO und ROSA unterscheiden. Konfigurieren Sie diese Einstellungen neu, um den externen Zugriff auf Ihre Dienste aufrechtzuerhalten.

Problem	Lösung
Umgang mit Zertifikaten und TLS	Wenn Ihre Anwendungen SSL-Zertifikate oder TLS verwenden, stellen Sie sicher, dass die Zertifikate gültig und in ROSA korrekt konfiguri ert sind.
Zugriff auf die Container-Registrierung	Wenn Ihre Container in einer externen Container-Registry gehostet werden, richten Sie die entsprechenden Authentifizierungs- und Zugriffsberechtigungen für ROSA ein.
Überwachung und Protokollierung	Aktualisieren Sie die Überwachungs- und Protokollierungskonfigurationen entsprechend der neuen Infrastruktur auf ROSA, sodass Sie den Zustand und die Leistung Ihrer Container weiterhin effektiv überwachen können.

Zugehörige Ressourcen

AWSVerweise

- Was ist Red Hat OpenShift Service in AWS? (ROSA-Dokumentation)
- Erste Schritte mit ROSA (ROSA-Dokumentation)
- Red Hat OpenShift Service in AWS Umsetzungsstrategien (AWS Prescriptive Guidance)
- Red Hat OpenShift Service in AWS Jetzt GA (AWS Blogbeitrag)
- ROSA-Werkstatt
- HÄUFIG GESTELLTE FRAGEN ZU ROSA
- Häufig gestellte Fragen zum ROSA-Workshop
- ROSA-Preisgestaltung

OpenShift Dokumentation zu Red Hat

- Schnelles Installieren eines Clusters auf AWS
- Installation eines Clusters AWS in einem eingeschränkten Netzwerk

- Installation eines Clusters AWS in einer vorhandenen VPC
- Installation eines Clusters auf einer vom Benutzer bereitgestellten Infrastruktur mithilfe von Vorlagen AWS CloudFormation
- Installation eines Clusters AWS in einem eingeschränkten Netzwerk mit einer vom Benutzer bereitgestellten Infrastruktur
- Installation eines Clusters auf AWS einem mit Anpassungen
- Erste Schritte mit der OpenShift CLI

Zusätzliche Informationen

Wählen Sie zwischen Optionen für die erneute Bereitstellung von MTC- und CI/CD-Pipelines

Die Migration von Anwendungen von einem OpenShift Cluster auf einen anderen erfordert sorgfältige Überlegungen. Idealerweise wünschen Sie sich einen reibungslosen Übergang, indem Sie eine CI/CD-Pipeline verwenden, um die Anwendung erneut bereitzustellen und die Migration persistenter Volume-Daten abzuwickeln. In der Praxis ist eine auf einem Cluster ausgeführte Anwendung jedoch anfällig für unvorhergesehene Änderungen im Laufe der Zeit. Diese Änderungen können dazu führen, dass die Anwendung allmählich von ihrem ursprünglichen Bereitstellungsstatus abweicht. MTC bietet eine Lösung für Szenarien, in denen der genaue Inhalt eines Namespaces ungewiss ist und eine nahtlose Migration aller Anwendungskomponenten auf einen neuen Cluster wichtig ist.

Um die richtige Wahl zu treffen, müssen Sie Ihr spezifisches Szenario bewerten und die Vorteile der einzelnen Ansätze abwägen. Auf diese Weise können Sie eine erfolgreiche und reibungslose Migration sicherstellen, die Ihren Bedürfnissen und Prioritäten entspricht. Im Folgenden finden Sie zusätzliche Richtlinien für die Auswahl zwischen den beiden Optionen.

Neuverteilung der CI/CD-Pipeline

Die CI/CD-Pipeline-Methode ist der empfohlene Ansatz, wenn Ihre Anwendung mithilfe einer Pipeline problemlos erneut bereitgestellt werden kann. Dadurch wird sichergestellt, dass die Migration kontrolliert und vorhersehbar ist und auf Ihre bestehenden Bereitstellungspraktiken abgestimmt ist. Wenn Sie sich für diese Methode entscheiden, können Sie die Bereitstellungsstrategien blau/grün oder kanarisch nutzen, um die Last schrittweise auf Bereitstellungen auf ROSA zu verlagern. Für dieses Szenario geht dieses Muster davon aus, dass Jenkins Anwendungsbereitstellungen von der lokalen Umgebung aus orchestriert.

Vorteile:

- Sie benötigen keinen Administratorzugriff auf den ARO-Quell-Cluster und müssen keine Operatoren auf dem Quell- oder Zielcluster bereitstellen.
- Dieser Ansatz hilft Ihnen, den Verkehr mithilfe einer DevOps Strategie schrittweise umzustellen.

Nachteile:

- Es erfordert mehr Aufwand, die Funktionalität Ihrer Anwendung zu testen.
- Wenn Ihre Anwendung persistente Daten enthält, sind zusätzliche Schritte erforderlich, um die Daten mithilfe von AWS DataSync oder anderen Tools zu kopieren.

MTC-Migration

In der Praxis können laufende Anwendungen unvorhergesehene Änderungen erfahren, die dazu führen, dass sie von der ursprünglichen Bereitstellung abweichen. Wählen Sie die MTC-Option, wenn Sie sich über den aktuellen Status Ihrer Anwendung auf dem Quell-Cluster nicht sicher sind. Wenn Ihr Anwendungsökosystem beispielsweise verschiedene Komponenten, Konfigurationen und Datenspeichervolumen umfasst, empfehlen wir Ihnen, MTC zu wählen, um eine vollständige Migration sicherzustellen, die die Anwendung und ihre gesamte Umgebung abdeckt.

Vorteile:

- MTC bietet eine vollständige Sicherung und Wiederherstellung des Workloads.
- Es kopiert die persistenten Daten von der Quelle zum Ziel, während der Workload migriert wird.
- Es ist kein Zugriff auf das Quellcode-Repository erforderlich.

Nachteile:

- Sie benötigen Administratorrechte, um den MTC-Operator auf den Quell- und Zielclustern zu installieren.
- Das DevOps Team benötigt eine Schulung, um das MTC-Tool verwenden und Migrationen durchführen zu können.

Optimieren Sie die von AWS App2Container generierten Docker-Images

Erstellt von Varun Sharma (AWS)

Übersicht

AWS App2Container ist ein Befehlszeilentool, das dabei hilft, bestehende Anwendungen, die lokal oder auf virtuellen Maschinen ausgeführt werden, in Container umzuwandeln, ohne dass Codeänderungen erforderlich sind.

Basierend auf dem Anwendungstyp verfolgt App2Container einen konservativen Ansatz zur Identifizierung von Abhängigkeiten. Im Prozessmodus sind alle Dateien auf dem Anwendungsserver im Container-Image enthalten. In solchen Fällen kann ein ziemlich großes Bild generiert werden.

Dieses Muster bietet einen Ansatz zur Optimierung der von App2Container generierten Container-Images. Es gilt für alle Java-Anwendungen, die von App2Container im Prozessmodus entdeckt wurden. Der im Muster definierte Workflow ist für die Ausführung auf dem Anwendungsserver konzipiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Java-Anwendung, die auf einem Anwendungsserver auf einem Linux-Server ausgeführt wird
- App2Container wurde unter Erfüllung aller Voraussetzungen auf dem Linux-Server installiert und eingerichtet

Architektur

Quelltechnologie-Stack

- Eine Java-Anwendung, die auf einem Linux-Server läuft

Zieltechnologie-Stack

- Ein von App2Container generiertes Docker-Image

Ablauf der Zielarchitektur

1. Ermitteln Sie die Anwendungen, die auf dem Anwendungsserver ausgeführt werden, und analysieren Sie die Anwendungen.
2. Containerisieren Sie die Anwendungen.
3. Bewerten Sie die Größe des Docker-Images. Wenn das Bild zu groß ist, fahren Sie mit Schritt 4 fort.
4. Verwenden Sie das Shell-Skript (im Anhang), um große Dateien zu identifizieren.
5. Aktualisieren Sie die `appSpecificFiles` Listen `appExcludedFiles` und in der `analysis.json` Datei.

Tools

Tools

- AWS App2Container — AWS App2Container (A2C) ist ein Befehlszeilentool, mit dem Sie Anwendungen, die in Ihrem lokalen Rechenzentrum oder auf virtuellen Maschinen ausgeführt werden, nach oben verschieben können, sodass sie in Containern ausgeführt werden, die von Amazon Elastic Container Service (Amazon ECS) oder Amazon Elastic Kubernetes Service (Amazon EKS) verwaltet werden.

Code

Das `optimizeImage.sh` Shell-Skript und eine Beispieldatei sind angehängt. `analysis.json`

Die `optimizeImage.sh` Datei ist ein Utility-Skript zur Überprüfung des Inhalts der von App2Container generierten Datei,. `ContainerFiles.tar` Bei der Überprüfung werden Dateien oder Unterverzeichnisse identifiziert, die groß sind und ausgeschlossen werden können. Das Skript ist ein Wrapper für den folgenden Tar-Befehl.

```
tar -Ptvf <path>|tr -s ' '|cut -d ' ' -f3,6| awk '$2 ~/<filetype>$/'| awk '$2 ~/
^<toplevel>/'| cut -f1-<depth> -d'/'|awk '{ if ($1>= <size>) arr[$2]+=$1 } END { for
 (key in arr) { if(<verbose>) printf("%-50s\t%-50s\n", key, arr[key]) else printf("%s,
\n", key) } } '|sort -k2 -nr
```

Im Befehl tar verwendet das Skript die folgenden Werte:

`path`	Der Pfad zu `ContainerFiles.tar`
`filetype`	Der passende Dateityp
`toplevel`	Das Verzeichnis auf oberster Ebene, das dem entsprechen soll
`depth`	Die Tiefe des absoluten Pfads
`size`	Die Größe für jede Datei

Das -Skript führt folgende Aktionen aus:

1. Es wird verwendet`tar -Ptvf`, um die Dateien aufzulisten, ohne sie zu extrahieren.
2. Es filtert die Dateien nach Dateityp, beginnend mit dem Verzeichnis der obersten Ebene.
3. Basierend auf der Tiefe generiert es den absoluten Pfad als Index.
4. Basierend auf dem Index und den Speichern gibt es die Gesamtgröße des Unterverzeichnisses an.
5. Es gibt die Größe des Unterverzeichnisses aus.

Sie können die Werte auch manuell im Befehl tar ersetzen.

Epen

Entdecken, analysieren und containerisieren Sie Anwendungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entdecken Sie die lokalen Java-Anwendungen.	Führen Sie den folgenden Befehl aus, um alle Anwendungen zu ermitteln , die auf dem Anwendung sserver ausgeführt werden. `sudo app2container inventory`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie die erkannten Anwendungen.	Führen Sie den folgenden Befehl aus`application-id`, um jede Anwendung anhand der in der Inventarp hase abgerufenen Anwendung en zu analysieren. `sudo app2container analyze --application-id <java-app-id>`	AWS DevOps
Containerisieren Sie die analysierten Anwendungen.	Führen Sie den folgenden Befehl aus, um eine Anwendung zu container isieren. `sudo app2container containerize --application-id <application-id>` Der Befehl generiert das Docker-Image zusammen mit einem Tar-Bundle am Workspace-Speicherort. Wenn das Docker-Image zu groß ist, fahren Sie mit dem nächsten Schritt fort.	AWS DevOps

Identifizieren appExcludedFiles und appSpecificFiles aus der App2Container extrahierte TAR-Datei

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Größe der Tar-Datei für Artefakte.	Identifizieren Sie die `ContainerFiles.tar` Datei`{workspace}/{java-app-id}/Artifacts`, in der sich der App2Container-Workspace `java-app-id` befindet und wo `workspace` sich die Anwendungs-ID befindet. `./optimizeImage.sh -p /{workspace}/{java-app-id}/Artifacts/ContainerFiles.tar -d 0 -t / -v` Dies ist die Gesamtgröße der TAR-Datei nach der Optimierung.	AWS DevOps

Listet die Unterverzeichnisse unter dem Verzeichnis/und ihre Größen auf.	Führen Sie den folgenden Befehl aus, um die Größe der wichtigsten Unterverzeichnisse unter dem Verzeichnis der / obersten Ebene zu ermitteln.
	`./optimizeImage.sh -p /{workspace}/{java-app-id}/Artifacts/ContainerFiles.tar -d 1 -t / -s 1000000 -v`
	`/var`
	`554144711`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`/usr 2097300819`
	`/tmp 18579660`
	`/root 43645397`
	`/opt 222320534`
	`/home 65212518`
	`/etc 11357677`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie große Unterverzeichnisse unter dem Verzeichnis/.	Identifizieren Sie für jedes Hauptunterverzeichnis, das im vorherigen Befehl aufgeführt ist, die Größe seiner Unterverzeichnisse. Wird verwendet-d, um die Tiefe zu erhöhen und das `-t` Verzeichnis der obersten Ebene anzugeben. Verwenden Sie es beispielsweise `/var` als Verzeichnis der obersten Ebene. Identifizieren Sie `/var` unter alle großen Unterverzeichnisse und ihre Größe. `./optimizeImage.sh -p /{workspace}/{java-app-id}/Artifacts/ContainerFiles.tar -d 2 -t /var -s 1000000 -v` Wiederholen Sie diesen Vorgang für jedes Unterverzeichnis, das im vorherigen Schritt aufgeführt wurde (z. B., `/usr` `/tmp`/`opt`, und/`home`).	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie den großen Ordner in jedem Unterverz eichnis unter dem Verzeichn is/.	Identifizieren Sie für jedes Unterverzeichnis, das im vorherigen Schritt aufgeführ t wurde, alle Ordner, die zum Ausführen der Anwendung erforderlich sind. Verwenden Sie beispiels weise die Unterverzeichnisse aus dem vorherigen Schritt und listen Sie alle Unterverz eichnisse im `/var` Verzeichnis und deren Größe auf. Identifiz ieren Sie alle Unterverz eichnisse, die von der Anwendung benötigt werden. `/var/tmp 237285851 /var/lib 24489984 /var/cache 237285851` Um Unterverzeichnisse auszuschließen, die von der Anwendung nicht benötigt werden, fügen Sie diese Unterverzeichnisse in der `analysis.json` Datei dem `appExcludedFiles` Abschnitt darunter hinzu. `containerParameters` Eine `analysis.json` Beispieldatei ist angehängt.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die benötigte n Dateien aus der AppExclud es-Liste.	Identifizieren Sie für jedes Unterverzeichnis, das der AppExcludes-Liste hinzugefü gt wird, alle Dateien in diesem Unterverzeichnis, die von der Anwendung benötigt werden. Fügen Sie in der Datei analysis.json die spezifisc hen Dateien oder Unterverz eichnisse im Abschnitt darunter hinzu. `appSpecif icFiles container Parameters` Wenn das `/usr/lib` Verzeichnis beispielsweise zur Ausschlussliste hinzugefügt wird, aber von der Anwendung benötigt `/usr/lib/jvm` wird, fügen Sie `/usr/lib/ jvm` es dem Abschnitt hinzu. `appSpecificFiles`	AWS DevOps

Extrahieren und containerisieren Sie die Anwendung erneut

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Containerisieren Sie die analysierte Anwendung.	Führen Sie den folgenden Befehl aus, um die Anwendung zu container isieren. `sudo app2container containerize --applica`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`tion-id <application-id>` Der Befehl generiert das Docker-Image zusammen mit einem Tar-Bundle am Workspace-Speicherort.	
Identifizieren Sie die Größe der Tar-Datei für Artefakte.	Identifizieren Sie die `ContainerFiles.tar` Datei`{workspace}/{java-app-id}/Artifacts`, in der sich der App2Container-Workspace `java-app-id` befindet und wo `workspace` sich die Anwendungs-ID befindet. `./optimizeImage.sh -p /{workspace}/{java-app-id}/Artifacts/ContainerFiles.tar -d 0 -t / -v` Dies ist die Gesamtgröße der TAR-Datei nach der Optimierung.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das Docker-Image aus.	Um zu überprüfen, ob das Image ohne Fehler gestartet wird, führen Sie das Docker-Image lokal mit den folgenden Befehlen aus. Um den des `imageId` Containers zu identifizieren, verwenden Sie`docker images |grep java-app-id .` Um den Container auszuführen, verwenden Sie`docker run -d <image id>`.	AWS DevOps

Zugehörige Ressourcen

- Was ist App2Container?
- AWS App2Container — Ein neues Containerisierungstool für Java- und .NET-Anwendungen (Blogbeitrag)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Platzieren Sie Kubernetes-Pods auf Amazon EKS mithilfe von Knotenaffinität, Taints und Toleranzen

Erstellt von Hitesh Parikh (AWS) und Raghu Bhamidimarri (AWS)

Übersicht

Dieses Muster veranschaulicht die Verwendung von Kubernetes-Knotenaffinität, Node-Taints und Pod-Toleranzen, um Anwendungs-Pods bewusst auf bestimmten Worker-Knoten in einem Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster in der Amazon Web Services (AWS) -Cloud zu planen.

Ein Taint ist eine Knoteneigenschaft, die es Knoten ermöglicht, eine Reihe von Pods abzulehnen. Eine Toleranz ist eine Pod-Eigenschaft, die es dem Kubernetes-Scheduler ermöglicht, Pods auf Knoten mit passenden Taints einzuplanen.

Toleranzen allein können einen Scheduler jedoch nicht daran hindern, einen Pod auf einem Worker-Knoten zu platzieren, der keine Makel aufweist. Beispielsweise kann ein rechenintensiver Pod mit einer Toleranz unbeabsichtigt auf einem Allzweckknoten eingeplant werden, der keinen Einfluss hat. In diesem Szenario weist die Eigenschaft „Knotenaffinität“ eines Pods den Scheduler an, den Pod auf einem Knoten zu platzieren, der die in der Knotenaffinität angegebenen Knotenauswahlkriterien erfüllt.

Taints, Tolerations und Node-Affinität zusammen weisen den Scheduler an, Pods konsistent auf den Knoten mit übereinstimmenden Taints und den Knotenbezeichnungen einzuplanen, die den im Pod angegebenen Auswahlkriterien für die Knotenaffinität entsprechen.

Dieses Muster enthält ein Beispiel für eine Kubernetes-Bereitstellungsmanifestdatei und die Schritte zum Erstellen eines EKS-Clusters, zum Bereitstellen einer Anwendung und zum Überprüfen der Pod-Platzierung.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein AWS-Konto mit Anmeldeinformationen, die zum Erstellen von Ressourcen auf Ihrem AWS-Konto konfiguriert sind
- AWS-Befehlszeilenschnittstelle (AWS Command Line Interface, AWS CLI)
- eksctl

- kubectl
- Docker wurde installiert (für das verwendete Betriebssystem) und die Engine wurde gestartet (Informationen zu den Docker-Lizenzanforderungen finden Sie auf der Docker-Website)
- Java-Version 11 oder höher
- Ein Java-Microservice, der in Ihrer bevorzugten integrierten Entwicklungsumgebung (IDE) ausgeführt wird, z. B. IntelliJ IDEA Community Edition oder Eclipse (falls Sie keinen Java-Microservice haben, finden Sie unter Deploy a sample java microservice on Amazon EKS pattern and Microservices with Spring für Hilfe bei der Erstellung des Microservices)

Einschränkungen

- Dieses Muster enthält keinen Java-Code und es wird davon ausgegangen, dass Sie bereits mit Java vertraut sind. Informationen zum Erstellen eines grundlegenden Java-Mikroservices finden Sie unter Bereitstellen eines Beispiel-Java-Mikroservices auf Amazon EKS.
- Mit den Schritten in diesem Artikel werden AWS-Ressourcen erstellt, für die Kosten anfallen können. Stellen Sie sicher, dass Sie die AWS-Ressourcen bereinigen, nachdem Sie die Schritte zur Implementierung und Validierung des Musters abgeschlossen haben.

Architektur

Zieltechnologie-Stack

- Amazon EKS
- Java
- Docker
- Amazon Elastic Container Registry (Amazon ECR)

Zielarchitektur

Das Lösungsarchitekturdiagramm zeigt Amazon EKS mit zwei Pods (Deployment 1 und Deployment 2) und zwei Knotengruppen (ng1 und ng2) mit jeweils zwei Knoten. Die Pods und Knoten haben die folgenden Eigenschaften.

	Bereitstellung: 1 Pod	Bereitstellung 2 Pod	Knotengruppe 1 (ng1)	Knotengruppe 2 (ng2)

Toleranz	Schlüssel: classified_workload, Wert: true, Effekt: NoSchedule Schlüssel: machine_learning_workload, Wert: true, Effekt: NoSchedule	Keine		
Knotenaffinität	Schlüssel: alpha.eksctl.io/nodegroup-name = ng1;	Keine	Knotengruppen.name = ng1	
Makel			Schlüssel: classified_workload, Wert: true, Effekt: NoSchedule Schlüssel: machine_learning_workload, Wert: true, Effekt: NoSchedule	Keine

1. Für den Deployment 1-Pod sind Toleranzen und eine Knotenaffinität definiert. Dadurch wird der Kubernetes-Scheduler angewiesen, die Bereitstellungs-Pods auf den Knoten der Knotengruppe 1 (ng1) zu platzieren.
2. Die Knotengruppe 2 (ng2) hat kein Knotenlabel, das dem Knotenauswahlausdruck für die Knotenaffinität für Deployment 1 entspricht, sodass die Pods nicht auf ng2-Knoten geplant werden.
3. Für den Deployment 2-Pod sind keine Toleranzen oder Knotenaffinität im Bereitstellungsmanifest definiert. Der Scheduler lehnt die Planung von Deployment 2-Pods auf Knotengruppe 1 aufgrund der Schwachstellen auf den Knoten ab.
4. Die Deployment 2-Pods werden stattdessen auf Knotengruppe 2 platziert, da die Knoten keine Makel aufweisen.

Dieses Muster zeigt, dass Sie mithilfe von Taints und Toleranzen in Kombination mit der Knotenaffinität die Platzierung von Pods auf bestimmten Gruppen von Worker-Knoten kontrollieren können.

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen, Kubernetes auf AWS auszuführen, ohne Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten zu müssen.
- eksctl ist das AWS-Äquivalent zu kubectl und hilft bei der Erstellung von EKS.

Andere Tools

- Docker ist eine Reihe von Platform-as-a-Service (PaaS) -Produkten, die Virtualisierung auf Betriebssystemebene nutzen, um Software in Containern bereitzustellen.
- kubectl ist eine Befehlszeilenschnittstelle, mit der Sie Befehle für Kubernetes-Cluster ausführen können.

Epen

Erstellen Sie den EKS-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Datei cluster.yaml.	Erstellen Sie eine Datei, die `cluster.yaml` mit dem folgenden Code aufgerufen wird.
	
	`apiVersion: eksctl.io/v1alpha5`
	`kind: ClusterConfig`
	
	`metadata:`
	`  name: eks-taint-demo`
	`  region: us-west-1`
	
	`# Unmanaged nodegroups with and without taints.`
	`nodeGroups:`
	`  - name: ng1`
	`  instanceType: m5.xlarge`
	`  minSize: 2`
	`  maxSize: 3`
	`  taints:`
	`  - key: classified_workload`
	`  value: "true"`
	`  effect: NoSchedule`
	`  - key: machine_learning_workload`
	`  value: "true"`
	`  effect: NoSchedule`
	
	`  - name: ng2`
		App-Besitzer, AWS DevOps, Cloud-Administrator, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`instanceType: m5.xlarge`
	`minSize: 2`
	`maxSize: 3`	

Erstellen Sie den Cluster mithilfe von eksctl.	Führen Sie die `cluster.yaml` Datei aus, um den EKS-Cluster zu erstellen. Das Erstellen des Clusters kann einige Minuten dauern. `eksctl create cluster -f cluster.yaml`	AWS DevOps, AWS-Systemadministrator, App-Entwickler

Erstellen Sie ein Bild und laden Sie es auf Amazon ECR hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein privates Amazon ECR-Repository.	Informationen zum Erstellen eines Amazon ECR-Repositorys finden Sie unter Privates Repository erstellen. Notieren Sie sich die URI des Repos.	AWS DevOps, DevOps Ingenieur, App-Entwickler
Erstellen Sie das Dockerfile.	Wenn Sie über ein vorhandenes Docker-Container-Image verfügen, das Sie zum Testen des Musters verwenden möchten, können Sie diesen Schritt überspringen. Verwenden Sie das folgende Snippet als Referenz, um ein Dockerfile zu erstellen. Wenn Sie auf Fehler stoßen, lesen	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Sie im Abschnitt Fehlerbeh ebung nach.
	
	`FROM adoptopenjdk/openjdk11:jdk-11.0.14.1_1-alpine`
	
	`RUN apk add maven`
	`WORKDIR /code`
	
	`# Prepare by downloading dependencies`
	`ADD pom.xml /code/pom.xml`
	`RUN ["mvn", "dependency:resolve"]`
	`RUN ["mvn", "verify"]`
	
	`# Adding source, compile and package into a fat jar`
	`ADD src /code/src`
	`RUN ["mvn", "package"]`
	
	`EXPOSE 4567`
	`CMD ["java", "-jar", "target/eksExample-jar-with-dependencies.jar"]`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Datei pom.xml und die Quelldateien und erstellen Sie das Docker-Image und übertragen Sie es.	Informationen zum Erstellen der `pom.xml` Datei und der Java-Quelldatei finden Sie unter Bereitstellen eines Beispielmusters für einen Java-Microservice auf Amazon EKS. Verwenden Sie die Anweisungen in diesem Muster, um das Docker-Image zu erstellen und zu pushen.	AWS DevOps, DevOps Ingenieur, App-Entwickler

Auf Amazon EKS bereitstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Datei deployment.yaml.	Verwenden Sie den Code im *`deployment.yaml`* Abschnitt Zusätzliche Informationen, um die Datei zu erstellen. Im Code ist der Schlüssel für die Knotenaffinität ein beliebiges Label, das Sie beim Erstellen von Knotengruppen erstellen. Dieses Muster verwendet das von eksctl erstellte Standardlabel. Informationen zum Anpassen von Labels finden Sie in der Kubernetes-Dokumentation unter Zuweisen von Pods zu Knoten.	AWS DevOps, DevOps Ingenieur, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Der Wert für den Knotenaff initätsschlüssel ist der Name der Knotengruppe, die von erstellt wurde. `cluster.yaml` Führen Sie den folgenden Befehl aus, um den Schlüssel und den Wert für den Taint abzurufen. `kubectl get nodes -o json | jq '.items[].spec.taints'` Das Bild ist der URI des Amazon ECR-Repositorys, das Sie in einem früheren Schritt erstellt haben.	
Stellen Sie die Datei bereit.	Führen Sie den folgenden Befehl aus, um die Bereitstellung auf Amazon EKS durchzuführen. `kubectl apply -f deployment.yaml`	App-Entwickler, DevOps Ingenieur, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Bereitstellung.	1. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die Pods BEREIT sind.
	`kubectl get pods -o wide`
	Wenn der POD bereit ist, sollte die Ausgabe wie folgt aussehen, mit dem Status STATUS Running.
	`NAME READY STATUS RESTARTS AGE IP NODE NOMINATED NODE READINESS GATES`
	`<pod_name> 1/1 Running 0 12d 192.168.18.50 ip-192-168-20-110.us-west-1.compute.internal <none> <none>`
	Notieren Sie sich den Namen des Pods und den Namen des Knotens. Sie können den nächsten Schritt überspringen.
	2. (Optional) Führen Sie den folgenden Befehl aus, um weitere Informationen zum Pod zu erhalten und die
		App-Entwickler, DevOps Ingenieur, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Toleranzen auf dem Pod zu überprüfen.
	
	`kubectl describe pod <pod_name>`
	
	Ein Beispiel für die Ausgabe finden Sie im Abschnitt Zusätzliche Informationen.
	3. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die Pod-Platzierung auf dem Knoten korrekt ist.
	
	`kubectl describe node <node name> | grep -A 1 "Taints"`
	
	Vergewissern Sie sich, dass der Makel auf dem Knoten der Toleranz entspricht und dass die Bezeichnung auf dem Knoten der unter definierten Knotenaffinität entspricht. `deployment.yaml`
	
	Der Pod mit den Toleranzen und der Knotenaffinität sollte auf einem Knoten mit den entsprechenden Merkmalen und den Knotenaffinitätsbezeichnungen platziert	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	werden. Der vorherige Befehl gibt Ihnen die Taints auf dem Knoten. Im Folgenden finden Sie eine Beispielausgabe.
	
	`kubectl describe node ip-192-168-29-181.us-west-1.compute.internal | grep -A 1 "Taints"`
	`Taints: classifled_workload=true:NoSchedule`
	
	`machine_learning_workload=true:NoSchedule`
	
	Führen Sie zusätzlich den folgenden Befehl aus, um zu überprüfen, ob der Knoten, auf dem sich der Pod befindet, eine Bezeichnung hat, die der Bezeichnung des Knotens mit der Knotenaffinität entspricht.
	
	`kubectl get node <node name> --show-labels`
	
	4. Um zu überprüfen, ob die Anwendung das tut, wofür sie vorgesehen ist, überprüfen Sie die Pod-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Protokolle, indem Sie den folgenden Befehl ausführen. `kubectl logs -f <name-of-the-pod>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine zweite Bereitstellungs-.yaml-Datei ohne Toleranz und Knotenaff inität.	Dieser zusätzliche Schritt besteht darin, zu überprüfe n, ob der resultierende Pod nicht auf einem Knoten mit Taints geplant ist, wenn keine Knotenaffinität oder Toleranze n in der Bereitstellungsman ifestdatei angegeben sind. (Er sollte auf einem Knoten geplant werden, der keine Taints aufweist). Verwenden Sie den folgenden Code, um eine neue Bereitstellungsdatei mit dem Namen `deploy_no _taint.yaml` zu erstellen.
	
	`apiVersion: apps/v1`
	`kind: Deployment`
	`metadata:`
	`  name: microservice-`
	`deployment-non-tainted`
	`spec:`
	`  replicas: 1`
	`  selector:`
	`  matchLabels:`
	`  app.kuber`
	`netes.io/name: java-`
	`microservice-no-taint`
	`  template:`
	`  metadata:`
	`  labels:`
	`  app.kuber`
	`netes.io/name: java-`
	`microservice-no-taint`
	`  spec:`
	`  containers:`
		App-Entwickler, AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>- name: java-
	microservice-container
	-2
	image:
	<account_number>.d
	kr.ecr<region>.ama
	zonaws.com/<reposi
	tory_name>:latest
	ports:
	- container
	Port: 4567</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die zweite Bereitstellungsdatei (.yaml) bereit und validieren Sie die Platzierung des Pods	1. Führen Sie den folgenden Befehl aus.
	`kubectl apply -f deploy_no_taint.yaml`
	2. Führen Sie nach erfolgreicher Bereitstellung dieselben Befehle aus, die Sie zuvor ausgeführt haben, um die Pod-Platzierung in einer Knotengruppe ohne Makel zu überprüfen.
	`kubectl describe node <node_name> | grep "Taints"`
	Die Ausgabe sollte wie folgt aussehen.
	`Taints: <none>`
	Damit ist der Test abgeschlossen.
		App-Entwickler, AWS DevOps, DevOps Ingenieur

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen Sie die Ressourcen.	Verwenden Sie den folgenden Befehl, um zu vermeiden, dass AWS-Gebühren für	AWS DevOps, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ressourcen anfallen, die weiterhin aktiv sind. `eksctl delete cluster --name <Name of the cluster> --region <region-code>`	

Fehlerbehebung

Problem	Lösung
Einige dieser Befehle werden möglicherweise nicht ausgeführt, wenn Ihr System die Arm64-Architektur verwendet (insbesondere, wenn Sie dies auf einem M1-Mac ausführen). In der folgenden Zeile ist möglicherweise ein Fehler aufgetreten. `FROM adoptopenjdk/openjdk11:jdk-11.0.14.1_1-alpine`	Wenn Sie beim Ausführen des Dockerfiles Fehler haben, ersetzen Sie die `FROM` Zeile durch die folgende Zeile. `FROM bellsoft/liberica-openjdk-alpine-musl:17`

Zugehörige Ressourcen

- Stellen Sie einen Beispiel-Java-Microservice auf Amazon EKS bereit
- Erstellen Sie ein privates Amazon ECR-Repository
- Zuweisen von Pods zu Knoten (Kubernetes-Dokumentation)
- Schwächen und Toleranzen (Kubernetes-Dokumentation)
- Amazon EKS
- Amazon ECR
- AWS-CLI
- Docker

- IntelliJ IDEA CE
- Eclipse

Zusätzliche Informationen

bereitstellung.yaml

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: microservice-deployment
spec:
  replicas: 1
  selector:
    matchLabels:
      app.kubernetes.io/name: java-microservice
  template:
    metadata:
      labels:
        app.kubernetes.io/name: java-microservice
    spec:
      affinity:
        nodeAffinity:
          requiredDuringSchedulingIgnoredDuringExecution:
            nodeSelectorTerms:
              - matchExpressions:
                  - key: alpha.eksctl.io/nodegroup-name
                    operator: In
                    values:
                      - <node-group-name-from-cluster.yaml>
      tolerations: #only this pod has toleration and is viable to go to ng with taint
        - key: "<Taint key>" #classified_workload in our case
          operator: Equal
          value: "<Taint value>" #true
          effect: "NoSchedule"
        - key: "<Taint key>" #machine_learning_workload in our case
          operator: Equal
          value: "<Taint value>" #true
          effect: "NoSchedule"
      containers:
        - name: java-microservice-container
```

```
          image: <account_number>.dkr.ecr<region>.amazonaws.com/
<repository_name>:latest
          ports:
            - containerPort: 4567
```

Beschreiben Sie die Pod-Beispielausgabe

```
Name:         microservice-deployment-in-tainted-nodes-5684cc495b-vpcfx
Namespace:    default
Priority:     0
Node:         ip-192-168-29-181.us-west-1.compute.internal/192.168.29.181
Start Time:   Wed, 14 Sep 2022 11:06:47 -0400
Labels:       app.kubernetes.io/name=java-microservice-taint
              pod-template-hash=5684cc495b
Annotations:  kubernetes.io/psp: eks.privileged
Status:       Running
IP:           192.168.13.44
IPs:
  IP:           192.168.13.44
Controlled By:  ReplicaSet/microservice-deployment-in-tainted-nodes-5684cc495b
Containers:
  java-microservice-container-1:
    Container ID:
 docker://5c158df8cc160de8f57f62f3ee16b12725a87510a809d90a1fb9e5d873c320a4
    Image:          934188034500.dkr.ecr.us-east-1.amazonaws.com/java-eks-apg
    Image ID:       docker-pullable://934188034500.dkr.ecr.us-east-1.amazonaws.com/
java-eks-apg@sha256:d223924aca8315aab20d54eddf3443929eba511b6433017474d01b63a4114835
    Port:           4567/TCP
    Host Port:      0/TCP
    State:          Running
      Started:      Wed, 14 Sep 2022 11:07:02 -0400
    Ready:          True
    Restart Count:  0
    Environment:    <none>
    Mounts:
      /var/run/secrets/kubernetes.io/serviceaccount from kube-api-access-ddvvw (ro)
Conditions:
  Type              Status
  Initialized       True
  Ready             True
  ContainersReady   True
  PodScheduled      True
Volumes:
```

```
  kube-api-access-ddvvw:
    Type:                    Projected (a volume that contains injected data from
 multiple sources)
    TokenExpirationSeconds:  3607
    ConfigMapName:           kube-root-ca.crt
    ConfigMapOptional:       <nil>
    DownwardAPI:             true
QoS Class:                   BestEffort
Node-Selectors:              <none>
Tolerations:                 classifled_workload=true:NoSchedule
                             machine_learning_workload=true:NoSchedule
                             node.kubernetes.io/not-ready:NoExecute op=Exists for 300s
                             node.kubernetes.io/unreachable:NoExecute op=Exists for
 300s
Events:                      <none>
```

Replizieren Sie gefilterte Amazon ECR-Container-Images über Konten oder Regionen hinweg

Erstellt von Abdal Garuba (AWS)

Übersicht

Amazon Elastic Container Registry (Amazon ECR) kann alle Container-Images in einem Image-Repository über Amazon Web Services (AWS) -Regionen und AWS-Konten nativ replizieren, indem die Funktionen für die regionsübergreifende und kontoübergreifende Replikation verwendet werden. (Weitere Informationen finden Sie im AWS-Blogbeitrag Regionsübergreifende Replikation in Amazon ECR ist gelandet.) Es gibt jedoch keine Möglichkeit, die Bilder, die zwischen AWS-Regionen oder Konten kopiert werden, anhand von Kriterien zu filtern.

Dieses Muster beschreibt, wie Container-Images, die in Amazon ECR gespeichert sind, auf Grundlage von Image-Tag-Mustern über AWS-Konten und Regionen hinweg repliziert werden. Das Muster verwendet Amazon CloudWatch Events, um auf Push-Ereignisse für Bilder zu warten, die ein vordefiniertes, benutzerdefiniertes Tag haben. Ein Push-Ereignis startet ein CodeBuild AWS-Projekt und übergibt die Bilddetails an dieses Projekt. Das CodeBuild Projekt kopiert die Bilder auf der Grundlage der bereitgestellten Details aus der Amazon ECR-Quellregistrierung in die Zielregistrierung.

Dieses Muster kopiert Bilder, die bestimmte Tags haben, kontenübergreifend. Sie können dieses Muster beispielsweise verwenden, um nur produktionsbereite, sichere Images auf das AWS-Produktionskonto zu kopieren. Im Entwicklungskonto können Sie, nachdem die Bilder gründlich getestet wurden, den sicheren Images ein vordefiniertes Tag hinzufügen und die markierten Bilder mithilfe der Schritte in diesem Muster in das Produktionskonto kopieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto für Amazon ECR-Quell- und Zielregister
- Administratorberechtigungen für die in diesem Muster verwendeten Tools
- Docker wurde zum Testen auf Ihrem lokalen Computer installiert
- AWS-Befehlszeilenschnittstelle (AWS CLI) für die Authentifizierung bei Amazon ECR

Einschränkungen

- Dieses Muster überwacht die Push-Ereignisse der Quellregistrierung nur in einer AWS-Region. Sie können dieses Muster in anderen Regionen bereitstellen, um Registrierungen in diesen Regionen zu überwachen.
- In diesem Muster wartet eine Amazon CloudWatch Events-Regel auf ein einzelnes Bild-Tag-Muster. Wenn Sie nach mehreren Mustern suchen möchten, können Sie Ereignisse hinzufügen, um auf zusätzliche Bild-Tag-Muster zu warten.

Architektur

Zielarchitektur

Automatisierung und Skalierung

Dieses Muster kann mit einem IaC-Skript (Infrastructure as Code) automatisiert und in großem Umfang eingesetzt werden. Um dieses Muster mithilfe von CloudFormation AWS-Vorlagen bereitzustellen, laden Sie den Anhang herunter und folgen Sie den Anweisungen im Abschnitt Zusätzliche Informationen.

Sie können mehrere Amazon CloudWatch Events-Ereignisse (mit unterschiedlichen benutzerdefinierten Ereignismustern) auf dasselbe CodeBuild AWS-Projekt verweisen, um mehrere Image-Tag-Muster zu replizieren. Sie müssen jedoch die sekundäre Validierung in der `buildspec.yaml` Datei (die im Anhang und im Abschnitt Tools enthalten ist) wie folgt aktualisieren, um mehrere Muster zu unterstützen.

```
...
if [[ ${IMAGE_TAG} != release-* ]]; then
...
```

Tools

Amazon-Dienste

- IAM — Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf AWS-Services und -Ressourcen sicher verwalten. In diesem Muster müssten Sie die kontoübergreifende IAM-Rolle erstellen, die AWS beim Push von Container-Images in die Zielregistrierung CodeBuild übernimmt.

- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) ist eine vollständig verwaltete Container-Registry, die es einfach macht, Ihre Container-Images und Artefakte überall zu speichern, zu verwalten, zu teilen und bereitzustellen. Image-Push-Aktionen an die Quellregistrierung senden Systemereignisdetails an den Event-Bus, der von Amazon CloudWatch Events abgeholt wird.
- AWS CodeBuild — AWS CodeBuild ist ein vollständig verwalteter Continuous Integration Service, der Rechenleistung für Aufgaben wie das Kompilieren von Quellcode, das Ausführen von Tests und das Erstellen von Artefakten bereitstellt, die sofort einsatzbereit sind. Dieses Muster verwendet AWS CodeBuild , um den Kopiervorgang von der Amazon ECR-Quellregistrierung zur Zielregistrierung durchzuführen.
- CloudWatch Ereignisse — Amazon CloudWatch Events liefert einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben. Dieses Muster verwendet Regeln, um Amazon ECR-Push-Aktionen einem bestimmten Image-Tag-Muster zuzuordnen.

Tools

- Docker CLI — Docker ist ein Tool, das das Erstellen und Verwalten von Containern erleichtert. Container packen eine Anwendung und all ihre Abhängigkeiten in einer Einheit oder einem Paket, das problemlos auf jeder Plattform bereitgestellt werden kann, die die Container-Laufzeit unterstützt.

Code

Sie können dieses Muster auf zwei Arten implementieren:

- Automatisierte Einrichtung: Stellen Sie die beiden CloudFormation AWS-Vorlagen bereit, die im Anhang enthalten sind. Anweisungen finden Sie im Abschnitt Zusätzliche Informationen.
- Manuelle Einrichtung: Folge den Schritten im Abschnitt Epics.

Beispiel buildspec.yaml

Wenn Sie die CloudFormation Vorlagen verwenden, die mit diesem Muster bereitgestellt werden, ist die `buildspec.yaml` Datei in den Ressourcen enthalten. CodeBuild

```
version: 0.2
env:
  shell: bash
```

```
  phases:
    install:
      commands:
        - export CURRENT_ACCOUNT=$(echo ${CODEBUILD_BUILD_ARN} | cut -d':' -f5)
        - export CURRENT_ECR_REGISTRY=${CURRENT_ACCOUNT}.dkr.ecr.
${AWS_REGION}.amazonaws.com
        - export DESTINATION_ECR_REGISTRY=${DESTINATION_ACCOUNT}.dkr.ecr.
${DESTINATION_REGION}.amazonaws.com
    pre_build:
      on-failure: ABORT
      commands:
        - echo "Validating Image Tag ${IMAGE_TAG}"
        - |
          if [[ ${IMAGE_TAG} != release-* ]]; then
            aws codebuild stop-build --id ${CODEBUILD_BUILD_ID}
            sleep 60
            exit 1
          fi
        - aws ecr get-login-password --region ${AWS_REGION} | docker login -u AWS --
password-stdin ${CURRENT_ECR_REGISTRY}
        - docker pull ${CURRENT_ECR_REGISTRY}/${REPO_NAME}:${IMAGE_TAG}
    build:
      commands:
        - echo "Assume cross-account role"
        - CREDENTIALS=$(aws sts assume-role --role-arn ${CROSS_ACCOUNT_ROLE_ARN} --
role-session-name Rolesession)
        - export AWS_DEFAULT_REGION=${DESTINATON_REGION}
        - export AWS_ACCESS_KEY_ID=$(echo ${CREDENTIALS} | jq -r
 '.Credentials.AccessKeyId')
        - export AWS_SECRET_ACCESS_KEY=$(echo ${CREDENTIALS} | jq -r
 '.Credentials.SecretAccessKey')
        - export AWS_SESSION_TOKEN=$(echo ${CREDENTIALS} | jq -r
 '.Credentials.SessionToken')
        - echo "Logging into cross-account registry"
        - aws ecr get-login-password --region ${DESTINATION_REGION} | docker login -u
 AWS --password-stdin ${DESTINATION_ECR_REGISTRY}
        - echo "Check if Destination Repository exists, else create"
        - |
          aws ecr describe-repositories --repository-names ${REPO_NAME} --region
 ${DESTINATION_REGION} \
          || aws ecr create-repository --repository-name ${REPO_NAME} --region
 ${DESTINATION_REGION}
        - echo "retag image and push to destination"
```

```
        - docker tag ${CURRENT_ECR_REGISTRY}/${REPO_NAME}:${IMAGE_TAG}
${DESTINATION_ECR_REGISTRY}/${REPO_NAME}:${IMAGE_TAG}
        - docker push ${DESTINATION_ECR_REGISTRY}/${REPO_NAME}:${IMAGE_TAG}
```

Epen

Erstellen Sie IAM-Rollen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Rolle „ CloudWatch Ereignisse“.	Erstellen Sie im AWS-Quell konto eine IAM-Rolle, die Amazon CloudWatch Events übernehmen soll. Die Rolle sollte über Berechtigungen zum Starten eines CodeBuild AWS-Projekts verfügen. Folgen Sie den Anweisungen in der IAM-Dokumentation, um die Rolle mithilfe der AWS-CLI zu erstellen. Beispiel für eine Vertrauen srichtlinie (`trustpolicy.json`): `{ "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Principal": {"Service": "events.amazonaws.com"}, "Action": "sts:AssumeRole" } }`	AWS-Administrator DevOps, AWS, AWS-Systemadministrator, Cloud-Administrator, Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Beispiel für eine Berechtigungsrichtlinie (`permissionpolicy.json`):
	
	`{`
	`  "Version": "2012-10-17",`
	`  "Statement": {`
	`  "Effect": "Allow",`
	`  "Action": "codebuild:StartBuild",`
	`  "Resource": "<CodeBuild Project ARN>"`
	`  }`
	`}`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CodeBuild Rolle.	Erstellen Sie eine IAM-Rolle , die AWS übernehmen CodeBuild soll, indem Sie den Anweisungen in der IAM-Dokumentation folgen. Die Rolle sollte über die folgenden Berechtigungen verfügen: • Erlaubnis, die kontoüber greifende Zielrolle zu übernehmen • Berechtigung zum Erstellen von Protokollgruppen und Protokollströmen sowie zum Speichern von Protokoll ereignissen • Schreibgeschützte Berechtigungen für alle Amazon ECR-Repositorys, indem die von Amazon EC2 ContainerRegistryReadOnly verwaltete Richtlinie zur Rolle hinzugefügt wird • Erlaubnis zum Beenden CodeBuild Beispiel für eine Vertrauen srichtlinie (`trustpoli cy.json`): `{ "Version": "2012-10-17", "Statement": [ {`	AWS-Administrator DevOps, AWS, AWS-Systemadminist rator, Cloud-Administrato r, Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Effect": "Allow",
	"Principal": {
	"Service":
	"codebuild.amazonaws.com"
	},
	"Action":
	"sts:AssumeRole"
	}
	]
	}</pre>
	Beispiel für eine Berechtigungsrichtlinie (`permissionpolicy.json`):
	<pre>{
	"Version":
	"2012-10-17",
	"Statement": [
	{
	"Action": [
	"codebuild:StartBuild",
	"codebuild:StopBuild",
	"codebuild:Get*",
	"codebuild:List*",
	"codebuild:BatchGet*"
	],
	"Resource":
	"*",
	"Effect":
	"Allow"
	},
	{</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Action": [
	
	"logs:CreateLogGro
	up",
	
	"logs:CreateLogStr
	eam",
	
	"logs:PutLogEvents"
	],
	"Resource":
	"*",
	"Effect":
	"Allow"
	},
	{
	"Action":
	"sts:AssumeRole",
	"Resource":
	"<ARN of destination
	role>",
	"Effect":
	"Allow",
	"Sid":
	"AssumeCrossAccoun
	tArn"
	}
	]
	}</pre> Hängen Sie die verwaltete Richtlinie wie folgt `AmazonEC2ContainerRegistryReadOnly` an den CLI-Befehl an: <pre>~$ aws iam attach-role-
	policy \
	--policy-arn arn:aws:i
	am::aws:policy/Ama</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`zonEC2ContainerReg istryReadOnly \ --role-name <name of CodeBuild Role>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine kontoüber greifende Rolle.	Erstellen Sie im AWS-Zielk onto eine IAM-Rolle für die CodeBuild AWS-Rolle, die das Quellkonto übernehmen soll. Die kontoübergreifende Rolle sollte es Container-Images ermöglichen, ein neues Repository zu erstellen und Container-Images auf Amazon ECR hochzuladen. Folgen Sie den Anweisung en in der IAM-Dokumentation, um die IAM-Rolle mithilfe der AWS-CLI zu erstellen. Verwenden Sie die folgende Vertrauensrichtlinie, um das CodeBuild AWS-Projekt aus dem vorherigen Schritt zuzulassen: `{ "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Principal": { "AWS": "<ARN of source codebuild role>" }, "Action": "sts:AssumeRole" } }`	AWS-Administrator DevOps, AWS, Cloud-Administrato r, Cloud-Architekt, DevOps Ingenieur, AWS-Syste madministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Verwenden Sie die folgende Berechtigungsrichtlinie, damit das CodeBuild AWS-Projekt aus dem vorherigen Schritt Bilder in der Zielregistrierung speichern kann: `{ "Version": "2012-10-17", "Statement": [ { "Action": [ "ecr:GetDownloadUrlForLayer", "ecr:BatchCheckLayerAvailability", "ecr:PutImage", "ecr:InitiateLayerUpload", "ecr:UploadLayerPart", "ecr:CompleteLayerUpload", "ecr:GetRepositoryPolicy", "ecr:DescribeRepositories", "ecr:GetAuthorizationToken",`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"ecr:CreateRepository"
	            ],
	            "Resource": "*",
	            "Effect": "Allow"
	        }
	    ]
	}</pre>	

Erstellen Sie das CodeBuild Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein CodeBuild Projekt.	Erstellen Sie ein CodeBuild AWS-Projekt im Quellkonto, indem Sie den Anweisungen in der CodeBuild AWS-Dokumentation folgen. Das Projekt sollte sich in derselben Region wie die Quellregistrierung befinden. Konfigurieren Sie das Projekt wie folgt: • Art der Umgebung: `LINUX CONTAINER` • Rolle im Dienst: `CodeBuild Role` • Privilegierter Modus: `true` • Umgebungsbild: `aws/codebuild/standard:x.x` (verwenden	AWS-Administrator DevOps, AWS, AWS-Systemadministrator, Cloud-Administrator, Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Sie das neueste verfügbare Image)
	• Umgebungsvariablen:
	  • `CROSS_ACCOUNT_ROLE_ARN` : Der Amazon-Ressourcenname (ARN) der kontoübergreifenden Rolle
	  • `DESTINATION_REGION` : Der Name der kontoübergreifenden Region
	  • `DESTINATION_ACCOUNT` : Die Nummer des Zielkontos
	• Build-Spezifikationen: Verwenden Sie die `buildspec.yaml` Datei, die im Abschnitt Tools aufgeführt ist.	

Erstellen Sie das Ereignis

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Ereignisregel.	Da das Muster die Inhaltsfilterfunktion verwendet, müssen Sie das Ereignis mithilfe von Amazon erstellen EventBridge. Erstellen Sie das Ereignis und das Ziel, indem Sie den Anweisungen in der EventBridge Dokumentation	AWS-Administrator DevOps, AWS, AWS-Systemadministrator, Cloud-Administrator, Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	folgen, mit einigen Änderungen: • Wählen Sie für Muster definieren die Option Ereignismuster und anschließend Benutzerdefiniertes Muster aus. • Kopieren Sie den folgenden Beispielcode für ein benutzerdefiniertes Ereignismuster in das dafür vorgesehene Textfeld: `{ "source": ["aws.ecr"], "detail-type": ["ECR Image Action"], "detail": { "action-type": ["PUSH"], "result": ["SUCCESS"], "image-tag": [{ "prefix": "release-"}] } }` • Wählen Sie für Select targets das CodeBuild AWS-Projekt aus und fügen Sie den ARN für das CodeBuild AWS-Projekt ein, das Sie im vorherigen Epic erstellt haben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	• Wählen Sie für Configure Input die Option Input Transformer aus.
	  • Fügen Sie in das Textfeld Eingabepfad Folgendes ein:
	  `{"IMAGE_TAG":"$.detail.image-tag","REPO_NAME":"$.detail.repository-name"}`
	  • Fügen Sie in das Textfeld Eingabevorlage Folgendes ein:
	  `{"environmentVariablesOverride":[ {"name": "IMAGE_TAG", "value":<IMAGE_TAG>},{"name":"REPO_NAME","value":<REPO_NAME>}]}`
	• Wählen Sie „Bestehende Rolle verwenden“ und anschließend den Namen der Rolle „ CloudWatch Ereignisse“, die Sie zuvor im Epos „IAM-Rollen erstellen“ erstellt haben.	

Validieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Authentifizieren Sie sich mit Amazon ECR.	Authentifizieren Sie sich sowohl bei der Quell- als auch bei der Zielregistrierung, indem Sie die Schritte in der Amazon ECR-Dokumentation befolgen.	AWS-Administrator DevOps, AWS, AWS-Systemadministrator, Cloud-Administrator, DevOps Ingenieur, Cloud-Architekt
Testen Sie die Image-Replikation.	Übertragen Sie in Ihrem Quellkonto ein Container-Image in ein neues oder vorhandenes Amazon ECR-Quell-Repository mit einem Image-Tag als Präfix. `release-` Um das Bild zu übertragen, folgen Sie den Schritten in der Amazon ECR-Dokumentation. Sie können den Fortschritt des CodeBuild Projekts in der CodeBuild Konsole überwachen. Melden Sie sich nach erfolgreichem Abschluss des CodeBuild Projekts beim AWS-Zielkonto an, öffnen Sie die Amazon ECR-Konsole und vergewissern Sie sich, dass das Bild in der Amazon ECR-Zielregistrierung vorhanden ist.	AWS-Administrator DevOps, AWS, AWS-Systemadministrator, Cloud-Administrator, Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie den Image-Ausschluss.	Übertragen Sie in Ihrem Quellkonto ein Container-Image in ein neues oder vorhandenes Amazon ECR-Quell-Repository mit einem Image-Tag, das nicht über das benutzerdefinierte Präfix verfügt. Vergewissern Sie sich, dass das CodeBuild Projekt nicht gestartet wurde und dass keine Container-Images in der Zielregistrierung erscheinen.	AWS-Administrator DevOps, AWS, AWS-Systemadministrator, Cloud-Administrator, Cloud-Architekt, DevOps Ingenieur

Zugehörige Ressourcen

- Erste Schritte mit CodeBuild
- Erste Schritte mit Amazon EventBridge
- Inhaltsbasierte Filterung in EventBridge Amazon-Ereignismustern
- Delegieren Sie den Zugriff über AWS-Konten hinweg mithilfe von IAM-Rollen
- Replikation privater Images

Zusätzliche Informationen

Gehen Sie folgendermaßen vor, um die Ressourcen für dieses Muster automatisch bereitzustellen:

1. Laden Sie den Anhang herunter und extrahieren Sie die beiden CloudFormation Vorlagen: `part-1-copy-tagged-images.yaml` und`part-2-destination-account-role.yaml`.
2. Melden Sie sich bei der CloudFormation AWS-Konsole an und führen Sie die Bereitstellung `part-1-copy-tagged-images.yaml` in demselben AWS-Konto und derselben Region wie die Amazon ECR-Quellregistrierungen durch. Aktualisieren Sie die Parameter nach Bedarf. Die Vorlage stellt die folgenden Ressourcen bereit:

- CloudWatch IAM-Rolle bei Amazon Events
- CodeBuild IAM-Rolle des AWS-Projekts
- CodeBuild AWS-Projekt
- CloudWatch AWS-Ereignisregel

3. Notieren Sie sich den Wert von `SourceRoleName` auf der Registerkarte Ausgaben. Sie benötigen diesen Wert im nächsten Schritt.
4. Stellen Sie die zweite CloudFormation Vorlage in dem AWS-Konto bereit, `part-2-destination-account-role.yaml` in das Sie die Amazon ECR-Container-Images kopieren möchten. Aktualisieren Sie die Parameter nach Bedarf. Geben Sie für den `SourceRoleName` Parameter den Wert aus Schritt 3 an. Diese Vorlage stellt die kontoübergreifende IAM-Rolle bereit.
5. Überprüfen Sie die Replikation und den Ausschluss von Images, wie im letzten Schritt des Abschnitts Epics beschrieben.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Datenbankanmeldedaten rotieren, ohne Container neu zu starten

Erstellt von Josh Joy (AWS)

Übersicht

In der Amazon Web Services (AWS) Cloud können Sie AWS Secrets Manager verwenden, um Datenbankanmeldedaten während ihres gesamten Lebenszyklus zu rotieren, zu verwalten und abzurufen. Benutzer und Anwendungen rufen Geheimnisse mit einem Aufruf der Secrets Manager Manager-API ab, sodass sensible Informationen nicht mehr im Klartext hartcodiert werden müssen.

Wenn Sie Container für Microservice-Workloads verwenden, können Sie Anmeldeinformationen sicher in AWS Secrets Manager speichern. Um die Konfiguration vom Code zu trennen, werden diese Anmeldeinformationen üblicherweise in den Container eingefügt. Es ist jedoch wichtig, dass Sie Ihre Anmeldeinformationen regelmäßig und automatisch wechseln. Es ist auch wichtig, die Möglichkeit zu unterstützen, Anmeldeinformationen nach dem Widerruf zu aktualisieren. Gleichzeitig müssen Anwendungen die Möglichkeit haben, Anmeldeinformationen abwechselnd auszutauschen und gleichzeitig mögliche Auswirkungen auf die Verfügbarkeit im Downstream-Bereich zu reduzieren.

Dieses Muster beschreibt, wie Sie Ihre mit AWS Secrets Manager gesicherten Secrets innerhalb Ihrer Container rotieren, ohne dass Ihre Container neu gestartet werden müssen. Darüber hinaus reduziert dieses Muster die Anzahl der Abfragen von Anmeldeinformationen in Secrets Manager, indem die clientseitige Caching-Komponente von Secrets Manager verwendet wird. Wenn Sie die clientseitige Caching-Komponente verwenden, um die Anmeldeinformationen innerhalb der Anwendung zu aktualisieren, muss der Container nicht neu gestartet werden, um rotierte Anmeldeinformationen abzurufen.

Dieser Ansatz funktioniert für Amazon Elastic Kubernetes Service (Amazon EKS) und Amazon Elastic Container Service (Amazon ECS).

Zwei Szenarien werden behandelt. Im Einzelbenutzer-Szenario werden die Datenbankanmeldeinformationen bei der geheimen Rotation aktualisiert, indem die abgelaufenen Anmeldeinformationen erkannt werden. Der Anmeldeinformations-Cache wird angewiesen, das Geheimnis zu aktualisieren, und dann stellt die Anwendung die Datenbankverbindung wieder her. Die clientseitige Caching-Komponente speichert die Anmeldeinformationen innerhalb der Anwendung im Cache und verhindert, dass bei jeder Suche nach Anmeldeinformationen der Secrets Manager kontaktiert werden muss. Die Anmeldeinformationen werden innerhalb der Anwendung rotiert, ohne dass die Aktualisierung der Anmeldeinformationen durch einen Neustart des Containers erzwungen werden muss.

Im zweiten Szenario wechselt das Geheimnis abwechselnd zwischen zwei Benutzern. Zwei aktive Benutzer reduzieren das Risiko von Ausfallzeiten, da die Anmeldeinformationen eines Benutzers immer aktiv sind. Die Rotation der Anmeldeinformationen für zwei Benutzer ist hilfreich, wenn Sie eine große Bereitstellung mit Clustern haben, in denen es zu einer geringen Verzögerung bei der Weitergabe von Anmeldeinformationen kommen kann.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine Anwendung, die in einem Container in Amazon EKS oder Amazon ECS ausgeführt wird.
- In Secrets Manager gespeicherte Anmeldeinformationen mit aktivierter Rotation.
- Ein zweiter Satz von Anmeldeinformationen, die in Secrets Manager gespeichert werden, wenn die Zweibenutzerlösung bereitgestellt wird. Codebeispiele finden Sie im GitHub Repo aws-secrets-manager-rotation -lambdas.
- Eine Amazon Aurora Aurora-Datenbank.

Einschränkungen

- Dieses Beispiel ist für Python-Anwendungen vorgesehen. Für Java-Anwendungen können Sie die clientseitige Java-Caching-Komponente oder die clientseitige JDBC-Caching-Bibliothek für Secrets Manager verwenden.

Architektur

Zielarchitektur

Szenario 1 — Rotation von Anmeldeinformationen für einen einzelnen Benutzer

Im ersten Szenario werden einzelne Datenbankanmeldedaten regelmäßig von Secrets Manager rotiert. Der Anwendungscontainer läuft in Fargate. Wenn die erste Datenbankverbindung hergestellt ist, ruft der Anwendungscontainer die Datenbankanmeldedaten für Aurora ab. Die Secrets Manager Manager-Caching-Komponente speichert dann die Anmeldeinformationen für den future Verbindungsaufbau zwischen. Nach Ablauf der Rotationsperiode laufen die Anmeldeinformationen ab und die Datenbank gibt einen Authentifizierungsfehler zurück. Die Anwendung ruft dann die rotierten

Anmeldeinformationen ab, macht den Cache ungültig und aktualisiert den Anmeldeinformationen-Cache über die clientseitige Caching-Komponente von Secrets Manager.

In diesem Szenario kann es zu einer minimalen Unterbrechung kommen, während die Anmeldeinformationen rotiert werden und veraltete Verbindungen die veralteten Anmeldeinformationen verwenden. Dieses Problem kann durch die Verwendung des Zwei-Benutzer-Szenarios behoben werden.

Szenario 2 — Rotation der Anmeldeinformationen für zwei Benutzer

Im zweiten Szenario werden zwei Datenbankbenutzeranmeldeinformationen (die von Alice und Bob) regelmäßig von Secrets Manager gewechselt. Der Anwendungscontainer läuft in einem Fargate-Cluster. Wenn die erste Datenbankverbindung hergestellt ist, ruft der Anwendungscontainer die Aurora-Datenbankanmeldedaten für den ersten Benutzer (Alice) ab. Die Secrets Manager Manager-Caching-Komponente speichert dann die Anmeldeinformationen für den future Verbindungsaufbau zwischen.

Obwohl es zwei Benutzer und Anmeldeinformationen gibt, wird nur ein aktiver Berechtigungsnachweis von Secrets Manager verwaltet. In diesem Fall läuft die Caching-Komponente regelmäßig ab und ruft die neuesten Anmeldeinformationen ab. Wenn die Secrets Manager Manager-Rotationsperiode länger als das Cache-Timeout ist, übernimmt die Caching-Komponente die rotierten Anmeldeinformationen für den zweiten Benutzer (Bob). Wenn beispielsweise der Cache-Ablauf in Minuten und der Rotationszeitraum in Tagen gemessen wird, ruft die Caching-Komponente die neuen Anmeldeinformationen im Rahmen ihrer regelmäßigen Cache-Aktualisierung ab. Auf diese Weise wird die Ausfallzeit minimiert, da die Anmeldeinformationen jedes Benutzers für eine Secrets Manager Manager-Rotation aktiv sind.

Automatisierung und Skalierung

Sie können AWS verwenden CloudFormation, um dieses Muster bereitzustellen, indem Sie Infrastruktur als Code verwenden. Dadurch wird der Anwendungscontainer erstellt und erstellt, die Fargate-Aufgabe erstellt, der Container in Fargate bereitgestellt und Secrets Manager mit Aurora eingerichtet und konfiguriert. Anweisungen zur step-by-step Bereitstellung finden Sie in der Readme-Datei.

Tools

Tools

- AWS Secrets Manager ermöglicht das Ersetzen von hartcodierten Anmeldeinformationen, einschließlich Passwörtern, durch einen API-Aufruf an Secrets Manager, um das Geheimnis abzurufen. Da Secrets Manager das Secret automatisch nach einem Zeitplan rotieren kann, können Sie langfristige Geheimnisse durch kurzfristige ersetzen und so das Risiko von Kompromissen verringern.
- Docker hilft Entwicklern dabei, jede Anwendung als leichten, portablen und autarken Container zu packen, zu versenden und auszuführen.

Code

Beispiel für Python-Code

Dieses Muster verwendet die clientseitige Python-Caching-Komponente für Secrets Manager, um die Authentifizierungsdaten abzurufen, wenn die Datenbankverbindung hergestellt wird. Durch die clientseitige Caching-Komponente wird vermieden, dass Sie jedes Mal den Secrets Manager kontaktieren müssen.

Wenn die Rotationsperiode nun abgelaufen ist, laufen die zwischengespeicherten Anmeldeinformationen ab und die Verbindung mit der Datenbank führt zu einem Authentifizierungsfehler. Für MySQL lautet der Authentifizierungsfehlercode 1045. In diesem Beispiel wird Amazon Aurora für MySQL verwendet, Sie könnten jedoch auch eine andere Engine wie PostgreSQL verwenden. Bei einem Authentifizierungsfehler fängt der Code zur Behandlung von Datenbankverbindungsausnahmen den Fehler ab. Anschließend informiert es die clientseitige Caching-Komponente von Secrets Manager, den Secret zu aktualisieren und anschließend die Datenbankverbindung erneut zu authentifizieren und wiederherzustellen. Wenn Sie PostgreSQL oder eine andere Engine verwenden, müssen Sie den entsprechenden Authentifizierungsfehlercode nachschlagen.

Die Containeranwendung kann jetzt das Datenbankkennwort mit dem rotierten Passwort aktualisieren, ohne den Container neu zu starten.

Fügen Sie den folgenden Code in Ihren Anwendungscode ein, der Datenbankverbindungen verarbeitet. In diesem Beispiel wird Django verwendet und das Datenbank-Backend mit einem Datenbank-Wrapper für Verbindungen untergliedert. Wenn Sie eine andere Programmiersprache oder Datenbankverbindungsbibliothek verwenden, finden Sie in Ihrer Datenbankverbindungsbibliothek nach, wie Sie das Abrufen von Datenbankverbindungen in Unterklassen unterteilen.

```
    def get_new_connection(self, conn_params):
```

```
        try:
            logger.info("get connection")
            databasecredentials.get_conn_params_from_secrets_manager(conn_params)
            conn =super(DatabaseWrapper,self).get_new_connection(conn_params)
            return conn
        except MySQLdb.OperationalError as e:
            error_code=e.args[0]
            if error_code!=1045:
                raise e

            logger.info("Authentication error. Going to refresh secret and try again.")
            databasecredentials.refresh_now()
            databasecredentials.get_conn_params_from_secrets_manager(conn_params)
            conn=super(DatabaseWrapper,self).get_new_connection(conn_params)
            logger.info("Successfully refreshed secret and established new database
connection.")
            return conn
```

AWS CloudFormation - und Python-Code

- https://github.com/aws-samples/aws-secrets-manager-credential-rotation-without-container-restart

Epen

Sorgen Sie bei der Rotation der Anmeldeinformationen für die Anwendungsverfügbarkeit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die Caching-K omponente.	Laden Sie die clientseitige Caching-Komponente von Secrets Manager für Python herunter und installieren Sie sie. Den Download-Link finden Sie im Abschnitt Verwandte Ressourcen.	Developer
Zwischenspeichern Sie die funktionierenden Anmeldein formationen.	Verwenden Sie die clientsei tige Caching-Komponente von Secrets Manager, um die funktionierenden Anmeldein	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	formationen lokal zwischenz uspeichern.	
Aktualisieren Sie den Anwendungscode, um die Anmeldeinformationen bei einem nicht autorisierten Fehler bei der Datenbank verbindung zu aktualisieren.	Aktualisieren Sie den Anwendungscode, um Secrets Manager zum Abrufen und Aktualisieren von Datenbank anmeldeinformationen zu verwenden. Fügen Sie die Logik zur Behandlung nicht autorisierter Fehlercodes hinzu und rufen Sie dann die neu rotierten Anmeldein formationen ab. Weitere Informationen finden Sie im Abschnitt Python-Beispielcod e.	Developer

Zugehörige Ressourcen

Ein Secrets Manager Manager-Geheimnis erstellen

- Schlüssel in AWS KMS erstellen
- Secrets mit AWS Secrets Manager erstellen und verwalten

Erstellen Sie einen Amazon Aurora Aurora-Cluster

- Eine Amazon RDS-DB-Instance erstellen

Erstellen Sie die Amazon ECS-Komponenten

- Erstellen eines Clusters mit der klassischen Konsole
- Erstellen Sie ein Docker-Image
- Ein privates Repository erstellen

- Privates Amazon ECR-Register
- Ein Docker-Image pushen
- Amazon ECS-Aufgabendefinitionen
- Einen Amazon ECS-Service in der klassischen Konsole erstellen

Laden Sie die clientseitige Caching-Komponente von Secrets Manager herunter und installieren Sie sie

- Python-Caching-Client

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Führen Sie Amazon ECS-Aufgaben auf Amazon WorkSpaces mit Amazon ECS Anywhere aus

Erstellt von Akash Kumar (AWS)

Übersicht

Amazon Elastic Container Service (Amazon ECS) Anywhere unterstützt die Bereitstellung von Amazon ECS-Aufgaben in jeder Umgebung, einschließlich der von Amazon Web Services (AWS) verwalteten Infrastruktur und der vom Kunden verwalteten Infrastruktur. Sie können dies tun, während Sie eine vollständig von AWS verwaltete Kontrollebene verwenden, die in der Cloud läuft und immer auf dem neuesten Stand ist.

Unternehmen nutzen Amazon häufig WorkSpaces für die Entwicklung containerbasierter Anwendungen. Dies erforderte Amazon Elastic Compute Cloud (Amazon EC2) oder AWS Fargate mit einem Amazon ECS-Cluster, um ECS-Aufgaben zu testen und auszuführen. Mit Amazon ECS Anywhere können Sie Amazon jetzt WorkSpaces als externe Instances direkt zu einem ECS-Cluster hinzufügen und Ihre Aufgaben direkt ausführen. Dies reduziert Ihre Entwicklungszeit, da Sie Ihren Container mit einem ECS-Cluster lokal auf Amazon testen können WorkSpaces. Sie können sich auch die Kosten für die Nutzung unserer EC2 Fargate-Instances zum Testen Ihrer Containeranwendungen sparen.

Dieses Muster zeigt, wie ECS-Aufgaben auf Amazon WorkSpaces mit Amazon ECS Anywhere bereitgestellt werden. Es richtet den ECS-Cluster ein und verwendet AWS Directory Service Simple AD, um den zu starten WorkSpaces. Dann startet die ECS-Beispielaufgabe NGINX in der. WorkSpaces

Voraussetzungen und Einschränkungen

- Ein aktives AWS-Konto
- AWS-Befehlszeilenschnittstelle (AWS Command Line Interface, AWS CLI)
- Auf Ihrem Computer konfigurierte AWS-Anmeldeinformationen

Architektur

Zieltechnologie-Stack

- Eine virtuelle private Cloud (VPC)

- Ein Amazon ECS-Cluster
- Amazon WorkSpaces
- AWS Directory Service mit Simple AD

Zielarchitektur

Die Architektur umfasst die folgenden Dienste und Ressourcen:

- Ein ECS-Cluster mit öffentlichen und privaten Subnetzen in einer benutzerdefinierten VPC
- Simple AD in der VPC, um Benutzern Zugriff auf Amazon zu gewähren WorkSpaces
- Amazon wird in der VPC mit Simple AD WorkSpaces bereitgestellt
- AWS Systems Manager wurde für das Hinzufügen von Amazon WorkSpaces als verwaltete Instances aktiviert
- Mithilfe von Amazon ECS und AWS Systems Manager Agent (SSM Agent) WorkSpaces fügte Amazon Systems Manager und dem ECS-Cluster hinzu
- Ein Beispiel für eine ECS-Aufgabe zur Ausführung WorkSpaces im ECS-Cluster

Tools

- AWS Directory Service Simple Active Directory (Simple AD) ist ein eigenständiges verwaltetes Verzeichnis, das von einem Samba 4 Active Directory-kompatiblen Server betrieben wird. Simple AD bietet einen Teil der Funktionen von AWS Managed Microsoft AD, einschließlich der Möglichkeit, Benutzer zu verwalten und eine sichere Verbindung zu EC2 Amazon-Instances herzustellen.
- Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Beenden und Verwalten von Containern in einem Cluster vereinfacht.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Systems Manager unterstützt Sie bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der AWS-Cloud ausgeführt werden. Es vereinfacht das Anwendungs- und

Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme und hilft Ihnen, Ihre AWS-Ressourcen sicher und skalierbar zu verwalten.

- Amazon WorkSpaces unterstützt Sie bei der Bereitstellung virtueller, Cloud-basierter Microsoft Windows- oder Amazon Linux-Desktops für Ihre Benutzer, bekannt als WorkSpaces. WorkSpaces macht die Beschaffung und Bereitstellung von Hardware oder die Installation komplexer Software überflüssig.

Epen

Richten Sie den ECS-Cluster ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und konfigurieren Sie den ECS-Cluster.	Um den ECS-Cluster zu erstellen, folgen Sie den Anweisungen in der AWS-Dokumentation, einschließlich der folgenden Schritte: • Wählen Sie für Select-Cluster-Kompatibilität die Option Nur Networking aus, wodurch Amazon WorkSpace als externe Instance für den ECS-Cluster unterstützt wird. • Wählen Sie, ob Sie eine neue VPC erstellen möchten.	Cloud-Architekt

Starten Sie Amazon WorkSpaces

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Simple AD ein und starten Sie Amazon WorkSpaces.	Folgen Sie den Anweisungen in der AWS-Dokumentation, um ein Simple AD AD-Verzeichnis für Ihre neu erstellte VPC bereitzustellen und Amazon WorkSpaces zu starten.	Cloud-Architekt

AWS Systems Manager für eine Hybridumgebung einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die angehängten Skripte herunter.	Laden Sie auf Ihrem lokalen Computer die `ssm-activation.json` Dateien `ssm-trust-policy.json` und herunter, die sich im Bereich Anlagen befinden.	Cloud-Architekt

Fügen Sie die IAM-Rolle hinzu.	Fügen Sie Umgebungsvariablen hinzu, die auf Ihren Geschäftsanforderungen basieren.
	`export AWS_DEFAULT_REGION=${AWS_REGION_ID}`
	`export ROLE_NAME=${ECS_TASK_ROLE}`
	`export CLUSTER_NAME=${ECS_CLUSTER_NAME}`
	`export SERVICE_NAME=${ECS_CLUSTER_SERVICE_NAME}`
		Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Führen Sie den folgenden Befehl aus. `aws iam create-role --role-name $ROLE_NAME --assume-role-policy-document file://ssm-trust-policy.json`	
Fügen Sie die SSMManaged InstanceCore Amazon-Richtlinie zur IAM-Rolle hinzu.	Führen Sie den folgenden Befehl aus. `aws iam attach-role-policy --role-name $ROLE_NAME --policy-arn arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`	Cloud-Architekt
Fügen Sie die EC2 Container Servicefor EC2 Amazon-Rollenrichtlinie zur IAM-Rolle hinzu.	Führen Sie den folgenden Befehl aus. `aws iam attach-role-policy --role-name $ROLE_NAME --policy-arn arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`	Cloud-Architekt
Überprüfen Sie die IAM-Rolle.	Führen Sie den folgenden Befehl aus, um die IAM-Rolle zu überprüfen. `aws iam list-attached-role-policies --role-name $ROLE_NAME`	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie den Systems Manager.	Führen Sie den folgenden Befehl aus. `aws ssm create-activation --iam-role $ROLE_NAME | tee ssm-activation.json`	Cloud-Architekt

WorkSpaces Zum ECS-Cluster hinzufügen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Connect dich mit deinem WorkSpaces.	Folgen Sie den Anweisungen in der AWS-Dokumentation, um eine Verbindung zu Ihren Workspaces herzustellen und diese einzurichten.	App-Developer
Laden Sie das ECS-Anywhere-Installationsskript herunter.	Führen Sie an der Eingabeaufforderung den folgenden Befehl aus. `curl -o "ecs-anywhere-install.sh" "https://amazon-ecs-agent-packages-preview.s3.us-east-1.amazonaws.com/ecs-anywhere-install.sh" && sudo chmod +x ecs-anywhere-install.sh`	App-Developer
Überprüfen Sie die Integrität des Shell-Skripts.	(Optional) Führen Sie den folgenden Befehl aus.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`curl -o "ecs-anywhere-install.sh.sha256" "https://amazon-ecs-agent-packages-preview.s3.us-east-1.amazonaws.com/ecs-anywhere-install.sh.sha256" && sha256sum -c ecs-anywhere-install.sh.sha256`	
Fügen Sie ein EPEL-Repository auf Amazon Linux hinzu.	Um ein EPEL-Repository (Extra Packages for Enterprise Linux) hinzuzufügen, führen Sie den Befehl aus. `sudo amazon-linux-extras install epel -y`	App-Developer
Installieren Sie Amazon ECS Anywhere.	Verwenden Sie den folgenden Befehl, um das Installationsskript auszuführen. `sudo ./ecs-anywhere-install.sh --cluster $CLUSTER_NAME --activation-id $ACTIVATION_ID --activation-code $ACTIVATION_CODE --region $AWS_REGION`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Instanzin formationen aus dem ECS-Cluster.	Führen Sie den folgenden Befehl auf Ihrem lokalen Computer aus, um die Informationen zu Systems Manager- und ECS-Clust erinstanzen zu überprüfen und zu überprüfen, ob sie dem Cluster hinzugefügt WorkSpaces wurden. `aws ssm describe-instance-informati on" && "aws ecs list-container-instances --cluster $CLUSTER_NAME`	App-Developer

Fügen Sie eine ECS-Aufgabe hinzu für WorkSpaces

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle für die Aufgabenausführung.	Laden Sie `task-execution-assume-role.json` und `external-task-definition.json` aus dem Bereich Anlagen herunter. Führen Sie auf Ihrem lokalen Computer den folgenden Befehl aus. `aws iam --region $AWS_DEFAULT_REGION create-role --role-name $ECS_TASK`	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`_EXECUTION_ROLE -- assume-role-policy- document file://ta sk-execution-assume- role.json`	
Fügen Sie die Richtlinie der Ausführungsrolle hinzu.	Führen Sie den folgenden Befehl aus. `aws iam --region $AWS_DEFAULT_REGIO N attach-role-policy --role-name $ECS_TASK _EXECUTION_ROLE -- policy-arn arn:aws:i am::aws:policy/ser vice-role/AmazonEC STaskExecutionRole Policy`	Cloud-Architekt
Erstellen Sie eine Aufgabenr olle.	Führen Sie den folgenden Befehl aus. `aws iam --region $AWS_DEFAULT_REGIO N create-role -- role-name $ECS_TASK _EXECUTION_ROLE -- assume-role-policy- document file://ta sk-execution-assume- role.json`	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Registrieren Sie die Aufgabendefinition im Cluster.	Führen Sie auf Ihrem lokalen Computer den folgenden Befehl aus. `aws ecs register-task-definition --cli-input-json file://external-task-definition.json`	Cloud-Architekt
Führen Sie die Aufgabe aus.	Führen Sie auf Ihrem lokalen Computer den folgenden Befehl aus. `aws ecs run-task --cluster $CLUSTER_NAME --launch-type EXTERNAL --task-definition nginx`	Cloud-Architekt

Überprüfen Sie den Status, in dem die Aufgabe ausgeführt wird.	Führen Sie den folgenden Befehl aus, um die Aufgaben-ID abzurufen.
	`export TEST_TASKID=$(aws ecs list-tasks --cluster $CLUSTER_NAME | jq -r '.taskArns[0]')`
	Führen Sie mit der Task-ID den folgenden Befehl aus.
	`aws ecs describe-tasks --cluster $CLUSTER_NAME --tasks ${TEST_TASKID}`
		Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Aufgabe auf dem WorkSpace.	Um zu überprüfen, ob NGINX auf dem läuft WorkSpace , führen Sie den Befehl aus. `curl http://localhost:8080`	App-Developer

Zugehörige Ressourcen

- ECS-Cluster
- Einrichtung einer Hybridumgebung
- Amazon WorkSpaces
- Simple AD

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Führen Sie einen ASP.NET Core-Web-API-Docker-Container auf einer Amazon EC2 Linux-Instance aus

Erstellt von Vijai Anand Ramalingam (AWS) und Sreelaxmi Pai (AWS)

Übersicht

Dieses Muster ist für Benutzer gedacht, die damit beginnen, ihre Anwendungen in der Amazon Web Services (AWS) Cloud zu containerisieren. Wenn Sie beginnen, Apps in der Cloud zu containerisieren, sind in der Regel keine Container-Orchestrierungsplattformen eingerichtet. Mit diesem Muster können Sie schnell eine Infrastruktur auf AWS einrichten, um Ihre containerisierten Anwendungen zu testen, ohne dass eine aufwändige Container-Orchestrierungsinfrastruktur erforderlich ist.

Der erste Schritt auf dem Weg zur Modernisierung besteht darin, die Anwendung zu transformieren. Wenn es sich um eine ältere .NET Framework-Anwendung handelt, müssen Sie zuerst die Laufzeit auf ASP.NET Core ändern. Führen Sie dann die folgenden Schritte aus:

- Erstellen Sie das Docker-Container-Image
- Führen Sie den Docker-Container mit dem erstellten Image aus
- Überprüfen Sie die Anwendung, bevor Sie sie auf einer beliebigen Container-Orchestrierungsplattform wie Amazon Elastic Container Service (Amazon ECS) oder Amazon Elastic Kubernetes Service (Amazon EKS) bereitstellen.

Dieses Muster behandelt die Aspekte der Erstellung, Ausführung und Validierung der modernen Anwendungsentwicklung auf einer Amazon Elastic Compute Cloud (Amazon EC2) Linux-Instance.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS) -Konto
- Eine AWS Identity and Access Management (IAM) -Rolle mit ausreichendem Zugriff, um AWS-Ressourcen für dieses Muster zu erstellen
- Visual Studio Community 2022 oder höher wurde heruntergeladen und installiert
- Ein auf ASP.NET Core modernisiertes .NET Framework-Projekt
- Ein Repository GitHub

Produktversionen

- Visual Studio Community 2022 oder höher

Architektur

Zielarchitektur

Dieses Muster verwendet eine CloudFormation AWS-Vorlage, um die im folgenden Diagramm gezeigte Architektur mit hoher Verfügbarkeit zu erstellen. Eine Amazon EC2 Linux-Instance wird in einem privaten Subnetz gestartet. AWS Systems Manager Session Manager wird verwendet, um auf die private Amazon EC2 Linux-Instance zuzugreifen und die API zu testen, die im Docker-Container läuft.

1. Zugriff auf die Linux-Instance über Session Manager

Tools

AWS-Services

- AWS-Befehlszeilenschnittstelle — AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool für die Interaktion mit AWS-Services über Befehle in Ihrer Befehlszeilen-Shell. Mit minimaler Konfiguration können Sie AWS-CLI-Befehle ausführen, die Funktionen implementieren, die denen der browserbasierten AWS-Managementkonsole entsprechen.
- AWS-Managementkonsole — Die AWS-Managementkonsole ist eine Webanwendung, die eine breite Sammlung von Servicekonsolen für die Verwaltung von AWS-Ressourcen umfasst und sich auf diese bezieht. Wenn Sie sich zum ersten Mal anmelden, sehen Sie die Startseite der Konsole. Die Startseite bietet Zugriff auf jede Servicekonsole und bietet einen zentralen Ort, an dem Sie auf die Informationen zugreifen können, die Sie zur Ausführung Ihrer AWS-bezogenen Aufgaben benötigen.
- AWS Systems Manager Session Manager — Session Manager ist eine vollständig verwaltete Funktion von AWS Systems Manager. Mit Session Manager können Sie Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Instances verwalten. Session Manager bietet eine sichere und überprüfbare Knotenverwaltung, ohne dass eingehende Ports geöffnet, Bastion-Hosts verwaltet oder SSH-Schlüssel verwaltet werden müssen.

Andere Tools

- Visual Studio 2022 — Visual Studio 2022 ist eine integrierte Entwicklungsumgebung (IDE).
- Docker — Docker ist eine Reihe von Platform-as-a-Service (PaaS) -Produkten, die Virtualisierung auf Betriebssystemebene nutzen, um Software in Containern bereitzustellen.

Code

```
FROM mcr.microsoft.com/dotnet/aspnet:5.0 AS base
 WORKDIR /app
EXPOSE 80
EXPOSE 443

FROM mcr.microsoft.com/dotnet/sdk:5.0 AS build
WORKDIR /src
COPY ["DemoNetCoreWebAPI/DemoNetCoreWebAPI.csproj", "DemoNetCoreWebAPI/"]
RUN dotnet restore "DemoNetCoreWebAPI/DemoNetCoreWebAPI.csproj"
COPY . .
WORKDIR "/src/DemoNetCoreWebAPI"
RUN dotnet build "DemoNetCoreWebAPI.csproj" -c Release -o /app/build

FROM build AS publish
RUN dotnet publish "DemoNetCoreWebAPI.csproj" -c Release -o /app/publish

FROM base AS final
WORKDIR /app
COPY --from=publish /app/publish .
ENTRYPOINT ["dotnet", "DemoNetCoreWebAPI.dll"]
```

Epen

Entwickeln Sie die ASP.NET Core-Web-API

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie mit Visual Studio ein Beispiel für eine ASP.NET Core-Web-API.	Gehen Sie wie folgt vor, um ein Beispiel für eine ASP.NET Core-Web-API zu erstellen:	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	1. Öffnen Sie Visual Studio 2022.
	2. Wählen Sie Create a new project (Neues Projekt erstellen).
	3. Wählen Sie die ASP.NET Core Web API-Proje ktvorlage aus und klicken Sie auf Weiter.
	4. Geben Sie als Projektna men DemoNetCoreWebAPI ein und wählen Sie Weiter aus.
	5. Wählen Sie Erstellen aus.
	6. Um das Projekt lokal auszuführen, drücken Sie F5.
	7. Stellen Sie mithilfe von Swagger sicher, dass der WeatherForecastStandard-API-Endpunkt die Ergebniss e zurückgibt.
	8. Öffnen Sie die Befehlsze ile, navigieren Sie zum Projektordner .csproj und führen Sie die folgenden Befehle aus, um die neue Web-API in Ihr Repository zu übertragen. GitHub
	`git add --all`
	`git commit -m “Initial Version”`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`git push`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Docker-Datei.	Gehen Sie wie folgt vor, um ein Dockerfile zu erstellen: • Erstellen Sie das Dockerfile manuell mithilfe des Dockerfile-Beispiels im Abschnitt Code. Wählen Sie je nach den Anforderungen das entsprechende .NET-Basisimage aus. Informationen zu Images, die sich auf .NET und ASP.NET Core beziehen, finden Sie unter Docker Hub. • Erstellen Sie das Dockerfile mit Visual Studio und Docker Desktop. Klicken Sie im Solution Explorer mit der rechten Maustaste auf das Projekt und wählen Sie Hinzufügen -> Docker Support. Wählen Sie für Target OS Linux aus. Stellen Sie sicher, dass sich das neue Dockerfile im selben Pfad wie die Lösungsdatei (.sln) befindet. Führen Sie den folgenden Befehl aus, um die Änderungen in Ihr GitHub Repository zu übertragen.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`git add --all`
	`git commit -m “Dockerfile added”`
	`git push`	

Richten Sie die Amazon EC2 Linux-Instance ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Infrastruktur ein.	Starten Sie die CloudFormation AWS-Vorlage, um die Infrastruktur zu erstellen, die Folgendes umfasst: • Eine virtuelle private Cloud (VPC), die den AWS VPC Quick Start verwendet, mit zwei öffentlichen und zwei privaten Subnetzen, die sich über zwei Availability Zones erstrecken. • Die für die Aktivierung von AWS Systems Manager erforderliche IAM-Rolle. • In einem der privaten Subnetze eine Amazon Linux 2-Demo-Instance mit dem neuesten SSM-Agenten. Obwohl diese Instance keine direkte Verbindung über das Internet hat, kann sie mit dem AWS Systems Manager Session Manager sicher aufgerufen werden,	App-Entwickler, AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ohne dass ein Bastion-Host erforderlich ist. **Note** Amazon Linux 2 nähert sich dem Ende des Supports. Weitere Informationen finden Sie unter Amazon Linux FAQs 2. Weitere Informationen zum Zugriff auf eine private EC2 Amazon-Instance mit Session Manager, ohne dass ein Bastion-Host erforderlich ist, finden Sie im Blogbeitrag Toward a bastion-less world.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie sich bei der Amazon EC2 Linux-Instance an.	Gehen Sie wie folgt vor, um eine Verbindung zur Amazon EC2 Linux-Instance im privaten Subnetz herzustellen: 1. Öffnen Sie die EC2 Amazon-Konsole. 2. Wählen Sie im Navigationsbereich Instances aus. 3. Wählen Sie die Amazon Linux 2-Demo-Instance und dann Connect aus. **Note** Amazon Linux 2 nähert sich dem Ende des Supports. Weitere Informationen finden Sie unter Amazon Linux FAQs 2. 4. Klicken Sie auf Session Manager. 5. Wählen Sie Connect, um ein neues Terminalfenster zu öffnen. 6. Führen Sie den folgenden Befehl aus. `sudo su`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren und starten Sie Docker.	Gehen Sie wie folgt vor, um Docker in der Amazon EC2 Linux-Instance zu installieren und zu starten:
	1. Führen Sie den folgenden Befehl aus, um Docker zu installieren.
	`yum install -y docker`
	2. Führen Sie den folgenden Befehl aus, um den Docker-Dienst zu starten.
	`service docker start`
	3. Führen Sie den folgenden Befehl aus, um die Docker-Installation zu überprüfen.
	`docker info`
		App-Entwickler, AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installiere Git und klone das Repository.	Gehen Sie wie folgt vor, um Git auf der Amazon EC2 Linux-Instance zu installieren und das Repository von GitHub zu klonen.
	1. Führen Sie den folgenden Befehl aus, um Git zu installieren.
	`yum install git -y`
	2. Führen Sie den folgenden Befehl aus, um das Repository zu klonen.
	`git clone https://github.com/<username>/<repo-name>.git`
	3. Führen Sie den folgenden Befehl aus, um zur Dockerfile zu navigieren.
	`cd <repo-name>/DemoNetCoreWebAPI/`
		App-Entwickler, AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den Docker-Container und führen Sie ihn aus.	Gehen Sie wie folgt vor, um das Docker-Image zu erstellen und den Container in der Amazon EC2 Linux-Instance auszuführen:
	1. Führen Sie den folgenden Befehl aus, um das Docker-Image zu erstellen.
	`docker build -t aspnetcorewebapiimage -f Dockerfile .`
	2. Führen Sie den folgenden Befehl aus, um alle Docker-Images anzuzeigen.
	`docker images`
	3. Führen Sie den folgenden Befehl aus, um den Container zu erstellen und auszuführen.
	`docker run -d -p 80:80 --name aspnetcorewebapicontainer aspnetcorewebapiimage`
		App-Entwickler, AWS-Administrator, AWS DevOps

Testen Sie die Web-API

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Web-API mit dem Befehl curl.	Führen Sie den folgenden Befehl aus, um die Web-API zu testen. `curl -X GET "http://localhost/WeatherForecast" -H  "accept: text/plain"` Überprüfen Sie die API-Antwort. **Note** Sie können die curl-Befehle für jeden Endpunkt von Swagger abrufen, wenn Sie ihn lokal ausführen.	App-Developer

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie alle Ressourcen.	Löschen Sie den Stapel, um alle Ressourcen zu entfernen. Dadurch wird sichergestellt, dass Ihnen keine Dienste in Rechnung gestellt werden, die Sie nicht nutzen.	AWS-Administrator, AWS DevOps

Zugehörige Ressourcen

- Stellen Sie mithilfe von PuTTY von Windows aus eine Connect zu Ihrer Linux-Instance her
- Erstellen Sie eine Web-API mit ASP.NET Core
- Auf dem Weg zu einer Welt ohne Bastionen

Mithilfe von AWS Fargate können Sie nachrichtengesteuerte Workloads in großem Umfang ausführen

Erstellt von Stan Zubarev (AWS)

Übersicht

Dieses Muster zeigt, wie nachrichtengesteuerte Workloads mithilfe von Containern und AWS Fargate in großem Umfang in der AWS-Cloud ausgeführt werden können.

Die Verwendung von Containern zur Verarbeitung von Daten kann hilfreich sein, wenn die Datenmenge, die eine Anwendung verarbeitet, die Beschränkungen funktionsbasierter serverloser Rechendienste überschreitet. Wenn eine Anwendung beispielsweise mehr Rechenkapazität oder Verarbeitungszeit benötigt als das, was AWS Lambda bietet, kann die Verwendung von Fargate die Leistung verbessern.

Das folgende Beispiel-Setup verwendet das AWS Cloud Development Kit (AWS CDK), TypeScript um die folgenden Ressourcen in der AWS-Cloud zu konfigurieren und bereitzustellen:

- Ein Fargate-Service
- Eine Amazon Simple Queue Service (Amazon SQS) -Warteschlange
- Eine Amazon DynamoDB-Tabelle.
- Ein CloudWatch Amazon-Dashboard

Der Fargate-Service empfängt und verarbeitet Nachrichten aus der Amazon SQS SQS-Warteschlange und speichert sie dann in der Amazon DynamoDB-Tabelle. Mithilfe des Dashboards können Sie überwachen, wie viele Amazon SQS SQS-Nachrichten verarbeitet und wie viele DynamoDB-Elemente von Fargate erstellt werden. CloudWatch

> **Note**
>
> Sie können den Beispielcode dieses Musters auch verwenden, um komplexere Datenverarbeitungs-Workloads in ereignisgesteuerten serverlosen Architekturen zu erstellen. Weitere Informationen finden Sie unter Ausführen von ereignisgesteuerten und geplanten Workloads in großem Umfang mit AWS Fargate.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Die neueste Version der AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert auf Ihrem lokalen Computer
- Git, auf Ihrem lokalen Computer installiert und konfiguriert
- Das AWS CDK, installiert und konfiguriert auf Ihrem lokalen Computer
- Go, auf Ihrem lokalen Computer installiert und konfiguriert
- Docker, auf Ihrem lokalen Computer installiert und konfiguriert

Architektur

Zieltechnologie-Stack

- Amazon SQS
- AWS Fargate
- Amazon-DynamoDB

Zielarchitektur

Das folgende Diagramm zeigt einen Beispiel-Workflow für die skalierbare Ausführung von nachrichtengesteuerten Workloads in der AWS-Cloud mithilfe von Fargate:

Das Diagramm zeigt den folgenden Workflow:

1. Der Fargate-Service verwendet Amazon SQS Long Polling, um Nachrichten aus einer Amazon SQS SQS-Warteschlange zu empfangen.
2. Der Fargate-Service verarbeitet dann die Amazon SQS SQS-Nachrichten und speichert sie in einer DynamoDB-Tabelle.

Automatisierung und Skalierung

Um die Skalierung Ihrer Fargate-Aufgabenanzahl zu automatisieren, können Sie Amazon Elastic Container Service (Amazon ECS) Service Auto Scaling konfigurieren. Es hat sich bewährt, die

Skalierungsrichtlinie auf der Grundlage der Anzahl der sichtbaren Nachrichten in der Amazon SQS SQS-Warteschlange Ihrer Anwendung zu konfigurieren.

Weitere Informationen finden Sie unter Skalierung auf Basis von Amazon SQS im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Tools

AWS-Services

- Mit AWS Fargate können Sie Container ausführen, ohne Server oder Amazon Elastic Compute Cloud (Amazon EC2) -Instances verwalten zu müssen. Es wird in Verbindung mit Amazon Elastic Container Service (Amazon ECS) verwendet.
- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- Amazon CloudWatch hilft Ihnen dabei, die Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie auf AWS ausführen, in Echtzeit zu überwachen.

Code

Der Code für dieses Muster ist im GitHub sqs-fargate-ddb-cdk-go-Repository verfügbar.

Epen

Erstellen und Bereitstellen der Ressourcen mithilfe des AWS CDK

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	Klonen Sie das GitHub sqs-fargate-ddb-cdk-go-Repository auf Ihren lokalen Computer, indem Sie den folgenden Befehl ausführen: `git clone https://github.com/aws-samp`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`les/sqs-fargate-dd b-cdk-go.git`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die AWS-CLI für das richtige AWS-Konto konfiguriert ist und dass das AWS-CDK über die erforderlichen Berechtigungen verfügt.	Um zu überprüfen, ob Ihre AWS-CLI-Konfigurationseinstellungen korrekt sind, können Sie den folgenden Amazon Simple Storage Service (Amazon S3) ls-Befehl ausführen: `aws s3 ls` Dieses Verfahren erfordert auch, dass das AWS-CDK über Berechtigungen zur Bereitstellung der Infrastruktur innerhalb Ihres AWS-Kontos verfügt. Um die erforderlichen Berechtigungen zu gewähren, müssen Sie ein benanntes AWS-Profil in der AWS-CLI erstellen und es als AWS_PROFILEUmgebungsvariable exportieren. **Note** Wenn Sie das AWS-CDK in Ihrem AWS-Konto noch nicht verwendet haben, müssen Sie zunächst die erforderlichen AWS-CDK-Ressourcen bereitstellen. Weitere Informationen finden Sie unter	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bootstrapping im AWS CDK v2 Developer Guide.	

Stellen Sie den AWS-CDK-Stack auf Ihrem AWS-Konto bereit.	1. Erstellen Sie ein Container-Image, indem Sie den folgenden AWS-CLI-Befehl ausführen:
	`docker build -t go-fargate .`
	2. Öffnen Sie das AWS-CDK-Verzeichnis, indem Sie den folgenden Befehl ausführen:
	`cd cdk`
	3. Installieren Sie die erforderlichen npm-Module, indem Sie den folgenden Befehl ausführen:
	`npm i`
	4. Stellen Sie das AWS-CDK-Muster für Ihr AWS-Konto bereit, indem Sie den folgenden Befehl ausführen:
	`cdk deploy --profile ${AWS_PROFILE}`
		App-Developer

Testen der Einrichtung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie eine Testnachricht an die Amazon SQS SQS-Warteschlange.	Anweisungen finden Sie unter Senden von Nachrichten an eine Warteschlange (Konsole) im Amazon SQS Developer Guide. Beispiel für eine Amazon SQS SQS-Nachricht testen `{ "message": "hello, Fargate" }`	App-Developer
Stellen Sie sicher, dass die Testnachricht in den CloudWatch Protokollen des Fargate-Dienstes erscheint.	Folgen Sie den Anweisungen unter CloudWatch Logs anzeigen im Amazon ECS Developer Guide. Stellen Sie sicher, dass Sie die Protokolle für die go-fargate-service Protokollgruppe im go-service-clusterECS-Cluster überprüfen.	App-Developer
Stellen Sie sicher, dass die Testnachricht in der DynamoDB-Tabelle angezeigt wird.	1. Öffnen Sie die DynamoDB-Konsole. 2. Wählen Sie im linken Navigationsbereich Tables (Tabellen) aus. Wählen Sie dann die folgende Tabelle aus der Liste aus:. sqs-fargate-ddb-table	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie Explore Table Items (Tabellenelemente erkudnen) aus. 4. Stellen Sie sicher, dass die Testnachricht in der Liste der zurückgegebenen Artikel angezeigt wird.	
Stellen Sie sicher, dass der Fargate-Dienst Nachrichten an CloudWatch Logs sendet.	1. Öffnen Sie die CloudWatch -Konsole. 2. Wählen Sie im linken Navigationsbereich Dashboards aus. 3. Wählen Sie in der Liste Benutzerdefinierte Dashboards das Dashboard mit dem Namen aus. go-service-dashboard 4. Stellen Sie sicher, dass die Testnachricht in den Protokollen erscheint. **Note** Das AWS CDK erstellt das CloudWatch Dashboard in Ihrem AWS-Konto automatis ch.	App-Developer

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Löschen Sie den AWS-CDK-Stack.	1. Öffnen Sie Ihr AWS-CDK-Verzeichnis in der AWS-CLI, indem Sie den folgenden Befehl ausführen:
	`cd cdk`
	2. Löschen Sie den AWS CDK-Stack, indem Sie den folgenden Befehl ausführen:
	`cdk destroy --profile ${AWS_PROFILE}`
		App-Developer

Stellen Sie sicher, dass der AWS-CDK-Stack gelöscht wurde.	Führen Sie den folgenden Befehl aus, um sicherzustellen, dass der Stack gelöscht wurde: `aws cloudformation list-stacks --query \ "StackSummaries[?contains(StackName,'SqsFargate')].StackStatus" \ --profile ${AWS_PROFILE}` Der in der Befehlsausgabe zurückgegebene `StackStatus` Wert gibt an`DELETE_COMPLETE`, ob der Stapel gelöscht wurde.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter Beispiele für CloudFormation Stack-Operationsbefehle für AWS CLI und PowerShell im CloudFormation AWS-Benutzerhandbuch.	

Zugehörige Ressourcen

- Konfiguration von AWS CLI (AWS CLI-Benutzerhandbuch für Version 2)
- API-Referenz (AWS CDK API-Referenz)
- AWS-SDK SDK for Go v2 (Go-Dokumentation)

Führen Sie statusbehaftete Workloads mit persistentem Datenspeicher aus, indem Sie Amazon EFS auf Amazon EKS mit AWS Fargate verwenden

Erstellt von Ricardo Morais (AWS), Rodrigo Bersa (AWS) und Lucio Pereira (AWS)

Übersicht

Dieses Muster bietet Anleitungen zur Aktivierung von Amazon Elastic File System (Amazon EFS) als Speichergerät für Container, die auf Amazon Elastic Kubernetes Service (Amazon EKS) ausgeführt werden, indem Sie AWS Fargate zur Bereitstellung Ihrer Rechenressourcen verwenden.

Das in diesem Muster beschriebene Setup folgt bewährten Sicherheitsmethoden und bietet standardmäßig Sicherheit im Ruhezustand und Sicherheit bei der Übertragung. Um Ihr Amazon EFS-Dateisystem zu verschlüsseln, verwendet es einen AWS Key Management Service (AWS KMS) -Schlüssel, aber Sie können auch einen Schlüsselalias angeben, der den Prozess der Erstellung eines KMS-Schlüssels auslöst.

Sie können den Schritten in diesem Muster folgen, um einen Namespace und ein Fargate-Profil für eine proof-of-concept (PoC-) Anwendung zu erstellen, den Amazon EFS Container Storage Interface (CSI) -Treiber zu installieren, der für die Integration des Kubernetes-Clusters in Amazon EFS verwendet wird, die Speicherklasse zu konfigurieren und die PoC-Anwendung bereitzustellen. Diese Schritte führen zu einem Amazon EFS-Dateisystem, das von mehreren Kubernetes-Workloads gemeinsam genutzt wird und über Fargate ausgeführt wird. Das Muster wird von Skripten begleitet, die diese Schritte automatisieren.

Sie können dieses Muster verwenden, wenn Sie Datenpersistenz in Ihren containerisierten Anwendungen wünschen und Datenverluste bei Skalierungsvorgängen vermeiden möchten. Zum Beispiel:

- DevOps Tools — Ein gängiges Szenario ist die Entwicklung eines Tools für kontinuierliche Integration und kontinuierliche Bereitstellung (Continuous Delivery). CI/CD) strategy. In this case, you can use Amazon EFS as a shared file system to store configurations among different instances of the CI/CD tool or to store a cache (for example, an Apache Maven repository) for pipeline stages among different instances of the CI/CD
- Webserver — Ein gängiges Szenario ist die Verwendung von Apache als HTTP-Webserver. Sie können Amazon EFS als gemeinsam genutztes Dateisystem verwenden, um statische Dateien zu speichern, die von verschiedenen Instanzen des Webservers gemeinsam genutzt werden. In diesem Beispielszenario werden Änderungen direkt auf das Dateisystem angewendet, anstatt statische Dateien in ein Docker-Image zu integrieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein vorhandener Amazon EKS-Cluster mit Kubernetes Version 1.17 oder höher (getestet bis Version 1.27)
- Ein vorhandenes Amazon EFS-Dateisystem zum Binden von Kubernetes StorageClass und zum dynamischen Bereitstellen von Dateisystemen
- Berechtigungen für die Clusterverwaltung
- Der Kontext ist so konfiguriert, dass er auf den gewünschten Amazon EKS-Cluster verweist

Einschränkungen

- Bei der Verwendung von Amazon EKS mit Fargate sind einige Einschränkungen zu beachten. Beispielsweise wird die Verwendung einiger Kubernetes-Konstrukte, wie z. B. DaemonSets privilegierte Container, nicht unterstützt. Weitere Informationen zu den Einschränkungen von Fargate finden Sie in den Überlegungen zu AWS Fargate in der Amazon EKS-Dokumentation.
- Der mit diesem Muster bereitgestellte Code unterstützt Workstations, auf denen Linux oder macOS ausgeführt wird.

Produktversionen

- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 2 oder höher
- Amazon EFS CSI-Treiber Version 1.0 oder höher (getestet bis Version 2.4.8)
- eksctl Version 0.24.0 oder höher (getestet bis Version 0.158.0)
- jq Version 1.6 oder höher
- kubectl Version 1.17 oder höher (getestet bis Version 1.27)
- Kubernetes Version 1.17 oder höher (getestet bis Version 1.27)

Architektur

Die Zielarchitektur besteht aus der folgenden Infrastruktur:

- Eine virtuelle private Cloud (VPC)
- Zwei Verfügbarkeitszonen
- Ein öffentliches Subnetz mit einem NAT-Gateway, das Internetzugang bietet
- Ein privates Subnetz mit einem Amazon EKS-Cluster und Amazon EFS-Mount-Zielen (auch bekannt als Mount-Points)
- Amazon EFS auf VPC-Ebene

Im Folgenden finden Sie die Umgebungsinfrastruktur für den Amazon EKS-Cluster:

- AWS Fargate-Profile, die die Kubernetes-Konstrukte auf Namespace-Ebene berücksichtigen
- Ein Kubernetes-Namespace mit:
  - Zwei Anwendungs-Pods, die über Availability Zones verteilt sind
  - Ein persistenter Volume Claim (PVC), der an ein persistentes Volume (PV) auf Clusterebene gebunden ist
- Ein clusterweiter PV, der an das PVC im Namespace gebunden ist und auf die Amazon EFS-Mount-Ziele im privaten Subnetz außerhalb des Clusters verweist

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über die Befehlszeile mit AWS-Services interagieren können.
- Amazon Elastic File System (Amazon EFS) unterstützt Sie bei der Erstellung und Konfiguration gemeinsam genutzter Dateisysteme in der AWS-Cloud. In diesem Muster bietet es ein einfaches, skalierbares, vollständig verwaltetes und gemeinsam genutztes Dateisystem für die Verwendung mit Amazon EKS.
- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen, Kubernetes auf AWS auszuführen, ohne Ihre eigenen Cluster installieren oder betreiben zu müssen.
- AWS Fargate ist eine serverlose Rechen-Engine für Amazon EKS. Sie erstellt und verwaltet Rechenressourcen für Ihre Kubernetes-Anwendungen.
- AWS Key Management Service (AWS KMS) unterstützt Sie bei der Erstellung und Kontrolle kryptografischer Schlüssel, um Ihre Daten zu schützen.

Andere Tools

- Docker ist eine Reihe von Platform-as-a-Service (PaaS) -Produkten, die Virtualisierung auf Betriebssystemebene nutzen, um Software in Containern bereitzustellen.
- eksctl ist ein Befehlszeilenprogramm zum Erstellen und Verwalten von Kubernetes-Clustern auf Amazon EKS.
- kubectl ist eine Befehlszeilenschnittstelle, mit der Sie Befehle für Kubernetes-Cluster ausführen können.
- jq ist ein Befehlszeilentool zum Parsen von JSON.

Code

Der Code für dieses Muster wird in der GitHub Persistenzkonfiguration mit Amazon EFS auf Amazon EKS mithilfe des AWS Fargate-Repos bereitgestellt. Die Skripts sind nach Epic in den Ordnern `epic01` bis angeordnet`epic06`, entsprechend der Reihenfolge im Abschnitt Epics in diesem Muster.

Bewährte Methoden

Die Zielarchitektur umfasst die folgenden Services und Komponenten und entspricht den Best Practices von AWS Well-Architected Framework:

- Amazon EFS, das ein einfaches, skalierbares, vollständig verwaltetes elastisches NFS-Dateisystem bietet. Dies wird als gemeinsam genutztes Dateisystem für alle Replikationen der PoC-Anwendung verwendet, die in Pods ausgeführt werden, die in den privaten Subnetzen des ausgewählten Amazon EKS-Clusters verteilt sind.
- Ein Amazon EFS-Mount-Ziel für jedes private Subnetz. Dies bietet Redundanz pro Availability Zone innerhalb der Virtual Private Cloud (VPC) des Clusters.
- Amazon EKS, das die Kubernetes-Workloads ausführt. Sie müssen einen Amazon EKS-Cluster bereitstellen, bevor Sie dieses Muster verwenden können, wie im Abschnitt Voraussetzungen beschrieben.
- AWS KMS bietet Verschlüsselung im Ruhezustand für den Inhalt, der im Amazon EFS-Dateisystem gespeichert ist.
- Fargate, das die Rechenressourcen für die Container verwaltet, sodass Sie sich auf die Geschäftsanforderungen konzentrieren können, anstatt die Infrastruktur zu belasten. Das Fargate-Profil wird für alle privaten Subnetze erstellt. Es bietet Redundanz pro Availability Zone innerhalb der Virtual Private Cloud (VPC) des Clusters.

- Kubernetes-Pods, mit denen überprüft wird, ob Inhalte von verschiedenen Instanzen einer Anwendung gemeinsam genutzt, genutzt und geschrieben werden können.

Epen

Bereitstellen eines Amazon EKS-Clusters (optional)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon-EKS-Cluster.	**Note** Wenn Sie bereits einen Cluster bereitgestellt haben, fahren Sie mit dem nächsten Epic fort. Erstellen Sie einen Amazon EKS-Cluster in Ihrem bestehend en AWS-Konto. Verwenden Sie im GitHub Verzeichn is eines der Muster, um einen Amazon EKS-Cluster mithilfe von Terraform oder eksctl bereitzustellen. Weitere Informati onen finden Sie unter Erstellen eines Amazon EKS-Clust ers in der Amazon EKS-Dokumentation. Das Terraform-Muster enthält auch Beispiele , die zeigen, wie Sie: Fargate-Profile mit	AWS-Administrator, Terraform - oder eksctl-Administrator, Kubernetes-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ihrem Amazon EKS-Cluster verknüpfen, ein Amazon EFS-Dateisystem erstellen und den Amazon EFS-CSI-Treiber in Ihrem Amazon EKS-Cluster bereitstellen können.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Exportieren Sie Umgebungsvariablen.	Führen Sie das Skript env.sh aus. Dadurch werden die Informationen bereitgestellt, die für die nächsten Schritte erforderlich sind.
	`source ./scripts/env.sh`
	`Inform the AWS Account ID: <13-digit-account-id>`
	`Inform your AWS Region: <aws-Region-code>`
	`Inform your Amazon EKS Cluster Name: <amazon-eks-cluster-name>`
	`Inform the Amazon EFS Creation Token: <self-genereated-uuid>`
	Falls noch nicht angegeben, können Sie alle oben angeforderten Informationen mit den folgenden CLI-Befehlen abrufen.
	`# ACCOUNT ID`
	`aws sts get-caller-identity --query "Account" --output text`
	`# REGION CODE`
	`aws configure get region`
	`# CLUSTER EKS NAME`
		AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`aws eks list-clusters --query "clusters" --output text`
	
	`# GENERATE EFS TOKEN uuidgen`	

Erstellen Sie einen Kubernetes-Namespace und ein verknüpftes Fargate-Profil

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Kubernetes-Namespace und ein Fargate-Profil für Anwendungsworkloads.	Erstellen Sie einen Namespace für den Empfang der Anwendungs-Workloads, die mit Amazon EFS interagieren. Führen Sie das `create-k8s-ns-and-linked-fargate-profile.sh` -Skript aus. Sie können wählen, ob Sie einen benutzerdefinierten Namespace-Namen oder den standardmäßig bereitgestellten Namespace verwenden möchten. `poc-efs-eks-fargate` Mit einem benutzerdefinierten Anwendungs-Namespace-Namen: `export $APP_NAMESPACE=<CUSTOM_NAME> ./scripts/epic01/create-k8s-ns-and`	Kubernetes-Benutzer mit erteilten Berechtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`-linked-fargate-pr ofile.sh \ -c "$CLUSTER_NAME" -n "$APP_NAMESPACE"`
	
	Ohne einen benutzerdefinierte n Anwendungs-Namespace-Namen:
	
	`./scripts/epic01/c reate-k8s-ns-and-l inked-fargate-prof ile.sh \ -c "$CLUSTER_NAME"`
	
	wo `$CLUSTER_NAME` ist der Name Ihres Amazon EKS-Clusters. Der `-n <NAMESPAC E>` Parameter ist optional. Wenn Sie nicht darüber informiert werden, wird ein standardmäßig generierter Namespace-Name bereitges tellt.	

Erstellen eines Amazon EFS-Dateisystems

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie ein eindeutig es Token.	Amazon EFS benötigt ein Erstellungstoken, um einen idempotenten Vorgang sicherzustellen (der Aufruf des Vorgangs mit demselben Erstellungstoken hat keine	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Auswirkung). Um diese Anforderung zu erfüllen, müssen Sie mithilfe einer verfügbaren Technik ein eindeutiges Token generiere n. Sie können beispielsweise einen Universally Unique Identifier (UUID) generieren, um ihn als Erstellungstoken zu verwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon EFS-Dateisystem.	Erstellen Sie das Dateisyst em für den Empfang der Datendateien, die von den Anwendungsworkloads gelesen und geschrieben werden. Sie können ein verschlüsseltes oder ein unverschlüsseltes Dateisyst em erstellen. (Es hat sich bewährt, dass der Code für dieses Muster ein verschlüs seltes System erstellt, sodass die Verschlüsselung im Ruhezustand standardm äßig aktiviert ist.) Sie können einen eindeutigen, symmetris chen AWS-KMS-Schlüssel verwenden, um Ihr Dateisyst em zu verschlüsseln. Wenn kein benutzerdefinierter Schlüssel angegeben ist, wird ein von AWS verwalteter Schlüssel verwendet. Verwenden Sie das Skript create-efs.sh, um ein verschlüsseltes oder unverschl üsseltes Amazon EFS-Datei system zu erstellen, nachdem Sie ein eindeutiges Token für Amazon EFS generiert haben. Mit Verschlüsselung im Ruhezustand, ohne KMS-Schlüssel:	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`./scripts/epic02/create-efs.sh \ -c "$CLUSTER_NAME" \ -t "$EFS_CREATION_TOKEN"`
	
	wo `$CLUSTER_NAME` ist der Name Ihres Amazon EKS-Clusters und `$EFS_CREATION_TOKEN` ist ein eindeutiges Erstellungstoken für das Dateisystem.
	
	Mit Verschlüsselung im Ruhezustand, mit einem KMS-Schlüssel:
	
	`./scripts/epic02/create-efs.sh \ -c "$CLUSTER_NAME" \ -t "$EFS_CREATION_TOKEN" \ -k "$KMS_KEY_ALIAS"`
	
	Dabei `$CLUSTER_NAME` handelt es sich um den Namen Ihres Amazon EKS-Clusters, um `$EFS_CREATION_TOKEN` ein eindeutiges Erstellungstoken für das Dateisystem und `$KMS_KEY_ALIAS` um den Alias für den KMS-Schlüssel.
	
	Ohne Verschlüsselung:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`./scripts/epic02/create-efs.sh -d \ -c "$CLUSTER_NAME" \ -t "$EFS_CREATION_TOKEN"` wobei `$CLUSTER_NAME` der Name Ihres Amazon EKS-Clusters `$EFS_CREATION_TOKEN` steht, ein eindeutiges Erstellungstoken für das Dateisystem ist und die Verschlüsselung im Ruhezustand `-d` deaktiviert.	
Erstellen einer Sicherheitsgruppe.	Erstellen Sie eine Sicherheitsgruppe, um dem Amazon EKS-Cluster den Zugriff auf das Amazon EFS-Dateisystem zu ermöglichen.	AWS-Systemadministrator
Aktualisieren Sie die Regel für eingehende Nachrichten für die Sicherheitsgruppe.	Aktualisieren Sie die Regeln für eingehenden Datenverkehr der Sicherheitsgruppe, um eingehenden Datenverkehr für die folgenden Einstellungen zuzulassen: • TCP-Protokoll — Port 2049 • Quelle — CIDR-Blockbereiche für die privaten Subnetze in der VPC, die den Kubernetes-Cluster enthält	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie für jedes private Subnetz ein Mount-Ziel hinzu.	Erstellen Sie für jedes private Subnetz des Kubernetes-Clusters ein Mount-Ziel für das Dateisystem und die Sicherheitsgruppe.	AWS-Systemadministrator

Installieren Sie Amazon EFS-Komponenten im Kubernetes-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Amazon EFS CSI-Treiber bereit.	Stellen Sie den Amazon EFS CSI-Treiber im Cluster bereit. Der Treiber stellt Speicher entsprechend den von Anwendungen generierten persistenten Volume-Ansprüchen bereit. Führen Sie das `create-k8s-efs-csi-sc.sh` Skript aus, um den Amazon EFS CSI-Treiber und die Speicherklasse im Cluster bereitzustellen. `./scripts/epic03/create-k8s-efs-csi-sc.sh` Dieses Skript verwendet das `kubectl` Hilfsprogramm. Stellen Sie also sicher, dass der Kontext konfiguriert wurde, und verweisen Sie auf den gewünschten Amazon EKS-Cluster.	Kubernetes-Benutzer mit erteilten Berechtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Speicherklasse bereit.	Stellen Sie die Speicherklasse im Cluster für den Amazon EFS-Provisioner bereit (efs.csi.aws.com).	Kubernetes-Benutzer mit erteilten Berechtigungen

Installieren Sie die PoC-Anwendung im Kubernetes-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie das persistente Volume bereit.	Stellen Sie das persistente Volume bereit und verknüpfen Sie es mit der erstellten Speicherklasse und der ID des Amazon EFS-Dateisystems. Die Anwendung verwendet das persistente Volume zum Lesen und Schreiben von Inhalten. Sie können eine beliebige Größe für das persistente Volume im Speicherfeld angeben. Kubernetes erfordert dieses Feld, aber da Amazon EFS ein elastisches Dateisystem ist, erzwingt es keine Dateisystemkapazität. Sie können das persistente Volume mit oder ohne Verschlüsselung bereitstellen. (Der Amazon EFS CSI-Treiber aktiviert standardmäßig die Verschlüsselung als bewährte Methode.) Führen Sie das `deploy-poc-app.sh` Skript aus,	Kubernetes-Benutzer mit erteilten Berechtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	um das persistente Volume, den Anspruch auf persisten te Volumes und die beiden Workloads bereitzustellen.
	
	Bei Verschlüsselung während der Übertragung:
	
	`./scripts/epic04/deploy-poc-app.sh \ -t "$EFS_CREATION_TOKEN"`
	
	wo `$EFS_CREATION_TOKEN` ist das eindeutige Erstellungstoken für das Dateisystem.
	
	Ohne Verschlüsselung bei der Übertragung:
	
	`./scripts/epic04/deploy-poc-app.sh -d \ -t "$EFS_CREATION_TOKEN"`
	
	wo `$EFS_CREATION_TOKEN` ist das eindeutige Erstellungstoken für das Dateisystem und `–d` deaktiviert die Verschlüsselung bei der Übertragung.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den von der Anwendung angeforderten Anspruch auf persistentes Volumen bereit.	Stellen Sie den von der Anwendung angeforderten Anspruch auf beständig es Volumen bereit und verknüpfen Sie ihn mit der Speicherklasse. Verwenden Sie denselben Zugriffsmodus wie das persistente Volume, das Sie zuvor erstellt haben. Sie können im Speicherfeld eine beliebige Größe für den Anspruch auf persistentes Volume angeben. Kubernetes erfordert dieses Feld, aber da Amazon EFS ein elastisches Dateisystem ist, erzwingt es keine Dateisystemkapazität.	Kubernetes-Benutzer mit erteilten Berechtigungen
Stellen Sie Workload 1 bereit.	Stellen Sie den Pod bereit, der Workload 1 der Anwendung darstellt. Dieser Workload schreibt Inhalt in die Datei `/data/out1.txt` .	Kubernetes-Benutzer mit erteilten Berechtigungen
Stellen Sie Workload 2 bereit.	Stellen Sie den Pod bereit, der Workload 2 der Anwendung darstellt. Dieser Workload schreibt Inhalt in die Datei `/data/out2.txt` .	Kubernetes-Benutzer mit erteilten Berechtigungen

Überprüfen Sie die Persistenz, Haltbarkeit und gemeinsame Nutzung des Dateisystems

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Status von`PersistentVolume` .	Geben Sie den folgenden Befehl ein, um den Status von zu überprüfen`PersistentVolume` . `kubectl get pv` Eine Beispielausgabe finden Sie im Abschnitt Zusätzliche Informationen.	Kubernetes-Benutzer mit erteilten Berechtigungen
Überprüfen Sie den Status von. `PersistentVolumeClaim`	Geben Sie den folgenden Befehl ein, um den Status von zu überprüfen`PersistentVolumeClaim` . `kubectl -n poc-efs-eks-fargate get pvc` Eine Beispielausgabe finden Sie im Abschnitt Zusätzliche Informationen.	Kubernetes-Benutzer mit erteilten Berechtigungen
Stellen Sie sicher, dass Workload 1 in das Dateisystem schreiben kann.	Geben Sie den folgenden Befehl ein, um zu überprüfen, ob Workload 1 schreibt`/data/out1.txt` . `kubectl exec -ti poc-app1 -n poc-efs-eks-fargate -- tail -f /data/out1.txt`	Kubernetes-Benutzer mit erteilten Berechtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Die Ergebnisse ähneln den folgenden:
	`...`
	`Thu Sep  3 15:25:07 UTC 2023 - PoC APP 1`
	`Thu Sep  3 15:25:12 UTC 2023 - PoC APP 1`
	`Thu Sep  3 15:25:17 UTC 2023 - PoC APP 1`
	`...`	

Stellen Sie sicher, dass Workload 2 in das Dateisystem schreiben kann.	Geben Sie den folgenden Befehl ein, um zu überprüfen, ob Workload 2 schreibt `/data/out2.txt` .
	`kubectl -n $APP_NAMESPACE exec -ti poc-app2 -- tail -f /data/out2.txt`
	Die Ergebnisse ähneln den folgenden:
	`...`
	`Thu Sep  3 15:26:48 UTC 2023 - PoC APP 2`
	`Thu Sep  3 15:26:53 UTC 2023 - PoC APP 2`
	`Thu Sep  3 15:26:58 UTC 2023 - PoC APP 2`
	`...`
		Kubernetes-Benutzer mit erteilten Berechtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie sicher, dass Workload 1 die von Workload 2 geschriebene Datei lesen kann.	Geben Sie den folgenden Befehl ein, um zu überprüfen, ob Workload 1 die von Workload 2 geschriebene `/data/out2.txt` Datei lesen kann.
	`kubectl exec -ti poc-app1 -n poc-efs-eks-fargate -- tail -n 3 /data/out2.txt`
	Die Ergebnisse ähneln den folgenden:
	`...`
	`Thu Sep 3 15:26:48 UTC 2023 - PoC APP 2`
	`Thu Sep 3 15:26:53 UTC 2023 - PoC APP 2`
	`Thu Sep 3 15:26:58 UTC 2023 - PoC APP 2`
	`...`
		Kubernetes-Benutzer mit erteilten Berechtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie sicher, dass Workload 2 die von Workload 1 geschriebene Datei lesen kann.	Geben Sie den folgenden Befehl ein, um zu überprüfen, ob Workload 2 die von Workload 1 geschriebene `/data/out1.txt` Datei lesen kann.
	`kubectl -n $APP_NAMESPACE exec -ti poc-app2 -- tail -n 3 /data/out1.txt`
	Die Ergebnisse ähneln den folgenden:
	`... Thu Sep 3 15:29:22 UTC 2023 - PoC APP 1 Thu Sep 3 15:29:27 UTC 2023 - PoC APP 1 Thu Sep 3 15:29:32 UTC 2023 - PoC APP 1 ...`
		Kubernetes-Benutzer mit erteilten Berechtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie sicher, dass Dateien beibehalten werden, nachdem Sie Anwendung skomponenten entfernt haben.	Als Nächstes verwenden Sie ein Skript, um die Anwendung skomponenten (persiste ntes Volume, Persistentes Volume Claim und Pods) zu entfernen und zu überprüfe n, ob die Dateien `/data/out1.txt` im Dateisyst em aufbewahrt `/data/out 2.txt` werden. Führen Sie das Skript `validate-efs-content.sh` mit dem folgenden Befehl aus.
	
	`./scripts/epic05/v alidate-efs-conten t.sh \ -t "$EFS_CRE ATION_TOKEN"`
	
	wo `$EFS_CREATION_TOKE N` ist das eindeutige Erstellun gstoken für das Dateisystem.
	
	Die Ergebnisse ähneln den folgenden:
	
	`pod/poc-app-validation created Waiting for pod get Running state... Waiting for pod get Running state... Waiting for pod get Running state... Results from execution of 'find /data' on`
		Kubernetes-Benutzer mit erteilten Berechtigungen, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	validation process pod: /data /data/out2.txt /data/out1.txt	

Überwachen Sie den Betrieb

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überwachen Sie Anwendung sprotokolle.	Senden Sie die Anwendung sprotokolle im Rahmen eines Vorgangs am zweiten Tag CloudWatch zur Überwachung an Amazon.	AWS-Systemadministrator, Kubernetes-Benutzer mit erteilten Berechtigungen
Überwachen Sie Amazon EKS- und Kubernetes-Container mit Container Insights.	Überwachen Sie im Rahmen eines Vorgangs am zweiten Tag die Amazon EKS- und Kubernetes-Systeme mithilfe von Amazon CloudWatch Container Insights. Dieses Tool sammelt, aggregiert und fasst Metriken aus containerisierten Anwendungen auf verschiedenen Ebenen und Dimensionen zusammen. Weitere Informationen finden Sie im Abschnitt Verwandte Ressourcen.	AWS-Systemadministrator, Kubernetes-Benutzer mit erteilten Berechtigungen
Überwachen Sie Amazon EFS mit CloudWatch.	Überwachen Sie im Rahmen eines Vorgangs am zweiten Tag die Dateisysteme mithilfe von Amazon CloudWatch,	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	das Rohdaten von Amazon EFS sammelt und zu lesbaren Metriken nahezu in Echtzeit verarbeitet. Weitere Informationen finden Sie im Abschnitt Verwandte Ressourcen.	

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen Sie alle erstellten Ressourcen für das Muster.	Nachdem Sie dieses Muster abgeschlossen haben, bereinigen Sie alle Ressourcen, um zu vermeiden, dass AWS-Gebühren anfallen. Führen Sie das `clean-up-resources.sh` Skript aus, um alle Ressourcen zu entfernen, nachdem Sie die PoC-Anwendung nicht mehr verwendet haben. Füllen Sie eine der folgenden Optionen aus. Mit Verschlüsselung im Ruhezustand, mit einem KMS-Schlüssel: `./scripts/epic06/clean-up-resources.sh \ -c "$CLUSTER_NAME" \ -t "$EFS_CREATION_TOKEN" \`	Kubernetes-Benutzer mit erteilten Berechtigungen, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`-k "$KMS_KEY_ALIAS"`
	
	wobei `$CLUSTER_NAME` der Name Ihres Amazon EKS-Clusters, `$EFS_CREATION_TOKEN` das Erstellungstoken für das Dateisystem und der Alias für den KMS-Schlüssel `$KMS_KEY_ALIAS` ist.
	
	Ohne Verschlüsselung im Ruhezustand:
	
	`./scripts/epic06/clean-up-resources.sh \ -c "$CLUSTER_NAME" \ -t "$EFS_CREATION_TOKEN"`
	
	wobei `$CLUSTER_NAME` der Name Ihres Amazon EKS-Clusters und das Erstellungstoken für das Dateisystem `$EFS_CREATION_TOKEN` ist.	

Zugehörige Ressourcen

Referenzen

- AWS Fargate für Amazon EKS unterstützt jetzt Amazon EFS (Ankündigung)
- So erfassen Sie Anwendungsprotokolle bei der Verwendung von Amazon EKS auf AWS Fargate (Blogbeitrag)

- Container Insights verwenden (CloudWatch Amazon-Dokumentation)
- Einrichtung von Container Insights auf Amazon EKS und Kubernetes (CloudWatch Amazon-Dokumentation)
- Kennzahlen zu Amazon EKS und Kubernetes Container Insights (CloudWatch Amazon-Dokumentation)
- Überwachung von Amazon EFS mit Amazon CloudWatch (Amazon EFS-Dokumentation)

GitHub Tutorials und Beispiele

- Statische Bereitstellung
- Verschlüsselung während der Übertragung
- Zugriff auf das Dateisystem von mehreren Pods aus
- Nutzung von Amazon EFS in StatefulSets
- Unterpfade werden eingebunden
- Verwenden von Amazon EFS-Zugriffspunkten
- Amazon EKS Blueprints für Terraform

Erforderliche Tools

- Installation der AWS-CLI Version 2
- Installation von eksctl
- Kubectl wird installiert
- jq installieren

Zusätzliche Informationen

Im Folgenden finden Sie ein Beispiel für die Ausgabe des `kubectl get pv` Befehls.

```
NAME         CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM
            STORAGECLASS   REASON   AGE
poc-app-pv   1Mi        RWX            Retain           Bound    poc-efs-eks-fargate/
poc-app-pvc   efs-sc                  3m56s
```

Im Folgenden finden Sie ein Beispiel für die Ausgabe des `kubectl -n poc-efs-eks-fargate get pvc` Befehls.

```
NAME          STATUS   VOLUME       CAPACITY   ACCESS MODES   STORAGECLASS   AGE
poc-app-pvc   Bound    poc-app-pv   1Mi        RWX            efs-sc         4m34s
```

Richten Sie ereignisgesteuertes Auto Scaling in Amazon EKS mithilfe von Amazon EKS Pod Identity und KEDA ein

Erstellt von Dipen Desai (AWS), Abhay Diwan (AWS), Kamal Joshi (AWS) und Mahendra Revanasiddappa (AWS)

Übersicht

Orchestrierungsplattformen wie Amazon Elastic Kubernetes Service (Amazon EKS) haben das Lebenszyklusmanagement containerbasierter Anwendungen optimiert. Dies hilft Unternehmen, sich auf die Entwicklung, Sicherung, den Betrieb und die Wartung containerbasierter Anwendungen zu konzentrieren. Da ereignisgesteuerte Bereitstellungen immer häufiger vorkommen, skalieren Unternehmen Kubernetes-Bereitstellungen immer häufiger auf der Grundlage verschiedener Ereignisquellen. Diese Methode kann in Kombination mit Auto Scaling zu erheblichen Kosteneinsparungen führen, da Rechenressourcen auf Abruf und eine effiziente Skalierung bereitgestellt werden, die auf die Anwendungslogik zugeschnitten ist.

KEDA ist ein auf Kubernetes basierender ereignisgesteuerter Autoscaler. KEDA hilft Ihnen dabei, jeden Container in Kubernetes auf der Grundlage der Anzahl der Ereignisse, die verarbeitet werden müssen, zu skalieren. Es ist leicht und lässt sich in jeden Kubernetes-Cluster integrieren. Es funktioniert auch mit Standard-Kubernetes-Komponenten wie Horizontal Pod Autoscaling (HPA). KEDA bietet auch eine Funktion TriggerAuthentication, mit der Sie die Authentifizierung delegieren können. Es ermöglicht Ihnen, Authentifizierungsparameter zu beschreiben, die von den Containern ScaledObject und den Bereitstellungscontainern getrennt sind.

AWS bietet AWS Identity and Access Management (IAM) -Rollen, die verschiedene Kubernetes-Bereitstellungsoptionen unterstützen, darunter Amazon EKS, Amazon EKS Anywhere Red Hat OpenShift Service in AWS (ROSA) und selbstverwaltete Kubernetes-Cluster auf Amazon Elastic Compute Cloud (Amazon). EC2 Diese Rollen verwenden IAM-Konstrukte wie OpenID Connect (OIDC) -Identitätsanbieter und IAM-Vertrauensrichtlinien, um in verschiedenen Umgebungen zu arbeiten, ohne sich direkt auf Amazon EKS-Services oder verlassen zu müssen. APIs Weitere Informationen finden Sie unter IAM-Rollen für Dienstkonten in der Amazon EKS-Dokumentation.

Amazon EKS Pod Identity vereinfacht den Prozess, bei dem Kubernetes-Servicekonten IAM-Rollen übernehmen können, ohne dass OIDC-Anbieter erforderlich sind. Es bietet die Möglichkeit, Anmeldeinformationen für Ihre Anwendungen zu verwalten. Anstatt Ihre AWS Anmeldeinformationen zu erstellen und an die Container zu verteilen oder die Rolle der EC2 Amazon-Instance zu verwenden, verknüpfen Sie eine IAM-Rolle mit einem Kubernetes-Dienstkonto und konfigurieren

Ihre Pods so, dass sie das Dienstkonto verwenden. Dies hilft Ihnen, eine IAM-Rolle in mehreren Clustern zu verwenden, und vereinfacht die Richtlinienverwaltung, indem die Wiederverwendung von Berechtigungsrichtlinien für alle IAM-Rollen ermöglicht wird.

Durch die Implementierung von KEDA mit Amazon EKS Pod Identity können Unternehmen eine effiziente ereignisgesteuerte auto Skalierung und eine vereinfachte Verwaltung von Anmeldeinformationen erreichen. Anwendungen werden je nach Bedarf skaliert, wodurch die Ressourcennutzung optimiert und die Kosten gesenkt werden.

Dieses Muster hilft Ihnen bei der Integration von Amazon EKS Pod Identity in KEDA. Es zeigt, wie Sie das `keda-operator` Dienstkonto verwenden und die Authentifizierung delegieren können. `TriggerAuthentication` Außerdem wird beschrieben, wie eine Vertrauensbeziehung zwischen einer IAM-Rolle für den KEDA-Operator und einer IAM-Rolle für die Anwendung eingerichtet wird. Diese Vertrauensbeziehung ermöglicht es KEDA, Nachrichten in den Ereigniswarteschlangen zu überwachen und die Skalierung für die Kubernetes-Zielobjekte anzupassen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- AWS Command Line Interface (AWS CLI) Version 2.13.17 oder höher, installiert
- Python-Version 3.11.5 oder höher, installiert
- AWS SDK für Python (Boto3) Version 1.34.135 oder höher, installiert
- Helm Version 3.12.3 oder höher, installiert
- kubectl Version 1.25.1 oder höher, installiert
- Docker Engine Version 26.1.1 oder höher, installiert
- Ein Amazon EKS-Cluster Version 1.24 oder höher, erstellt
- Voraussetzungen für die Erstellung des Amazon EKS Pod Identity-Agenten, erfüllt

Einschränkungen

- Es ist erforderlich, dass Sie eine Vertrauensbeziehung zwischen der `keda-operator` Rolle und der `keda-identity` Rolle einrichten. Anweisungen finden Sie im Abschnitt Epen dieses Musters.

Architektur

In diesem Muster erstellen Sie die folgenden AWS Ressourcen:

- Amazon Elastic Container Registry (Amazon ECR) -Repository — In diesem Muster wird dieses Repo benannt. `keda-pod-identity-registry` Dieses private Repo wird zum Speichern von Docker-Images der Beispielanwendung verwendet.
- Amazon Simple Queue Service (Amazon SQS) -Warteschlange — In diesem Muster wird diese Warteschlange benannt`event-messages-queue`. Die Warteschlange fungiert als Nachrichtenpuffer, der eingehende Nachrichten sammelt und speichert. KEDA überwacht die Warteschlangenmetriken, z. B. die Anzahl der Nachrichten oder die Länge der Warteschlange, und skaliert die Anwendung automatisch auf der Grundlage dieser Messwerte.
- IAM-Rolle für die Anwendung — In diesem Muster wird diese Rolle benannt. `keda-identity` Die `keda-operator` Rolle übernimmt diese Rolle. Diese Rolle ermöglicht den Zugriff auf die Amazon SQS SQS-Warteschlange.
- IAM-Rolle für den KEDA-Operator — In diesem Muster wird diese Rolle benannt. `keda-operator` Der KEDA-Operator verwendet diese Rolle, um die erforderlichen AWS API-Aufrufe durchzuführen. Diese Rolle ist berechtigt, die `keda-identity` Rolle zu übernehmen. Aufgrund der Vertrauensstellung zwischen den Rollen `keda-operator` und den `keda-identity` Rollen verfügt die `keda-operator` Rolle über Amazon SQS SQS-Berechtigungen.

Über die benutzerdefinierten Ressourcen `TriggerAuthentication` und `ScaledObject` Kubernetes verwendet der Operator die `keda-identity` Rolle, um eine Verbindung mit einer Amazon SQS SQS-Warteschlange herzustellen. Basierend auf der Größe der Warteschlange skaliert KEDA die Anwendungsbereitstellung automatisch. Es fügt 1 Pod für jeweils 5 ungelesene Nachrichten in der Warteschlange hinzu. Wenn sich in der Standardkonfiguration keine ungelesenen Nachrichten in der Amazon SQS SQS-Warteschlange befinden, wird die Anwendung auf 0 Pods herunterskaliert. Der KEDA-Operator überwacht die Warteschlange in einem von Ihnen festgelegten Intervall.

Die folgende Abbildung zeigt, wie Sie Amazon EKS Pod Identity verwenden, um der `keda-operator` Rolle sicheren Zugriff auf die Amazon SQS SQS-Warteschlange zu gewähren.

Das Diagramm zeigt den folgenden Workflow:

1. Sie installieren den Amazon EKS Pod Identity-Agenten im Amazon EKS-Cluster.
2. Sie stellen den KEDA-Operator im KEDA-Namespace im Amazon EKS-Cluster bereit.
3. Sie erstellen die Rollen `keda-operator` und `keda-identity` IAM im Ziel. AWS-Konto

4. Sie stellen eine Vertrauensbeziehung zwischen den IAM-Rollen her.
5. Sie stellen die Anwendung im `security` Namespace bereit.
6. Der KEDA-Operator fragt Nachrichten in einer Amazon SQS SQS-Warteschlange ab.
7. KEDA initiiert HPA, wodurch die Anwendung automatisch auf der Grundlage der Warteschlangengröße skaliert wird.

Tools

AWS-Services

- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Mit Amazon Elastic Kubernetes Service (Amazon EKS) können Sie Kubernetes ausführen, AWS ohne dass Sie Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten müssen.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.

Andere Tools

- KEDA ist ein auf Kubernetes basierender ereignisgesteuerter Autoscaler.

Code-Repository

Der Code für dieses Muster ist im GitHub Event-Driven Auto Scaling using EKS Pod Identity and KEDA Repository verfügbar.

Bewährte Methoden

Wir empfehlen Ihnen, die ACM bewährte Methode für zu befolgen.

- Bewährte Methoden für Amazon EKS

- Bewährte Methoden für die Sicherheit in IAM
- Bewährte Methoden für Amazon SQS

Epen

Ressourcen erstellen AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Rolle für den KEDA-Operator.	1. Melden Sie sich bei der AWS Management Console an und öffnen Sie dann die IAM-Konsole. 2. Wählen Sie im Navigatio nsbereich Rollen aus. 3. Wählen Sie Create role (Rolle erstellen) aus. 4. Wählen Sie den Rollentyp Custom trust policy (Benutzerdefinierte Vertrauensrichtlinie). 5. Geben Sie im Abschnitt Benutzerdefinierte Vertrauensrichtlinie die folgende benutzerdefinierte Vertrauensrichtlinie für diese Rolle ein: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principa l": {`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Service": "pods.eks
	.amazonaws.com"
	},
	"Action":
	[
	
	"sts:AssumeRole",
	
	"sts:TagSession"
	]
	}
	]
	}</pre>
	6. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die Option Next (Weiter) aus. Sie fügen dieser Rolle keine Richtlinien hinzu.
	7. Geben Sie für Role name (Rollenname) den Namen `keda-operator` ein.
	8. Wählen Sie Rolle erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Rolle für die Beispielanwendung.	1. Wählen Sie in der IAM-Konsole im Navigationsbereich die Option Rollen aus. 2. Wählen Sie Rolle erstellen aus. 3. Wählen Sie den Rollentyp Custom trust policy (Benutzerdefinierte Vertrauensrichtlinie). 4. Geben Sie im Abschnitt Benutzerdefinierte Vertrauensrichtlinie die folgende benutzerdefinierte Vertrauensrichtlinie für diese Rolle ein. `<account number>`Ersetzen Sie durch Ihre Zielkonto nummer: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "pods.eks.amazonaws.com", "AWS": "arn:aws:iam::<account number>:role/keda-operator" }, ...`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Action":
	[
	"sts:AssumeRole",
	"sts:TagSession"
	]
	}
	]
	}</pre>
	5. Fügen Sie auf der Seite „Berechtigungen hinzufügen“ der Rolle die folgenden AWS verwalteten Richtlinien hinzu:
	• `AmazonSQSReadOnlyAccess`
	• `AWSLambdaSQSQueueExecutionRole`
	6. Wählen Sie Weiter aus.
	7. Geben Sie für Role name (Rollenname) den Namen `keda-identity` ein.
	8. Wählen Sie Rolle erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Amazon SQS-Warteschlange	1. Öffnen Sie die Amazon-SQS-Konsole. 2. Wählen Sie Create queue (Warteschlange erstellen) aus. 3. Wählen Sie unter Type (Typ) die Option Standard aus. 4. Geben Sie auf der Seite „Warteschlange erstellen“ als Namen ein `event-messages-queue` . 5. Wählen Sie Create queue (Warteschlange erstellen) aus. Sie ändern keine der Standardeinstellungen für diese Warteschlange.	Allgemeines AWS
Erstellen Sie ein Amazon-ECR-Repository.	1. Öffnen Sie die Amazon ECR-Konsole. 2. Wählen Sie Repository erstellen aus. 3. Geben `keda-pod-identity-registry` Sie als Repository-Name ein. 4. Wählen Sie Repository erstellen aus. Sie ändern keine der Standardeinstellungen für dieses Repository.	Allgemeines AWS

Den Amazon EKS-Cluster einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Amazon EKS Pod Identity-Agenten bereit.	Richten Sie für den Amazon EKS-Zielcluster den Amazon EKS Pod Identity-Agenten ein. Folgen Sie den Anweisung en unter Amazon EKS Pod Identity Agent einrichten in der Amazon EKS-Dokumentation.	AWS DevOps

Stellen Sie KEDA bereit.	1. Geben Sie die folgenden Befehle ein, um KEDA auf dem Amazon EKS-Zielc luster bereitzustellen:
	`# Add Helm Repo for Keda`
	`helm repo add kedacore https://kedacore.github.io/charts`
	`# Update Helm repo`
	`helm repo update`
	`# Install Keda`
	`helm install keda kedacore/keda --namespace keda --create-namespace`
	Weitere Informationen finden Sie unter Deployment with Helm in der KEDA-Dokumentation.
	2. Überprüfen Sie nach erfolgreicher Bereitstellung in der Ausgabe, ob drei Bereitstellungen für den KEDA-Operator erstellt
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wurden. Im Folgenden finden Sie ein Beispiel für eine Ausgabe: `NAME READY UP-TO-DATE AVAILABLE AGE keda-admission-webhooks 1/1 1 1 89s keda-operator 1/1 1 1 89s keda-operator-metrics-apiserver 1/1 1 1 89s`	
Weisen Sie dem Kubernetes-Dienstkonto die IAM-Rolle zu.	Folgen Sie den Anweisungen unter Zuweisen einer IAM-Rolle zu einem Kubernetes-Servicekonto in der Amazon EKS-Dokumentation. Verwenden Sie die folgenden Werte: • Geben Sie für die IAM-Rolle ein. `keda-operator` • Geben Sie für den Kubernetes-Namespace ein. `keda` • Geben Sie für das Kubernetes-Dienstkonto ein. `keda-operator`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen -Namespace.	Geben Sie den folgenden Befehl ein, um einen `security` Namespace im Amazon EKS-Zielcluster zu erstellen: `kubectl create ns security`	DevOps Ingenieur

Bereitstellen der Beispielanwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie die Anwendung sdateien.	Geben Sie den folgenden Befehl ein, um die ereignisg esteuerte auto Skalierung mithilfe von EKS Pod Identity und dem KEDA-Repository von zu klonen: GitHub `git clone https://github.com/aws-samples/event-driven-autoscaling-using-podidentity-and-keda.git`	DevOps Ingenieur
Erstellen Sie das Docker-Image.	1. Geben Sie den folgenden Befehl ein, um zum geklonten Repository zu navigieren: `cd event-driven-autoscaling-using-podidentity-and-keda`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Geben Sie den folgenden Befehl ein, um das Docker-Image für die Beispielanwendung zu erstellen: `docker build -t keda-pod-identity-registry .`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Senden Sie das Docker-Image an Amazon ECR.	1. Geben Sie in dem Terminal, in dem Sie das Docker-Image erstellt haben, den folgenden Befehl ein, um sich bei Amazon ECR anzumelden. Ersetzen Sie <AWS_REGION> und <AWS_ACCOUNT_ID> durch Werte aus Ihrer AWS Umgebung:
	`aws ecr get-login-password \ --region <AWS_REGION> | docker login \ --username AWS \ --password-stdin <AWS_ACCOUNT_ID>.dkr.ecr.<AWS_REGION>.amazonaws.com`
	2. Geben Sie den folgenden Befehl ein, um das Bild zu taggen. Ersetzen Sie <AWS_REGION> und <AWS_ACCOUNT_ID> durch Werte aus Ihrer AWS Umgebung:
	`docker tag keda-pod-identity-registry: latest <AWS_ACCOUNT_ID>.dkr.ecr.<AWS_REGION>.amazonaws.com/keda-pod-id`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`entity-registry:latest`
	3. Geben Sie den folgenden Befehl ein, um das Bild an Amazon ECR zu übertragen. Ersetzen Sie `<AWS_REGION>` und `<AWS_ACCOUNT_ID>` durch Werte aus Ihrer AWS Umgebung:
	`docker push <AWS_ACCOUNT_ID>.dkr.ecr.<AWS_REGION>.amazonaws.com/keda-pod-identity-registry:latest`
	Note
	Sie finden Push-Befehle, indem Sie zur Amazon ECR-Repository-Seite navigieren und dann Push-Befehle anzeigen wählen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Beispielanwendung bereit.	1. Öffnen Sie im geklonten Repository die Datei deploy.yaml. 2. Ersetzen Sie `<AWS_ACCOUNT_ID>` und durch Werte aus `<AWS_REGION>` Ihrer Umgebung. 3. Speichern und schließen Sie die Datei deploy.yaml. 4. Geben Sie den folgenden Befehl ein, um die Beispielanwendung auf dem Amazon EKS-Zielcluster bereitzustellen: `kubectl apply -f deploy.yaml` Dieser Befehl erstellt ein Bereitstellungs- und Servicekonto im Cluster.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Weisen Sie dem Anwendungsdienstkonto die IAM-Rolle zu.	Gehen Sie wie folgt vor, um die `keda-identity` IAM-Rolle dem Dienstkonto für die Beispielanwendung zuzuordnen:
	• Folgen Sie den Anweisungen unter Zuweisen einer IAM-Rolle zu einem Kubernetes-Servicekonto in der Amazon EKS-Dokumentation. Verwenden Sie die folgenden Werte:
	  • Geben Sie für die IAM-Rolle ein. `keda-identity`
	  • Geben Sie für den Kubernetes-Namespace ein. `security`
	  • Geben Sie für das Kubernetes-Dienstkonto ein. `my-sqs-read-msgs`
	• Geben Sie den folgenden AWS CLI Befehl ein. `<cluster-name>` Ersetzen Sie durch den Namen des Amazon EKS-Ziel-Clusters und `<role-ARN>` ersetzen Sie ihn durch den Amazon-Ressourcennamen (ARN) der `keda-identity` Rolle:
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws eks create-pod-identity-association \ --cluster-name <cluster-name> \ --role-arn <role-ARN> \ --namespace security \ --service-account my-sqs-read-msgs`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereitstellen `ScaledObject` und`TriggerAuthentication` .	1. Öffnen Sie im geklonten Repository die Datei keda.yaml. 2. Ersetzen Sie sie durch die `{{AWS_ACCOUNT_ID}}` ID Ihres Ziels. AWS-Konto 3. Ersetze es `{{AWS_REGION}}` durch dein Ziel AWS-Region. 4. (Optional) Aktualisieren Sie in den Zeilen 21—24 die Parameter für die `ScaledObject` Skalierungsrichtlinie. Im Folgenden finden Sie weitere Informationen zu diesen Parametern: • PollingInterval • Abklingzeit • idleReplicaCount • minReplicaCount 5. Speichern und schließen Sie die Datei keda.yaml. 6. Geben Sie den folgenden Befehl ein, um die Ressourcen und bereitzustellen: `ScaledObject` `TriggerAuthentication` `kubectl -n security apply -f keda.yaml`	DevOps Ingenieur

Testen Sie die auto Skalierung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Senden Sie Nachrichten an die Amazon SQS SQS-Warteschlange.	1. Geben Sie den folgenden Befehl ein, um zum geklonten Repository zu navigieren:
	`cd event-driven-autoscaling-using-podidentity-and-keda`
	2. Geben Sie den folgenden Befehl ein, um Testnachrichten an die Amazon SQS SQS-Warteschlange zu senden:
	`python sqs_send_msg.py`
	Das Skript sqs_send_msg.py fungiert als Anwendung, die Meldungen zum Testen von Auto Scaling generiert.
	Note
	Wenn Sie Python 3 ausführen, geben Sie ein`python3 sqs_send_msg.py .`
		DevOps Ingenieur

Überwachen Sie die Anwendungs-Pods.	1. Geben Sie in einem anderen Terminal den	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	folgenden Befehl ein, um die Pods zu überwachen:
	
	`kubectl -n security get po`
	
	2. Für jeweils 5 ungelesene Nachrichten in der Amazon SQS SQS-Warteschlange fügt KEDA einen Pod hinzu. Bestätigen Sie in der Ausgabe des vorherigen Befehls, dass neue Pods hinzugefügt werden. Im Folgenden finden Sie ein Beispiel für eine Ausgabe:
	
	`kubectl -n security get po`
	`NAME READY STATUS RESTARTS AGE`
	`q-read-797f4c7589-2bj76 1/1 Running 0 2s`
	`q-read-797f4c7589-4zxph 1/1 Running 0 49s`
	`q-read-797f4c7589-cg9dt 1/1 Running 0 18s`
	`q-read-797f4c7589-slc69 1/1 Running 0 33s`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wenn Sie mit dem Testen fertig sind, geben Sie im ursprünglichen Terminal STRG + C (Windows) oder CMD+ C (macOS) ein. Dadurch wird das Python-Skript sqs_send_msg.py gestoppt.	

Fehlerbehebung

Problem	Lösung
Der KEDA-Operator kann die Anwendung nicht skalieren.	Geben Sie den folgenden Befehl ein, um die Protokolle der `keda-operator` IAM-Rolle zu überprüfen: `kubectl logs -n keda -l app=keda-operator -c keda-operator` Wenn es einen `HTTP 403` Antwortcode gibt, verfügen die Anwendung und der KEDA-Scal er nicht über ausreichende Berechtigungen, um auf die Amazon SQS SQS-Warteschlange zuzugreifen. Führen Sie folgende Schritte aus: 1. Überprüfen Sie die IAM-Richtlinien und -Anweisungen für die `keda-identity` Rolle, um sicherzustellen, dass dieser Warteschlange Lesezugriff gewährt wurde. 2. Überprüfen Sie die Vertrauensbeziehung zwischen den IAM-Rollen. Im Folgenden wird ein Beispiel gezeigt:

Problem	Lösung

	<pre>{
	    "Version": "2012-10-17",
	    "Statement": [
	        {
	            "Effect": "Allow",
	            "Principal": {
	                "Service": "pods.eks
	.amazonaws.com"
	            },
	            "Action": [
	                "sts:AssumeRole",
	                "sts:TagSession"
	            ]
	        }
	    ]
	}</pre>
	Wenn ein `Assume-Role` Fehler auftritt, kann eine Amazon EKS-Knoten-IAM-Rolle die IAM-Rolle, für die definiert ist, nicht übernehmen. `TriggerAuthentication` Führen Sie folgende Schritte aus:
	1. Geben Sie den folgenden Befehl ein, um den `keda-operator` Pod zu löschen und einen neuen zu erstellen:
	<pre>kubectl delete pod keda-operator-
	<alphenumeric-value> --namespace
	 keda</pre>
	2. Geben Sie den folgenden Befehl ein, um die Identität zu überprüfen, die der Pod annimmt:
	<pre>kubectl describe pod <keda-operator-
	pod-name> --namespace keda</pre>

Problem	Lösung
	3. Wenn der Pod erfolgreich neu gestartet wurde, vergewissern Sie sich, dass die folgenden beiden Variablen zur Pod-Besch reibung hinzugefügt wurden: • `AWS_CONTAINER_CREDENTIALS_F ULL_URI` • `AWS_CONTAINER_AUTHORIZATION _TOKEN_FILE`

Zugehörige Ressourcen

- Den Amazon EKS Pod Identity Agent einrichten (Amazon EKS-Dokumentation)
- Bereitstellung von KEDA (KEDA-Dokumentation)
- ScaledObject Spezifikation (KEDA-Dokumentation)
- Authentifizierung mit TriggerAuthentication (KEDA-Dokumentation)

Optimieren Sie PostgreSQL-Bereitstellungen auf Amazon EKS mithilfe von PGO

Erstellt von Shalaka Dengale (AWS)

Übersicht

Dieses Muster integriert den Postgres-Operator von Crunchy Data (PGO) mit Amazon Elastic Kubernetes Service (Amazon EKS), um PostgreSQL-Bereitstellungen in cloudnativen Umgebungen zu optimieren. PGO bietet Automatisierung und Skalierbarkeit für die Verwaltung von PostgreSQL-Datenbanken in Kubernetes. Wenn Sie PGO mit Amazon EKS kombinieren, bildet es eine robuste Plattform für die effiziente Bereitstellung, Verwaltung und Skalierung von PostgreSQL-Datenbanken.

Diese Integration bietet die folgenden Hauptvorteile:

- Automatisierte Bereitstellung: Vereinfacht die Bereitstellung und Verwaltung von PostgreSQL-Clustern.
- Benutzerdefinierte Ressourcendefinitionen (CRDs): Verwendet Kubernetes-Primitive für das PostgreSQL-Management.
- Hohe Verfügbarkeit: Unterstützt automatisches Failover und synchrone Replikation.
- Automatisierte Backups und Wiederherstellungen: Optimiert Sicherungs- und Wiederherstellungsprozesse.
- Horizontale Skalierung: Ermöglicht die dynamische Skalierung von PostgreSQL-Clustern.
- Versionsupgrades: Ermöglicht fortlaufende Upgrades mit minimalen Ausfallzeiten.
- Sicherheit: Erzwingt Verschlüsselungs-, Zugriffskontrollen und Authentifizierungsmechanismen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto.
- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 2, installiert und konfiguriert unter Linux, macOS oder Windows.
- AWS CLI Config, um AWS Ressourcen über die Befehlszeile zu verbinden.
- eksctl, installiert und konfiguriert unter Linux, MacOS oder Windows.

- `kubectl`, installiert und konfiguriert für den Zugriff auf Ressourcen in Ihrem Amazon EKS-Cluster. Weitere Informationen finden Sie unter Kubectl und eksctl einrichten in der Amazon EKS-Dokumentation.
- Ihr Computerterminal ist für den Zugriff auf den Amazon EKS-Cluster konfiguriert. Weitere Informationen finden Sie in der Amazon EKS-Dokumentation unter Konfiguration Ihres Computers für die Kommunikation mit Ihrem Cluster.

Produktversionen

- Kubernetes-Versionen 1.21—1.24 oder höher (siehe PGO-Dokumentation).
- PostgreSQL Version 10 oder höher. Dieses Muster verwendet PostgreSQL Version 16.

Einschränkungen

- Einige AWS-Services sind nicht in allen verfügbar. AWS-Regionen Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie auf der Seite Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Architektur

Zieltechnologie-Stack

- Amazon EKS
- Amazon Virtual Private Cloud (Amazon VPC)
- Amazon Elastic Compute Cloud (Amazon EC2)

Zielarchitektur

Dieses Muster erstellt eine Architektur, die einen Amazon EKS-Cluster mit drei Knoten enthält. Jeder Knoten läuft auf einer Reihe von EC2 Instances im Backend. Dieses PostgreSQL-Setup folgt einer primären Replikatarchitektur, die besonders für leseintensive Anwendungsfälle effektiv ist. Die Architektur umfasst die folgenden Komponenten:

- Der primäre Datenbankcontainer (pg-primary) hostet die PostgreSQL-Hauptinstanz, an die alle Schreibvorgänge gerichtet sind.
- Sekundäre Replikatcontainer (pg-replica) hosten die PostgreSQL-Instanzen, die die Daten aus der Primärdatenbank replizieren und Lesevorgänge abwickeln.
- PgBouncerist ein leichter Verbindungspooler für PostgreSQL-Datenbanken, der in PGO enthalten ist. Es befindet sich zwischen dem Client und dem PostgreSQL-Server und fungiert als Vermittler für Datenbankverbindungen.
- PGO automatisiert die Bereitstellung und Verwaltung von PostgreSQL-Clustern in dieser Kubernetes-Umgebung.
- Patroni ist ein Open-Source-Tool, das Hochverfügbarkeitskonfigurationen für PostgreSQL verwaltet und automatisiert. Es ist in PGO enthalten. Wenn Sie Patroni mit PGO in Kubernetes verwenden, spielt dies eine entscheidende Rolle bei der Sicherstellung der Widerstandsfähigkeit und Fehlertoleranz eines PostgreSQL-Clusters. Weitere Informationen finden Sie in der Patroni-Dokumentation.

Der Workflow umfasst die folgenden Schritte:

- Stellen Sie den PGO-Operator bereit. Sie stellen den PGO-Operator auf Ihrem Kubernetes-Cluster bereit, der auf Amazon EKS läuft. Dies kann mithilfe von Kubernetes-Manifesten oder Helm-Diagrammen erfolgen. Dieses Muster verwendet Kubernetes-Manifeste.
- Definieren Sie PostgreSQL-Instanzen. Wenn der Operator ausgeführt wird, erstellen Sie benutzerdefinierte Ressourcen (CRs), um den gewünschten Status von PostgreSQL-Instanzen anzugeben. Dazu gehören Konfigurationen wie Speicher-, Replikations- und Hochverfügbarkeitseinstellungen.
- Betreiberverwaltung. Sie interagieren mit dem Operator über Kubernetes-API-Objekte, z. B. CRs um PostgreSQL-Instanzen zu erstellen, zu aktualisieren oder zu löschen.
- Überwachung und Wartung. Sie können den Zustand und die Leistung der PostgreSQL-Instances überwachen, die auf Amazon EKS ausgeführt werden. Betreiber stellen häufig Metriken und Protokollierung zu Überwachungszwecken bereit. Sie können bei Bedarf routinemäßige Wartungsaufgaben wie Upgrades und Patches durchführen. Weitere Informationen finden Sie unter Überwachen der Cluster-Leistung und Anzeigen von Protokollen in der Amazon EKS-Dokumentation.
- Skalierung und Backup: Sie können die vom Betreiber bereitgestellten Funktionen verwenden, um PostgreSQL-Instanzen zu skalieren und Backups zu verwalten.

Dieses Muster deckt keine Überwachungs-, Wartungs- und Sicherungsvorgänge ab.

Automatisierung und Skalierung

- Sie können es verwenden AWS CloudFormation , um die Erstellung der Infrastruktur zu automatisieren. Weitere Informationen finden Sie unter Amazon EKS-Ressourcen erstellen mit AWS CloudFormation in der Amazon EKS-Dokumentation.
- Sie können Build Numbers GitVersion oder Jenkins verwenden, um die Bereitstellung von Datenbank-Instances zu automatisieren.

Tools

AWS-Services

- Mit Amazon Elastic Kubernetes Service (Amazon EKS) können Sie Kubernetes ausführen, AWS ohne dass Sie Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten müssen.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell interagieren AWS-Services können.

Andere Tools

- eksctl ist ein einfaches Befehlszeilentool zum Erstellen von Clustern auf Amazon EKS.
- kubectl ist ein Befehlszeilenprogramm zum Ausführen von Befehlen für Kubernetes-Cluster.
- PGO automatisiert und skaliert die Verwaltung von PostgreSQL-Datenbanken in Kubernetes.

Bewährte Methoden

Folgen Sie diesen Best Practices, um eine reibungslose und effiziente Bereitstellung zu gewährleisten:

- Schützen Sie Ihren EKS-Cluster. Implementieren Sie bewährte Sicherheitsmethoden für Ihren EKS-Cluster, z. B. die Verwendung von AWS Identity and Access Management (IAM-) Rollen für Dienstkonten (IRSA), Netzwerkrichtlinien und VPC-Sicherheitsgruppen. Beschränken Sie den Zugriff auf den EKS-Cluster-API-Server und verschlüsseln Sie die Kommunikation zwischen den Knoten und dem API-Server mithilfe von TLS.

- Stellen Sie die Versionskompatibilität zwischen PGO und Kubernetes sicher, die auf Amazon EKS ausgeführt werden. Einige PGO-Funktionen erfordern möglicherweise bestimmte Kubernetes-Versionen oder führen zu Kompatibilitätseinschränkungen. Weitere Informationen finden Sie in der PGO-Dokumentation unter Komponenten und Kompatibilität.
- Planen Sie die Ressourcenzuweisung für Ihre PGO-Bereitstellung, einschließlich CPU, Arbeitsspeicher und Speicher. Berücksichtigen Sie die Ressourcenanforderungen sowohl von PGO als auch der von ihr verwalteten PostgreSQL-Instanzen. Überwachen Sie die Ressourcennutzung und skalieren Sie die Ressourcen nach Bedarf.
- Design für hohe Verfügbarkeit. Gestalten Sie Ihre PGO-Bereitstellung für hohe Verfügbarkeit, um Ausfallzeiten zu minimieren und die Zuverlässigkeit zu gewährleisten. Stellen Sie aus Gründen der Fehlertoleranz mehrere PGO-Repliken in mehreren Availability Zones bereit.
- Implementieren Sie Sicherungs- und Wiederherstellungsverfahren für Ihre von PGO verwalteten PostgreSQL-Datenbanken. Verwenden Sie Funktionen von PGO oder Backup-Lösungen von Drittanbietern, die mit Kubernetes und Amazon EKS kompatibel sind.
- Richten Sie die Überwachung und Protokollierung für Ihre PGO-Bereitstellung ein, um Leistung, Zustand und Ereignisse zu verfolgen. Verwenden Sie Tools wie Prometheus für die Überwachung von Metriken und Grafana für die Visualisierung. Konfigurieren Sie die Protokollierung so, dass PGO-Protokolle zur Fehlerbehebung und Prüfung erfasst werden.
- Konfigurieren Sie das Netzwerk ordnungsgemäß, um die Kommunikation zwischen PGO, PostgreSQL-Instanzen und anderen Diensten in Ihrem Kubernetes-Cluster zu ermöglichen. Verwenden Sie Amazon VPC-Netzwerkfunktionen und Kubernetes-Netzwerk-Plugins wie Calico oder Amazon VPC CNI für die Durchsetzung von Netzwerkrichtlinien und die Isolierung des Datenverkehrs.
- Wählen Sie geeignete Speicheroptionen für Ihre PostgreSQL-Datenbanken aus und berücksichtigen Sie dabei Faktoren wie Leistung, Haltbarkeit und Skalierbarkeit. Verwenden Sie Amazon Elastic Block Store (Amazon EBS) -Volumes oder AWS verwaltete Speicherdienste für persistenten Speicher. Weitere Informationen finden Sie unter Speichern von Kubernetes-Volumes mit Amazon EBS in der Amazon EKS-Dokumentation.
- Verwenden Sie Infrastructure-as-Code-Tools (IaC) AWS CloudFormation , um beispielsweise die Bereitstellung und Konfiguration von PGO auf Amazon EKS zu automatisieren. Definieren Sie Infrastrukturkomponenten — einschließlich des EKS-Clusters, der Netzwerk- und PGO-Ressourcen — als Code, um Konsistenz, Wiederholbarkeit und Versionskontrolle zu gewährleisten.

Epen

Erstellen einer IAM-Rolle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine IAM-Rolle.	1. Erstellen Sie eine IAM-Rolle mit dem folgenden Befehl in: AWS CLI
	
	`aws iam create-role \`
	`  --role-name {YourRoleName} \`
	`  --assume-role-policy-document '{`
	`  "Version": "2012-10-17",`
	`  "Statement": [`
	`  {`
	`  "Effect": "Allow",`
	`  "Principal": {`
	`  "Service": "eks.amazonaws.com"`
	`  },`
	`  "Action": "sts:AssumeRole"`
	`  }`
	`  ]`
	`  }' && \`
	`aws iam attach-role-policy \`
	`  --role-name {YourRoleName}\`
	`  --policy-arn arn:aws:iam::aws:policy/AmazonEKSClusterPolicy && \`
		AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>aws iam attach-role-policy \
	    --role-name {YourRoleName}\
	    --policy-arn arn:aws:iam::aws:policy/AmazonEKSServicePolicy && \
	aws iam attach-role-policy \
	    --role-name {YourRoleName}\
	     --policy-arn arn:aws:iam::aws:policy/CloudWatchFullAccess</pre>
	2. Überprüfen Sie die Rolle in: AWS Management Console
	a. Öffnen Sie die IAM-Konsole.
	b. Wählen Sie Rollen und suchen Sie nach dem Rollennamen, den Sie erstellt haben.
	c. Vergewissern Sie sich, dass die folgenden Richtlinien beigefügt sind:
	`AmazonEKSClusterPolicy`
	`AmazonEKSServicePolicy`
	`CloudWatchFullAccess`	

Erstellen Sie einen Amazon EKS-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon-EKS-Cluster.	Wenn Sie bereits einen Cluster bereitgestellt haben, überspringen Sie diesen Schritt. Andernfalls stellen Sie einen Amazon EKS-Cluster in Ihrem aktuellen mithilfe AWS-Konto `eksctl` von Terraform oder bereit. AWS CloudFormation Dieses Muster wird `eksctl` für die Cluster-Bereitstellung verwendet. **Note** Dieses Muster verwendet Amazon EC2 als Knotengruppe für Amazon EKS. Wenn Sie es verwenden möchten AWS Fargate, sehen Sie sich die `managedNodeGroups` Konfiguration in der eksctl-Dokumentation an. 1. Verwenden Sie die folgende `eksctl` Eingabedatei, um den Cluster zu generieren.	AWS-Administrator, Terraform - oder eksctl-Administrator, Kubernetes-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`sample-cluster.yaml`:
	
	`apiVersion: eksctl.io/v1alpha5`
	`kind: ClusterConfig`
	`metadata:`
	`  name: postgresql`
	`  region: us-east-1`
	`  version: "1.29"`
	`accessConfig:`
	`  authenticationMode: API_AND_CONFIG_MAP`
	`availabilityZones:`
	`- us-east-1a`
	`- us-east-1b`
	`- us-east-1c`
	`nodeGroups:`
	`  - name: ng-1`
	`  instanceType: m5.16xlarge`
	`  desiredCapacity: 2`
	`  - name: ng-2`
	`  instanceType: m5.16xlarge`
	`  desiredCapacity: 2`
	`  - name: ng-3`
	`  instanceType: m5.16xlarge`
	`  desiredCapacity: 2`
	`vpc:`
	`  cidr: 192.168.0.0/16`
	`  clusterEndpoints:`
	`  publicAccess: true`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> nat:
	    gateway: HighlyAva
	ilable
	iamIdentity
	Mappings:
	  - arn: arn:aws:i
	am::<account-id>:r
	ole/<role-name> #
	 update the IAM role
	 ARN created in step 1
	    username: <user-
	name> # Enter the
	 user name per your
	 choice
	    noDuplicateARNs:
	 false</pre>	

	2. Führen Sie den folgenden Befehl aus, um den Cluster zu erstellen (geben Sie den Dateipfad zu Ihrer `sample-cluster.yaml` Datei an):
	<pre>eksctl create
	 cluster -f sample-cl
	uster.yaml</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Status des Clusters.	Führen Sie den folgenden Befehl aus, um den aktuellen Status der Knoten im Cluster zu überprüfen: `kubectl get nodes` Wenn Sie auf Fehler stoßen, lesen Sie den Abschnitt zur Fehlerbehebung in der Amazon EKS-Dokumentation.	AWS-Administrator, Terraform - oder eksctl-Administrator, Kubernetes-Administrator

Erstellen Sie einen OIDC-Identitätsanbieter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie den IAM OIDC-Anbieter.	Als Voraussetzung für den Amazon EBS Container Storage Interface (CSI) -Treiber benötigen Sie einen vorhandenen IAM OpenID Connect (OIDC) -Anbieter für Ihren Cluster. Aktivieren Sie den IAM OIDC-Anbieter mit dem folgenden Befehl: `eksctl utils associate -iam-oidc-provider --region={region} --cluster={YourClusterNameHere} --approve`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen zu diesem Schritt finden Sie in der Amazon EKS-Dokumentation.	
Erstellen Sie eine IAM-Rolle für den Amazon EBS CSI-Treiber.	Verwenden Sie den folgenden `eksctl` Befehl, um die IAM-Rolle für den CSI-Treiber zu erstellen: `eksctl create iamserviceaccount \ --region {RegionName} \ --name ebs-csi-controller-sa \ --namespace kube-system \ --cluster {YourClusterNameHere} \ --attach-policy-arn arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy \ --approve \ --role-only \ --role-name AmazonEKS_EBS_CSI_DriverRole` Wenn Sie verschlüsselte Amazon EBS-Laufwerke verwenden, müssen Sie die Richtlinie weiter konfigurieren. Anweisungen finden Sie in der Amazon EBS SCI-Treiberdokumentation.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie den Amazon EBS CSI-Treiber hinzu.	Verwenden Sie den folgenden `eksctl` Befehl, um den Amazon EBS CSI-Treiber hinzuzufügen: `eksctl create addon \ --name aws-ebs-csi-driver \ --cluster <YourClusterName> service-account-role-arn arn:aws:iam::$(aws sts get-caller-identity \ --query Account \ --output text):role/AmazonEKS_EBS_CSI_DriverRole \ --force`	AWS-Administrator

Installieren Sie PGO

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das PGO-Repository.	Klonen Sie das GitHub Repository für PGO: `git clone https://github.com/CrunchyData/postgres-operator-examples.git`	AWS DevOps
Geben Sie die Rollendetails für die Erstellung des Dienstkontos an.	Um dem Amazon EKS-Cluster Zugriff auf die erforderlichen AWS Ressourcen zu gewähren, geben Sie den Amazon-Ressourcennamen	AWS-Administrator, Kubernetes-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	(ARN) der OIDC-Rolle an, die Sie zuvor in der `service_account.yaml` Datei erstellt haben. Diese Datei befindet sich im Namespace-Ordner des Repositorys.
	
	`cd postgres-operator-examples`
	
	`--- metadata: annotations: eks.amazonaws.com/role-arn: arn:aws:iam::<accountId>:role/<role_name> # Update the OIDC role ARN created earlier`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den Namespace und die PGO-Voraussetzungen.	1. Führen Sie den folgenden Befehl aus, um den Namespace zu erstellen:
	`kubectl apply -k kustomize/install/namespace`
	Dadurch wird ein dediziert er Namespace für PGO eingerichtet. Bei Bedarf können Sie die `namespace.yml` Datei ändern und dem Namespace einen anderen Namen zuweisen.
	2. Führen Sie den folgenden Befehl aus, um die Standardkonfiguration auf den Cluster anzuwenden:
	`kubectl apply --server-side -k kustomize/install/default`
	`kustomize/install/default` stellt die Standardkonfiguration für die rollenbasierte Zugriffsk ontrolle (RBAC) von Kubernetes, die benutzerd efinierte Ressource ndefinition (CRD) und die Kubernetes Manager-D ateien bereit.
		Kunernetes-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Erstellung von Pods.	Stellen Sie sicher, dass der Namespace und die Standardkonfiguration erstellt wurden: `kubectl get pods -n postgres-operator`	AWS-Administrator, Kubernetes-Administrator
Überprüfen. PVCs	Verwenden Sie den folgenden Befehl, um Ansprüche auf persistente Volumes (PVCs) zu überprüfen: `kubectl describe pvc -n postgres-operator`	AWS-Administrator, Kubernetes-Administrator

Erstellen Sie einen Operator und stellen Sie ihn bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie einen Operator.	Überarbeiten Sie den Inhalt der Datei unter `/kustomize/postgres/postgres.yaml` , sodass er den folgenden Kriterien entspricht:
	`spec:`
	`  instances:`
	`  - name: pg-1`
	`  replicas: 3`
	`  patroni:`
	`  dynamicConfiguration:`
	`  postgresql:`
	`  pg_hba:`
		AWS-Administrator, DBA, Kubernetes-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>- "host all all 0.0.0.0/0 trust"
	# this line enabled logical replication with programmatic access
	- "host all postgres 127.0.0.1/32 md5"
	synchronous_mode: true
	users:
	- name: replicator
	databases:
	- testdb
	options: "REPLICATION"</pre>
	Diese Updates bewirken Folgendes:
	• Passen Sie die PostgreSQL-Konfigurationseinstellungen an, um den Zugriff auf die PostgreSQL-Instanz zu erleichtern.
	• Fügen Sie Konfigurationen für Replikationsbenutzer, Datenbankbenutzer und Superuser hinzu, um Streaming-Replikation, Datenbankzugriff und Clustermanagement zu ermöglichen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Operator bereit.	Stellen Sie den PGO-Operator bereit, um die Verwaltung und den Betrieb von PostgreSQL-Datenbanken in Kubernetes-Umgebungen zu optimieren: `kubectl apply -k kustomize/postgres`	AWS-Administrator, DBA, Kubernetes-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Bereitstellung.	1. Stellen Sie sicher, dass der Operator bereitgestellt wurde:
	`kubectl get pods -n postgres-operator --selector=postgres-operator.crunchydata.com/instance-set \ -L postgres-operator.crunchydata.com/role`
	2. Stellen Sie sicher, dass die dem Operator-Pod zugeordnete Dienstressource erstellt wurde:
	`kubectl get svc -n postgres-operator`
	Notieren Sie sich in der Befehlsausgabe das primäre Replikat (`primary_pod_name`) und das Leserepli kat (`read_pod_name`). Sie werden diese in den nächsten Schritten verwenden.
		AWS-Administrator, DBA, Kubernetes-Administrator

Überprüfen Sie die Streaming-Replikation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schreiben Sie Daten in das primäre Replikat.	Verwenden Sie die folgenden Befehle, um eine Verbindun	AWS-Administrator, Kubernetes-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	g zum primären PostgreSQ L-Replikat herzustellen und Daten in die Datenbank zu schreiben:
	`kubectl exec -it <primary_pod_name> bash -n postgres-operator`
	`psql`
	`CREATE TABLE customers (firstname text, customer_id serial, date_created timestamp );`
	`\dt`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Vergewissern Sie sich, dass die Read Replica dieselben Daten enthält.	Connect zur PostgreSQ L-Read Replica her und überprüfen Sie, ob die Streaming-Replikation ordnungsgemäß funktioniert:
	`kubectl exec -it {read_pod_name} bash -n postgres-operator`
	`psql`
	`\dt`
	Die Read Replica sollte die Tabelle enthalten, die Sie im vorherigen Schritt im primären Replikat erstellt haben.
		AWS-Administrator, Kubernetes-Administrator

Fehlerbehebung

Problem	Lösung

Der Pod startet nicht.	• Verwenden Sie den folgenden Befehl, um den Pod-Status zu überprüfen:
	`kubectl get pods -n your-namespace`
	• Untersuchen Sie die Protokolle auf Fehler:
	`kubectl logs your-pod-name -n your-namespace`

Problem	Lösung
	• Überprüfen Sie die Pod-Ereignisse auf ungewöhnliche Ereignisse im Zusammenhang mit Ihren Pods: `kubectl describe pod your-pod-name -n your-namespace`

Replikate liegen deutlich hinter der Primärdatenbank zurück.	• Prüfen Sie, ob die Replikation verzögert ist:
	`SELECT * FROM pg_stat_replication;`
	• Stellen Sie sicher, dass Replikate über genügend CPU- und Speicherressourcen verfügen. Überprüfen Sie die Ressourcenlimits:
	`kubectl describe pod your-replica-pod -n your-namespace`
	• Stellen Sie sicher, dass das Speicher-Backend optimal funktioniert. Langsames Festplatten-I/O kann zu Verzögerungen bei der Replikation führen.

Sie haben keinen Einblick in die Leistung und den Zustand des PostgreSQL-Clusters.	• Aktivieren Sie Amazon CloudWatch Logs und stellen Sie sicher, dass die Protokolle CloudWatch zur Analyse an Amazon gesendet werden. Weitere Informationen finden Sie in der Amazon EKS-Dokumentation. • Prüfen Sie **`pg_stat_activity`** : `SELECT * FROM pg_stat_activity;`

Problem	Lösung

Die Replikation funktioniert nicht.	• Überprüfen Sie die Primärkonfiguration, indem Sie sich die Replikationseinstellungen ansehen unter `postgresql.conf` :
	`wal_level = replica`
	`max_wal_senders = 10`
	`wal_keep_size = 64  # or wal_keep_segments in older versions`
	• Stellen Sie sicher, dass dies Replikationsberechtigungen `pg_hba.conf` beinhaltet:
	`host replication replica_user all md5`
	• Überprüfen Sie die Replikatkonfiguration. Vergewissern Sie sich, dass die `recovery.conf` oder die entsprechenden Einstellungen (`standby.signal` und `primary_conninfo`) auf den Replikaten korrekt eingerichtet sind.

Zugehörige Ressourcen

- Amazon Elastic Kubernetes Service (Überblick über Bereitstellungsoptionen auf AWS-Whitepaper)
- AWS CloudFormation(Whitepaper über die Bereitstellungsoptionen auf AWS)
- Erste Schritte mit Amazon EKS — eksctl (Amazon EKS-Benutzerhandbuch)
- Kubectl und eksctl einrichten (Amazon EKS-Benutzerhandbuch)
- Eine Rolle für den OpenID Connect-Verbund erstellen (IAM-Benutzerhandbuch)
- Konfiguration der Einstellungen für das AWS CLI (AWS CLI Benutzerhandbuch)

- Dokumentation zu Crunchy Postgres für Kubernetes
- Crunch & Learn: Crunchy Postgres für Kubernetes 5.0 (Video)

Vereinfachen Sie die Anwendungsauthentifizierung mit gegenseitigem TLS in Amazon ECS mithilfe von Application Load Balancer

Erstellt von Olawale Olaleye (AWS) und Shamanth Devagari (AWS)

Übersicht

Dieses Muster hilft Ihnen dabei, Ihre Anwendungsauthentifizierung zu vereinfachen und Sicherheitsbelastungen mit gegenseitigem TLS in Amazon Elastic Container Service (Amazon ECS) mithilfe von Application Load Balancer (ALB) zu entlasten. Mit ALB können Sie X.509-Client-Zertifikate von authentifizieren. AWS Private Certificate Authority Diese leistungsstarke Kombination trägt zu einer sicheren Kommunikation zwischen Ihren Diensten bei und reduziert so den Bedarf an komplexen Authentifizierungsmechanismen innerhalb Ihrer Anwendungen. Darüber hinaus verwendet das Muster Amazon Elastic Container Registry (Amazon ECR) zum Speichern von Container-Images.

Das Beispiel in diesem Muster verwendet Docker-Bilder aus einer öffentlichen Galerie, um die Beispiel-Workloads zunächst zu erstellen. Anschließend werden neue Docker-Images für die Speicherung in Amazon ECR erstellt. Ziehen Sie als Quelle ein Git-basiertes System wie GitHub, oder Bitbucket in Betracht GitLab, oder verwenden Sie Amazon Simple Storage Service Amazon S3 (Amazon S3). Für die Erstellung der Docker-Images sollten Sie die Verwendung AWS CodeBuild für die nachfolgenden Images in Betracht ziehen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein Aktiv AWS-Konto mit Zugriff auf die Bereitstellung von AWS CloudFormation Stacks. Stellen Sie sicher, dass Sie über AWS Identity and Access Management (IAM-) Benutzer- oder Rollenberechtigungen für die Bereitstellung verfügen. CloudFormation
- AWS Command Line Interface (AWS CLI) installiert. Konfigurieren Sie Ihre AWS Anmeldeinformationen auf Ihrem lokalen Computer oder in Ihrer Umgebung, indem Sie entweder die AWS CLI oder verwenden, indem Sie die Umgebungsvariablen in der `~/.aws/credentials` Datei festlegen.
- OpenSSL installiert.
- Docker installiert.
- Vertrautheit mit den AWS-Services unter Tools beschriebenen Funktionen.
- Kenntnisse von Docker und NGINX.

Einschränkungen

- Mutual TLS für Application Load Balancer unterstützt nur X.509v3-Clientzertifikate. X.509v1-Clientzertifikate werden nicht unterstützt.
- Die CloudFormation Vorlage, die im Code-Repository dieses Musters bereitgestellt wird, beinhaltet nicht die Bereitstellung eines CodeBuild Projekts als Teil des Stacks.
- Einige AWS-Services sind nicht in allen AWS-Regionen verfügbar. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie unter AWS Dienste nach Regionen. Informationen zu bestimmten Endpunkten finden Sie unter Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Produktversionen

- Docker-Version 27.3.1 oder höher
- AWS CLI Version 2.14.5 oder höher

Architektur

Das folgende Diagramm zeigt die Architekturkomponenten für dieses Muster.

Das Diagramm zeigt den folgenden Workflow:

1. Erstellen Sie ein Git-Repository und übertragen Sie den Anwendungscode in das Repository.
2. Erstellen Sie eine private Zertifizierungsstelle (CA) in AWS Private CA.
3. Erstellen Sie ein CodeBuild Projekt. Das CodeBuildproject wird durch Commit-Änderungen ausgelöst und erstellt das Docker-Image und veröffentlicht das erstellte Image in Amazon ECR.
4. Kopieren Sie die Zertifikatskette und den Zertifikatshauptteil von der CA und laden Sie das Zertifikatspaket auf Amazon S3 hoch.
5. Erstellen Sie einen Trust Store mit dem CA-Bundle, das Sie auf Amazon S3 hochgeladen haben. Ordnen Sie den Trust Store den gegenseitigen TLS-Listenern auf dem Application Load Balancer (ALB) zu.
6. Verwenden Sie die private CA, um Client-Zertifikate für die Container-Workloads auszustellen. Erstellen Sie auch ein privates TLS-Zertifikat mit AWS Private CA.
7. Importieren Sie das private TLS-Zertifikat in AWS Certificate Manager (ACM) und verwenden Sie es mit dem ALB.

8. Der Container-Workload in `ServiceTwo` verwendet das ausgestellte Client-Zertifikat, um sich bei der ALB zu authentifizieren, wenn er mit dem Container-Workload in kommuniziert. `ServiceOne`
9. Der Container-Workload in `ServiceOne` verwendet das ausgestellte Client-Zertifikat zur Authentifizierung bei der ALB, wenn er mit dem Container-Workload in kommuniziert. `ServiceTwo`

Automatisierung und Skalierung

Dieses Muster kann vollständig automatisiert werden CloudFormation, indem AWS Cloud Development Kit (AWS CDK) , oder API-Operationen aus einem SDK zur Bereitstellung der AWS Ressourcen verwendet werden.

Sie können AWS CodePipeline damit eine CI/CD-Pipeline (Continuous Integration and Continuous Deployment) implementieren, CodeBuild um den Prozess der Container-Image-Erstellung zu automatisieren und neue Versionen für die Amazon ECS-Cluster-Services bereitzustellen.

Tools

AWS-Services

- AWS Certificate Manager (ACM) unterstützt Sie bei der Erstellung, Speicherung und Erneuerung von öffentlichen und privaten SSL/TLS X.509-Zertifikaten und Schlüsseln, die Ihre Websites und Anwendungen schützen. AWS
- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über und zu verwalten. AWS-Konten AWS-Regionen
- AWS CodeBuildist ein vollständig verwalteter Build-Service, der Ihnen hilft, Quellcode zu kompilieren, Komponententests durchzuführen und Artefakte zu erstellen, die sofort einsatzbereit sind.
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service zum Ausführen, Stoppen und Verwalten von Containern in einem Cluster. Sie können Ihre Aufgaben und Dienste auf einer serverlosen Infrastruktur ausführen, die von AWS Fargate verwaltet wird. Für mehr Kontrolle über Ihre Infrastruktur können Sie Ihre Aufgaben und Dienste alternativ auf einem Cluster von Amazon Elastic Compute Cloud (Amazon EC2) -Instances ausführen, die Sie verwalten.

- Amazon ECS Exec ermöglicht Ihnen die direkte Interaktion mit Containern, ohne zuerst mit dem Host-Container-Betriebssystem interagieren, eingehende Ports öffnen oder SSH-Schlüssel verwalten zu müssen. Sie können ECS Exec verwenden, um Befehle in einem Container auszuführen oder eine Shell für einen Container zu erhalten, der auf einer EC2 Amazon-Instance oder auf AWS Fargate einem läuft.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Traffic auf EC2 Amazon-Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen. ELB überwacht den Zustand seiner registrierten Ziele und leitet den Datenverkehr nur an die fehlerfreien Ziele weiter. ELB skaliert Ihren Load Balancer, wenn sich Ihr eingehender Datenverkehr im Laufe der Zeit ändert. Es kann automatisch auf die meisten Workloads skaliert werden.
- AWS Fargatehilft Ihnen beim Betrieb von Containern, ohne Server oder EC2 Amazon-Instances verwalten zu müssen. Fargate ist sowohl mit Amazon ECS als auch mit Amazon Elastic Kubernetes Service (Amazon EKS) kompatibel. Sie können Ihre Amazon ECS-Aufgaben und -Services mit dem Starttyp Fargate oder einem Fargate-Kapazitätsanbieter ausführen. Verpacken Sie dazu Ihre Anwendung in Containern, geben Sie die CPU- und Speicheranforderungen an, definieren Sie Netzwerk- und IAM-Richtlinien und starten Sie die Anwendung. Jede Fargate-Aufgabe hat ihre eigene Isolationsgrenze und teilt den zugrunde liegenden Kernel, die CPU-Ressourcen, Speicherressourcen oder die elastic network interface nicht mit einer anderen Aufgabe.
- AWS Private Certificate Authorityermöglicht die Erstellung von privaten Zertifizierungsstellenhierarchien (CA), einschließlich Stamm- und untergeordneter Zertifizierungsstellen CAs, ohne dass die Investitions- und Wartungskosten für den Betrieb einer lokalen Zertifizierungsstelle anfallen.

Andere Tools

- Docker ist eine Reihe von Platform-as-a-Service (PaaS) -Produkten, die Virtualisierung auf Betriebssystemebene nutzen, um Software in Containern bereitzustellen.
- GitHub, GitLab, und Bitbucket sind einige der am häufigsten verwendeten Git-basierten Quellcodeverwaltungssysteme, um Quellcodeänderungen zu verfolgen.
- NGINX Open Source ist ein Open-Source-Loadbalancer, ein Inhalts-Cache und ein Webserver. Dieses Muster verwendet es als Webserver.
- OpenSSL ist eine Open-Source-Bibliothek, die Dienste bereitstellt, die von den OpenSSL-Implementierungen von TLS und CMS verwendet werden.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub MTLS-with-Application-Load-Balancer-In-Amazon-ECS verfügbar.

Bewährte Methoden

- Verwenden Sie Amazon ECS Exec, um Befehle auszuführen oder eine Shell für einen Container abzurufen, der auf Fargate läuft. Sie können ECS Exec auch verwenden, um Diagnoseinformationen für das Debuggen zu sammeln.
- Verwenden Sie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten (ACLs), um den eingehenden und ausgehenden Verkehr zwischen den Diensten zu kontrollieren. Fargate-Aufgaben erhalten eine IP-Adresse aus dem konfigurierten Subnetz in Ihrer Virtual Private Cloud (VPC).

Epen

Erstellen Sie das Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Quellcode herunter.	Um den Quellcode dieses Patterns herunterzuladen, forken oder klonen Sie das GitHub MTLS-with-Application-Load-Balancer-In-Amazon-ECS-Repository.	DevOps Ingenieur
Erstellen Sie ein Git-Repository.	Gehen Sie wie folgt vor, um ein Git-Repository zu erstellen, das das Dockerfile und die `buildspec.yaml` Dateien enthält: 1. Erstellen Sie einen Ordner in Ihrer virtuellen Umgebung. Benennen Sie ihn mit Ihrem Projektnamen.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Öffnen Sie ein Terminal auf Ihrem lokalen Computer und navigieren Sie zu diesem Ordner. 3. Um das MTLS-with-Application-Load-Balancer-In-Amazon-ECS-Repository in Ihr Projektverzeichnis zu klonen, geben Sie den folgenden Befehl ein: `git clone https://github.com/aws-samples/mTLS-with-Application-Load-Balancer-in-Amazon-ECS.git`	

CA erstellen und Zertifikate generieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine private CA in AWS Private CA.	Um eine private Zertifizierungsstelle (CA) zu erstellen, führen Sie die folgenden Befehle in Ihrem Terminal aus. Ersetzen Sie die Werte in den Beispielvariablen durch Ihre eigenen Werte. `export AWS_DEFAULT_REGION="us-west-2"`	DevOps Ingenieur, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	``
	export SERVICES_
	DOMAIN="www.exampl
	e.com"
	
	export ROOT_CA_A
	RN=`aws acm-pca create-
	certificate-authority
	 \
	    --certificate-auth
	ority-type ROOT \
	    --certificate-auth
	ority-configuration \
	    "KeyAlgorithm=RSA_
	2048,
	    SigningAlgorithm=S
	HA256WITHRSA,
	    Subject={
	        Country=US,
	        State=WA,
	        Locality=
	Seattle,
	        Organizat
	ion=Build on AWS,
	        Organizat
	ionalUnit=mTLS Amazon
	 ECS and ALB Example,
	        CommonName=
	${SERVICES_DOMAIN}}" \
	        --query
	 CertificateAuthori
	tyArn --output text`
	``
	
	Weitere Informationen finden Sie AWS Private CA in der AWS Dokumentation unter Eine private Zertifizierungsstelle erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen und installieren Sie Ihr privates CA-Zertifikat.	Um ein Zertifikat für Ihre private Root-CA zu erstellen und zu installieren, führen Sie die folgenden Befehle in Ihrem Terminal aus:
	
	1. Generieren Sie eine Zertifikatsignieranforderung (CSR).
	
	`ROOT_CA_CSR=`aws acm-pca get-certificate-authority-csr \ --certificate-authority-arn ${ROOT_CA_ARN} \ --query Csr --output text``
	
	2. Stellen Sie das Stammzert ifikat aus.
	
	`AWS_CLI_VERSION=$( aws --version 2>&1 | cut -d/ -f2 | cut -d. -f1) [[ ${AWS_CLI_VERSION} -gt 1 ]] && ROOT_CA_CSR="$(echo ${ROOT_CA_CSR} | base64)" ROOT_CA_CERT_ARN= `aws acm-pca issue-certificate \ --certificate-authority-arn ${ROOT_CA_ARN} \ --template-arn arn:aws:acm-pca:::`
		AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`template/RootCACertificate/V1 \` `--signing-algorithm SHA256WITHRSA \` `--validity Value=10,Type=YEARS \` `--csr "${ROOT_CA_CSR}" \` `--query CertificateArn --output text` 3. Rufen Sie das Stammzertifikat ab. `ROOT_CA_CERT=`aws acm-pca get-certificate \` `--certificate-arn ${ROOT_CA_CERT_ARN} \` `--certificate-authority-arn ${ROOT_CA_ARN} \` `--query Certificate --output text`  `# store for later use` `aws acm-pca get-certificate \` `--certificate-arn ${ROOT_CA_CERT_ARN} \` `--certificate-authority-arn ${ROOT_CA_ARN} \` `--query Certificate --output text > ca-cert.pem`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	4. Importieren Sie das Root-CA-Zertifikat, um es auf der CA zu installieren.
	
	`[[ ${AWS_CLI_VERSION} -gt 1 ]] && ROOT_CA_CERT="$(echo ${ROOT_CA_CERT} | base64)"`
	
	`aws acm-pca import-certificate-authority-certificate \ --certificate-authority-arn $ROOT_CA_ARN \ --certificate "${ROOT_CA_CERT}"`
	
	Weitere Informationen finden Sie in der AWS Dokumentation unter Installation des CA-Zertifikats.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fordern Sie ein verwaltetes Zertifikat an.	Verwenden Sie den folgenden Befehl AWS Certificate Manager , um ein privates Zertifikat zur Verwendung mit Ihrem privaten ALB anzuforderrn: `export TLS_CERTIFICATE_ARN=`aws acm request-certificate \ --domain-name "*.${DOMAIN_DOMAIN}" \ --certificate-authority-arn ${ROOT_CA_ARN} \ --query CertificateArn --output text``	DevOps Ingenieur, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Verwenden Sie die private CA, um ein Client-Zertifikat auszustellen.	• Verwenden Sie den folgenden AWS CLI Befehl, um eine Certificate Signing Request (CSR) für die beiden Dienste zu erstellen:
	
	`openssl req -out client_csr1.pem -new -newkey rsa:2048 -nodes -keyout client_private-key 1.pem`
	
	`openssl req -out client_csr2.pem -new -newkey rsa:2048 -nodes -keyout client_private-key 2.pem`
	
	Dieser Befehl gibt die CSR und den privaten Schlüssel für die beiden Dienste zurück.
	
	• Um ein Zertifikat für die Dienste auszustellen, führen Sie die folgenden Befehle aus, um die von Ihnen erstellte private Zertifizi erungsstelle zu verwenden:
	
	`SERVICE_ONE_CERT_ARN=`aws acm-pca issue-certificate \`
		DevOps Ingenieur, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--certificate-authority-arn ${ROOT_CA_ARN} \` `--csr fileb://client_csr1.pem \` `--signing-algorithm "SHA256WITHRSA" \` `--validity Value=5,Type="YEARS" --query CertificateArn --output text` `echo "SERVICE_ONE_CERT_ARN: ${SERVICE_ONE_CERT_ARN}"` `aws acm-pca get-certificate \` `--certificate-authority-arn ${ROOT_CA_ARN} \` `--certificate-arn ${SERVICE_ONE_CERT_ARN} \` `| jq -r '.Certificate' > client_cert1.cert` `SERVICE_TWO_CERT_ARN=`aws acm-pca issue-certificate \` `--certificate-authority-arn ${ROOT_CA_ARN} \` `--csr fileb://client_csr2.pem \` `--signing-algorithm "SHA256WITHRSA" \` `--validity Value=5,Type="YEARS" --query CertificateArn --output text`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	``
	echo "SERVICE_TWO_CERT_
	ARN: ${SERVICE
	_TWO_CERT_ARN}"
	
	aws acm-pca get-certi
	ficate \
	    --certificate-auth
	ority-arn ${ROOT_CA
	_ARN} \
	    --certificate-arn
	 ${SERVICE_TWO_CERT
	_ARN} \
	     | jq -r '.Certifi
	cate' > client_ce
	rt2.cert
	``
	
	Weitere Informationen finden Sie in der AWS Dokumentation unter Ausstellen von privaten Endentitätszertifikaten.	

Bereitstellung von AWS-Services

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereitstellung AWS-Services mit der CloudFormation Vorlage.	Verwenden Sie die Vorlage, um die Virtual Private Cloud (VPC), den Amazon ECS-Cluster, die Amazon ECS-Services, den Application Load Balancer und das Amazon Elastic Container Registry (Amazon ECR)	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bereitzustellen. CloudFormation	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Holen Sie sich Variablen.	Stellen Sie sicher, dass Sie über einen Amazon ECS-Cluster verfügen, auf dem zwei Dienste ausgeführt werden. Verwenden Sie die folgenden Befehle, um die Ressourcendetails abzurufen und als Variablen zu speichern:
	`export LoadBalancerDNS=$(aws cloudformation describe-stacks --stack-name ecs-mtls \ --output text \ --query 'Stacks[0].Outputs[?OutputKey==`LoadBalancerDNS`].OutputValue')`
	`export ECRRepositoryUri=$(aws cloudformation describe-stacks --stack-name ecs-mtls \ --output text \ --query 'Stacks[0].Outputs[?OutputKey==`ECRRepositoryUri`].OutputValue')`
	`export ECRRepositoryServiceOneUri=$(aws cloudformation describe-stacks --stack-name ecs-mtls \ --output text \ --query 'Stacks[0].Outputs[?OutputKey==`ECRRepository`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ServiceOneUri`].Ou tputValue')  export ECRReposi toryServiceTwoUri= $(aws cloudformation  describe-stacks -- stack-name ecs-mtls \ --output text \ --query 'Stacks[0 ].Outputs[?OutputK ey==`ECRRepository ServiceTwoUri`].Ou tputValue')  export ClusterName= $(aws cloudformation  describe-stacks -- stack-name ecs-mtls \ --output text \ --query 'Stacks[0 ].Outputs[?OutputK ey==`ClusterName`] .OutputValue')  export BucketName= $(aws cloudformation  describe-stacks -- stack-name ecs-mtls \ --output text \ --query 'Stacks[0 ].Outputs[?OutputK ey==`BucketName`]. OutputValue') export Service1L istenerArn=$(aws cloudformation describe-stacks -- stack-name ecs-mtls \ --output text \	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`--query 'Stacks[0 ].Outputs[?OutputK ey==`Service1Liste nerArn`].OutputVal ue')`
	
	`export Service2L istenerArn=$(aws cloudformation describe-stacks -- stack-name ecs-mtls \ --output text \ --query 'Stacks[0 ].Outputs[?OutputK ey==`Service2Liste nerArn`].OutputVal ue')`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein CodeBuild Projekt.	Gehen Sie wie folgt vor, um ein CodeBuild Projekt zur Erstellung der Docker-Images für Ihre Amazon ECS-Services zu verwenden: 1. Melden Sie sich bei AWS Management Consolehttps://console.aws.amazon.com/codesuite/codebuild/ an und öffnen Sie die CodeBuild Konsole. 2. Erstellt ein neues Projekt. Wählen Sie für Source das Git-Repository aus, das Sie erstellt haben. Informationen zu verschiedenen Arten der Git-Repository-Integration finden Sie in der AWS Dokumentation unter Arbeiten mit Verbindungen. 3. Vergewissern Sie sich, dass der privilegierte Modus aktiviert ist. Um Docker-Images zu erstellen, ist dieser Modus erforderlich. Andernfalls wird das Image nicht erfolgreich erstellt. 4. Verwenden Sie die benutzerdefinierte `buildspec.yaml` Datei, die für jeden Dienst gemeinsam genutzt wird.	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Geben Sie Werte für den Projektnamen und die Beschreibung an. Weitere Informationen finden Sie AWS CodeBuild in der AWS Dokumentation unter Erstellen eines Build-Projekts.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Docker-Images.	Sie können es verwenden CodeBuild , um den Image-Erstellungsprozess durchzuführen. CodeBuild benötigt Berechtigungen, um mit Amazon ECR zu interagieren und mit Amazon S3 zu arbeiten.
	
	Im Rahmen des Prozesses wird das Docker-Image erstellt und in die Amazon ECR-Registrierung übertragen. Einzelheiten zur Vorlage und zum Code finden Sie unter Zusätzliche Informationen.
	
	(Optional) Verwenden Sie den folgenden Befehl, um lokal zu Testzwecken zu erstellen:
	
	`# login to ECR`
	`aws ecr get-login`
	`-password | docker`
	`login --username`
	`AWS --password-stdin`
	`$ECRRepositoryUri`
	
	`# build image for`
	`service one`
	`cd /service1`
	`aws s3 cp s3://$Buc`
	`ketName/serviceone/`
	`service1/ --recursive`
	`docker build -t`
	`$ECRRepositoryServ`
	`iceOneUri .`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`docker push $ECRRepos itoryServiceOneUri`
	
	`# build image for service two`
	`cd ../service2`
	`aws s3 cp s3://$Buc ketName/servicetwo/ service2/ --recursive`
	`docker build -t $ECRRepositoryServ iceTwoUri .`
	`docker push $ECRRepos itoryServiceTwoUri`	

Mutual TLS aktivieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das CA-Zertifikat auf Amazon S3 hoch.	Verwenden Sie den folgenden Beispielbefehl, um das CA-Zertifikat in den Amazon S3 S3-Bucket hochzuladen: `aws s3 cp ca-cert.pem s3://$BucketName/a cm-trust-store/`	AWS DevOps, DevOps Ingenieur
Erstellen Sie den Trust Store.	Verwenden Sie den folgenden Beispielbefehl, um den Trust Store zu erstellen: `TrustStoreArn=`aws elbv2 create-trust-store --name acm-pca-t rust-certs \`	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--ca-certificates-bundle-s3-bucket $BucketName \ --ca-certificates-bundle-s3-key acm-trust-store/ca-cert.pem --query 'TrustStores[].TrustStoreArn' --output text`	

Laden Sie Kundenzertifikate hoch.	Verwenden Sie den folgenden Beispielbefehl, um Client-Zertifikate für Docker-Images auf Amazon S3 hochzuladen:
	`# for service one aws s3 cp client_cert1.cert s3://$BucketName/serviceone/ aws s3 cp client_private-key1.pem s3://$BucketName/serviceone/`
	`# for service two aws s3 cp client_cert2.cert s3://$BucketName/servicetwo/ aws s3 cp client_private-key2.pem s3://$BucketName/servicetwo/`
		AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Ändern Sie den Listener.	Um Mutual TLS auf dem ALB zu aktivieren, ändern Sie die HTTPS-Listener mit den folgenden Befehlen:
	
	`aws elbv2 modify-listener \`
	`  --listener-arn $Service1ListenerArn \`
	`  --certificates CertificateArn=$TLS_CERTIFICATE_ARN_TWO \`
	`  --ssl-policy ELBSecurityPolicy-2016-08 \`
	`  --protocol HTTPS \`
	`  --port 8080 \`
	`  --mutual-authentication Mode=verify,TrustStoreArn=$TrustStoreArn,IgnoreClientCertificateExpiry=false`
	
	`aws elbv2 modify-listener \`
	`  --listener-arn $Service2ListenerArn \`
	`  --certificates CertificateArn=$TLS_CERTIFICATE_ARN_TWO \`
	`  --ssl-policy ELBSecurityPolicy-2016-08 \`
	`  --protocol HTTPS \`
	`  --port 8090 \`
		AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--mutual-authentication Mode=verify,TrustStoreArn=$TrustStoreArn,IgnoreClientCertificateExpiry=false` Weitere Informationen finden Sie in der AWS Dokumentation unter Konfiguration von gegenseitigem TLS auf einem Application Load Balancer.	

Aktualisieren Sie die Dienste

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Amazon ECS-Aufgabendefinition.	Um die Amazon ECS-Aufgabendefinition zu aktualisieren, ändern Sie den `image` Parameter in der neuen Version. Um die Werte für die jeweiligen Services abzurufen, aktualisieren Sie die Aufgabendefinitionen mit dem neuen Docker-Images-URI, den Sie in den vorherigen Schritten erstellt haben: oder `echo $ECRRepositoryServiceOneUri echo $ECRRepositoryServiceTwoUri`	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"containerDefiniti
	ons": [
	{
	"name":
	"nginx",
	"image":
	"public.ecr.aws/ng
	inx/nginx:latest",
	# <----- change to new
	Uri
	"cpu": 0,</pre>
	Weitere Informationen finden Sie in der AWS Dokumenta tion unter Aktualisieren einer Amazon ECS-Aufgabendefini tion mithilfe der Konsole.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie den Amazon ECS-Service.	Aktualisieren Sie den Service mit der neuesten Aufgabend efinition. Diese Aufgabend efinition ist der Entwurf für die neu erstellten Docker-Im ages und enthält das Client-Ze rtifikat, das für die gegenseit ige TLS-Authentifizierung erforderlich ist. Gehen Sie wie folgt vor, um den Dienst zu aktualisieren: 1. Öffnen Sie die Amazon ECS-Konsole auf https://c onsole.aws.amazon.com/ ecs/Version 2. 2. Wählen Sie auf der Cluster-Seite den Cluster aus. 3. Aktivieren Sie auf der Seite mit den Cluster-Details im Abschnitt Services das Kontrollkästchen neben dem Service und wählen Sie dann Update aus. 4. Wählen Sie Force new deployment (Neue Bereitste llung erzwingen) aus, damit Ihr Service eine neue Bereitstellung startet. 5. Wählen Sie unter Aufgabendefinition die Aufgabendefinitionsfamilie	AWS-Administrator, AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und die neueste Version aus. 6. Wählen Sie Aktualisieren. Wiederholen Sie die Schritte für den anderen Dienst.	

Greifen Sie auf die Anwendung zu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopieren Sie die Anwendung s-URL.	Verwenden Sie die Amazon ECS-Konsole, um die Aufgabe anzusehen. Wenn der Aufgabenstatus auf Wird ausgeführt aktualisiert wurde, wählen Sie die Aufgabe aus. Kopieren Sie im Abschnitt Aufgabe die Aufgaben-ID.	AWS-Administrator, AWS DevOps

Testen Sie Ihre Anwendung.	Um Ihre Anwendung zu testen, verwenden Sie ECS Exec, um auf die Aufgaben zuzugreifen.
	1. Verwenden Sie für Service One den folgenden Befehl:
	`container="nginx"`
	`ECS_EXEC_TASK_ARN="<TASK ARN>"`
	`aws ecs execute-command --cluster $ClusterName \`
		AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>--task $ECS_EXEC
	_TASK_ARN \
	--container
	$container \
	--interactive \
	--command "/bin/
	bash"</pre>
	2. Verwenden Sie im Container der Aufgabe Service One den folgenden Befehl, um den internen Load Balancer `url` und den Listener-Port einzugeben, der auf Service Two verweist. Geben Sie dann den Pfad zum Client-Zertifikat an, um die Anwendung zu testen:
	<pre>curl -kvs https://<
	internal-alb-url>:
	8090 --key /usr/loca
	l/share/ca-certifi
	cates/client.key
	--cert /usr/loca
	l/share/ca-certifi
	cates/client.crt</pre>
	3. Geben Sie im Container der zweiten Dienstaufgabe den folgenden Befehl ein, um den internen Load Balancer `url` und den Listener-Port einzugeben, der auf Service One verweist. Geben Sie dann den Pfad	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zum Client-Zertifikat an, um die Anwendung zu testen: `curl -kvs https://<internal-alb-url>:8080 --key /usr/local/share/ca-certificates/client.key --cert /usr/local/share/ca-certificates/client.crt` **Note** Das `-k` Flag in den curl-Befehlen (als Teil von `-kvs`) deaktiviert die SSL-Zertifikatsvalidierung. Sie können dieses Kennzeichen entfernen, wenn Sie ein SSL-Zertifikat verwenden, das Ihrem Domainnamen entspricht, um eine ordnungsgemäße Zertifikatsvalidierung zu ermöglichen.	

Zugehörige Ressourcen

Amazon ECS-Dokumentation

- Erstellen einer Amazon ECS-Aufgabendefinition mithilfe der Konsole
- Erstellen eines Container-Images zur Verwendung auf Amazon ECS
- Amazon-ECS-Cluster
- Amazon ECS für AWS Fargate
- Bewährte Methoden für Amazon ECS-Netzwerke
- Parameter der Amazon ECS-Servicedefinition

Andere AWS Ressourcen

- Wie verwende ich AWS private CA, um mTLS auf dem Application Load Balancer zu konfigurieren? ()AWS re:Post

Zusätzliche Informationen

Das Dockerfile bearbeiten

Der folgende Code zeigt die Befehle, die Sie im Dockerfile für Service 1 bearbeiten:

```
FROM public.ecr.aws/nginx/nginx:latest
WORKDIR /usr/share/nginx/html
RUN echo "Returning response from Service 1: Ok" > /usr/share/nginx/html/index.html
ADD client_cert1.cert client_private-key1.pem /usr/local/share/ca-certificates/
RUN chmod -R 400 /usr/local/share/ca-certificates/
```

Der folgende Code zeigt die Befehle, die Sie im Dockerfile für Dienst 2 bearbeiten:

```
FROM public.ecr.aws/nginx/nginx:latest
WORKDIR /usr/share/nginx/html
RUN echo "Returning response from Service 2: Ok" > /usr/share/nginx/html/index.html
ADD client_cert2.cert client_private-key2.pem /usr/local/share/ca-certificates/
RUN chmod -R 400 /usr/local/share/ca-certificates/
```

Wenn Sie die Docker-Images mit erstellen, verwendet die `buildspec` Datei die CodeBuild Build-Nummer CodeBuild, um Image-Versionen eindeutig als Tag-Wert zu identifizieren. Sie können die `buildspec` Datei an Ihre Anforderungen anpassen, wie im folgenden `buildspec` benutzerdefinierten Code gezeigt:

```
version: 0.2
```

```
phases:
  pre_build:
    commands:
      - echo Logging in to Amazon ECR...
      - aws ecr get-login-password --region $AWS_DEFAULT_REGION | docker login --
username AWS --password-stdin $ECR_REPOSITORY_URI
      - COMMIT_HASH=$(echo $CODEBUILD_RESOLVED_SOURCE_VERSION | cut -c 1-7)
      - IMAGE_TAG=${COMMIT_HASH:=latest}
  build:
    commands:
        # change the S3 path depending on the service
      - aws s3 cp s3://$YOUR_S3_BUCKET_NAME/serviceone/ $CodeBuild_SRC_DIR/ --
recursive
      - echo Build started on `date`
      - echo Building the Docker image...
      - docker build -t $ECR_REPOSITORY_URI:latest .
      - docker tag $ECR_REPOSITORY_URI:latest $ECR_REPOSITORY_URI:$IMAGE_TAG
  post_build:
    commands:
      - echo Build completed on `date`
      - echo Pushing the Docker images...
      - docker push $ECR_REPOSITORY_URI:latest
      - docker push $ECR_REPOSITORY_URI:$IMAGE_TAG
      - echo Writing image definitions file...
      # for ECS deployment reference
      - printf '[{"name":"%s","imageUri":"%s"}]' $CONTAINER_NAME $ECR_REPOSITORY_URI:
$IMAGE_TAG > imagedefinitions.json

artifacts:
  files:
    - imagedefinitions.json
```

Mehr Muster

- Beurteilen Sie die Anwendungsbereitschaft für die Migration in die AWS-Cloud mithilfe von CAST Highlight
- Automatisieren Sie das Löschen von AWS CloudFormation Stacks und zugehörigen Ressourcen
- Automatisieren Sie das dynamische Pipeline-Management für die Bereitstellung von Hotfix-Lösungen in Gitflow-Umgebungen mithilfe von und AWS Service CatalogAWS CodePipeline
- Automatisches Erstellen von CI/CD-Pipelines und Amazon ECS-Clustern für Microservices mithilfe von AWS CDK
- Erstellen und übertragen Sie Docker-Images mithilfe von GitHub Actions und Terraform auf Amazon ECR
- Containerisieren Sie Mainframe-Workloads, die von Blu Age modernisiert wurden
- Erstellen Sie einen benutzerdefinierten Protokollparser für Amazon ECS mithilfe eines Firelens-Protokollrouters
- Stellen Sie eine CI/CD-Pipeline für Java-Microservices auf Amazon ECS bereit
- Stellen Sie mithilfe eines EC2 Instanzprofils einen Amazon EKS-Cluster aus AWS Cloud9 bereit
- Stellen Sie mithilfe von Terraform eine Umgebung für containerisierte Blu Age-Anwendungen bereit
- Stellen Sie mithilfe einer Inferenz-Pipeline in Amazon Vorverarbeitungslogik in einem ML-Modell an einem einzigen Endpunkt bereit SageMaker
- Verwalten Sie Blau/Grün-Bereitstellungen von Microservices für mehrere Konten und Regionen mithilfe von AWS-Code-Services und AWS KMS-Regionsschlüsseln für mehrere Regionen
- Verwalten Sie lokale Containeranwendungen, indem Sie Amazon ECS Anywhere mit dem AWS CDK einrichten
- Migrieren Sie von Oracle GlassFish zu AWS Elastic Beanstalk
- Migrieren Sie von Oracle WebLogic zu Apache Tomcat (ToMEE) auf Amazon ECS
- Richten Sie einen nutzbaren Mindestdatenraum für die gemeinsame Nutzung von Daten zwischen Organisationen ein
- Modernisieren Sie ASP.NET Web Forms-Anwendungen auf AWS
- Überwachen Sie Amazon ECR-Repositorys mit AWS und AWS CloudFormation Config auf Platzhalterberechtigungen
- Überwachen Sie die Anwendungsaktivität mithilfe von CloudWatch Logs Insights
- Richten Sie mithilfe von AWS CDK eine CI/CD-Pipeline für Hybrid-Workloads auf Amazon ECS Anywhere ein und GitLab

- Richten Sie ein Helm v3-Chart-Repository in Amazon S3 ein
- Richten Sie die end-to-end Verschlüsselung für Anwendungen auf Amazon EKS mithilfe von cert-manager und Let's Encrypt ein
- Vereinfachen Sie die Bereitstellung von Amazon EKS-Anwendungen für mehrere Mandanten mithilfe von Flux
- Optimieren Sie mithilfe von SageMaker KI und Hydra Workflows für maschinelles Lernen — von der lokalen Entwicklung bis hin zu skalierbaren Experimenten
- Strukturieren Sie ein Python-Projekt in hexagonaler Architektur mit AWS Lambda
- Testen Sie die AWS Infrastruktur mithilfe LocalStack von Terraform-Tests
- Trainieren und implementieren Sie ein benutzerdefiniertes GPU-unterstütztes ML-Modell auf Amazon SageMaker
- Koordinieren Sie die Ressourcenabhängigkeit und die Aufgabenausführung mithilfe des AWS Fargate WaitCondition Hook-Konstrukts
- Verwenden Sie Amazon Bedrock-Agenten, um die Erstellung von Zugriffskontrollen in Amazon EKS durch textbasierte Eingabeaufforderungen zu automatisieren

Serverless

Themen

- Erstellen Sie mithilfe von AWS Amplify eine serverlose mobile React Native-App
- Mandanten für mehrere SaaS-Produkte auf einer einzigen Steuerebene verwalten
- Erstellen Sie eine kontoübergreifende EventBridge Amazon-Verbindung in einer Organisation
- Stellen Sie DynamoDB-Datensätze mithilfe von Kinesis Data Streams und Firehose an Amazon S3 bereit mit AWS CDK
- Implementieren Sie eine pfadbasierte API-Versionierung mithilfe benutzerdefinierter Domains in Amazon API Gateway
- Importieren Sie die psycopg2-Bibliothek, AWS Lambda um mit Ihrer PostgreSQL-Datenbank zu interagieren
- Integrieren Sie Amazon API Gateway mit Amazon SQS, um asynchrones REST zu handhaben APIs
- Ereignisse asynchron mit Amazon API Gateway und AWS Lambda verarbeiten
- Ereignisse asynchron mit Amazon API Gateway und Amazon DynamoDB Streams verarbeiten
- Ereignisse asynchron mit Amazon API Gateway, Amazon SQS und AWS Fargate verarbeiten
- Führen Sie AWS Systems Manager Automation Automation-Aufgaben synchron über AWS Step Functions aus
- parallel Lesevorgänge von S3-Objekten mithilfe von Python in einer AWS Lambda Funktion ausführen
- Senden Sie Telemetriedaten von AWS Lambda zu OpenSearch für Analysen und Visualisierungen in Echtzeit
- Richten Sie einen serverlosen Mobilfunkrouter für eine zellenbasierte Architektur ein
- Richten Sie den privaten Zugriff auf einen Amazon S3 S3-Bucket über einen VPC-Endpunkt ein
- Problembehebung bei Zuständen AWS Step Functions mithilfe von Amazon Bedrock
- Verketten Sie AWS-Services mithilfe eines serverlosen Ansatzes
- Mehr Muster

Erstellen Sie mithilfe von AWS Amplify eine serverlose mobile React Native-App

Erstellt von Deekshitulu Pentakota (AWS)

Übersicht

Dieses Muster zeigt, wie Sie mithilfe von AWS Amplify und den folgenden AWS-Services ein serverloses Backend für eine mobile React Native-App erstellen:

- AWS AppSync
- Amazon Cognito
- Amazon-DynamoDB

Nachdem Sie das Backend der App mithilfe von Amplify konfiguriert und bereitgestellt haben, authentifiziert Amazon Cognito App-Benutzer und autorisiert sie für den Zugriff auf die App. AWS interagiert AppSync dann mit der Frontend-App und mit einer DynamoDB-Backend-Tabelle, um Daten zu erstellen und abzurufen.

> **Note**
>
> Dieses Muster verwendet eine einfache App „ToDoList“ als Beispiel, aber Sie können ein ähnliches Verfahren verwenden, um jede beliebige mobile React Native-App zu erstellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Amplify Command Line Interface (Amplify CLI), installiert und konfiguriert
- XCode (jede Version)
- Microsoft Visual Studio (jede Version, jeder Code-Editor, jeder Texteditor)
- Vertrautheit mit Amplify
- Vertrautheit mit Amazon Cognito

- Vertrautheit mit AWS AppSync
- Vertrautheit mit DynamoDB
- Vertrautheit mit Node.js
- Vertrautheit mit npm
- Vertrautheit mit React und React Native
- Vertrautheit mit JavaScript und ECMAScript 6 () ES6
- Vertrautheit mit GraphQL

Architektur

Das folgende Diagramm zeigt eine Beispielarchitektur für die Ausführung des Backends einer mobilen React Native-App in der AWS-Cloud:

Das Diagramm zeigt die folgende Architektur:

1. Amazon Cognito authentifiziert App-Benutzer und autorisiert sie, auf die App zuzugreifen.
2. Um Daten zu erstellen und abzurufen, AppSync verwendet AWS eine GraphQL-API, um mit der Frontend-App und einer Backend-DynamoDB-Tabelle zu interagieren.

Tools

AWS-Services

- AWS Amplify ist eine Reihe von speziell entwickelten Tools und Funktionen, mit denen Frontend-Web- und Mobilentwickler schnell Full-Stack-Anwendungen auf AWS erstellen können.
- AWS AppSync bietet eine skalierbare GraphQL-Schnittstelle, mit der Anwendungsentwickler Daten aus mehreren Quellen kombinieren können, darunter Amazon DynamoDB, AWS Lambda und HTTP. APIs
- Amazon Cognito bietet Authentifizierung, Autorisierung und Benutzerverwaltung für Web- und mobile Apps.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.

Code

Der Code für die Beispielanwendung, die in diesem Muster verwendet wird, ist im ios-todo-app Repository GitHub aws-amplify-react-native- verfügbar. Um die Beispieldateien zu verwenden, folgen Sie den Anweisungen im Abschnitt Epics dieses Musters.

Epen

Erstelle deine React Native-App und führe sie aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine React Native-Entwicklungsumgebung ein.	Anweisungen finden Sie unter Einrichten der Entwicklungsumgebung in der React Native-Dokumentation.	App-Developer

Erstellen Sie die mobile ToDoList React Native-App und führen Sie sie im iOS-Simulator aus.	1. Erstellen Sie ein neues React Native-Projektverzeichnis für mobile Apps in Ihrer lokalen Umgebung, indem Sie den folgenden Befehl in einem neuen Terminalfenster ausführen:
	`npx react-native init ToDoListAmplify`
	2. Navigieren Sie zum Stammverzeichnis des Projekts, indem Sie den folgenden Befehl ausführen:
	`cd ToDoListAmplify`
	3. Führen Sie die App aus, indem Sie den folgenden Befehl ausführen:
	`npx react-native run-ios`
		App-Developer

Initialisieren Sie eine neue Backend-Umgebung für die App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Backend-Dienste, die zur Unterstützung der App in Amplify erforderlich sind.	1. Führen Sie in Ihrer lokalen Umgebung den folgenden Befehl im Stammverzeichnis des Projekts aus () ToDoListAmplifyaus:
	`amplify init`
	2. Es wird eine Aufforderung angezeigt, in der Sie aufgefordert werden, Informationen zur App anzugeben. Geben Sie die erforderlichen Informationen basierend auf Ihrem Anwendungsfall ein. Drücken Sie anschließend die Eingabetaste.
	
	Wenden Sie für das in diesem Muster verwendete ToDoList App-Setup die folgende Beispielkonfiguration an.
	
	Beispiel für die Konfiguration der React Native Amplify App
	`? Name: ToDoListAmplify`
	`? Environment: dev`
	`? Default editor: Visual Studio Code`
	`? App type: javascript`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	``` ? Javascript framework : react-native ? Source Directory Path: src ? Distribution Directory Path: / ? Build Command: npm run-script build ? Start Command: npm run-script start ? Select the authentic ation method you want to use: AWS profile ? Please choose the profile you want to use: default ```	
	Weitere Informationen finden Sie unter Erstellen eines neuen Amplify-Backends in der Amplify Dev Center-Dokumentation.	
	Note Der `amplify init` Befehl stellt mithilfe von AWS die folgenden Ressourcen bereit CloudFormation:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• AWS Identity and Access Management (IAM) -Rollen für authentifizierte und nicht authentifizierte Benutzer (Auth Role und Unauth Role) • Ein Amazon Simple Storage Service (Amazon S3) - Bucket für die Bereitstellung (für die Beispiel-App dieses Musters, Amplify-Meta.json) • Eine Backend-Umgebung in Amplify Hosting	

Fügen Sie Ihrer Amplify React Native-App die Amazon Cognito Cognito-Authentifizierung hinzu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon Cognito Cognito-Authentifizierungsservice.	1. Führen Sie in Ihrer lokalen Umgebung den folgenden Befehl im Stammverzeichnis des Projekts aus (ToDoListAmplify) aus: `amplify add auth` 2. Es wird eine Aufforderung angezeigt, in der Sie aufgefordert werden, Informationen zu den Konfigurationseinstellungen des Authentifizierungsdienstes einzugeben. Geben Sie die erforderlichen Informationen	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	basierend auf Ihrem Anwendungsfall ein. Drücken Sie anschließend die Eingabetaste.
	
	Wenden Sie für das in diesem Muster verwendete ToDoList App-Setup die folgende Beispielkonfiguration an.
	
	Beispiel für Konfigurationseinstellungen für den Authentifizierungsdienst
	
	`? Do you want to use the default authentication and security configuration? \`
	`Default configuration`
	
	`? How do you want users to be able to sign in? \`
	`Username`
	
	`? Do you want to configure advanced settings? \`
	`No, I am done`
	
	Note
	Der `amplify add auth` Befehl erstellt die erforderlichen Ordner, Dateien und Abhängigkeitsdatei	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en in einem lokalen Ordner (Amplify) im Stammverzeichnis des Projekts. Für das in diesem Muster verwendete ToDoList App-Setup wird die Datei aws-exports.js zu diesem Zweck erstellt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie den Amazon Cognito-Service in der AWS-Cloud bereit.	1. Führen Sie im Stammverz eichnis des Projekts den folgenden Amplify CLI-Befehl aus:
	
	`amplify push`
	
	2. Eine Aufforderung zur Bestätigung der Bereitste llung wird angezeigt. Geben Sie Ja ein. Drücken Sie anschließend die Eingabeta ste.
	
	Note
	Um die in Ihrem Projekt bereitgestellten Dienste zu sehen, rufen Sie die Amplify-K onsole auf, indem Sie den folgenden Befehl ausführen:
	
	`amplify console`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie die erforderlichen Amplify-Bibliotheken für React Native und die CocoaPods Abhängigkeiten für iOS.	1. Installieren Sie die erforderlichen Amplify-Open-Source-Clientbibliotheken, indem Sie den folgenden Befehl im Stammverzeichnis des Projekts ausführen:
	`npm install aws-amplify aws-amplify-react-native \ amazon-cognito-identity-js @react-native-community/netinfo \ @react-native-async-storage/async-storage`
	2. Installieren Sie die erforderlichen CocoaPods Abhängigkeiten für iOS, indem Sie den folgenden Befehl ausführen:
	`npx pod-install`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Importieren und konfigurieren Sie den Amplify-Dienst.	Importieren und laden Sie in der Einstiegspunktdatei der App (z. B. App.js) die Konfigurationsdatei des Amplify-Dienstes, indem Sie die folgenden Codezeilen eingeben:
	`import Amplify from 'aws-amplify'`
	`import config from './src/aws-exports'`
	`Amplify.configure(config)`
	Note
	Wenn Sie nach dem Import des Amplify-Dienstes in die Einstiegspunktdatei der App eine Fehlermeldung erhalten, beenden Sie die App. Öffnen Sie dann die ToDoListAmplifyDatei .xcworkspace aus dem iOS-Ordner des Projekts, wählen Sie sie aus und führen Sie die App aus.
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Einstiegspunktdatei Ihrer App, um die WithAuthenticator-Komponente höherer Ordnung (HOC) zu verwenden.	**Note** Der `withAuthenticator` HOC bietet Workflows zum Anmelden, Registrieren und Vergessen von Passwörtern in Ihrer App, wobei nur wenige Codezeilen verwendet werden. Weitere Informationen finden Sie unter Option 1: Verwenden Sie vorgefertigte UI-Komponenten im Amplify Dev Center. Außerdem Komponenten höherer Ordnung in der React-Dokumentation. 1. Importieren Sie den `withAuthenticator` HOC in der Einstiegspunktdatei der App (z. B. App.js), indem Sie die folgenden Codezeilen eingeben: `import { withAuthenticator } from 'aws-amplify-react-native'`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	2. Exportieren Sie den WithAuthenticator-HOC, indem Sie den folgenden Code eingeben:
	
	`export default withAuthenticator(App)`
	
	Beispiel für den WITHAuthenticator HOC-Code
	
	`import Amplify from 'aws-amplify'`
	`import config from './src/aws-exports'`
	`Amplify.configure(config)`
	`import { withAuthenticator } from 'aws-amplify-react-native';`
	
	`const App = () => {`
	`  return null;`
	`};`
	
	`export default withAuthenticator(App);`
	
	Note
	Im iOS-Simulator zeigt die App den Anmeldebildschirm an, der vom Amazon	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Cognito-Service bereitgestellt wird.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Einrichtung des Authentifizierungsdienstes.	Gehen Sie im iOS-Simulator wie folgt vor: 1. Erstellen Sie ein neues Konto in der App, indem Sie eine echte E-Mail-Adresse verwenden. Ein Bestätigungscode wird dann an die registrierte E-Mail gesendet. 2. Überprüfen Sie das eingerichtete Konto mithilfe des Codes, den Sie in der Bestätigungs-E-Mail erhalten. 3. Geben Sie den Benutzernamen und das Passwort ein, die Sie erstellt haben. Wählen Sie dann Anmelden. Ein Willkommensbildschirm wird angezeigt. **Note** Sie können auch die Amazon Cognito Cognito-Konsole öffnen und überprüfen, ob ein neuer Benutzer im Identity Pool erstellt wurde oder nicht.	App-Developer

Eine AppSync AWS-API und eine DynamoDB-Datenbank mit der App Connect

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AppSync AWS-API und eine DynamoDB-Datenbank.	1. Fügen Sie Ihrer App eine AppSync AWS-API hinzu und stellen Sie automatisch eine DynamoDB-Datenbank bereit, indem Sie den folgenden Amplify-CLI-Befehl im Stammverz eichnis des Projekts ausführen: `amplify add api` 2. Es wird eine Aufforder ung angezeigt, in der Sie aufgefordert werden, Informationen zu den API- und Datenbank konfigurationseinstellungen anzugeben. Geben Sie die erforderlichen Informati onen basierend auf Ihrem Anwendungsfall ein. Drücken Sie anschließ end die Eingabetaste. Die Amplify CLI öffnet die GraphQL-Schemadatei in Ihrem Texteditor. Wenden Sie für das in diesem Muster verwendete ToDoList App-Setup die folgende Beispielkonfiguration an.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Beispiel für API- und Datenbankkonfigurationseinstellungen
	
	`? Please select from one of the below mentioned services: \`
	`GraphQL`
	
	`? Provide API name: todolistamplify`
	
	`? Choose the default authorization type for the API \`
	`Amazon Cognito User Pool`
	
	`Do you want to use the default authentication and security configuration`
	
	`? Default configuration How do you want users to be able to sign in? \`
	`Username`
	
	`Do you want to configure advanced settings? \`
	`No, I am done.`
	
	`? Do you want to configure advanced settings for the GraphQL API \`
	`No, I am done.`
	
	`? Do you have an annotated GraphQL schema? \`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	No
	
	? Choose a schema
	template: \
	Single object with
	fields (e.g., “Todo”
	with ID, name,
	description)
	
	? Do you want to edit
	the schema now? \
	Yes
	
	Beispiel für ein GraphQL-Schema
	
	type Todo @model {
	id: ID!
	name: String!
	description: String
	}	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die AppSync AWS-API bereit.	1. Führen Sie im Stammverz eichnis des Projekts den folgenden Amplify CLI-Befehl aus: `amplify push` 2. Es wird eine Aufforder ung angezeigt, in der Sie aufgefordert werden, weitere Informationen zu den API- und Datenbank konfigurationseinstellungen anzugeben. Geben Sie die erforderlichen Informati onen basierend auf Ihrem Anwendungsfall ein. Drücken Sie anschließend die Eingabetaste. Ihre App kann jetzt mit der AppSync AWS-API interagieren. Wenden Sie für das in diesem Muster verwendete ToDoList App-Setup die folgende Beispielkonfiguration an. Beispiel für AppSync AWS-API-Konfigurationseinst ellungen **Note** Die folgende Konfigura tion erstellt die GraphQL-API in	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	AWS AppSync und eine Todo-Tabelle in Dynamo DB.
	
	`? Are you sure you want to continue? Yes`
	`? Do you want to generate code for your newly created GraphQL API Yes`
	`? Choose the code generation language target javascript`
	`? Enter the file name pattern of graphql queries, mutations and subscriptions src/graphql/**/*.js`
	`? Do you want to generate/update all possible GraphQL operations - \ queries, mutations and subscriptions Yes`
	`? Enter maximum statement depth \ [increase from default if your schema is deeply nested] 2`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Connect das Frontend der App mit der AppSync AWS-API.	Um die in diesem Muster bereitgestellte ToDoList Beispiel-App zu verwenden , kopieren Sie den Code aus der Datei App.js im ios-todo-app GitHub Repository aws-amplify-react-native-. Integrieren Sie dann den Beispielcode in Ihre lokale Umgebung. Der in der Datei App.js des Repositorys enthalten e Beispielcode bewirkt Folgendes: • Zeigt das Formular zum Erstellen eines ToDo Elements mit den Feldern Titel und Beschreibung • Zeigt die Liste der zu erledigenden Aufgaben an (Titel und Beschreibung) • Postet Daten mithilfe von Methoden und ruft sie ab `aws-amplify`	App-Developer

Zugehörige Ressourcen

- AWS Amplify
- Amazon Cognito
- AWS AppSync
- Amazon-DynamoDB
- React (React-Dokumentation)

Mandanten für mehrere SaaS-Produkte auf einer einzigen Steuerebene verwalten

Erstellt von Ramanna Avancha (AWS), Jenifer Pascal (AWS), Kishan Kavala (AWS) und Anusha Mandava (AWS)

Übersicht

Dieses Muster zeigt, wie Mandantenlebenszyklen für mehrere SaaS-Produkte (Software as a Service) auf einer einzigen Steuerungsebene in der AWS-Cloud verwaltet werden. Die bereitgestellte Referenzarchitektur kann Unternehmen dabei helfen, die Implementierung redundanter, gemeinsam genutzter Funktionen in ihren einzelnen SaaS-Produkten zu reduzieren und die Governance-Effizienz in großem Umfang zu steigern.

Große Unternehmen können mehrere SaaS-Produkte in verschiedenen Geschäftsbereichen anbieten. Diese Produkte müssen häufig für die Nutzung durch externe Mandanten mit unterschiedlichen Abonnementstufen bereitgestellt werden. Ohne eine gemeinsame Mandantenlösung müssen IT-Administratoren Zeit damit verbringen, undifferenzierte Funktionen über mehrere SaaS hinweg zu verwalten APIs, anstatt sich auf die Entwicklung der Kernproduktfunktionen zu konzentrieren.

Die in diesem Muster bereitgestellte Common-Tenant-Lösung kann dazu beitragen, die Verwaltung vieler gemeinsam genutzter SaaS-Produktfunktionen eines Unternehmens zu zentralisieren, darunter die folgenden:

- Sicherheit
- Bereitstellung von Mandanten
- Speicherung von Mieterdaten
- Kommunikation mit Mietern
- Produktmanagement
- Protokollierung und Überwachung von Metriken

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

- Kenntnisse über Amazon Cognito oder einen externen Identitätsanbieter (IdP)
- Kenntnisse über Amazon API Gateway
- Kenntnisse über AWS Lambda
- Kenntnisse über Amazon DynamoDB
- Kenntnisse in AWS Identity and Access Management (IAM)
- Kenntnis von AWS Step Functions
- Kenntnisse von AWS CloudTrail und Amazon CloudWatch
- Kenntnisse von Python-Bibliotheken und Code
- Kenntnisse über SaaS APIs, einschließlich der verschiedenen Benutzertypen (Organisationen, Mandanten, Administratoren und Anwendungsbenutzer), Abonnementmodelle und Modelle zur Mandantenisolierung
- Kenntnis der SaaS-Anforderungen Ihres Unternehmens für mehrere Produkte und Mehrmandantenabonnements

Einschränkungen

- Integrationen zwischen der Common-Tenant-Lösung und einzelnen SaaS-Produkten werden in diesem Muster nicht behandelt.
- Dieses Muster stellt den Amazon Cognito-Service nur in einer einzigen AWS-Region bereit.

Architektur

Zieltechnologie-Stack

- Amazon API Gateway
- Amazon Cognito
- AWS CloudTrail
- Amazon CloudWatch
- Amazon-DynamoDB
- IAM
- AWS Lambda
- Amazon Simple Storage Service (Amazon-S3)
- Amazon-Simple-Notification-Service (Amazon-SNS)

- Funktionen von AWS Step

Zielarchitektur

Das folgende Diagramm zeigt einen Beispiel-Workflow für die Verwaltung von Mandantenlebenszyklen für mehrere SaaS-Produkte auf einer einzigen Steuerungsebene in der AWS-Cloud.

Das Diagramm zeigt den folgenden Workflow:

1. Ein AWS-Benutzer initiiert die Mandantenbereitstellung, Produktbereitstellung oder verwaltungsbezogene Aktionen, indem er einen API-Gateway-Endpunkt aufruft.
2. Der Benutzer wird durch ein Zugriffstoken authentifiziert, das aus einem Amazon Cognito Cognito-Benutzerpool oder einem anderen IdP abgerufen wird.
3. Einzelne Bereitstellungs- oder Verwaltungsaufgaben werden von Lambda-Funktionen ausgeführt, die in API Gateway API-Endpunkte integriert sind.
4. APIs Bei der Verwaltung der gemeinsamen Mandantenlösung (für Mandanten, Produkte und Benutzer) werden alle erforderlichen Eingabeparameter, Header und Token erfasst. Dann APIs ruft die Administration die zugehörigen Lambda-Funktionen auf.
5. IAM-Berechtigungen sowohl für die Administration APIs als auch für die Lambda-Funktionen werden vom IAM-Dienst validiert.
6. Lambda-Funktionen speichern und rufen Daten aus den Katalogen (für Mandanten, Produkte und Benutzer) in DynamoDB und Amazon S3 ab.
7. Nachdem die Berechtigungen validiert wurden, wird ein AWS Step Functions Functions-Workflow aufgerufen, um eine bestimmte Aufgabe auszuführen. Das Beispiel im Diagramm zeigt einen Workflow zur Mandantenbereitstellung.
8. Einzelne AWS Step Functions Functions-Workflow-Aufgaben werden in einem vordefinierten Workflow (State Machine) ausgeführt.
9. Alle wichtigen Daten, die für die Ausführung der Lambda-Funktion benötigt werden, die jeder Workflow-Aufgabe zugeordnet ist, werden entweder von DynamoDB oder Amazon S3 abgerufen. Andere AWS-Ressourcen müssen möglicherweise mithilfe einer CloudFormation AWS-Vorlage bereitgestellt werden.
10. Bei Bedarf sendet der Workflow eine Anfrage zur Bereitstellung zusätzlicher AWS-Ressourcen für ein bestimmtes SaaS-Produkt an das AWS-Konto dieses Produkts.

11. Wenn die Anfrage erfolgreich ist oder fehlschlägt, veröffentlicht der Workflow die Statusaktualisierung als Nachricht zu einem Amazon SNS SNS-Thema.
12. Amazon SNS hat das Amazon SNS-Thema des Step Functions Functions-Workflows abonniert.
13. Amazon SNS sendet dann die Workflow-Status-Aktualisierung zurück an den AWS-Benutzer.
14. Protokolle der Aktionen der einzelnen AWS, einschließlich eines Prüfprotokolls mit API-Aufrufen, werden an gesendet CloudWatch. CloudWatch Für jeden Anwendungsfall können spezifische Regeln und Alarme konfiguriert werden.
15. Protokolle werden zu Prüfungszwecken in Amazon S3 S3-Buckets archiviert.

Automatisierung und Skalierung

Dieses Muster verwendet eine CloudFormation Vorlage, um die Bereitstellung der Common-Tenant-Lösung zu automatisieren. Die Vorlage kann Ihnen auch dabei helfen, die zugehörigen Ressourcen schnell nach oben oder unten zu skalieren.

Weitere Informationen finden Sie unter Arbeiten mit CloudFormation AWS-Vorlagen im CloudFormation AWS-Benutzerhandbuch.

Tools

AWS-Services

- Amazon API Gateway unterstützt Sie bei der Erstellung, Veröffentlichung, Wartung, Überwachung und Sicherung von REST, HTTP und WebSocket APIs in jeder Größenordnung.
- Amazon Cognito bietet Authentifizierung, Autorisierung und Benutzerverwaltung für Web- und mobile Apps.
- AWS CloudTrail unterstützt Sie bei der Prüfung der Unternehmensführung, der Einhaltung von Vorschriften und des Betriebsrisikos Ihres AWS-Kontos.
- Amazon CloudWatch hilft Ihnen dabei, die Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie auf AWS ausführen, in Echtzeit zu überwachen.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.

- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.
- AWS Step Functions ist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen.

Bewährte Methoden

Die Lösung in diesem Muster verwendet eine einzige Steuerungsebene, um das Onboarding mehrerer Mandanten zu verwalten und den Zugriff auf mehrere SaaS-Produkte bereitzustellen. Die Steuerungsebene hilft administrativen Benutzern bei der Verwaltung von vier weiteren, funktionsspezifischen Ebenen:

- Sicherheitsebene
- Workflow-Ebene
- Kommunikationsebene
- Protokollierungs- und Überwachungsebene

Epen

Konfigurieren Sie die Sicherheitsebene

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie die Anforderungen für Ihre Multi-Tenant-SaaS-Plattform fest.	Legen Sie detaillierte Anforderungen für Folgendes fest: • Mandanten • Benutzer	Cloud-Architekt, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Rollen • SaaS-Produkte • Subscriptions (Abonnements) • Austausch von Profilen	
Richten Sie den Amazon Cognito-Service ein.	Folgen Sie den Anweisungen unter Erste Schritte mit Amazon Cognito im Amazon Cognito Developer Guide.	Cloud-Architekt
Konfigurieren Sie die erforderlichen IAM-Richtlinien.	Erstellen Sie die erforderlichen IAM-Richtlinien für Ihren Anwendungsfall. Ordnen Sie dann die Richtlinien den IAM-Rollen in Amazon Cognito zu. Weitere Informationen finden Sie unter Verwaltung des Zugriffs mithilfe von Richtlinien und rollenbasierter Zugriffskontrolle im Amazon Cognito Developer Guide.	Cloud-Administrator, Cloud-Architekt, AWS IAM-Sicherheit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die erforderlichen API-Berechtigungen.	Richten Sie API-Gateway-Zugriffsberechtigungen mithilfe von IAM-Rollen und -Richtlinien sowie Lambda-Autorisierern ein. Anweisungen finden Sie in den folgenden Abschnitten des Amazon API Gateway Developer Guide: • Steuern Sie den Zugriff auf eine API mit IAM-Berechtigungen • Verwenden Sie API Gateway Lambda-Autorisierer	Cloud-Administrator, Cloud-Architekt

Konfigurieren Sie die Datenebene

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die erforderlichen Datenkataloge.	1. Erstellen Sie DynamoDB-Tabellen zum Speichern von Daten für die Benutzerkataloge. Stellen Sie sicher, dass Sie Benutzerattribute und Rollen angeben. Stellen Sie außerdem sicher, dass Sie Datenmodellierung für die Katalogtabellen durchführen, um die erforderlichen und optionalen Attribute für	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	jeden Benutzer und jede Rolle beizubehalten. 2. Erstellen Sie DynamoDB-Tabellen zum Speichern von Daten für die Produktkataloge. Stellen Sie sicher, dass Sie die spezifischen Anwendungsfälle für Ihre SaaS-Produkte modellieren. 3. Erstellen Sie DynamoDB-Tabellen zum Speichern von Daten für die Mandantenkataloge. Stellen Sie sicher, dass Sie Abonnementmodelle für Mandanten, Produkte und Lizenzen für Multi-SaaS-Abonnements und Tags einrichten. Weitere Informationen finden Sie unter Setting up DynamoDB im Amazon DynamoDB Developer Guide.	

Konfigurieren Sie die Steuerungsebene

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Lambda-Funktionen und API Gateway APIs , um die erforderlichen Aufgaben auf der Steuerungsebene auszuführen.	Erstellen Sie separate Lambda-Funktionen und API Gateway, APIs um Folgendes hinzuzufügen, zu löschen und zu verwalten:	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Benutzer • Mandanten • Produkte Weitere Informationen finden Sie unter Using AWS Lambda with Amazon API Gateway im AWS Lambda Developer Guide.	

Konfigurieren Sie die Workflow-Ebene

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Aufgaben, die AWS Step Functions Functions-Workflows ausführen müssen.	Identifizieren und dokumentieren Sie die detaillierten AWS Step Functions Functions-Workflow-Anforderungen für Folgendes: • Benutzer • Mandanten • Produkte ⚠ Important Stellen Sie sicher, dass die wichtigsten Beteiligten die Anforderungen genehmigen.	Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die erforderl ichen AWS Step Functions Functions-Workflows.	1. Erstellen Sie die erforderl ichen Workflows für Benutzer, Mandanten und Produkte in AWS Step Functions. Weitere Informati onen finden Sie im AWS Step Functions Developer Guide. 2. Identifizieren Sie die Mechanismen zur Wiederholung und zur Fehlerbehandlung. Weitere Informationen finden Sie im AWS-Blog unter Umgang mit Fehlern, Wiederhol ungen und Hinzufügen von Warnmeldungen zu Step Function State Machines. 3. Implementieren Sie die Workflow-Schritte mithilfe von Lambda-Funktionen. Anweisungen finden Sie im AWS Step Functions Developer Guide unter Creating a Step Functions -Zustandsmaschine, die Lambda verwendet. 4. Integrieren Sie alle externen Services nach Bedarf in AWS Step Functions. 5. Behalten Sie den Status jedes Workflows in einer DynamoDB-Tabelle bei und kommunizieren Sie den	App-Entwickler, Lead aufbauen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Status jedes Workflows mithilfe von Amazon SNS.	

Konfigurieren Sie die Kommunikationsebene

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Amazon SNS SNS-Themen.	Erstellen Sie Amazon SNS SNS-Themen, um Benachric htigungen zu folgenden Themen zu erhalten: • Workflow-Status • Fehler • Wiederholversuche Weitere Informationen finden Sie unter dem Thema Creating an SNS im Amazon SNS Developer Guide.	App-Besitzer, Cloud-Architekt
Abonnieren Sie Endpunkte für jedes Amazon SNS SNS-Thema.	Um Nachrichten zu erhalten, die zu einem Amazon SNS SNS-Thema veröffentlicht wurden, müssen Sie für jedes Thema einen Endpunkt abonnieren. Weitere Informationen finden Sie unter Amazon SNS SNS-Abonnement im Amazon SNS SNS-Entwicklerhandbuch.	App-Entwickler, Cloud-Arc hitekt

Konfigurieren Sie die Protokollierungs- und Überwachungsebene

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie die Protokollierung für jede Komponente der Common-Tenant-Lösung.	Aktivieren Sie die Protokollierung auf Komponentenebene für jede Ressource in der Common Tenant-Lösung, die Sie erstellt haben. Detaillierte Informationen finden Sie hier: • Wie aktiviere ich CloudWatch Logs zur Fehlerbehebung bei meiner API Gateway REST API oder WebSocket API? (AWS-Wissenszentrum) • Protokollierung mithilfe von CloudWatch Protokollen (AWS Step Functions Developer Guide) • Protokollierung von AWS Lambda-Funktionen in Python (AWS Lambda Developer Guide) • Protokollierung und Überwachung in Amazon Cognito (Amazon Cognito Developer Guide) • Überwachung mit Amazon CloudWatch (Amazon DynamoDB DynamoDB-Entwicklerhandbuch)	App-Entwickler, AWS-Systemadministrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Mithilfe von IAM-Richtlinien können Sie Protokolle für jede Ressource in einem zentralen Protokollierungskonto konsolidieren. Weitere Informationen finden Sie unter Zentralisierte Protokollierung und Sicherheitsvorkehrungen für mehrere Konten.	

Bereitstellung und Bereitstellung der Common-Tenant-Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
CloudFormation Vorlagen erstellen.	Automatisieren Sie mithilfe von CloudFormation Vorlagen die Bereitstellung und Wartung der vollständigen Common-Tenant-Lösung und all ihrer Komponenten. Weitere Informationen finden Sie im CloudFormation AWS-Benutzerhandbuch.	App-Entwickler, DevOps Ingenieur, CloudFormation Entwickler

Zugehörige Ressourcen

- Steuern Sie den Zugriff auf eine REST-API mithilfe von Amazon Cognito Cognito-Benutzerpools als Autorisierer (Amazon API Gateway Developer Guide)
- Verwenden Sie API Gateway Lambda-Autorisierer (Amazon API Gateway Gateway-Entwicklerhandbuch)
- Amazon Cognito Cognito-Benutzerpools (Amazon Cognito Cognito-Entwicklerhandbuch)
- Kontoübergreifende, regionsübergreifende CloudWatch Konsole (CloudWatch Amazon-Benutzerhandbuch)

Erstellen Sie eine kontoübergreifende EventBridge Amazon-Verbindung in einer Organisation

Erstellt von Sam Wilson (AWS) und Robert Stone (AWS)

Übersicht

Große verteilte Systeme verwenden Amazon EventBridge , um Statusänderungen zwischen verschiedenen Amazon Web Services (AWS) -Konten in einer AWS Organizations Organisation zu kommunizieren. EventBridge Ist jedoch in der Regel in der Lage, nur Endgeräte oder Verbraucher in derselben AWS-Konto Umgebung anzusprechen. Die Ausnahme ist ein Event-Bus in einem anderen Konto. Dieser Event-Bus ist ein gültiges Ziel. Um Ereignisse aus einem Event-Bus in einem anderen Konto zu verarbeiten, müssen die Ereignisse vom Event-Bus des Quellkontos in den Event-Bus des Zielkontos übertragen werden. Verwenden Sie den in diesem Muster beschriebenen empfohlenen Ansatz AWS-Konten, um Probleme bei der Verwaltung kritischer Ereignisse zwischen Anwendungen innerhalb verschiedener Anwendungen zu vermeiden.

Dieses Muster veranschaulicht, wie eine ereignisgesteuerte Architektur implementiert wird EventBridge , an der mehrere Personen AWS-Konten in einer AWS Organizations Organisation beteiligt sind. Das Muster verwendet AWS Cloud Development Kit (AWS CDK) Toolkit und. AWS CloudFormation

EventBridge bietet einen serverlosen Event-Bus, der Sie beim Empfangen, Filtern, Transformieren, Weiterleiten und Bereitstellen von Ereignissen unterstützt. Als wichtige Komponente ereignisgesteuerter Architekturen EventBridge unterstützt es die Trennung zwischen Nachrichtenproduzenten und Empfängern dieser Nachrichten. In einem einzigen Konto ist das ganz einfach. Bei einer Struktur mit mehreren Konten sind zusätzliche Überlegungen erforderlich, damit Ereignisse auf dem Event-Bus in einem Konto auf andere Konten innerhalb derselben Organisation übertragen werden können.

Informationen zu kontospezifischen Überlegungen für Produzenten und Verbraucher finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine AWS Organizations Organisation, der mindestens zwei Personen angehören AWS-Konten

- Eine AWS Identity and Access Management (IAM-) Rolle in beiden AWS-Konten , mit der Sie die Infrastruktur in beiden bereitstellen können, AWS-Konten indem Sie AWS CloudFormation
- Git lokal installiert
- AWS Command Line Interface (AWS CLI) lokal installiert
- AWS CDK lokal installiert und in beiden Bootstrapping AWS-Konten

Produktversionen

Dieses Muster wurde mit den folgenden Tools und Versionen erstellt und getestet:

- AWS CDK Toolkit 2.126.0
- Node.js 18.19.0
- npm 10.2.3
- Python 3.12

Dieses Muster sollte mit jeder Version von AWS CDK v2 oder npm funktionieren. Die Versionen 13.0.0 bis 13.6.0 von Node.js sind nicht kompatibel mit. AWS CDK

Architektur

Zielarchitektur

Das folgende Diagramm zeigt den Architektur-Workflow für die Übertragung eines Ereignisses von einem Konto aus und dessen Verarbeitung in einem anderen Konto.

Der Workflow umfasst die folgenden Schritte:

1. Die AWS Lambda Producer-Funktion im Quellkonto platziert ein Ereignis auf dem EventBridge Event-Bus des Kontos.
2. Die kontenübergreifende EventBridge Regel leitet das Ereignis an einen EventBridge Event-Bus im Zielkonto weiter.
3. Der EventBridge Eventbus im Zielkonto hat eine Lambda-Zielregel, die die Consumer-Lambda-Funktion aufruft.

Eine bewährte Methode ist die Verwendung einer Dead Letter Queue (DLQ) für die Behandlung fehlgeschlagener Aufrufe der Consumer-Lambda-Funktion. Aus Gründen der Übersichtlichkeit

wurde die DLQ in dieser Lösung jedoch weggelassen. Weitere Informationen darüber, wie Sie eine DLQ in Ihren Workflows implementieren und die Fähigkeit Ihrer Workflows zur Wiederherstellung nach Fehlern verbessern können, finden Sie im Blogbeitrag Implementieren von AWS Lambda Fehlerbehandlungsmustern.

Automatisierung und Skalierung

AWS CDK stellt automatisch die erforderliche Architektur bereit. EventBridge kann je nach auf Tausende von Datensätzen pro Sekunde skaliert AWS-Region werden. Weitere Informationen finden Sie in der Dokumentation zu EventBridge Amazon-Kontingenten.

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK)ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung von AWS Cloud Infrastruktur im Code unterstützt. Dieses Muster verwendet das AWS CDK Toolkit, ein Cloud-Entwicklungskit für die Befehlszeile, mit dem Sie mit Ihrer AWS CDK App interagieren können.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS Lambda Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen. AWS-Konten
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Organizationsist ein Kontoverwaltungsservice, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie erstellen und zentral verwalten.

Andere Tools

- Node.js ist eine ereignisgesteuerte JavaScript Laufzeitumgebung, die für die Erstellung skalierbarer Netzwerkanwendungen entwickelt wurde.
- npm ist eine Softwareregistrierung, die in einer Node.js -Umgebung ausgeführt wird und verwendet wird, um Pakete gemeinsam zu nutzen oder auszuleihen und die Bereitstellung von privaten Paketen zu verwalten.
- Python ist eine Allzweck-Computerprogrammiersprache.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub cross-account-eventbridge-in-organization verfügbar.

Bewährte Methoden

Bewährte Methoden für die Arbeit mit EventBridge finden Sie in den folgenden Ressourcen:

- Bewährte Methoden für EventBridge Amazon-Event-Muster
- Bewährte Methoden bei der Definition von Regeln in Amazon EventBridge

Epen

Bereiten Sie Ihre lokale AWS CDK Bereitstellungsumgebung vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie lokale Anmeldeinformationen für das Quellkonto und das Zielkonto.	Lesen Sie unter Neue Konfiguration und neue Anmeldeinformationen einrichten und verwenden Sie die Authentifizierungs- und Anmeldemethode, die für Ihre Umgebung am sinnvollsten ist. **Important** Stellen Sie sicher, dass Sie die Authentifizierung sowohl AWS CLI für das Quellkonto als auch für das Zielkonto konfigurieren.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bei diesen Anweisungen wird davon ausgegangen, dass Sie zwei AWS-Profile lokal konfiguriert haben: `sourceAccount` und `destinationAccount`.	

Bootstrap für beide AWS-Konten.	Führen Sie die folgenden Befehle aus, um die Konten zu booten:
	`cdk bootstrap --profile sourceAccount`
	`cdk bootstrap --profile destinationAccount`
		App-Developer

Klonen Sie den Mustercode.	Führen Sie den folgenden Befehl aus, um das Repository zu klonen:
	`git clone git@github.com:aws-samples/aws-cdk-examples.git`
	Ändern Sie dann das Verzeichnis in den neu geklonten Projektordner:
	`cd aws-cdk-examples/python/cross-account-eventbridge-in-organization`
		App-Developer

Auf ProducerStack das Quellkonto bereitstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie `cdk.json` mit Ihren Daten AWS Organizations und Ihren Kontodaten.	Nehmen Sie im Stammordner des Projekts die folgenden Änderungen vor`cdk.json`: • `organization_id` – Die Organisations-ID der Konten, die an Ihrer Bereitstellung beteiligt sind • `event_bus_name` – `CrossAccount`, oder Sie können sie umbenennen • `rules[].targets[].arn` – Die AWS-Konto ID des verbrauchenden Kontos (Zielkonto)	App-Developer
Stellen Sie die ProducerStack Ressourcen bereit.	Führen Sie den folgenden Befehl im Stammverzeichnis des Projekts aus: `cdk deploy ProducerStack --profile sourceAccount` Wenn Sie dazu aufgefordert werden, akzeptieren Sie die neuen IAM-Rollen und andere sicherheitsrelevante Berechtigungen, die durch erstellt wurden. AWS CloudFormation	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die ProducerStack Ressourcen bereitgestellt wurden.	Gehen Sie wie folgt vor, um die Ressourcen zu überprüfen: 1. Wählen Sie im Konto AWS Management Console für das Quellkonto die Option CloudFormation. 2. Wählen Sie aus der Liste der Stacks die Option ProducerStack. 3. Vergewissern Sie sich auf der Registerkarte Stack-Info, dass der Stack-Status lautet`CREATE_COMPLETE` . Überprüfen Sie optional auf der Registerkarte Ressourcen die konfigurierten Ressourcen.	App-Developer

Auf ConsumerStack dem Zielkonto bereitstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die ConsumerStack Ressourcen bereit.	Führen Sie den folgenden Befehl im Stammverzeichnis des Projekts aus: `cdk deploy ConsumerStack --profile destinationAccount` Wenn Sie dazu aufgefordert werden, akzeptieren Sie die neuen IAM-Rollen und andere	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	sicherheitsrelevante Berechtigungen, die durch erstellt wurden. AWS CloudFormation	
Stellen Sie sicher, dass die Ressourcen bereitgestellt wurden ConsumerStack	1. Wählen Sie auf der Konsole für das Zielkonto die Option CloudFormation. 2. Wählen Sie aus der Liste der Stacks die Option ConsumerStack. 3. Vergewissern Sie sich auf der Registerkarte Stack-Info, dass der Stack-Status lautet`CREATE_COMPLETE` . Überprüfen Sie optional auf der Registerkarte Ressourcen die konfigurierten Ressourcen.	App-Developer

Ereignisse produzieren und nutzen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie die Producer Lambda-Funktion auf.	1. Wählen Sie auf der Konsole für das Quellkonto Lambda aus. 2. Wählen Sie aus der Liste der Funktionen ProducerStack- ProducerLambda XXXX (XXXX steht für eine automatisch von AWS CDK generierte Zeichenfolge). 3. Wählen Sie die Registerkarte Test.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie im Abschnitt Testereignis die Option Test aus. Der Inhalt des Event-JSON-Textbereichs kann jedes gültige JSON sein, das der Lambda-Funktion als Nutzlast zur Verfügung gestellt wird. In diesem Fall ist das standardmäßig bereitgestellte JSON ausreichend. 5. Vergewissern Sie sich, dass die Meldung Funktion ausgeführt: Erfolgreich ausgeführt in einem grünen Banner über dem Abschnitt Testereignis angezeigt wird.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass das Ereignis empfangen wurde.	1. Wählen Sie auf der Konsole für das Zielkonto Lambda aus. 2. Wählen Sie aus der Liste der Funktionen ConsumerStack- ConsumerLambda XXXX (XXXX steht für eine automatisch von AWS CDK generierte Zeichenfolge). 3. Wählen Sie den Tab Überwachung. 4. Wählen Sie im Bereich Monitor die Option Protokolle anzeigen aus. CloudWatch 5. Wählen Sie auf der neu geöffneten Registerkarte den Namen des Log-Streams des neuesten Log-Streams aus. 6. Vergewissern Sie sich, dass eine Protokollanweisung wie die folgende angezeigt wird: `[DEBUG] 2024-04-08T19:08:10.091Z 9c16844a-f9de-444d-b621-86afe64d4cc8 Event: {'version':'0', 'id':'0b9faa96-973f-8be2-ecf8-75e4f328b980', 'detail-t`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`ype':'TestType', 'source':'Producer', 'account':'XXXXXXXXXXXX', 'time':'2024-04-08T19:08:09Z', 'region':'us-east-1', 'resources': [], 'detail': {'key1':'value1', 'key2':'value2', 'key3':'value3'}}`	

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Zerstöre die ConsumerStack Ressourcen.	Wenn Sie dieses Muster als Test verwenden, bereinigen Sie die bereitgestellten Ressourcen, um zusätzliche Kosten zu vermeiden. Führen Sie den folgenden Befehl im Stammverzeichnis des Projekts aus: `cdk destroy ConsumerStack --profile destinationAccount` Sie werden aufgefordert, das Löschen des Stacks zu bestätigen.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Zerstöre die ProducerStack Ressourcen.	Führen Sie den folgenden Befehl im Stammverzeichnis des Projekts aus: `cdk destroy ProducerStack --profile sourceAccount` Sie werden aufgefordert, das Löschen des Stacks zu bestätigen.	App-Developer

Fehlerbehebung

Problem	Lösung
Im Zielkonto wurde kein Ereignis empfangen.	1. Stellen Sie sicher, dass die angegebene Organisations-ID korrekt ist. 2. Stellen Sie sicher, dass das Quellkonto Teil der angegebenen Organisation ist. 3. Stellen Sie sicher, dass die Event-Bus-Regeln im Quellkonto den richtigen Informationen im Zielkonto zugeordnet sind.
Beim Aufrufen einer Lambda-Funktion von der Konsole aus wird der folgende Fehler zurückgegeben: `User: arn:aws:iam::123456789012:user/XXXXX is not authorized to perform: lambda:Invoke`	Wenden Sie sich an Ihren AWS-Konto Administrator, um die entsprechenden `lambda:Invoke` Aktionsberechtigungen für die `ProducerStack-ProducerLambdaXXXX` Lambda-Funktion zu erhalten.

Zugehörige Ressourcen

Referenzen

- AWS Organizations Benutzerhandbuch
- EventBridge Amazon-Ereignismuster
- Regeln bei Amazon EventBridge

Tutorials und Videos

- Tutorial: Organisation erstellen und konfigurieren
- AWS re:Invent 2023 — Fortgeschrittene ereignisgesteuerte Muster mit Amazon (01-R) EventBridge COM3

Zusätzliche Informationen

Regel des Produzenten

Im Quellkonto wird ein EventBridge Event-Bus erstellt, der Nachrichten von Produzenten akzeptiert (wie im Abschnitt Architektur gezeigt). Für diesen Eventbus wird eine Regel mit zugehörigen IAM-Berechtigungen erstellt. Die Regeln zielen auf den EventBridge Event-Bus im Zielkonto ab und basieren auf der folgenden `cdk.json` Struktur:

```
"rules": [
  {
    "id": "CrossAccount",
    "sources": ["Producer"],
    "detail_types": ["TestType"],
    "targets": [
      {
        "id": "ConsumerEventBus",
        "arn": "arn:aws:events:us-east-2:012345678901:event-bus/CrossAccount"
      }
    ]
  }
]
```

Für jeden konsumierenden Event-Bus müssen das Ereignismuster und der Ziel-Event-Bus angegeben werden.

Ereignismuster

Mit Ereignismustern wird gefiltert, für welche Ereignisse diese Regel gilt. Für dieses Beispiel geben die Ereignisquellen und der Datensatz an, `detail_types` welche Ereignisse vom Ereignisbus des Quellkontos an den Ereignisbus des Zielkontos übertragen werden sollen.

Ziel-Event-Bus

Diese Regel zielt auf einen Eventbus ab, der in einem anderen Konto vorhanden ist. Der vollständige Name `arn` (Amazon-Ressourcenname) wird benötigt, um den Ziel-Event-Bus eindeutig zu identifizieren, und das `id` ist die logische ID, die von verwendet wird AWS CloudFormation. Der Ziel-Event-Bus muss zum Zeitpunkt der Erstellung der Zielregel noch nicht vorhanden sein.

Spezifische Überlegungen zum Zielkonto

Im Zielkonto wird ein EventBridge Ereignisbus erstellt, um Nachrichten vom Ereignisbus des Quellkontos zu empfangen. Damit Ereignisse vom Quellkonto aus veröffentlicht werden können, müssen Sie eine ressourcenbasierte Richtlinie erstellen:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowOrgToPutEvents",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "events:PutEvents",
    "Resource": "arn:aws:events:us-east-2:012345678901:event-bus/CrossAccount",
    "Condition": {
      "StringEquals": {
        "aws:PrincipalOrgID": "o-XXXXXXXXX"
      }
    }
  }]
}
```

Es ist besonders wichtig, die `events:PutEvents` Erlaubnis zu erteilen, die es jedem anderen Konto in derselben Organisation ermöglicht, Ereignisse in diesem Event-Bus zu veröffentlichen. Wenn Sie `aws:PrincipalOrgId` die Organisations-ID angeben, werden die erforderlichen Berechtigungen gewährt.

Muster des Ereignisses

Sie können das enthaltene Ereignismuster an Ihren Anwendungsfall anpassen:

```
rule = events.Rule(
    self,
    self.id + 'Rule' + rule_definition['id'],
    event_bus=event_bus,
    event_pattern=events.EventPattern(
        source=rule_definition['sources'],
        detail_type=rule_definition['detail_types'],
    )
)
```

Um unnötige Verarbeitung zu vermeiden, sollte im Ereignismuster festgelegt werden, dass nur Ereignisse, die vom Zielkonto verarbeitet werden sollen, an den Ereignisbus des Zielkontos übertragen werden.

Ressourcenbasierte Richtlinie

In diesem Beispiel wird anhand der Organisations-ID gesteuert, welche Konten Ereignisse auf den Event-Bus des Zielkontos übertragen dürfen. Erwägen Sie, eine restriktivere Richtlinie zu verwenden, z. B. die Angabe des Quellkontos.

EventBridge Kontingente

Beachten Sie die folgenden Kontingente:

- 300 Regeln pro Event-Bus sind das Standardkontingent. Dies kann bei Bedarf erweitert werden, sollte aber für die meisten Anwendungsfälle geeignet sein.
- Fünf Ziele pro Regel sind das zulässige Maximum. Wir empfehlen Anwendungsarchitekten, für jedes Zielkonto eine eigene Regel zu verwenden, um eine genaue Steuerung des Ereignismusters zu ermöglichen.

Stellen Sie DynamoDB-Datensätze mithilfe von Kinesis Data Streams und Firehose an Amazon S3 bereit mit AWS CDK

Erstellt von Shashank Shrivastava (AWS) und Daniel Matuki da Cunha (AWS)

Übersicht

Dieses Muster enthält Beispielcode und eine Anwendung für die Übermittlung von Datensätzen von Amazon DynamoDB an Amazon Simple Storage Service (Amazon S3) mithilfe von Amazon Kinesis Data Streams und Amazon Data Firehose. Der Ansatz des Musters verwendet AWS Cloud Development Kit (AWS CDK) L3-Konstrukte und beinhaltet ein Beispiel dafür, wie eine Datentransformation durchgeführt wird, AWS Lambda bevor Daten an den Ziel-S3-Bucket in der Amazon Web Services (AWS) Cloud geliefert werden.

Kinesis Data Streams zeichnet Änderungen auf Elementebene in DynamoDB-Tabellen auf und repliziert sie in den erforderlichen Kinesis-Datenstrom. Ihre Anwendungen können auf den Kinesis Data Stream zugreifen und die Änderungen auf Elementebene nahezu in Echtzeit anzeigen. Kinesis Data Streams bietet auch Zugriff auf andere Amazon Kinesis Kinesis-Services wie Firehose und Amazon Managed Service für Apache Flink. Das bedeutet, dass Sie Anwendungen entwickeln können, die Echtzeit-Dashboards bereitstellen, Warnmeldungen generieren, dynamische Preisgestaltung und Werbung implementieren und anspruchsvolle Datenanalysen durchführen.

Sie können dieses Muster für Ihre Anwendungsfälle zur Datenintegration verwenden. Beispielsweise können Transportfahrzeuge oder Industrieanlagen große Datenmengen an eine DynamoDB-Tabelle senden. Diese Daten können dann transformiert und in einem in Amazon S3 gehosteten Data Lake gespeichert werden. Anschließend können Sie die Daten abfragen und verarbeiten und potenzielle Fehler vorhersagen, indem Sie serverlose Dienste wie Amazon Athena, Amazon Redshift Spectrum, Amazon Rekognition und verwenden. AWS Glue

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver. AWS-Konto
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert. Weitere Informationen finden Sie AWS CLI in der AWS CLI Dokumentation unter Erste Schritte mit dem.
- Node.js (18.x+) und npm, installiert und konfiguriert. Weitere Informationen finden Sie in der Dokumentation unter Node.js und npm herunterladen und installieren. `npm`

- aws-cdk (2.x+), installiert und konfiguriert. Weitere Informationen finden Sie in der Dokumentation unter Erste Schritte mit dem. AWS CDK AWS CDK
- Das GitHub aws-dynamodb-kinesisfirehose-s3-Ingestion-Repository, geklont und auf Ihrem lokalen Computer konfiguriert.
- Bestehende Beispieldaten für die DynamoDB-Tabelle. Die Daten müssen das folgende Format haben: `{"SourceDataId": {"S": "123"},"MessageData":{"S": "Hello World"}}`

Architektur

Das folgende Diagramm zeigt einen Beispiel-Workflow für die Übermittlung von Datensätzen von DynamoDB an Amazon S3 mithilfe von Kinesis Data Streams und Firehose.

Das Diagramm zeigt den folgenden Workflow:

1. Daten werden mit Amazon API Gateway als Proxy für DynamoDB aufgenommen. Sie können auch jede andere Quelle verwenden, um Daten in DynamoDB aufzunehmen.
2. Änderungen auf Artikelebene werden nahezu in Echtzeit in Kinesis Data Streams generiert und an Amazon S3 übermittelt.
3. Kinesis Data Streams sendet die Datensätze zur Transformation und Bereitstellung an Firehose.
4. Eine Lambda-Funktion konvertiert die Datensätze von einem DynamoDB-Datensatzformat in das JSON-Format, das nur die Namen und Werte der Datensatzelementattribute enthält.

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK)ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS CDK Toolkit ist ein Cloud-Entwicklungskit für die Befehlszeile, mit dem Sie mit Ihrer AWS CDK App interagieren können.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie AWS-Services über Befehle in Ihrer Befehlszeilen-Shell interagieren können.
- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über und zu verwalten. AWS-Konten AWS-Regionen

Code-Repository

Der Code für dieses Muster ist im GitHub [aws-dynamodb-kinesisfirehose-s3-Ingestion-Repository verfügbar.]

Epen

Richten Sie den Beispielcode ein und konfigurieren Sie ihn

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie die Abhängigkeiten.	Installieren Sie auf Ihrem lokalen Computer die Abhängigkeiten aus den `package.json` Dateien in den `sample-application` Verzeichnissen `pattern/aws-dynamodb-kinesisstreams-s3` und, indem Sie die folgenden Befehle ausführen:
	`cd <project_root>/pattern/aws-dynamodb-kinesisstreams-s3`
	`npm install && npm run build`
	`cd <project_root>/sample-application/`
	`npm install && npm run build`
		App-Entwickler, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie die CloudFormation Vorlage.	1. Führen Sie den Befehl `cd <project_root>/sample-application/` aus. 2. Führen Sie den `cdk synth` Befehl aus, um die CloudFormation Vorlage zu generieren. 3. Die `AwsDynamodbKinesisfirehoseS3IngestionStack.template.json` Ausgabe wird im `cdk.out` Verzeichnis gespeichert. 4. Verwenden Sie AWS CDK oder AWS Management Console , um die Vorlage in zu verarbeiten CloudFormation.	App-Entwickler, General AWS, AWS DevOps

Stellen Sie die Ressourcen bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Ressourcen und setzen Sie sie ein.	1. Führen Sie den `cdk diff` Befehl aus, um die Ressourcentypen zu identifizieren, die durch das AWS CDK Konstrukt erstellt wurden. 2. Führen Sie den `cdk deploy` Befehl aus, um die Ressourcen bereitzustellen.	App-Entwickler, General AWS, AWS DevOps

Daten in die DynamoDB-Tabelle aufnehmen, um die Lösung zu testen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Nehmen Sie Ihre Beispieldaten in die DynamoDB-Tabelle auf.	Senden Sie eine Anfrage an Ihre DynamoDB-Tabelle, indem Sie den folgenden Befehl in ausführen: AWS CLI
	
	`aws dynamodb put-item --table-name <your_table_name> --item '{"<table_partition_key>": {"S": "<partition_key_ID>"},"MessageData":{"S": "<data>"}}'`
	
	Beispiel:
	
	`aws dynamodb put-item --table-name SourceData_table --item '{"SourceDataId": {"S": "123"},"MessageData":{"S": "Hello World"}}'`
	
	Standardmäßig `put-item` gibt der keinen Wert als Ausgabe zurück, wenn der Vorgang erfolgreich ist. Wenn der Vorgang fehlschlägt, wird ein Fehler zurückgegeben. Die Daten werden in DynamoDB gespeichert und dann an
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Kinesis Data Streams und Firehose gesendet. **Note** Sie verwenden unterschiedliche Methoden, um Daten zu einer DynamoDB-Tabelle hinzuzufügen. Weitere Informationen finden Sie unter Daten in Tabellen laden in der DynamoDB-Dokumentation.	
Stellen Sie sicher, dass ein neues Objekt im S3-Bucket erstellt wurde.	Melden Sie sich beim S3-Bucket an AWS Management Console und überwachen Sie den S3-Bucket, um sicherzustellen, dass mit den von Ihnen gesendeten Daten ein neues Objekt erstellt wurde. Weitere Informationen finden Sie GetObjectin der Amazon S3 S3-Dokumentation.	App-Entwickler, General AWS

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen von Ressourcen.	Führen Sie den `cdk destroy` Befehl aus, um alle	App-Entwickler, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	von diesem Muster verwendet en Ressourcen zu löschen.	

Zugehörige Ressourcen

- static-site-stacks3-.ts (GitHub Repository)
- aws-apigateway-dynamodb Modul (GitHub Repositorium)
- aws-kinesisstreams-kinesisfirehose-s3-Modul (GitHub Repositorium)
- Erfassung von Änderungsdaten für DynamoDB Streams (DynamoDB-Dokumentation)
- Verwenden von Kinesis Data Streams zur Erfassung von Änderungen an DynamoDB (DynamoDB-Dokumentation)

Implementieren Sie eine pfadbasierte API-Versionierung mithilfe benutzerdefinierter Domains in Amazon API Gateway

Erstellt von Corey Schnedl (AWS), Anbazhagan Ponnuswamy (AWS), Marcelo Barbosa (AWS), Gaurav Samudra (AWS), Mario Lopez Martinez (AWS) und Abhilash Vinod (AWS)

Übersicht

Dieses Muster zeigt, wie Sie die API-Zuordnungsfunktion von benutzerdefinierten Domains verwenden können, um eine pfadbasierte API-Versionierungslösung für Amazon API Gateway zu implementieren.

Amazon API Gateway ist ein vollständig verwalteter Service, mit dem Sie in jeder Größenordnung etwas erstellen, veröffentlichen, verwalten, überwachen und sichern APIs können. Mithilfe der Funktion für benutzerdefinierte Domains des Services können Sie benutzerdefinierte Domainnamen erstellen, die einfacher und intuitiver URLs sind und Ihren API-Benutzern zur Verfügung stellen können. Sie können API-Zuordnungen verwenden, um API-Stufen mit einem benutzerdefinierten Domainnamen zu verbinden. Nachdem Sie einen Domainnamen erstellt und DNS-Einträge konfiguriert haben, verwenden Sie API-Zuordnungen, um Traffic APIs über Ihren benutzerdefinierten Domainnamen an Sie zu senden.

Sobald eine API öffentlich verfügbar ist, wird sie von Verbrauchern verwendet. Mit der Weiterentwicklung einer öffentlichen API wird auch ihr Servicevertrag weiterentwickelt, um neuen Funktionen und Fähigkeiten Rechnung zu tragen. Es ist jedoch unklug, bestehende Funktionen zu ändern oder zu entfernen. Alle grundlegenden Änderungen können sich auf die Anwendungen des Verbrauchers auswirken und diese zur Laufzeit beschädigen. Die API-Versionierung ist wichtig, um zu verhindern, dass die Abwärtskompatibilität beeinträchtigt wird und ein Vertrag verletzt wird.

Sie benötigen eine klare Strategie für die API-Versionierung, um den Verbrauchern zu helfen, sie zu übernehmen. Die pfadbasierte Versionierung APIs URLs ist der einfachste und am häufigsten verwendete Ansatz. Bei dieser Art der Versionierung werden Versionen explizit als Teil der API definiert. URIs Das folgende Beispiel URLs zeigt, wie ein Verbraucher den URI verwenden kann, um eine API-Version für seine Anfrage anzugeben:

```
https://api.example.com/api/v1/orders
```

```
https://api.example.com/api/v2/orders
```

```
https://api.example.com/api/vX/orders
```

Dieses Muster verwendet die, AWS Cloud Development Kit (AWS CDK) um eine Beispielimplementierung einer skalierbaren pfadbasierten Versionierungslösung für Ihre API zu erstellen, bereitzustellen und zu testen. AWS CDK ist ein Open-Source-Framework für die Softwareentwicklung, mit dem Sie Ihre Cloud-Anwendungsressourcen mithilfe vertrauter Programmiersprachen modellieren und bereitstellen können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto.
- Der Besitz einer Domain ist erforderlich, um das Beispiel-Repository dieses Musters und die benutzerdefinierte Domain-Funktionalität von Amazon API Gateway verwenden zu können. Sie können Amazon Route 53 verwenden, um Ihre Domains für Ihre Organisation zu erstellen und zu verwalten. Informationen zur Registrierung oder Übertragung einer Domain bei Route 53 finden Sie unter Neue Domains registrieren in der Route 53-Dokumentation.
- Bevor Sie einen benutzerdefinierten Domainnamen für eine API einrichten können, müssen Sie über ein SSL/TLS-Zertifikat verfügen. AWS Certificate Manager
- Sie müssen den Ressourceneintrag Ihres DNS-Anbieters erstellen oder aktualisieren, bevor Sie ihn dem API-Endpunkt zuordnen können. Ohne eine solche Zuordnung können API-Anfragen, die für den benutzerdefinierten Domainnamen gebunden sind, API Gateway nicht erreichen.

Einschränkungen

- Benutzerdefinierte Domainnamen werden für private Domains nicht unterstützt APIs.
- Ein benutzerdefinierter Domainname muss innerhalb eines Bereichs AWS-Region eindeutig sein AWS-Konten.
- Sie müssen einen regionalen benutzerdefinierten Domainnamen verwenden und die Sicherheitsrichtlinie TLS 1.2 anwenden, um API-Zuordnungen auf mehreren Ebenen konfigurieren zu können.
- Bei einer API-Zuordnung APIs müssen der benutzerdefinierte Domainname und der zugeordnete Domainname identisch AWS-Konto sein.
- API-Zuordnungen dürfen nur Buchstaben, Zahlen und die folgenden Zeichen enthalten: `$-_.+!*'()/`
- Die maximale Länge für den Pfad in eines API-Mappings beträgt 300 Zeichen.
- Es können 200 API-Zuweisungen mit mehreren Ebenen für jeden Domainnamen vorhanden sein.

- Mit der Sicherheitsrichtlinie TLS 1.2 können Sie HTTP APIs nur einem regionalen benutzerdefinierten Domainnamen zuordnen.
- Sie können nicht demselben benutzerdefinierten Domainnamen wie eine HTTP-API oder REST-API zuordnen. WebSocket APIs
- Einige AWS-Services sind nicht in allen verfügbar AWS-Regionen. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie unter AWS Dienste nach Regionen. Informationen zu bestimmten Endpunkten finden Sie unter Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Produktversionen

- Diese Beispielimplementierung verwendet AWS CDK in TypeScript Version 2.149.0.

Architektur

Das folgende Diagramm zeigt den Architektur-Workflow.

Das Diagramm veranschaulicht folgende Vorgänge:

1. Der API-Benutzer sendet eine Anfrage mit einem benutzerdefinierten Domainnamen an Amazon API Gateway.
2. API Gateway leitet die Anfrage des Benutzers dynamisch an eine entsprechende Instanz und Phase von API Gateway weiter, basierend auf dem in der URL der Anfrage angegebenen Pfad. Die folgende Tabelle zeigt ein Beispiel dafür, wie die verschiedenen URL-basierten Pfade an bestimmte Stufen für verschiedene Instanzen von API Gateway weitergeleitet werden können.

API	Stufe	Pfad	Standard-Endpunkt
Berechnung APIv1	api	apiv1	Aktiviert
Berechnung APIv2	api	apiv2	Aktiviert
Berechnung X APIv	api	API vX	Aktiviert

3. Die API-Gateway-Zielinstanz verarbeitet die Anfrage und gibt das Ergebnis an den Benutzer zurück.

Automatisierung und Skalierung

Wir empfehlen, dass Sie für jede Version Ihrer API separate AWS CloudFormation Stacks verwenden. Mit diesem Ansatz können Sie eine vollständige Isolierung zwischen den Backends erreichen, zu APIs denen die benutzerdefinierte Domain-API-Zuordnungsfunktion weitergeleitet werden kann. Ein Vorteil dieses Ansatzes besteht darin, dass verschiedene Versionen Ihrer API unabhängig voneinander bereitgestellt oder entfernt werden können, ohne dass das Risiko besteht, dass eine andere API geändert wird. Dieser Ansatz erhöht die Widerstandsfähigkeit durch die Isolierung von CloudFormation Stacks. Außerdem bietet es Ihnen verschiedene Back-End-Optionen für Ihre API wie AWS Lambda, AWS Fargate, HTTP-Endpunkte und Aktionen von. AWS-Services

Du kannst Git-Branching-Strategien wie Gitflow in Kombination mit isolierten CloudFormation Stacks verwenden, um den Quellcode zu verwalten, der in verschiedenen Versionen der API bereitgestellt wird. Mit dieser Option können Sie verschiedene Versionen Ihrer API verwalten, ohne den Quellcode für neue Versionen duplizieren zu müssen. Mit Gitflow kannst du Tags zu Commits in deinem Git-Repository hinzufügen, wenn Releases veröffentlicht werden. Als Ergebnis hast du einen vollständigen Überblick über den Quellcode, der sich auf eine bestimmte Version bezieht. Wenn Aktualisierungen durchgeführt werden müssen, können Sie den Code aus einer bestimmten Version auschecken, Aktualisierungen vornehmen und dann den aktualisierten Quellcode auf dem CloudFormation Stack bereitstellen, der der entsprechenden Hauptversion entspricht. Dieser Ansatz reduziert das Risiko, dass eine andere API-Version beschädigt wird, da jede Version der API über isolierten Quellcode verfügt und in separaten CloudFormation Stacks bereitgestellt wird.

Tools

AWS-Services

- Amazon API Gateway unterstützt Sie bei der Erstellung, Veröffentlichung, Wartung, Überwachung und Sicherung von REST, HTTP und WebSocket APIs in jeder Größenordnung.
- AWS Certificate Manager (ACM) unterstützt Sie bei der Erstellung, Speicherung und Erneuerung von öffentlichen und privaten SSL/TLS X.509-Zertifikaten und Schlüsseln, die Ihre AWS Websites und Anwendungen schützen.
- AWS Cloud Development Kit (AWS CDK)ist ein Open-Source-Framework für die Softwareentwicklung, mit dem Sie Ihre Cloud-Infrastruktur im Code definieren und bereitstellen können. AWS CloudFormationDie Beispielimplementierung dieses Musters verwendet das in AWS CDK . TypeScript Bei der Arbeit mit dem AWS CDK In werden vertraute Tools TypeScript verwendet, darunter der TypeScript Microsoft-Compiler (`tsc`), Node.js und der Node-Paketmanager (`npm`). Wenn Sie möchten, können Sie Yarn verwenden, obwohl die Beispiele

in diesem Muster dies tun. `npm` Die Module, aus denen die AWS Construct-Bibliothek besteht, werden über das `npm` Repository npmjs.org verteilt.

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über und zu verwalten. AWS-Konten AWS-Regionen
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.
- AWS WAFist eine Firewall für Webanwendungen, mit der Sie HTTP- und HTTPS-Anfragen überwachen können, die an Ihre geschützten Webanwendungsressourcen weitergeleitet werden.

Andere Tools

- Bruno ist ein Git-freundlicher Open-Source-API-Testclient.
- cdk-nag ist ein Open-Source-Hilfsprogramm, das AWS CDK Anwendungen mithilfe von Regelpaketen auf bewährte Verfahren überprüft.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub path-based-versioning-with-api-gateway verfügbar.

Bewährte Methoden

- Verwenden Sie eine robuste CI/CD-Pipeline (Continuous Integration and Continuous Delivery), um das Testen und Bereitstellen Ihrer CloudFormation Stacks zu automatisieren, die mit dem erstellt wurden. AWS CDK Weitere Informationen zu dieser Empfehlung finden Sie in den AWS Well-Architected Guidance DevOps .
- AWS WAF ist eine verwaltete Firewall, die sich problemlos in Dienste wie Amazon API Gateway integrieren lässt. Es AWS WAF ist zwar keine notwendige Komponente, damit dieses Versionierungsmuster funktioniert, wir empfehlen jedoch aus Sicherheitsgründen, es in API Gateway AWS WAF zu integrieren.
- Ermutigen Sie API-Nutzer, regelmäßig auf die neueste Version Ihrer API zu aktualisieren, damit ältere Versionen Ihrer API als veraltet gelten und effizient entfernt werden können.

- Bevor Sie diesen Ansatz in einer Produktionsumgebung verwenden, implementieren Sie eine Firewall- und Autorisierungsstrategie für Ihre API.
- Implementieren Sie den Zugriff auf die Verwaltung Ihrer AWS Ressourcen, AWS-Konto indem Sie das Zugriffsmodell mit den geringsten Rechten verwenden.
- Um bewährte Verfahren und Sicherheitsempfehlungen für Anwendungen durchzusetzen AWS CDK, die mit dem erstellt wurden, empfehlen wir die Verwendung des Dienstprogramms cdk-nag.

Epen

Bereite deine lokale Umgebung vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Führen Sie den folgenden Befehl aus, um das Beispielanwendungs-Repository zu klonen: `git clone https://github.com/aws-samples/path-based-versioning-with-api-gateway`	App-Developer
Navigieren Sie zum geklonten Repository.	Führen Sie den folgenden Befehl aus, um zum Speicherort des geklonten Repository-Ordners zu navigieren: `cd api-gateway-custom-domain-versioning`	App-Developer
Installieren Sie die erforderlichen Abhängigkeiten.	Führen Sie den folgenden Befehl aus, um die erforderlichen Abhängigkeiten zu installieren:	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`npm install`	

Stellen Sie den CloudFormation Routing-Stack bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initiieren Sie die Bereitstellung des Routing-Stacks.	Um die Bereitstellung des CloudFormation Routing-Stacks zu initiieren `CustomDomainRouterStack`, führen Sie den folgenden Befehl aus und ersetzen Sie `example.com` ihn durch den Namen der Domain, der Sie gehören: `npx cdk deploy CustomDomainRouterStack --parameters PrerequisiteDomainName=example.com` **Note** Die Stack-Bereitstellung ist erst erfolgreich, wenn die folgende Domain-DNS-Validierungsaufgabe erfolgreich ausgeführt wurde.	App-Developer

Überprüfen des Domäneneigentümers

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie die Inhabersc haft Ihrer Domain.	Das Zertifikat verbleibt im Status Ausstehende Validieru ng, bis Sie nachweisen, dass Sie Eigentümer der zugehörig en Domain sind. Um die Inhaberschaft nachzuweisen, fügen Sie CNAME-Einträge zur Hosting-Zone hinzu, die der Domain zugeordnet ist. Weitere Informationen finden Sie in der AWS Certificate Manager Dokumentation unter DNS-Validierung. Durch das Hinzufügen der entsprechenden Datensätz e kann die `CustomDom ainRouterStack` Bereitstellung erfolgreich abgeschlossen werden.	App-Entwickler, AWS-Syste madministrator, Netzwerka dministrator
Erstellen Sie einen Aliaseint rag, der auf Ihre benutzerd efinierte API Gateway Gateway-Domain verweist.	Nachdem das Zertifikat erfolgreich ausgestellt und validiert wurde, erstellen Sie einen DNS-Eintrag, der auf Ihre benutzerdefinierte Amazon API Gateway Gateway-Domain-URL verweist. Die benutzerdefinierte Domain-URL wird durch die	App-Entwickler, AWS-Syste madministrator, Netzwerka dministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bereitstellung der benutzerd efinierten Domain eindeutig generiert und als CloudForm ation Ausgabeparameter angegeben. Es folgt ein Beispiel für den Datensatz: Routing-Richtlinie: Einfaches Routing Name des Datensatzes: `demo.api-gateway-c ustom-domain-versi oning.example.com` Alias: Ja Eintragstyp: Ein DNS-Eintr ag vom Typ „A“, der auf eine AWS Ressource verweist Value (Wert): `d-xxxxxxx xxx.execute-api.xx- xxxx-x.amazonaws.com` TTL (Sekunden): 300	

CloudFormation Stacks bereitstellen und die API aufrufen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den `ApiStackV1` Stack bereit.	Verwenden Sie den folgenden Befehl, um den `ApiStackV1` Stack bereitzustellen: `npm run deploy-v1`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Der folgende CDK-Code fügt die API-Zuordnung hinzu: `var apiMapping = new CfnApiMapping(this, "ApiMapping", { apiId: this.lambdaRestApi.restApiId, domainName: props.customDomainName.domainName, stage: "api", apiMappingKey: "api/v1", });`	
Stellen Sie den `ApiStackV2` Stack bereit.	Verwenden Sie den folgenden Befehl, um den `ApiStackV2` Stack bereitzustellen: `npm run deploy-v2`	App-Developer
Rufen Sie die API auf.	Informationen zum Aufrufen der API und zum Testen der API-Endpunkte mithilfe von Bruno finden Sie in den Anweisungen unter Zusätzliche Informationen.	App-Developer

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen von Ressourcen.	Verwenden Sie den folgenden Befehl, um die mit dieser	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Beispielanwendung verknüpften Ressourcen zu löschen: `npx cdk destroy --all` **Note** Stellen Sie sicher, dass Sie alle Route 53-DNS-Einträge bereinigen, die manuell für die Überprüfung des Domainbesitzes hinzugefügt wurden.	

Fehlerbehebung

Problem	Lösung
Bei der Bereitstellung von `CustomDomainRouterStack` Zeitüberschreitungen tritt ein Timeout auf, da das Zertifikat nicht validiert werden kann.	Stellen Sie sicher, dass Sie die richtigen CNAME-Einträge für die DNS-Validierung hinzugefügt haben, wie in der vorherigen Aufgabe beschrieben. Ihr neues Zertifikat zeigt nach dem Hinzufügen der DNS-Validierungseinträge möglicherweise noch bis zu 30 Minuten den Status Ausstehende Validierung an. Weitere Informationen finden Sie in der AWS Certificate Manager Dokumentation unter DNS-Validierung.

Zugehörige Ressourcen

- Implementierung der Header-basierten API-Gateway-Versionierung mit Amazon CloudFront — Dieser AWS Compute-Blogbeitrag bietet eine Header-basierte Versionierungsstrategie als Alternative zu der in diesem Muster beschriebenen pfadbasierten Versionierungsstrategie.
- AWS CDK Workshop — Dieser Einführungsworkshop konzentriert sich auf das Erstellen und Bereitstellen von Anwendungen mithilfe von. AWS AWS Cloud Development Kit (AWS CDK) Dieser Workshop unterstützt Go, Python und TypeScript.

Zusätzliche Informationen

Testen Sie Ihre API mit Bruno

Wir empfehlen Ihnen, Bruno, ein Open-Source-API-Testtool, zu verwenden, um zu überprüfen, ob das pfadbasierte Routing für die Beispielanwendung ordnungsgemäß funktioniert. Dieses Muster bietet eine Beispielsammlung, um das Testen Ihrer Beispiel-API zu erleichtern.

Gehen Sie wie folgt vor, um Ihre API aufzurufen und zu testen:

1. Installieren Sie Bruno.
2. Öffne Bruno.
3. Wählen Sie im Code-Repository dieses Musters Bruno/Sample-API- Gateway-Custom-Domain-Versioning aus und öffnen Sie die Sammlung.
4. Um das Drop-down-Menü Umgebungen oben rechts auf der Benutzeroberfläche (UI) zu sehen, wählen Sie eine beliebige Anfrage in der Sammlung aus.
5. Wählen Sie im Drop-down-Menü Umgebungen die Option Konfigurieren aus.
6. Ersetzen Sie den `REPLACE_ME_WITH_YOUR_DOMAIN` Wert durch Ihre benutzerdefinierte Domain.
7. Wählen Sie Speichern und schließen Sie dann den Abschnitt Konfiguration.
8. Vergewissern Sie sich, dass für Sandbox Environment die Option Aktiv ausgewählt ist.
9. Rufen Sie Ihre API auf, indem Sie die Schaltfläche -> für die ausgewählte Anfrage verwenden.
10. Beachten Sie, wie die Validierung (Weitergabe von Werten, die keine Zahlen sind) in V1 im Vergleich zu V2 gehandhabt wird.

Screenshots eines Beispiel-API-Aufrufs und eines Vergleichs der V1- und V2-Validierung finden Sie unter Testen Ihrer Beispiel-API in der `README.md` Datei im Code-Repository dieses Musters.

Importieren Sie die psycopg2-Bibliothek, AWS Lambda um mit Ihrer PostgreSQL-Datenbank zu interagieren

Erstellt von Louis Hourcade (AWS)

Übersicht

Psycopg ist ein PostgresSQL-Datenbankadapter für Python. Entwickler verwenden die `psycopg2` Bibliothek, um Python-Anwendungen zu schreiben, die mit PostgreSQL-Datenbanken interagieren.

Auf Amazon Web Services (AWS) verwenden Entwickler auch, AWS Lambdaum Code für Anwendungen oder Backend-Services auszuführen. Lambda ist ein serverloser, ereignisgesteuerter Rechendienst, der Code ausführt, ohne dass Server bereitgestellt oder verwaltet werden müssen.

Wenn Sie eine neue Funktion erstellen, die eine Python-Laufzeit (Version 3.9, 3.8 oder 3.7) verwendet, wird die Lambda-Laufzeitumgebung standardmäßig aus einem Basis-Image für Lambda erstellt, das von bereitgestellt wird. AWS Bibliotheken wie `pandas` oder `psycopg2` sind nicht im Basisimage enthalten. Um eine Bibliothek zu verwenden, müssen Sie sie in einem benutzerdefinierten Paket bündeln und an Lambda anhängen.

Es gibt mehrere Möglichkeiten, eine Bibliothek zu bündeln und anzuhängen, darunter die folgenden:

- Stellen Sie Ihre Lambda-Funktion aus einem ZIP-Dateiarchiv bereit.
- Stellen Sie Ihre Lambda-Funktion von einem benutzerdefinierten Container-Image aus bereit.
- Erstellen Sie eine Lambda-Schicht und fügen Sie sie Ihrer Lambda-Funktion hinzu.

Dieses Muster demonstriert die ersten beiden Optionen.

Mit einem ZIP-Bereitstellungspaket ist das Hinzufügen der `pandas` Bibliothek zu Ihrer Lambda-Funktion relativ einfach. Erstellen Sie einen Ordner auf Ihrem Linux-Computer, fügen Sie das Lambda-Skript zusammen mit der `pandas` Bibliothek und den Abhängigkeiten der Bibliothek zum Ordner hinzu, komprimieren Sie den Ordner und stellen Sie ihn als Quelle für Ihre Lambda-Funktion bereit.

Obwohl die Verwendung eines ZIP-Bereitstellungspakets eine gängige Praxis ist, funktioniert dieser Ansatz für die Bibliothek nicht. `psycopg2` Dieses Muster zeigt zunächst den Fehler, den Sie erhalten, wenn Sie ein ZIP-Bereitstellungspaket verwenden, um die `psycopg2` Bibliothek zu Ihrer Lambda-Funktion hinzuzufügen. Das Muster zeigt dann, wie Lambda aus einem Dockerfile bereitgestellt und das Lambda-Image bearbeitet wird, damit die Bibliothek funktioniert. `psycopg2`

Informationen zu den drei Ressourcen, die das Muster bereitstellt, finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein Aktiv AWS-Konto mit ausreichenden Berechtigungen, um die von diesem Muster verwendeten AWS Ressourcen bereitzustellen
- AWS Cloud Development Kit (AWS CDK) wird global installiert, indem Folgendes ausgeführt wird `npm install -g aws-cdk`
- Ein Git-Client
- Python
- Docker

Einschränkungen

- Einige AWS-Services sind nicht in allen verfügbar AWS-Regionen. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie auf der Seite Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Produktversionen

- AWS Lambda Lambda-Laufzeitversion: Python 3.8 (Das Muster kann für andere Python-Versionen angepasst werden.)
- Psycopg2 Version 2.9.3
- Pandas versie 1.5.2

Architektur

Überblick über die Lösung

Um die Herausforderungen zu veranschaulichen, denen Sie bei der Verwendung der `psycopg2` Bibliothek in Lambda begegnen könnten, stellt das Muster zwei Lambda-Funktionen bereit:

- Eine Lambda-Funktion mit der Python 3.8-Laufzeit, die aus einer ZIP-Datei erstellt wurde. Die `pandas` Bibliotheken `psycopg2` und werden in diesem ZIP-Bereitstellungspaket mithilfe von pip installiert.
- Eine Lambda-Funktion mit der Python 3.8-Laufzeit, die aus einem Dockerfile erstellt wurde. Das Dockerfile installiert die `pandas` Bibliotheken `psycopg2` und im Lambda-Container-Image.

Die erste Lambda-Funktion installiert die `pandas` Bibliothek und ihre Abhängigkeiten in einer ZIP-Datei, und Lambda kann diese Bibliothek verwenden.

Die zweite Lambda-Funktion zeigt, dass Sie die `psycopg2` Bibliotheken `pandas` und in Lambda ausführen können, indem Sie ein Container-Image für Ihre Lambda-Funktion erstellen.

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK)ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.

Andere Tools

- Docker ist eine Reihe von Platform-as-a-Service (PaaS) -Produkten, die Virtualisierung auf Betriebssystemebene nutzen, um Software in Containern bereitzustellen.
- pandas ist ein Python-basiertes Open-Source-Tool zur Datenanalyse und -manipulation.
- Psycopg ist ein PostgreSQL-Datenbankadapter für die Python-Sprache, der für Multithread-Anwendungen entwickelt wurde. Dieses Muster verwendet Psycopg 2.
- Python ist eine Allzweck-Computerprogrammiersprache.

Code-Repository

Der Code für dieses Muster ist im import-psycopg2- in-lambda-to-interact -Repository unter verfügbar. with-postgres-database GitHub

Bewährte Methoden

Dieses Muster bietet Ihnen ein funktionierendes Beispiel für die Erstellung einer Lambda-Funktion aus einem Dockerfile. AWS CDK Wenn Sie diesen Code in Ihrer Anwendung wiederverwenden, stellen Sie sicher, dass die bereitgestellten Ressourcen alle Sicherheitsanforderungen erfüllen. Verwenden Sie Tools wie Checkov, das Cloud-Infrastrukturkonfigurationen scannt, um Fehlkonfigurationen zu finden, bevor die Infrastruktur bereitgestellt wird.

Epen

Klonen Sie das Repository und konfigurieren Sie die Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Klonen Sie das Repository	Führen Sie die folgenden Befehle aus, um das GitHub Repository auf Ihrem lokalen Computer zu klonen:
	`git clone https://github.com/aws-samples/import-psycopg2-in-lambda-to-interact-with-postgres-database.git`
	`cd AWS-lambda-psycopg2`
		Allgemeines AWS

Konfigurieren Sie Ihre Bereitstellung.	Bearbeiten Sie die `app.py` Datei mit Informationen zu Ihren AWS-Konto:
	`aws_acccount = "AWS_ACCOUNT_ID"`
	`region = "AWS_REGION"`
	`# Select the CPU architecture you are using to build the image (ARM or X86)`
	`architecture = "ARM"`
		Allgemeines AWS

Starten Sie Ihr AWS-Konto und stellen Sie die Anwendung bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bootstrap dein AWS-Konto.	Wenn Sie Ihre AWS-Umgebung noch nicht gebootet haben, führen Sie die folgenden Befehle mit den AWS Anmeldeinformationen Ihres AWS Kontos aus: `cdk bootstrap aws://<tooling-account-id>/<aws-region>`	Allgemeines AWS
Stellen Sie den Code bereit.	Führen Sie den folgenden Befehl aus, um die AWS CDK Anwendung bereitzustellen: `cdk deploy AWSLambdaPyscopg2`	Allgemeines AWS

Testen Sie die Lambda-Funktionen von der AWS-Managementkonsole aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Lambda-Funktion, die aus der ZIP-Datei erstellt wurde.	Gehen Sie wie folgt vor, um die Lambda-Funktion zu testen, die aus der ZIP-Datei erstellt wurde: 1. Melden Sie sich bei der Konsole an und öffnen Sie die Lambda-Konsole unter https://console.aws.amazon.com/lambda/.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie die `lambda-from-zip` Lambda-Funktion aus. 3. Erstellen Sie ein Testereignis, um die Funktion aufzurufen. 4. Wenn die Funktion aufgerufen wird, sollte sie einen Fehler auslösen, der die folgende Meldung enthält: `"errorMessage": Unable to import module 'lambda_code': libpq.so.5: cannot open shared object, "stackTrace": [] "errorType": Runtime.ImportModuleError",` 5. Öffnen Sie die CloudWatch Amazon-Konsole unter https://console.aws.amazon.com/cloudwatch/. Aus den CloudWatch Protokollen geht hervor, dass die `pandas` Bibliothek erfolgreich importiert wurde, der `psycopg2` Bibliotheksimport jedoch fehlgeschlagen ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Da Lambda die erforderlichen PostgreSQL-Bibliotheken im Standard-Image nicht findet, kann es die Bibliothek nicht verwenden. `psycopg2`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Testen Sie die Lambda-Funktion, die aus dem Dockerfile erstellt wurde.	Um die `psycopg2` Bibliothek in Ihrer Lambda-Funktion zu verwenden, müssen Sie das Lambda Amazon Machine Image (AMI) bearbeiten.
	
	Gehen Sie wie folgt vor, um die Lambda-Funktion zu testen, die aus dem Dockerfile erstellt wurde:
	
	1. Melden Sie sich bei der Konsole an und öffnen Sie die Lambda-Konsole.
	2. Wählen Sie die `lambda-from-docker` Lambda-Funktion aus.
	3. Erstellen Sie ein Testereignis, um die Funktion aufzurufen.
	4. Wenn die Funktion aufgerufen wird, sollte sie erfolgreich ausgeführt werden.
	
	Der folgende Code zeigt das Dockerfile, das die AWS CDK Vorlage erstellt:
	
	`# Start from lambda Python3.8 image`
	`FROM public.ecr.aws/lambda/python:3.8`
		Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	``
	# Copy the lambda code,
	 together with its
	 requirements
	COPY lambda/requirement
	s.txt ${LAMBDA_
	TASK_ROOT}
	COPY lambda/lambda_code
	.py ${LAMBDA_TASK_ROOT
	}
	
	# Install postgresql-
	devel in your image
	RUN yum install -y gcc
	 postgresql-devel
	
	# install the requireme
	nts for the Lambda code
	RUN pip3 install -r
	 requirements.txt
	 --target "${LAMBDA
	_TASK_ROOT}"
	
	# Command can be
	 overwritten by
	 providing a different
	 command in the template
	 directly.
	CMD ["lambda_code.hand
	ler"]
	``
	
	Das Dockerfile verwendet das AWS bereitgestellte Lambda-Image für die Python 3.8-Laufzeit und installiert postgresql-devel, das die Bibliotheken enthält, die zum Kompilieren von Anwendungen benötigt werden, die direkt mit dem PostgreSQL-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Managementserver interagieren. Das Dockerfile installiert auch die Bibliotheken und, die in der Datei angegeben sind. `pandas` `psycopg2` `requirements.txt`	

Zugehörige Ressourcen

- AWS CDK Dokumentation
- AWS Lambda Dokumentation

Zusätzliche Informationen

In diesem Muster stellt die AWS CDK Vorlage einen AWS Stapel mit drei Ressourcen bereit:

- Eine AWS Identity and Access Management (IAM-) Rolle für die Lambda-Funktionen.
- Eine Lambda-Funktion mit einer Python 3.8-Laufzeit. Die Funktion wird aus dem `Constructs/lambda/lambda_deploy.zip` Bereitstellungspaket bereitgestellt.
- Eine Lambda-Funktion mit einer Python 3.8-Laufzeit. Die Funktion wird über das Dockerfile unter dem Ordner bereitgestellt `Constructs`

Das Skript für beide Lambda-Funktionen prüft, ob die `psycopg2` Bibliotheken `pandas` und d erfolgreich importiert wurden:

```
import pandas
print("pandas successfully imported")

import psycopg2
print("psycopg2 successfully imported")

def handler(event, context):
    """Function that checks whether psycopg2  and pandas are successfully imported or
 not"""
    return {"Status": "psycopg2 and pandas successfully imported"}
```

Das `lambda_deploy.zip` Bereitstellungspaket wird mit dem `Constructs/lambda/build.sh` Bash-Skript erstellt. Dieses Skript erstellt einen Ordner, kopiert das Lambda-Skript, installiert die `psycopg2` Bibliotheken `pandas` und und generiert die ZIP-Datei. Um die .zip-Datei selbst zu generieren, führen Sie dieses Bash-Skript aus und stellen Sie den Stack erneut bereit. AWS CDK

Das Dockerfile beginnt mit dem AWS bereitgestellten Basis-Image für Lambda mit einer Python 3.8-Laufzeit. Das Dockerfile installiert die `psycopg2` Bibliotheken `pandas` und über dem Standard-Image.

Integrieren Sie Amazon API Gateway mit Amazon SQS, um asynchrones REST zu handhaben APIs

Erstellt von Natalia Colantonio Favero (AWS) und Gustavo Martim (AWS)

Übersicht

Wenn Sie REST bereitstellen APIs, müssen Sie manchmal eine Nachrichtenwarteschlange bereitstellen, die Client-Anwendungen veröffentlichen können. Möglicherweise haben Sie Probleme mit der Latenz von Drittanbietern APIs und Verzögerungen bei den Antworten, oder Sie möchten die Antwortzeit von Datenbankabfragen vermeiden oder vermeiden, den Server zu skalieren, wenn eine große Anzahl gleichzeitiger APIs Server vorhanden ist. In diesen Szenarien müssen die Client-Anwendungen, die in der Warteschlange veröffentlichen, nur wissen, dass die API die Daten empfangen hat — nicht, was nach dem Empfang der Daten passiert.

Dieses Muster erstellt einen REST-API-Endpunkt, indem Amazon API Gateway verwendet wird, um eine Nachricht an Amazon Simple Queue Service (Amazon SQS) zu senden. Es schafft eine easy-to-implement Integration zwischen den beiden Diensten, wodurch ein direkter Zugriff auf die SQS-Warteschlange vermieden wird.

Voraussetzungen und Einschränkungen

- Ein aktives Konto AWS

Architektur

Das Diagramm veranschaulicht diese Schritte:

1. Fordern Sie einen POST-REST-API-Endpunkt an, indem Sie ein Tool wie Postman, eine andere API oder andere Technologien verwenden.
2. API Gateway stellt eine Nachricht, die im Hauptteil der Anfrage empfangen wird, in die Warteschlange.
3. Amazon SQS empfängt die Nachricht und sendet eine Antwort mit einem Erfolgs- oder Fehlercode an API Gateway.

Tools

- Amazon API Gateway unterstützt Sie bei der Erstellung, Veröffentlichung, Wartung, Überwachung und Sicherung von REST, HTTP und WebSocket APIs in jeder Größenordnung.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.

Epen

Erstellen Sie eine SQS-Warteschlange

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Warteschlange.	So erstellen Sie eine SQS-Warteschlange, die die Nachrichten von der REST-API empfängt: 1. Melden Sie sich bei AWS-Konto an. 2. Öffnen Sie die Amazon SQS SQS-Konsole unter https://console.aws.amazon.com/sqs/. 3. Wählen Sie Create queue (Warteschlange erstellen) aus. 4. Wählen Sie auf der Seite Warteschlange erstellen die richtige Option AWS-Region aus der Dropdownliste Region aus.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Behalten Sie für Typ die Standardeinstellung (Standard) bei. 6. Geben Sie einen Namen für die Warteschlange ein. 7. Behalten Sie die Standardwerte für alle anderen Einstellungen bei. 8. Wählen Sie Create queue (Warteschlange erstellen) aus.	

Zugriff auf Amazon SQS bereitstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle.	Diese IAM-Rolle gewährt API Gateway Gateway-Ressourcen vollen Zugriff auf Amazon SQS. 1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole. 2. Wählen Sie im Navigationsbereich Roles (Rollen) und Create Role (Rolle erstellen) aus. 3. Wählen Sie für Vertrauenswürdige Entität die Option AWS-Service aus. 4. Wählen Sie unter Anwendungsfall die Option	App-Entwickler, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	API Gateway aus der Dropdownliste aus und wählen Sie dann Weiter, Weiter aus. 5. Geben Sie als Rollenname AWSGateway RoleForSQS und eine optionale Beschreibung ein und wählen Sie dann Rolle erstellen aus. 6. Suchen Sie im Bereich Rollen nach AWSGatewayRoleForSQS und aktivieren Sie das entsprechende Kontrollkästchen. 7. Unter Berechtigungsrichtlinien im Abschnitt Berechtigungen hinzufügen wählen Sie Richtlinien anfügen aus. 8. Suchen Sie nach Amazon SQSFull Access und wählen Sie es aus. 9. Wählen Sie Add permissions (Berechtigungen hinzufügen) aus. 10. Kopieren Sie im Abschnitt Zusammenfassung von AWSGatewayRoleForSQS die Amazon-Ressourcennummer (ARN). Sie werden diese ID in einem späteren Schritt verwenden.	

Erstellen Sie eine REST-API

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine REST-API.	Dies ist die REST-API, an die HTTP-Anfragen gesendet werden. 1. Öffnen Sie die API Gateway Gateway-Konsole unter https://console.aws.amazon.com/apigateway/. 2. Wählen Sie im Abschnitt REST-API die Option Build aus. 3. Geben Sie als API-Name einen Namen und eine optionale Beschreibung für Ihre API ein, behalten Sie alle anderen Standarde instellungen bei und wählen Sie dann Create API aus.	App-Developer
Connect API Gateway mit Amazon SQS.	Dieser Schritt ermöglicht es, dass die Nachricht aus dem Hauptteil der HTTP-Anfrage an Amazon SQS weitergeleitet wird. 1. Wählen Sie in der API Gateway Gateway-Konsole die API aus, die Sie erstellt haben. 2. Wählen Sie auf der Seite Ressourcen im Abschnitt Methoden die Option Methode erstellen aus.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie in Method type (Methodentyp) POST. 4. Wählen Sie als Integrationstyp die Option AWS-Service. 5. Wählen Sie für die Region aus AWS-Region, in der Sie Ihre SQS-Warteschlange erstellt haben. 6. Wählen Sie für AWS-Service SimpleQueue Service (SQS). 7. Wählen Sie als HTTP-Methode POST aus. 8. Wählen Sie als Aktionstyp die Option Pfadüberschreibung verwenden aus. 9. Geben Sie für Path Override den Wert/<AWS account ID>ein<name of SQS queue>. 10. Fügen Sie für die Ausführungsrolle den ARN der Rolle ein, die Sie zuvor erstellt haben. 11. Wählen Sie Methode erstellen aus.	

Testen Sie die REST-API

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Testen Sie die REST-API.	Führen Sie einen Test durch, um zu überprüfen, ob die Konfiguration fehlt:
	1. Wählen Sie in der API Gateway Gateway-Konsole die REST-API aus, die Sie erstellt haben.
	2. Wählen Sie im Bereich Ressourcen die POST-Methode aus.
	3. Wählen Sie die Registerkarte Test. (Verwenden Sie den Rechtspfeil, wenn die Registerkarte nicht angezeigt wird.)
	4. Fügen Sie in das Feld Hauptteil der Anfrage den folgenden JSON-Code ein:
	`{ "message": "lorem ipsum" }`
	5. Wählen Sie Test aus.
	Sie erhalten eine Fehlermeldung, die der folgenden ähnelt:
	`<UnknownOperationException/>`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die API-Integration, um die Anfrage ordnungsgemäß an Amazon SQS weiterzuleiten.	Vervollständigen Sie die Konfiguration, um den Integrationsfehler zu beheben: 1. Wählen Sie in der API Gateway Gateway-Konsole die API aus, die Sie erstellt haben, und wählen Sie dann POST. 2. Der Abschnitt Method Execution zeigt die visuelle Zuordnung zwischen API Gateway und Amazon SQS. Wählen Sie in diesem Abschnitt Integrationsanfrage und dann Bearbeiten aus. 3. Erweitern Sie den Abschnitt HTTP-Header und wählen Sie dann den Parameter Anforderungsheader hinzufügen aus. • Geben Sie für Name Content-Type an. • Geben Sie für Zugeordnet von den Namen „application/“ ein. x-www-form-urlencoded Achten Sie darauf, die einfachen Anführungszeichen einzuschließen. • Wählen Sie das Kontrollkästchen Caching aus. 4. Erweitern Sie den Abschnitt Mapping-Vorlagen.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wählen Sie Add mapping template. • Geben Sie als Inhaltstyp application/json ein. • Fügen Sie für den Vorlagentext diesen Code ein: `Action=SendMessage&MessageBody=$input.body` • Wählen Sie Speichern.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen und validieren Sie die Nachricht in Amazon SQS.	Führen Sie einen Test durch, um zu bestätigen, dass der Test erfolgreich abgeschlossen wurde: 1. Wählen Sie in der API Gateway Gateway-Konsole die REST-API aus, die Sie erstellt haben. 2. Wählen Sie im Bereich Ressourcen die POST-Methode aus. 3. Wählen Sie die Registerkarte Test. (Verwenden Sie den Rechtspfeil, wenn die Registerkarte nicht angezeigt wird.) 4. Fügen Sie in das Feld Hauptteil der Anfrage den folgenden JSON-Code ein: `{ "message": "lorem ipsum" }` 5. Wählen Sie Test aus. 6. Öffnen Sie die Amazon-SQS-Konsole. 7. Wählen Sie im Navigationsbereich Warteschlangen und dann Ihre Warteschlange aus. 8. Wählen Sie Nachrichten senden und empfangen.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	9. Wählen Sie Abfragen von Nachrichten. 10. Wählen Sie Message (Nachricht)aus. Es sollte Folgendes angezeigt werden: `Body { "message": "lorem ipsum" }`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Testen Sie API Gateway mit einem Sonderzeichen.	Führen Sie einen Test aus, der Sonderzeichen (wie &) enthält, die in einer Nachricht nicht zulässig sind:
	1. Wählen Sie in der API Gateway Gateway-Konsole Ihre API aus.
	2. Wiederholen Sie den Test aus dem vorherigen Schritt, indem Sie den folgenden JSON-Code verwenden:
	`{ "message": "lorem ipsum &" }`
	3. Wählen Sie Test aus.
	Sie erhalten eine Fehlermeldung wie die folgende:
	`{ "Error": { "Code": "AccessDenied", "Message": "Access to the resource https://sqs.us-east-2.amazonaws.com/976166761794/Apg2 is denied.", "Type": "Sender" }, "RequestId": "e83c9c67-bcf6-5e9`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>a-91e9-c737094b17a
	b"
	}</pre>
	Das liegt daran, dass Sonderzeichen im Nachricht entext standardmäßig nicht unterstützt werden. Im nächsten Schritt konfigurieren Sie API Gateway so, dass es Sonderzeichen unterstüt zt. Weitere Informationen zu Inhaltstypkonvertierungen finden Sie in der API Gateway Gateway-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die API-Konfiguration, sodass Sonderzeichen unterstützt werden.	Passen Sie die Konfiguration so an, dass Sonderzeichen in der Nachricht akzeptiert werden: 1. Wählen Sie in der API Gateway Gateway-Konsole die API aus, die Sie erstellt haben, und wählen Sie dann POST. 2. Wählen Sie Integrationsanforderung aus und klicken Sie dann auf Bearbeiten. 3. Ändern Sie die Inhaltsverwaltung in In Text konvertieren. 4. Gehen Sie im Abschnitt Mapping-Vorlagen wie folgt vor: • Geben Sie als Inhaltstyp application/json ein. • Geben Sie für den Hauptteil der Vorlage Folgendes an: `Action=SendMessage&MessageBody=$util.urlEncode($input.body)` • Wählen Sie Speichern. 5. Wählen Sie die Registerkarte Test.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Geben Sie für Request body den JSON-Code von früher ein: `{ " message": "lorem ipsum &" }` 7. Wählen Sie Test aus. 8. Öffnen Sie die Amazon-SQS-Konsole. 9. Wählen Sie Ihre Warteschlange aus und wählen Sie dann Nachrichten senden und empfangen, Nach Nachrichten abfragen, Nachricht wie zuvor aus. Die neue Nachricht sollte das Sonderzeichen enthalten.	

Stellen Sie die REST-API bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die API bereit.	So stellen Sie die REST-API bereit: 1. Öffnen Sie die API Gateway-Konsole. 2. Wählen Sie Ihre API aus. 3. Klicken Sie auf Deploy API. Weitere Informationen zu diesem Schritt finden Sie in	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der API Gateway Gateway-Dokumentation.	
Testen Sie mit einem externen Tool.	Führen Sie einen Test mit einem externen Tool durch, um zu bestätigen, dass die Nachricht erfolgreich empfangen wurde: 1. Öffnen Sie ein Tool wie Postman, Insomnia oder cURL. 2. Führen Sie Ihre API aus. 3. Öffnen Sie die Amazon-SQS-Konsole. 4. Wählen Sie Ihre Warteschlange aus. 5. Laden Sie Nachrichten, um die neue Nachricht zu sehen.	App-Developer

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die API.	Wählen Sie in der API Gateway Gateway-Konsole die API aus, die Sie erstellt haben, und klicken Sie dann auf Löschen.	App-Developer
Löschen Sie die IAM-Rolle.	Wählen Sie in der IAM-Konsole im Bereich Rollen die	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Option AWSGatewayRoleForSQS und dann Löschen aus.	
Löschen Sie die SQS-Warteschlange.	Wählen Sie auf der Amazon SQS SQS-Konsole im Bereich Warteschlangen die SQS-Warteschlange aus, die Sie erstellt haben, und klicken Sie dann auf Löschen.	App-Developer

Zugehörige Ressourcen

- SQS- SendMessage (API Gateway Gateway-Dokumentation)
- Inhaltstypkonvertierungen in API Gateway (API Gateway Gateway-Dokumentation)
- $util-Variablen (API Gateway Gateway-Dokumentation)
- Wie integriere ich eine API Gateway Gateway-REST-API in Amazon SQS und behebe häufig auftretende Fehler? (AWS Re:POST-Artikel)

Ereignisse asynchron mit Amazon API Gateway und AWS Lambda verarbeiten

Erstellt von Andrea Meroni (AWS), Nadim Majed (AWS), Mariem Kthiri (AWS) und Michael Wallner (AWS)

Übersicht

Amazon API Gateway ist ein vollständig verwalteter Service, mit dem Entwickler in jeder Größenordnung erstellen, veröffentlichen, warten, überwachen und sichern APIs können. Er erledigt die Aufgaben, die mit der Annahme und Verarbeitung von bis zu Hunderttausenden von gleichzeitigen API-Aufrufen verbunden sind.

Eine wichtige Servicequote von API Gateway ist das Integrations-Timeout. Das Timeout ist die maximale Zeit, in der ein Backend-Dienst eine Antwort zurückgeben muss, bevor die REST-API einen Fehler zurückgibt. Das feste Limit von 29 Sekunden ist für synchrone Workloads im Allgemeinen akzeptabel. Dieses Limit stellt jedoch eine Herausforderung für Entwickler dar, die API Gateway mit asynchronen Workloads verwenden möchten.

Dieses Muster zeigt eine Beispielarchitektur für die asynchrone Verarbeitung von Ereignissen mithilfe von API Gateway und AWS Lambda. Die Architektur unterstützt die Ausführung von Verarbeitungsaufträgen mit einer Dauer von bis zu 15 Minuten und verwendet eine einfache REST-API als Schnittstelle.

Projen wird verwendet, um die lokale Entwicklungsumgebung einzurichten und die Beispielarchitektur in Kombination mit dem AWS Cloud Development Kit (AWS CDK) Toolkit AWS-Konto, Docker und Node.js auf einem Ziel bereitzustellen. Projen richtet automatisch eine virtuelle Python-Umgebung mit Pre-Commit und den Tools ein, die für die Qualitätssicherung des Codes, Sicherheitsscans und Unit-Tests verwendet werden. Weitere Informationen finden Sie im Abschnitt Tools.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Die folgenden Tools sind auf Ihrer Workstation installiert:
  - AWS Cloud Development Kit (AWS CDK) Toolkit-Version 2.85.0
  - Docker-Version 20.10.21
  - Node.js, Version 18.13.0

- Bewährte Version 0.71.111
- Python-Version 3.9.16

Einschränkungen

- Die maximale Laufzeit eines Jobs ist durch die maximale Laufzeit für Lambda-Funktionen (15 Minuten) begrenzt.
- Die maximale Anzahl gleichzeitiger Jobanfragen ist durch die reservierte Parallelität der Lambda-Funktion begrenzt.

Architektur

Das folgende Diagramm zeigt die Interaktion der Jobs-API mit den Lambda-Funktionen zur Ereignisverarbeitung und Fehlerbehandlung, wobei Ereignisse in einem Amazon-Ereignisarchiv gespeichert werden. EventBridge

Ein typischer Arbeitsablauf umfasst die folgenden Schritte:

1. Sie authentifizieren sich bei AWS Identity and Access Management (IAM) und erhalten Sicherheitsanmeldedaten.
2. Sie senden eine `POST` HTTP-Anfrage an den `/jobs` Jobs-API-Endpunkt und geben dabei die Jobparameter im Hauptteil der Anfrage an.
3. Die Jobs-API, bei der es sich um eine API-Gateway-REST-API handelt, gibt Ihnen eine HTTP-Antwort zurück, die die Job-ID enthält.
4. Die Jobs-API ruft asynchron die Lambda-Funktion zur Ereignisverarbeitung auf.
5. Die Funktion zur Ereignisverarbeitung verarbeitet das Ereignis und fügt dann die Auftragsergebnisse in die Amazon DynamoDB-Tabelle der Jobs ein.
6. Sie senden eine `GET` HTTP-Anfrage an den `/jobs/{jobId}` Job-API-Endpunkt mit der Job-ID aus Schritt 3 als. `{jobId}`
7. Die Jobs-API fragt die `jobs` DynamoDB-Tabelle ab, um die Auftragsergebnisse abzurufen.
8. Die Jobs-API gibt eine HTTP-Antwort zurück, die die Auftragsergebnisse enthält.
9. Wenn die Ereignisverarbeitung fehlschlägt, sendet die Ereignisverarbeitungsfunktion das Ereignis an die Fehlerbehandlungsfunktion.
10. Die Fehlerbehandlungsfunktion platziert die Jobparameter in der `jobs` DynamoDB-Tabelle.

11. Sie können die Job-Parameter abrufen, indem Sie eine `GET` HTTP-Anfrage an den `/jobs/{jobId}` Jobs-API-Endpunkt senden.
12. Wenn die Fehlerbehandlung fehlschlägt, sendet die Fehlerbehandlungsfunktion das Ereignis an ein EventBridge Ereignisarchiv.

    Sie können die archivierten Ereignisse erneut abspielen, indem Sie. EventBridge

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK)ist ein Softwareentwicklungs-Framework, das Ihnen hilft, AWS Cloud Infrastruktur im Code zu definieren und bereitzustellen.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel Lambda-Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen. AWS-Konten
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.

Andere Tools

- autopep8 formatiert Python-Code automatisch auf der Grundlage des Python Enhancement Proposal (PEP) 8-Styleguides.
- Bandit scannt Python-Code, um häufig auftretende Sicherheitsprobleme zu finden.
- Commitizen ist ein Git-Commit-Checker und -Generator. `CHANGELOG`
- cfn-lint ist ein Linter AWS CloudFormation
- Checkov ist ein statisches Code-Analyse-Tool, das Infrastructure as Code (IaC) auf Sicherheits- und Compliance-Fehlkonfigurationen überprüft.
- jq ist ein Befehlszeilentool zum Parsen von JSON.
- Postman ist eine API-Plattform.

- pre-commit ist ein Git-Hooks-Manager.
- Projen ist ein Projektgenerator.
- pytest ist ein Python-Framework zum Schreiben kleiner, lesbarer Tests.

Code-Repository

Dieser Beispielarchitekturcode befindet sich im Repository GitHub Asynchronous Event Processing with API Gateway and Lambda.

Bewährte Methoden

- Diese Beispielarchitektur beinhaltet keine Überwachung der bereitgestellten Infrastruktur. Wenn Ihr Anwendungsfall eine Überwachung erfordert, sollten Sie das Hinzufügen von CDK Monitoring Constructs oder einer anderen Überwachungslösung in Betracht ziehen.
- Diese Beispielarchitektur verwendet IAM-Berechtigungen, um den Zugriff auf die Jobs-API zu steuern. Jeder, der autorisiert ist, `JobsAPIInvokeRole` dies anzunehmen, kann die Jobs-API aufrufen. Daher ist der Zugriffskontrollmechanismus binär. Wenn Ihr Anwendungsfall ein komplexeres Autorisierungsmodell erfordert, sollten Sie es mit einem anderen Zugriffskontrollmechanismus testen.
- Wenn ein Benutzer eine `POST` HTTP-Anfrage an den `/jobs` Jobs-API-Endpunkt sendet, werden die Eingabedaten auf zwei verschiedenen Ebenen validiert:
  - Amazon API Gateway ist für die erste Anforderungsvalidierung verantwortlich.
  - Die Funktion zur Ereignisverarbeitung führt die zweite Anfrage durch.

    Es wird keine Überprüfung durchgeführt, wenn der Benutzer eine `GET` HTTP-Anfrage an den `/jobs/{jobId}` Jobs-API-Endpunkt sendet. Wenn Ihr Anwendungsfall eine zusätzliche Eingabevalidierung und ein höheres Maß an Sicherheit erfordert, sollten Sie die Verwendung von AWS WAF zum Schutz Ihrer API in Betracht ziehen.

Epen

Richte die Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Führen Sie den folgenden Befehl aus, um das Repository lokal zu klonen: `git clone https://github.com/aws-samples/asynchronous-event-processing-api-gateway-lambda-cdk.git`	DevOps Ingenieur

Richten Sie das Projekt ein.	Ändern Sie das Verzeichnis in das Repository-Stammverzeichnis und richten Sie die virtuelle Python-Umgebung und alle Tools mithilfe von Projen ein:
	`cd asynchronous-event-processing-api-gateway-api-gateway-lambda-cdk`
	`npx projen`
		DevOps Ingenieur

Installieren Sie Pre-Commit-Hooks.	Gehen Sie wie folgt vor, um Pre-Commit-Hooks zu installieren: 1. Aktivieren Sie die virtuelle Python-Umgebung: `source .env/bin/activate`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	2. Installieren Sie die Pre-Commit-Hooks:
	`pre-commit install`
	`pre-commit install --hook-type commit-msg`	

Stellen Sie die Beispielarchitektur bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bootstrap. AWS CDK	Um AWS CDK in Ihrem zu booten AWS-Konto, führen Sie den folgenden Befehl aus: `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen bootstrap`	AWS DevOps
Stellen Sie die Beispielarchitektur bereit.	Führen Sie den folgenden Befehl aus AWS-Konto, um die Beispielarchitektur in Ihrem bereitzustellen: `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen deploy`	AWS DevOps

Testen Sie die Architektur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die Testvoraussetzungen.	Installieren Sie auf Ihrer Workstation the AWS	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Command Line Interface (AWS CLI), Postman und jq. Die Verwendung von Postman zum Testen dieser Beispiela rchitektur wird empfohlen , ist aber nicht zwingend erforderlich. Wenn Sie sich für ein alternatives API-Testt ool entscheiden, stellen Sie sicher, dass es die Authentif izierung mit AWS Signature Version 4 unterstützt, und beziehen Sie sich auf die exponierten API-Endpunkte, die durch den Export der REST-API überprüft werden können.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gehen Sie von der ausJobsAPIInvokeRole .	Gehen Sie davon ausJobsAPIInvokeRole , dass das als Ausgabe des Befehls deploy gedruckt wurde: `CREDENTIALS=$(AWS_ PROFILE=$<YOUR_AWS _PROFILE> aws sts assume-role \ --no-cli-pager \ --role-arn $<JOBS_AP I_INVOKE_ROLE_ARN> \ --role-session-name JobsAPIInvoke) export AWS_ACCES S_KEY_ID=$(cat $CREDENTIALS \| jq '.Credentials''.Ac cessKeyId') export AWS_SECRE T_ACCESS_KEY=$(cat $CREDENTIALS \| jq '.Credentials''.Se cretAccessKey') export AWS_SESSI ON_TOKEN==$(cat $CREDENTIALS | jq '.Credentials''.Se ssionToken')`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Postman konfigurieren.	1. Folgen Sie den Anweisungen in der Postman-Dokumentation, um die im Repository enthaltene Postman-Sammlung zu importieren. 2. Stellen Sie die `JobsAPI` Variablen mit den folgenden Werten ein: • `accessKey` – Der Wert des `Credentials.AccessKeyId` Attributs aus dem `assume-role` Befehl • `baseUrl`– Der Wert der `JobsApiJobsAPIEndpoint` Ausgabe des Befehls deploy ohne den abschließenden Schrägstrich • `region`– Der Wert der AWS-Region Stelle, an der Sie die Beispielarchitektur bereitgestellt haben • `seconds`– Der Wert des Eingabeparameters für den Beispieljob. Es muss eine positive Ganzzahl sein • `secretKey` – Der Wert des `Credentials.Secret`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`AccessKey` Attributs aus dem `assume-role` Befehl • `sessionToken` – Der Wert des `Credentials.SessionToken` Attributs aus dem `assume-role` Befehl	
Testen Sie die Beispielarchitektur.	Um die Beispielarchitektur zu testen, senden Sie Anfragen an die Jobs-API. Weitere Informationen finden Sie in der Postman-Dokumentation.	DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Die Zerstörung und anschließende erneute Bereitstellung der Beispielarchitektur schlägt fehl, da die Amazon CloudWatch Logs-Protokollgruppe `/aws/apigateway/JobsAPIAccessLogs` bereits existiert.	1. Exportieren Sie bei Bedarf Ihre Protokolldaten nach Amazon S3. 2. Löschen Sie die CloudWatch Protokollgruppe Logs `/aws/apigateway/JobsAPIAccessLogs` . 3. Stellen Sie die Beispielarchitektur erneut bereit.

Zugehörige Ressourcen

- API-Gateway-Zuordnungsvorlage und Referenz zur Zugriffsprotokollierungsvariablen
- Richten Sie den asynchronen Aufruf der Backend-Lambda-Funktion ein

Ereignisse asynchron mit Amazon API Gateway und Amazon DynamoDB Streams verarbeiten

Erstellt von Andrea Meroni (AWS), Alessandro Trisolini (AWS), Nadim Majed (AWS), Mariem Kthiri (AWS) und Michael Wallner (AWS)

Übersicht

Amazon API Gateway ist ein vollständig verwalteter Service, den Entwickler nutzen können, um sie in jeder Größenordnung zu erstellen, zu veröffentlichen, zu verwalten, APIs zu überwachen und zu sichern. Er erledigt die Aufgaben, die mit der Annahme und Verarbeitung von bis zu Hunderttausenden von gleichzeitigen API-Aufrufen verbunden sind.

Eine wichtige Servicequote von API Gateway ist das Integrations-Timeout. Das Timeout ist die maximale Zeit, in der ein Backend-Dienst eine Antwort zurückgeben muss, bevor die REST-API einen Fehler zurückgibt. Das feste Limit von 29 Sekunden ist für synchrone Workloads im Allgemeinen akzeptabel. Dieses Limit stellt jedoch eine Herausforderung für Entwickler dar, die API Gateway mit asynchronen Workloads verwenden möchten.

Dieses Muster zeigt eine Beispielarchitektur für die asynchrone Verarbeitung von Ereignissen mithilfe von API Gateway, Amazon DynamoDB Streams und. AWS Lambda Die Architektur unterstützt die Ausführung von Parallelverarbeitungsjobs mit denselben Eingabeparametern und verwendet eine grundlegende REST-API als Schnittstelle. In diesem Beispiel begrenzt die Verwendung von Lambda als Backend die Dauer von Jobs auf 15 Minuten. Sie können dieses Limit umgehen, indem Sie einen alternativen Dienst zur Verarbeitung eingehender Ereignisse verwenden (z. B. AWS Fargate).

Projen wird verwendet, um die lokale Entwicklungsumgebung einzurichten und die Beispielarchitektur in Kombination mit dem AWS Cloud Development Kit (AWS CDK) Toolkit AWS-Konto, Docker und Node.js auf einem Ziel bereitzustellen. Projen richtet automatisch eine virtuelle Python-Umgebung mit Pre-Commit und den Tools ein, die für die Qualitätssicherung des Codes, Sicherheitsscans und Unit-Tests verwendet werden. Weitere Informationen finden Sie im Abschnitt Tools.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Die folgenden Tools sind auf Ihrer Workstation installiert:
  - AWS Cloud Development Kit (AWS CDK) Toolkit-Version 2.85.0 oder höher

- Docker-Version 20.10.21 oder höher
- Node.js Version 18 oder höher
- Projen Version 0.71.111 oder höher
- Python-Version 3.9.16 oder höher

Einschränkungen

- Die empfohlene maximale Anzahl von Lesern für DynamoDB Streams ist zwei, um eine Drosselung zu vermeiden.
- Die maximale Laufzeit eines Jobs ist durch die maximale Laufzeit für Lambda-Funktionen (15 Minuten) begrenzt.
- Die maximale Anzahl gleichzeitiger Jobanfragen ist durch die reservierte Parallelität der Lambda-Funktionen begrenzt.

Architektur

Architektur

Das folgende Diagramm zeigt die Interaktion der Jobs-API mit DynamoDB Streams und den Lambda-Funktionen zur Ereignisverarbeitung und Fehlerbehandlung mit Ereignissen, die in einem Amazon-Ereignisarchiv gespeichert sind. EventBridge

Ein typischer Arbeitsablauf umfasst die folgenden Schritte:

1. Sie authentifizieren sich bei AWS Identity and Access Management (IAM) und erhalten Sicherheitsanmeldedaten.
2. Sie senden eine `POST` HTTP-Anfrage an den `/jobs` Jobs-API-Endpunkt und geben dabei die Jobparameter im Hauptteil der Anfrage an.
3. Die Jobs-API gibt Ihnen eine HTTP-Antwort zurück, die die Job-ID enthält.
4. Die Job-API platziert die Job-Parameter in der `jobs_table` Amazon DynamoDB-Tabelle.
5. Der `jobs_table` DynamoDB-Stream der DynamoDB-Tabelle ruft die Lambda-Funktionen zur Ereignisverarbeitung auf.
6. Die Lambda-Funktionen zur Ereignisverarbeitung verarbeiten das Ereignis und fügen dann die Auftragsergebnisse in die `jobs_table` DynamoDB-Tabelle ein. Um konsistente Ergebnisse

zu gewährleisten, implementieren die Funktionen zur Ereignisverarbeitung einen optimistischen Sperrmechanismus.

7. Sie senden eine `GET` HTTP-Anfrage an den `/jobs/{jobId}` Job-API-Endpunkt mit der Job-ID aus Schritt 3 als. `{jobId}`
8. Die Jobs-API fragt die `jobs_table` DynamoDB-Tabelle ab, um die Auftragsergebnisse abzurufen.
9. Die Jobs-API gibt eine HTTP-Antwort zurück, die die Auftragsergebnisse enthält.
10. Wenn die Ereignisverarbeitung fehlschlägt, sendet die Quellenzuordnung der Ereignisverarbeitungsfunktion das Ereignis an das Thema Amazon Simple Notification Service (Amazon SNS) zur Fehlerbehandlung.
11. Das SNS-Thema zur Fehlerbehandlung überträgt das Ereignis asynchron an die Fehlerbehandlungsfunktion.
12. Die Fehlerbehandlungsfunktion platziert die Jobparameter in der `jobs_table` DynamoDB-Tabelle.

    Sie können die Job-Parameter abrufen, indem Sie eine `GET` HTTP-Anfrage an den `/jobs/{jobId}` Jobs-API-Endpunkt senden.
13. Wenn die Fehlerbehandlung fehlschlägt, sendet die Fehlerbehandlungsfunktion das Ereignis an ein EventBridge Amazon-Archiv.

    Sie können die archivierten Ereignisse erneut abspielen, indem Sie EventBridge

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK)ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS-Lambda-Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen AWS-Konten.

- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.

Andere Tools

- autopep8 formatiert Python-Code automatisch auf der Grundlage des Python Enhancement Proposal (PEP) 8-Styleguides.
- Bandit scannt Python-Code, um häufig auftretende Sicherheitsprobleme zu finden.
- Commitizen ist ein Git-Commit-Checker und -Generator. `CHANGELOG`
- cfn-lint ist ein Linter AWS CloudFormation
- Checkov ist ein statisches Code-Analyse-Tool, das Infrastructure as Code (IaC) auf Sicherheits- und Compliance-Fehlkonfigurationen überprüft.
- jq ist ein Befehlszeilentool zum Parsen von JSON.
- Postman ist eine API-Plattform.
- pre-commit ist ein Git-Hooks-Manager.
- Projen ist ein Projektgenerator.
- pytest ist ein Python-Framework zum Schreiben kleiner, lesbarer Tests.

Code-Repository

Dieser Beispielarchitekturcode befindet sich im Repository GitHub Asynchronous Processing with API Gateway und DynamoDB Streams.

Bewährte Methoden

- Diese Beispielarchitektur beinhaltet keine Überwachung der bereitgestellten Infrastruktur. Wenn Ihr Anwendungsfall eine Überwachung erfordert, sollten Sie das Hinzufügen von CDK Monitoring Constructs oder einer anderen Überwachungslösung in Betracht ziehen.
- Diese Beispielarchitektur verwendet IAM-Berechtigungen, um den Zugriff auf die Jobs-API zu steuern. Jeder, der autorisiert ist, `JobsAPIInvokeRole` dies anzunehmen, kann die Jobs-API aufrufen. Daher ist der Zugriffskontrollmechanismus binär. Wenn Ihr

Anwendungsfall ein komplexeres Autorisierungsmodell erfordert, sollten Sie es mit einem anderen Zugriffskontrollmechanismus testen.

- Wenn ein Benutzer eine `POST` HTTP-Anfrage an den `/jobs` Jobs-API-Endpunkt sendet, werden die Eingabedaten auf zwei verschiedenen Ebenen validiert:
  - API Gateway ist für die erste Anforderungsvalidierung verantwortlich.
  - Die Funktion zur Ereignisverarbeitung führt die zweite Anfrage aus.

    Es wird keine Überprüfung durchgeführt, wenn der Benutzer eine `GET` HTTP-Anfrage an den `/jobs/{jobId}` Jobs-API-Endpunkt sendet. Wenn Ihr Anwendungsfall eine zusätzliche Eingabevalidierung und ein erhöhtes Sicherheitsniveau erfordert, sollten Sie den Einsatz AWS WAF zum Schutz Ihrer API in Betracht ziehen.

- Um eine Drosselung zu vermeiden, rät die DynamoDB Streams-Dokumentation Benutzern davon ab, mit mehr als zwei Verbrauchern vom Shard desselben Streams zu lesen. Um die Anzahl der Verbraucher zu erhöhen, empfehlen wir die Verwendung von Amazon Kinesis Data Streams.
- In diesem Beispiel wurde optimistisches Sperren verwendet, um sicherzustellen, dass Elemente in der `jobs_table` DynamoDB-Tabelle konsistent aktualisiert werden. Je nach Anforderung des Anwendungsfalls müssen Sie möglicherweise zuverlässigere Sperrmechanismen implementieren, z. B. pessimistisches Sperren.

Epen

Richte die Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Führen Sie den folgenden Befehl aus, um das Repository lokal zu klonen: `git clone https://github.com/aws-samples/asynchronous-event-processing-api-gateway-dynamodb-streams-cdk.git`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie das Projekt ein.	Ändern Sie das Verzeichnis in das Repository-Stammverzeichnis und richten Sie die virtuelle Python-Umgebung und alle Tools mithilfe von Projen ein:
	`cd asynchronous-event-processing-api-gateway-api-gateway-dynamodb-streams-cdk`
	`npx projen`
		DevOps Ingenieur

Installieren Sie Pre-Commit-Hooks.	Gehen Sie wie folgt vor, um Pre-Commit-Hooks zu installieren:
	1. Aktivieren Sie die virtuelle Python-Umgebung:
	`source .env/bin/activate`
	2. Installieren Sie die Pre-Commit-Hooks:
	`pre-commit install`
	`pre-commit install --hook-type commit-msg`
		DevOps Ingenieur

Stellen Sie die Beispielarchitektur bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bootstrap. AWS CDK	Um AWS CDKin Ihrem zu booten AWS-Konto, führen Sie den folgenden Befehl aus: `AWS_PROFILE=$YOUR_ AWS_PROFILE npx projen bootstrap`	AWS DevOps
Stellen Sie die Beispiela rchitektur bereit.	Führen Sie den folgenden Befehl aus AWS-Konto, um die Beispielarchitektur in Ihrem bereitzustellen: `AWS_PROFILE=$YOUR_ AWS_PROFILE npx projen deploy`	AWS DevOps

Testen Sie die Architektur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die Testvorau ssetzungen.	Installieren Sie auf Ihrer Workstation the AWS Command Line Interface (AWS CLI), Postman und jq. Die Verwendung von Postman zum Testen dieser Beispiela rchitektur wird empfohlen , ist aber nicht zwingend erforderlich. Wenn Sie sich für ein alternatives API-Testt ool entscheiden, stellen	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie sicher, dass es die AWS Signature Version 4-Authentifizierung unterstützt, und verweisen Sie auf die exponierten API-Endpunkte, die durch Exportieren der REST-API überprüft werden können.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gehen Sie von der aus`JobsAPIInvokeRole` .	Gehen Sie davon aus`JobsAPIInvokeRole` , dass das als Ausgabe des `deploy` Befehls gedruckt wurde: `CREDENTIALS=$(AWS_ PROFILE=$<YOUR_AWS _PROFILE> aws sts assume-role \ --no-cli-pager \ --role-arn $<JOBS_AP I_INVOKE_ROLE_ARN> \ --role-session-name JobsAPIInvoke) export AWS_ACCES S_KEY_ID=$(cat $CREDENTIALS \| jq '.Credentials''.Ac cessKeyId') export AWS_SECRE T_ACCESS_KEY=$(cat $CREDENTIALS \| jq '.Credentials''.Se cretAccessKey') export AWS_SESSI ON_TOKEN==$(cat $CREDENTIALS | jq '.Credentials''.Se ssionToken')`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Postman konfigurieren.	• Folgen Sie den Anweisungen in der Postman-Dokumentation, um die im Repository enthaltene Postman-Sammlung zu importieren.
	• Stellen Sie die `JobsAPI` Variablen mit den folgenden Werten ein:
	  • `accessKey` – Der Wert des `Credentials.AccessKeyId` Attributs aus dem `assume-role` Befehl.
	  • `baseUrl`– Der Wert der `JobsApiJobsAPIEndpoint` `deploy` Befehlsausgabe ohne den abschließenden Schrägstrich.
	  • `region`– Der Wert der AWS-Region Stelle, an der Sie die Beispielarchitektur bereitgestellt haben.
	  • `seconds`– Der Wert des Eingabeparameters für den Beispieljob. Es muss eine positive Ganzzahl sein.
	  • `secretKey` – Der Wert des `Credentials.Secret`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`AccessKey` Attributs aus dem `assume-role` Befehl. • `sessionToken` – Der Wert des `Credentials.SessionToken` Attributs aus dem `assume-role` Befehl.	
Testen Sie die Beispielarchitektur.	Um die Beispielarchitektur zu testen, senden Sie Anfragen an die Jobs-API. Weitere Informationen finden Sie in der Postman-Dokumentation.	DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Die Zerstörung und anschließende erneute Bereitstellung der Beispielarchitektur schlägt fehl, da die Amazon CloudWatch Logs-Protokollgruppe `/aws/apigateway/JobsAPIAccessLogs` bereits existiert.	1. Exportieren Sie bei Bedarf Ihre Protokolldaten nach Amazon Simple Storage Service (Amazon S3). 2. Löschen Sie die CloudWatch Protokollgruppe Logs `/aws/apigateway/JobsAPIAccessLogs` . 3. Stellen Sie die Beispielarchitektur erneut bereit.

Zugehörige Ressourcen

- API-Gateway-Zuordnungsvorlage und Referenz zur Zugriffsprotokollierungsvariablen
- Erfassung von Änderungsdaten für DynamoDB Streams
- Optimistisches Sperren mit Versionsnummer

- Verwenden von Kinesis Data Streams zur Erfassung von Änderungen an DynamoDB

Ereignisse asynchron mit Amazon API Gateway, Amazon SQS und AWS Fargate verarbeiten

Erstellt von Andrea Meroni (AWS), Alessandro Trisolini (AWS), Nadim Majed (AWS), Mariem Kthiri (AWS) und Michael Wallner (AWS)

Übersicht

Amazon API Gateway ist ein vollständig verwalteter Service, den Entwickler nutzen können, um sie in jeder Größenordnung zu erstellen, zu veröffentlichen, zu verwalten, APIs zu überwachen und zu sichern. Er erledigt die Aufgaben, die mit der Annahme und Verarbeitung von bis zu Hunderttausenden von gleichzeitigen API-Aufrufen verbunden sind.

Eine wichtige Servicequote von API Gateway ist das Integrations-Timeout. Das Timeout ist die maximale Zeit, in der ein Backend-Dienst eine Antwort zurückgeben muss, bevor die REST-API einen Fehler zurückgibt. Das feste Limit von 29 Sekunden ist für synchrone Workloads im Allgemeinen akzeptabel. Dieses Limit stellt jedoch eine Herausforderung für Entwickler dar, die API Gateway mit asynchronen Workloads verwenden möchten.

Dieses Muster zeigt eine Beispielarchitektur für die asynchrone Verarbeitung von Ereignissen mithilfe von API Gateway, Amazon Simple Queue Service (Amazon SQS) und. AWS Fargate Die Architektur unterstützt die Ausführung von Verarbeitungsaufträgen ohne zeitliche Einschränkungen und verwendet eine einfache REST-API als Schnittstelle.

Projen wird verwendet, um die lokale Entwicklungsumgebung einzurichten und die Beispielarchitektur in Kombination mit Docker und Node.js AWS Cloud Development Kit (AWS CDK)auf einem Ziel AWS-Konto bereitzustellen. Projen richtet automatisch eine virtuelle Python-Umgebung mit Pre-Commit und den Tools ein, die für die Qualitätssicherung des Codes, Sicherheitsscans und Unit-Tests verwendet werden. Weitere Informationen finden Sie im Abschnitt Tools.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Die folgenden Tools sind auf Ihrer Workstation installiert:
  - AWS Cloud Development Kit (AWS CDK) Toolkit-Version 2.85.0 oder höher
  - Docker-Version 20.10.21 oder höher

- Node.js Version 18 oder höher
- Projen Version 0.71.111 oder höher
- Python-Version 3.9.16 oder höher

Einschränkungen

- Gleichzeitige Jobs sind auf 500 Aufgaben pro Minute begrenzt. Dies ist die maximale Anzahl von Aufgaben, die Fargate bereitstellen kann.

Architektur

Das folgende Diagramm zeigt die Interaktion der Jobs-API mit der `jobs` Amazon DynamoDB-Tabelle, dem Fargate-Dienst zur Ereignisverarbeitung und der Fehlerbehandlungsfunktion. AWS Lambda Ereignisse werden in einem EventBridge Amazon-Eventarchiv gespeichert.

Ein typischer Arbeitsablauf umfasst die folgenden Schritte:

1. Sie authentifizieren sich bei AWS Identity and Access Management (IAM) und erhalten Sicherheitsanmeldedaten.
2. Sie senden eine `POST` HTTP-Anfrage an den `/jobs` Jobs-API-Endpunkt und geben dabei die Jobparameter im Hauptteil der Anfrage an.
3. Die Jobs-API, bei der es sich um eine API-Gateway-REST-API handelt, gibt Ihnen eine HTTP-Antwort zurück, die die Job-ID enthält.
4. Die Jobs-API sendet eine Nachricht an die SQS-Warteschlange.
5. Fargate ruft die Nachricht aus der SQS-Warteschlange ab, verarbeitet das Ereignis und fügt dann die Auftragsergebnisse in die `jobs` DynamoDB-Tabelle ein.
6. Sie senden eine `GET` HTTP-Anfrage an den `/jobs/{jobId}` Job-API-Endpunkt mit der Job-ID aus Schritt 3 als. `{jobId}`
7. Die Jobs-API fragt die `jobs` DynamoDB-Tabelle ab, um die Auftragsergebnisse abzurufen.
8. Die Jobs-API gibt eine HTTP-Antwort zurück, die die Auftragsergebnisse enthält.
9. Wenn die Ereignisverarbeitung fehlschlägt, sendet die SQS-Warteschlange das Ereignis an die Dead-Letter-Warteschlange (DLQ).
10. Ein EventBridge Ereignis initiiert die Fehlerbehandlungsfunktion.
11. Die Fehlerbehandlungsfunktion platziert die Jobparameter in der `jobs` DynamoDB-Tabelle.

12. Sie können die Job-Parameter abrufen, indem Sie eine `GET` HTTP-Anfrage an den `/jobs/{jobId}` Job-API-Endpunkt senden.
13. Wenn die Fehlerbehandlung fehlschlägt, sendet die Fehlerbehandlungsfunktion das Ereignis an ein EventBridge Archiv.

    Sie können die archivierten Ereignisse erneut abspielen, indem Sie EventBridge

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK)ist ein Softwareentwicklungs-Framework, das Ihnen hilft, AWS Cloud Infrastruktur im Code zu definieren und bereitzustellen.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- AWS Fargatehilft Ihnen dabei, Container auszuführen, ohne Server oder Amazon Elastic Compute Cloud (Amazon EC2) -Instances verwalten zu müssen. Es wird in Verbindung mit Amazon Elastic Container Service (Amazon ECS) verwendet.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel Lambda-Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen. AWS-Konten
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.

Andere Tools

- autopep8 formatiert Python-Code automatisch auf der Grundlage des Python Enhancement Proposal (PEP) 8-Styleguides.
- Bandit scannt Python-Code, um häufig auftretende Sicherheitsprobleme zu finden.
- Commitizen ist ein Git-Commit-Checker und -Generator. `CHANGELOG`
- cfn-lint ist ein Linter AWS CloudFormation

- Checkov ist ein statisches Code-Analyse-Tool, das Infrastructure as Code (IaC) auf Sicherheits- und Compliance-Fehlkonfigurationen überprüft.
- jq ist ein Befehlszeilentool zum Parsen von JSON.
- Postman ist eine API-Plattform.
- pre-commit ist ein Git-Hooks-Manager.
- Projen ist ein Projektgenerator.
- pytest ist ein Python-Framework zum Schreiben kleiner, lesbarer Tests.

Code-Repository

Dieser Beispielarchitekturcode befindet sich im Repository GitHub Asynchronous Processing with API Gateway und SQS.

Bewährte Methoden

- Diese Beispielarchitektur beinhaltet keine Überwachung der bereitgestellten Infrastruktur. Wenn Ihr Anwendungsfall eine Überwachung erfordert, sollten Sie das Hinzufügen von CDK Monitoring Constructs oder einer anderen Überwachungslösung in Betracht ziehen.
- Diese Beispielarchitektur verwendet IAM-Berechtigungen, um den Zugriff auf die Jobs-API zu steuern. Jeder, der autorisiert ist, `JobsAPIInvokeRole` dies anzunehmen, kann die Jobs-API aufrufen. Daher ist der Zugriffskontrollmechanismus binär. Wenn Ihr Anwendungsfall ein komplexeres Autorisierungsmodell erfordert, sollten Sie es mit einem anderen Zugriffskontrollmechanismus testen.
- Wenn ein Benutzer eine `POST` HTTP-Anfrage an den `/jobs` Jobs-API-Endpunkt sendet, werden die Eingabedaten auf zwei verschiedenen Ebenen validiert:
  - API Gateway ist für die erste Anforderungsvalidierung verantwortlich.
  - Die Funktion zur Ereignisverarbeitung führt die zweite Anfrage aus.

    Es wird keine Überprüfung durchgeführt, wenn der Benutzer eine `GET` HTTP-Anfrage an den `/jobs/{jobId}` Jobs-API-Endpunkt sendet. Wenn Ihr Anwendungsfall eine zusätzliche Eingabevalidierung und ein erhöhtes Sicherheitsniveau erfordert, sollten Sie den Einsatz AWS WAF zum Schutz Ihrer API in Betracht ziehen.

Epen

Richte die Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Führen Sie den folgenden Befehl aus, um das Repository lokal zu klonen: `git clone https://github.com/aws-samples/asynchronous-event-processing-api-gateway-sqs-cdk.git`	DevOps Ingenieur

Richten Sie das Projekt ein.	Ändern Sie das Verzeichnis in das Repository-Stammverzeichnis und richten Sie die virtuelle Python-Umgebung und alle Tools mithilfe von Projen ein:
	`cd asynchronous-event-processing-api-gateway-api-gateway-sqs-cdk`
	`npx projen`
		DevOps Ingenieur

Installieren Sie Pre-Commit-Hooks.	Gehen Sie wie folgt vor, um Pre-Commit-Hooks zu installieren: 1. Aktivieren Sie die virtuelle Python-Umgebung: `source .env/bin/activate`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	2. Installieren Sie die Pre-Commit-Hooks:
	`pre-commit install`
	`pre-commit install --hook-type commit-msg`	

Stellen Sie die Beispielarchitektur bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bootstrap. AWS CDK	Um AWS CDKin Ihrem zu booten AWS-Konto, führen Sie den folgenden Befehl aus: `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen bootstrap`	AWS DevOps
Stellen Sie die Beispielarchitektur bereit.	Führen Sie den folgenden Befehl aus AWS-Konto, um die Beispielarchitektur in Ihrem bereitzustellen: `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen deploy`	AWS DevOps

Testen Sie die Architektur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die Testvoraussetzungen.	Installieren Sie auf Ihrer Workstation the AWS	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Command Line Interface (AWS CLI), Postman und jq. Die Verwendung von Postman zum Testen dieser Beispiela rchitektur wird empfohlen , ist aber nicht zwingend erforderlich. Wenn Sie sich für ein alternatives API-Testt ool entscheiden, stellen Sie sicher, dass es die Authentif izierung mit AWS Signature Version 4 unterstützt, und beziehen Sie sich auf die exponierten API-Endpunkte, die durch den Export der REST-API überprüft werden können.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gehen Sie von der aus`JobsAPIInvokeRole` .	Gehen Sie davon aus`JobsAPIInvokeRole` , dass das als Ausgabe des `deploy` Befehls gedruckt wurde: `CREDENTIALS=$(AWS_ PROFILE=$<YOUR_AWS _PROFILE> aws sts assume-role \ --no-cli-pager \ --role-arn $<JOBS_AP I_INVOKE_ROLE_ARN> \ --role-session-name JobsAPIInvoke) export AWS_ACCES S_KEY_ID=$(cat $CREDENTIALS \| jq '.Credentials''.Ac cessKeyId') export AWS_SECRE T_ACCESS_KEY=$(cat $CREDENTIALS \| jq '.Credentials''.Se cretAccessKey') export AWS_SESSI ON_TOKEN==$(cat $CREDENTIALS | jq '.Credentials''.Se ssionToken')`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Postman konfigurieren.	• Folgen Sie den Anweisungen in der Postman-Dokumentation, um die im Repository enthaltene Postman-Sammlung zu importieren.
	• Stellen Sie die `JobsAPI` Variablen mit den folgenden Werten ein:
	  • `accessKey` – Der Wert des `Credentials.AccessKeyId` Attributs aus dem `assume-role` Befehl.
	  • `baseUrl`– Der Wert der `JobsApiJobsAPIEndpoint` `deploy` Befehlsausgabe ohne den abschließenden Schrägstrich.
	  • `region`– Der Wert der AWS-Region Stelle, an der Sie die Beispielarchitektur bereitgestellt haben.
	  • `seconds`– Der Wert des Eingabeparameters für den Beispieljob. Es muss eine positive Ganzzahl sein.
	  • `secretKey` – Der Wert des `Credentials.Secret`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`AccessKey` Attributs aus dem `assume-role` Befehl. • `sessionToken` – Der Wert des `Credentials.SessionToken` Attributs aus dem `assume-role` Befehl.	
Testen Sie die Beispielarchitektur.	Um die Beispielarchitektur zu testen, senden Sie Anfragen an die Jobs-API. Weitere Informationen finden Sie in der Postman-Dokumentation.	DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Die Zerstörung und anschließende erneute Bereitstellung der Beispielarchitektur schlägt fehl, da die Amazon CloudWatch Logs-Protokollgruppe `/aws/apigateway/JobsAPIAccessLogs` bereits existiert.	1. Exportieren Sie bei Bedarf Ihre Protokolldaten nach Amazon Simple Storage Service (Amazon S3). 2. Löschen Sie die CloudWatch Protokollgruppe Logs `/aws/apigateway/JobsAPIAccessLogs` . 3. Stellen Sie die Beispielarchitektur erneut bereit.
Die Zerstörung und anschließende erneute Bereitstellung der Beispielarchitektur schlägt fehl, da die Protokollgruppe CloudWatch Logs `/aws/ecs/EventProcessingServiceLogs` bereits vorhanden ist.	1. Exportieren Sie bei Bedarf Ihre Protokolldaten nach Amazon S3. 2. Löschen Sie die CloudWatch Protokollgruppe Logs `/aws/ecs/EventProcessingServiceLogs.`

Problem	Lösung
	3. Stellen Sie die Beispielarchitektur erneut bereit.

Zugehörige Ressourcen

- API-Gateway-Zuordnungsvorlage und Referenz zur Zugriffsprotokollierungsvariablen
- Wie integriere ich eine API Gateway Gateway-REST-API in Amazon SQS und behebe häufig auftretende Fehler?

Führen Sie AWS Systems Manager Automation Automation-Aufgaben synchron über AWS Step Functions aus

Erstellt von Elie El khoury (AWS)

Übersicht

Dieses Muster erklärt, wie man mit integriert AWS Step Functions . AWS Systems Manager Es verwendet AWS SDK-Dienstintegrationen, um die Systems Manager startAutomationExecutionManager-API mit einem Task-Token aus einem State-Machine-Workflow aufzurufen, und pausiert, bis das Token mit einem erfolgreichen oder fehlerhaften Aufruf zurückkehrt. Um die Integration zu demonstrieren, implementiert dieses Muster einen Wrapper für Automatisierungsdokumente (Runbook) um das `AWS-RunPowerShellScript` OR-Dokument und wird verwendet`.waitForTaskToken`, um `AWS-RunShellScript` oder synchron aufzurufen. `AWS-RunShellScript` `AWS-RunPowerShellScript` Weitere Informationen zu AWS SDK-Dienstintegrationen in Step Functions finden Sie im AWS Step Functions Entwicklerhandbuch.

Step Functions ist ein visueller Workflow-Dienst mit geringem Programmieraufwand, mit dem Sie mithilfe von Diensten verteilte Anwendungen erstellen, IT- und Geschäftsprozesse automatisieren und Daten- und Machine-Learning-Pipelines erstellen können. AWS Workflows verwalten Fehler, Wiederholungen, Parallelisierung, Serviceintegrationen und Beobachtbarkeit, sodass Sie sich auf die wertvollere Geschäftslogik konzentrieren können.

Automatisierung, eine Funktion von AWS Systems Manager, vereinfacht allgemeine Wartungs-, Bereitstellungs- und Problembehebungsaufgaben für AWS-Services Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS), Amazon Redshift und Amazon Simple Storage Service (Amazon S3). Durch die Automatisierung haben Sie eine detaillierte Kontrolle über die Parallelität Ihrer Automatisierungen. Sie können beispielsweise angeben, auf wie viele Ressourcen gleichzeitig zugegriffen werden soll und wie viele Fehler auftreten können, bevor eine Automatisierung gestoppt wird.

Einzelheiten zur Implementierung, einschließlich Runbook-Schritten, Parametern und Beispielen, finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Konto AWS

- AWS Identity and Access Management (IAM) -Berechtigungen für den Zugriff auf Step Functions und Systems Manager
- Eine EC2 Instanz, auf der Systems Manager Agent (SSM Agent) installiert ist
- Ein IAM-Instanzprofil für Systems Manager, das an die Instance angehängt ist, auf der Sie das Runbook ausführen möchten
- Eine Step Functions Functions-Rolle mit den folgenden IAM-Berechtigungen (die dem Prinzip der geringsten Rechte folgen):

```
{
            "Effect": "Allow",
            "Action": "ssm:StartAutomationExecution",
            "Resource": "*"
 }
```

Produktversionen

- SSM-Dokumentschema Version 0.3 oder höher
- SSM Agent Version 2.3.672.0 oder höher

Architektur

Zieltechnologie-Stack

- AWS Step Functions
- AWS Systems Manager -Automatisierung

Zielarchitektur

Automatisierung und Skalierung

- Dieses Muster bietet eine AWS CloudFormation Vorlage, mit der Sie die Runbooks auf mehreren Instanzen bereitstellen können. (Weitere Informationen finden Sie im Implementierungs-Repository von GitHub Step Functions und Systems Manager.)

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend AWS-Konten zu verwalten.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und zu deren Nutzung autorisiert ist.
- AWS Step Functionsist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Funktionen und andere Funktionen kombinieren können, um geschäftskritische Anwendungen AWS-Services zu erstellen.
- AWS Systems Managerhilft Ihnen bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der ausgeführt werden. AWS Cloud Es vereinfacht das Anwendungs- und Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme und hilft Ihnen, Ihre AWS Ressourcen sicher und in großem Umfang zu verwalten.

Code

Der Code für dieses Muster ist im Implementierungs-Repository von GitHub Step Functions und Systems Manager verfügbar.

Epen

Runbooks erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die CloudFormation Vorlage herunter.	Laden Sie die `ssm-automation-documents.cfn.json` Vorlage aus dem `cloudformation` Ordner des GitHub Repositorys herunter.	AWS DevOps
Runbooks erstellen.	Melden Sie sich bei der an AWS Management	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Console, öffnen Sie die AWS CloudFormation Konsole und stellen Sie die Vorlage bereit. Weitere Informationen zum Bereitstellen von CloudFormation Vorlagen finden Sie in der CloudFormation Dokumentation unter Erstellen eines Stacks auf der AWS CloudFormation Konsole. Die CloudFormation Vorlage stellt drei Ressourcen bereit: • `SfnRunCommandByInstanceIds` — Runbook, mit dem Sie eine Instanz ausführen `AWS-RunShellScript` oder `AWS-RunPowerShellScript` verwenden können. IDs • `SfnRunCommandByTargets` — Runbook, mit dem Sie Ziele ausführen `AWS-RunShellScript` oder `AWS-RunPowerShellScript` verwenden können. • `SSMSyncRole` — Die von den Runbooks übernommene IAM-Rolle.	

Erstellen Sie eine Beispiel-Zustandsmaschine

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Teststatus-Maschine.	Folgen Sie den Anweisungen im AWS Step Functions Entwicklerhandbuch, um einen State Machine zu erstellen und auszuführen. Verwenden Sie für die Definition den folgenden Code. Achten Sie darauf, den `InstanceIds` Wert mit der ID einer gültigen Systems Manager-fähigen Instanz in Ihrem Konto zu aktualisieren. `{ "Comment": "A description of my state machine", "StartAt": "StartAutomationWaitForCallBack", "States": { "StartAutomationWaitForCallBack": { "Type": "Task", "Resource": "arn:aws:states:::aws-sdk:ssm:startAutomationExecution.waitForTaskToken", "Parameters": { "DocumentName": "SfnRunCommandByInstanceIds", "Parameters": { "InstanceIds": [`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"i-123456
	7890abcdef0"
	],
	"taskToken.
	$": "States.Array($$.T
	ask.Token)",
	"workingD
	irectory": [
	"/home/ssm-
	user/"
	],
	"Commands": [
	"echo \"This
	is a test running
	automation waitForTa
	skToken\" >> automatio
	n.log",
	"sleep 100"
	],
	"executio
	nTimeout": [
	"10800"
	],
	"delivery
	Timeout": [
	"30"
	],
	"shell": [
	"Shell"
	]
	}
	},
	"End": true
	}
	}
	}</pre> Dieser Code ruft das Runbook auf, um zwei Befehle auszuführen, die den `waitForTaskToken`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Aufruf von Systems Manager Automation demonstrieren. Der `shell` Parameterwert (`ShelloderPowerShell`) bestimmt, ob das Automatisierungsdokument ausgeführt wird `AWS-RunShellScript` oder`AWS-RunPowerShellScript` . Die Aufgabe schreibt „Dies ist ein waitForTask Automatisierungstoken für die Testausführung“ in die `/home/ssm-user/automation.log` Datei und ruht dann 100 Sekunden lang, bevor sie mit dem Aufgabentoken antwortet und die nächste Aufgabe im Workflow freigibt. Wenn Sie stattdessen das `SfnRunCommandByTargets` Runbook aufrufen möchten, ersetzen Sie den `Parameters` Abschnitt des vorherigen Codes durch den folgenden: `"Parameters": { "Targets": [ { "Key": "InstanceIds", "Values": [`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"i-02573cafcfEXAMPLE",
	
	"i-0471e04240EXAMPLE"
	]
	}
	],</pre>	

Aktualisieren Sie die IAM-Rolle für den State Machine.	Im vorherigen Schritt wird automatisch eine dediziert e IAM-Rolle für den State Machine erstellt. Es gewährt jedoch keine Berechtigungen zum Aufrufen des Runbooks. Aktualisieren Sie die Rolle, indem Sie die folgenden Berechtigungen hinzufügen:
	<pre>{
	"Effect": "Allow",
	"Action":
	"ssm:StartAutomationExecution",
	"Resource": "*"
	}</pre>
		AWS DevOps

Validieren Sie die synchronen Aufrufe.	Führen Sie die Zustandsmaschine aus, um den synchronen Aufruf zwischen Step Functions und Systems Manager Automation zu validieren. Eine Beispielausgabe finden Sie im Abschnitt Zusätzliche Informationen.	AWS DevOps

Zugehörige Ressourcen

- Erste Schritte mit AWS Step Functions (AWS Step Functions Entwicklerhandbuch)
- Warten Sie auf einen Rückruf mit dem Task-Token (AWS Step Functions Developer Guide, Service Integration Patterns)
- API-Aufrufe send_task_success und send_task_failure (Boto3-Dokumentation)
- AWS Systems Manager Automatisierung AWS Systems Manager (Benutzerhandbuch)

Zusätzliche Informationen

Implementierungsinformationen

Dieses Muster stellt eine CloudFormation Vorlage bereit, die zwei Systems Manager Manager-Runbooks bereitstellt:

- `SfnRunCommandByInstanceIds`führt den `AWS-RunPowerShellScript` Befehl `AWS-RunShellScript` or mithilfe einer Instanz aus. IDs
- `SfnRunCommandByTargets`führt den `AWS-RunPowerShellScript` Befehl `AWS-RunShellScript` or mithilfe von Zielen aus.

Jedes Runbook implementiert vier Schritte, um einen synchronen Aufruf zu erreichen, wenn die `.waitForTaskToken` Option in Step Functions verwendet wird.

Schritt	Action (Aktion)	Beschreibung
1	`Branch`	Prüft den `shell` Parameter wert (`ShelloderPowerShell`), um zu entscheiden, ob die Ausführung `AWS-RunShellScript` für Linux oder `AWS-RunPowerShellScript` für Windows erfolgen soll.
2	`RunCommand_Shell` oder `RunCommand_PowerShell`	Nimmt mehrere Eingaben entgegen und führt den `RunPowerShellScript`

		Befehl `RunShellScript` oder aus. Weitere Informationen finden Sie auf der Registerkarte Details für das Dokument `RunCommand_Shell` oder `RunCommand_PowerShell` Automation in der Systems Manager Manager-Konsole.
3	`SendTaskFailure`	Wird ausgeführt, wenn Schritt 2 abgebrochen oder abgebrochen wird. Es ruft die Step Functions send_task_failure API auf, die drei Parameter als Eingabe akzeptiert: das von der Zustandsmaschine übergebene Token, den Fehlerfehler und eine Beschreibung der Fehlerursache.
4	`SendTaskSuccess`	Wird ausgeführt, wenn Schritt 2 erfolgreich ist. Es ruft die Step Functions send_task_success API auf, die das von der Zustandsmaschine übergebene Token als Eingabe akzeptiert.

Runbook-Parameter

`SfnRunCommandByInstanceIds`Runbook:

Parametername	Typ	Optional oder erforderlich	Beschreibung

`shell`	String	Erforderlich	Die Shell der Instanz entscheidet, ob sie `AWS-RunShellScript` für Linux oder `AWS-RunPowerShellScript` für Windows ausgeführt werden soll.
`deliveryTimeout`	Ganzzahl	Optional	Die Wartezeit in Sekunden, bis ein Befehl an den SSM-Agenten auf einer Instance übermittelt wird. Dieser Parameter hat einen Mindestwert von 30 (0,5 Minuten) und einen Höchstwert von 2592000 (720 Stunden).
`executionTimeout`	String	Optional	Die Zeit in Sekunden, bis ein Befehl abgeschlossen ist, bevor er als fehlgeschlagen betrachtet wird. Der Standardwert ist 3600 (1 Stunde). Der Höchstwert ist 172800 (48 Stunden).
`workingDirectory`	String	Optional	Der Pfad zum Arbeitsverzeichnis auf der Instance.

`Commands`	StringList	Erforderlich	Das auszuführende Shell-Skript oder der auszuführende Befehl.
`InstanceIds`	StringList	Erforderlich	Die IDs Instanzen, in denen Sie den Befehl ausführen möchten.
`taskToken`	String	Erforderlich	Das Task-Token, das für Rückrufantworten verwendet werden soll.

`SfnRunCommandByTargets`Runbook:

Name	Typ	Optional oder erforderlich	Beschreibung
`shell`	String	Erforderlich	Die Shell der Instanz entscheidet, ob sie `AWS-RunShellScript` für Linux oder `AWS-RunPowerShellScript` für Windows ausgeführt werden soll.
`deliveryTimeout`	Ganzzahl	Optional	Die Wartezeit in Sekunden, bis ein Befehl an den SSM-Agenten auf einer Instance übermittelt wird. Dieser Parameter hat einen Mindestwert von 30

			(0,5 Minuten) und einen Höchstwert von 2592000 (720 Stunden).
`executionTimeout`	Ganzzahl	Optional	Die Zeit in Sekunden, bis ein Befehl abgeschlossen ist, bevor er als fehlgeschlagen betrachtet wird. Der Standardwert ist 3600 (1 Stunde). Der Höchstwert ist 172800 (48 Stunden).
`workingDirectory`	String	Optional	Der Pfad zum Arbeitsverzeichnis auf der Instance.
`Commands`	StringList	Erforderlich	Das auszuführende Shell-Skript oder der auszuführende Befehl.

`Targets`	MapList	Erforderlich	Eine Reihe von Suchkriterien, die Instanzen anhand von Schlüssel-Wert-Paaren identifizieren, die Sie angeben. Beispiel: `[{"Key":"InstanceIds","Values":["i-02573cafcfEXAMPLE","i-0471e04240EXAMPLE"]}]`
`taskToken`	String	Erforderlich	Das Task-Token, das für Rückrufantworten verwendet werden soll.

Beispielausgabe

Die folgende Tabelle enthält ein Beispiel für die Ausgabe der Step-Funktion. Sie zeigt, dass die Gesamtlaufzeit zwischen Schritt 5 (`TaskSubmitted`) und Schritt 6 (`TaskSucceeded`) über 100 Sekunden beträgt. Dies zeigt, dass die Step-Funktion auf die Beendigung des `sleep 100` Befehls gewartet hat, bevor sie zur nächsten Aufgabe im Workflow überging.

ID (ID)	Typ	Schritt	Ressource	Verstrichene Zeit (ms)	Zeitstempel
1	`ExecutionStarted`		-	0	11. März 2022 14:50:34.303 Uhr
2	`TaskStateEntered`	`StartAutomationWai`	-	40	11. März 2022

		tForCallBack			14:50:34,343 Uhr
3	TaskScheduled	StartAutomationWaitForCallBack	-	40	11. März 2022 14:50:34,343 Uhr
4	TaskStarted	StartAutomationWaitForCallBack	-	154	11. März 2022 14:50:34.457 Uhr
5	TaskSubmitted	StartAutomationWaitForCallBack	-	657	11. März 2022 14:50:34.960 Uhr
6	TaskSucceeded	StartAutomationWaitForCallBack	-	10:3835	11. März 2022 14:52:18.138 Uhr
7	TaskStateExited	StartAutomationWaitForCallBack	-	1038 60	11. März 2022 14:52:18.163 Uhr
8	ExecutionSucceeded		-	103 897	11. März 2022 14:52:18.200 Uhr

parallel Lesevorgänge von S3-Objekten mithilfe von Python in einer AWS Lambda Funktion ausführen

Erstellt von Eduardo Bortoluzzi (AWS)

Übersicht

Sie können dieses Muster verwenden, um eine Liste von Dokumenten aus Amazon Simple Storage Service (Amazon S3) -Buckets in Echtzeit abzurufen und zusammenzufassen. Das Muster bietet Beispielcode zum parallel Lesen von Objekten aus S3-Buckets auf Amazon Web Services (AWS). Das Muster zeigt, wie I/O-gebundene Aufgaben mit AWS Lambda Funktionen, die Python verwenden, effizient ausgeführt werden können.

Ein Finanzunternehmen verwendete dieses Muster in einer interaktiven Lösung, um korrelierte Finanztransaktionen manuell in Echtzeit zu genehmigen oder abzulehnen. Die Dokumente zu Finanztransaktionen wurden in einem marktbezogenen S3-Bucket gespeichert. Ein Mitarbeiter wählte eine Liste von Dokumenten aus dem S3-Bucket aus, analysierte den Gesamtwert der Transaktionen, die die Lösung berechnete, und entschied, den ausgewählten Stapel zu genehmigen oder abzulehnen.

I/O-gebundene Aufgaben unterstützen mehrere Threads. In diesem Beispielcode die Datei concurrent.futures. ThreadPoolExecutorwird mit maximal 30 Threads gleichzeitig verwendet, obwohl Lambda-Funktionen bis zu 1.024 Threads unterstützen (wobei einer dieser Threads Ihr Hauptprozess ist). Dieses Limit ist darauf zurückzuführen, dass zu viele Threads aufgrund von Kontextwechsel und Nutzung von Rechenressourcen zu Latenzproblemen führen. Sie müssen auch die maximale Anzahl an Poolverbindungen erhöhen, `botocore` damit alle Threads den S3-Objekt-Download gleichzeitig durchführen können.

Der Beispielcode verwendet ein 8,3-KB-Objekt mit JSON-Daten in einem S3-Bucket. Das Objekt wird mehrfach gelesen. Nachdem die Lambda-Funktion das Objekt gelesen hat, werden die JSON-Daten in ein Python-Objekt dekodiert. Im Dezember 2024 wurden nach der Ausführung dieses Beispiels 1.000 Lesevorgänge in 2,3 Sekunden und 10.000 Lesevorgänge in 27 Sekunden mithilfe einer Lambda-Funktion, die mit 2.304 MB Speicher konfiguriert war, verarbeitet. AWS Lambda unterstützt Speicherkonfigurationen von 128 MB bis 10.240 MB (10 GB), obwohl eine Erhöhung des Lambda-Speichers über 2.304 MB nicht dazu beigetragen hat, die Zeit für die Ausführung dieser speziellen I/O-bezogenen Aufgabe zu verkürzen.

Das AWS Lambda Power Tuning-Tool wurde verwendet, um verschiedene Lambda-Speicherkonfigurationen zu testen und das beste performance-to-cost Verhältnis für die Aufgabe zu überprüfen. Die Testergebnisse finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Kenntnisse in der Python-Entwicklung

Einschränkungen

- Eine Lambda-Funktion kann höchstens 1.024 Ausführungsprozesse oder Threads haben.
- Neue AWS-Konten haben ein Lambda-Speicherlimit von 3.008 MB. Passen Sie das AWS Lambda Power Tuning Tool entsprechend an. Weitere Informationen finden Sie im Abschnitt Problembehandlung.
- Amazon S3 hat ein Limit von 5.500 GET/HEAD-Anfragen pro Sekunde pro partitioniertem Präfix.

Produktversionen

- Python 3.9 oder höher
- AWS Cloud Development Kit (AWS CDK) v2
- AWS Command Line Interface (AWS CLI) Ausführung 2
- AWS Lambda Power Tuning 4.3.6 (optional)

Architektur

Zieltechnologie-Stack

- AWS Lambda
- Amazon S3
- AWS Step Functions (wenn AWS Lambda Power Tuning eingesetzt wird)

Zielarchitektur

Das folgende Diagramm zeigt eine Lambda-Funktion, die Objekte parallel aus einem S3-Bucket liest. Das Diagramm enthält auch einen Step Functions Functions-Workflow für das AWS Lambda Power Tuning-Tool zur Feinabstimmung des Lambda-Funktionsspeichers. Diese Feinabstimmung trägt dazu bei, ein ausgewogenes Verhältnis zwischen Kosten und Leistung zu erreichen.

Automatisierung und Skalierung

Die Lambda-Funktionen lassen sich bei Bedarf schnell skalieren. Um 503 Slow-Down-Fehler von Amazon S3 bei hoher Nachfrage zu vermeiden, empfehlen wir, der Skalierung einige Grenzen zu setzen.

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK) v2 ist ein Softwareentwicklungs-Framework, das Ihnen hilft, AWS Cloud Infrastruktur im Code zu definieren und bereitzustellen. Die Beispielinfrastruktur wurde für die Bereitstellung mit erstellt AWS CDK.
- AWS Command Line InterfaceAWS CLIist ein Open-Source-Tool, mit dem Sie AWS-Services über Befehle in Ihrer Befehlszeilen-Shell interagieren können. In diesem Muster wird AWS CLI Version 2 verwendet, um eine JSON-Beispieldatei hochzuladen.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Storage Service Amazon S3 ist ein cloudbasierter Objektspeicherservice, mit dem Sie beliebige Datenmengen speichern, schützen und abrufen können.
- AWS Step Functionsist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen.

Andere Tools

- Python ist eine Allzweck-Computerprogrammiersprache. Die Wiederverwendung inaktiver Worker-Threads wurde in Python-Version 3.8 eingeführt, und der Lambda-Funktionscode in diesem Muster wurde für Python-Version 3.9 und höher erstellt.

Code-Repository

Der Code für dieses Muster ist im aws-lambda-parallel-download GitHub Repository verfügbar.

Bewährte Methoden

- Dieses AWS CDK Konstrukt stützt sich auf Ihre AWS-Konto Benutzerberechtigungen zur Bereitstellung der Infrastruktur. Wenn Sie AWS CDK Pipelines oder kontoübergreifende Bereitstellungen verwenden möchten, finden Sie weitere Informationen unter Stack-Synthesizer.
- Für diese Beispielanwendung sind die Zugriffsprotokolle im S3-Bucket nicht aktiviert. Es hat sich bewährt, Zugriffsprotokolle im Produktionscode zu aktivieren.

Epen

Bereiten Sie die Entwicklungsumgebung vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die installierte Python-Version.	Dieser Code wurde speziell auf Python 3.9 und Python 3.13 getestet und sollte auf allen Versionen zwischen diesen Versionen funktioni eren. Um Ihre Python-Ve rsion zu überprüfen, führen Sie es `python3 -V` in Ihrem Terminal aus und installieren Sie bei Bedarf eine neuere Version. Führen Sie den Befehl aus, um zu überprüfen, ob die erforderlichen Module installiert sind`python3 -c "import pip, venv"`. Keine Fehlermeldung bedeutet, dass die Module	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ordnungsgemäß installiert sind und Sie bereit sind, dieses Beispiel auszuführen.	
Installieren AWS CDK.	Um das zu installieren, AWS CDK falls es noch nicht installiert ist, folgen Sie den Anweisungen unter Erste Schritte mit dem AWS CDK. Um zu überprüfen, ob es sich bei der installierten AWS CDK Version um Version 2.0 oder höher handelt, führen Sie den Befehl aus`cdk -version`.	Cloud-Architekt
Bootstrapping für Ihre Umgebung	Um Ihre Umgebung zu booten, folgen Sie, falls dies noch nicht geschehen ist, den Anweisungen unter Bootstrap Ihre Umgebung zur Verwendung mit dem. AWS CDK	Cloud-Architekt

Klonen Sie das Beispiel-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Führen Sie den folgenden Befehl aus, um die neueste Version des Repositorys zu klonen: `git clone --depth 1 --branch v1.2.0 \`	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`git@github.com:aws-samples/aws-lambda-parallel-download.git`	
Ändern Sie das Arbeitsverzeichnis in das geklonte Repository.	Führen Sie den folgenden Befehl aus: `cd aws-lambda-parallel-download`	Cloud-Architekt
Erstellen Sie die virtuelle Python-Umgebung.	Führen Sie den folgenden Befehl aus, um eine virtuelle Python-Umgebung zu erstellen: `python3 -m venv .venv`	Cloud-Architekt
Aktivieren Sie die virtuelle Umgebung.	Führen Sie den folgenden Befehl aus, um die virtuelle Umgebung zu aktivieren: `source .venv/bin/activate`	Cloud-Architekt
Installieren Sie die Abhängigkeiten.	Führen Sie den `pip` folgenden Befehl aus, um die Python-Abhängigkeiten zu installieren: `pip install -r requirements.txt`	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Durchsuchen Sie den Code.	(Optional) Der Beispielcode, der ein Objekt aus dem S3-Bucket herunterlädt, befindet sich unter `resources/parallel.py` . Der Infrastrukturcode befindet sich im `parallel_download` Ordner.	Cloud-Architekt

Stellen Sie die App bereit und testen Sie sie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung bereit.	Führen Sie `cdk deploy`. Notieren Sie sich die AWS CDK Ergebnisse: • `ParallelDownloadStack.LambdaFunctionARN` • `ParallelDownloadStack.SampleS3BucketName` • `ParallelDownloadStack.StateMachineARN`	Cloud-Architekt
Laden Sie eine JSON-Beispieldatei hoch.	Das Repository enthält eine JSON-Beispieldatei mit einer Größe von etwa 9 KB. Führen Sie den folgenden Befehl aus, um die Datei in den S3-	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bucket des erstellten Stacks hochzuladen: `aws s3 cp sample.json s3://<ParallelDownloadStack.SampleS3BucketName>` `<ParallelDownloadStack.SampleS3BucketName>` Ersetzen Sie durch den entsprechenden Wert aus der AWS CDK Ausgabe.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die App aus.	Gehen Sie wie folgt vor, um die App auszuführen: 1. Melden Sie sich bei der an AWS Management Console, navigieren Sie zur Lambda-Konsole und suchen Sie die Lambda-Funktion, die den ARN aus der AWS CDK Ausgabe hat. `ParallelDownloadStack.LambdaFunctionARN` 2. Ändern Sie auf der Registerkarte Test den Event-JSON wie folgt: `{"objectKey": "sample.json"}` 3. Wählen Sie Test aus. 4. Um das Ergebnis zu sehen, wählen Sie Details aus. In den Details werden die Statistiken des parallel Downloads, die Informationen des Laufs und die Protokolle angezeigt.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die Anzahl der Downloads hinzu.	(Optional) Um 1.500 Get-Object-Aufrufe auszuführen, verwenden Sie den folgenden JSON-Code im Event-JSON des `Test` Parameters: `{"repeat": 1500, "objectKey": "sample.json"}`	Cloud-Architekt

Optional: Führen Sie AWS Lambda Power Tuning aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das AWS Lambda Power Tuning-Tool aus.	1. Melden Sie sich bei der Konsole an und navigieren Sie zu Step Functions. 2. Suchen Sie die Zustandsmaschine mit dem ARN aus der AWS CDK Ausgabe `ParallelDownloadStack.StateMachineARN` . 3. Wählen Sie Ausführung starten und fügen Sie den folgenden JSON-Code ein: `{ "lambdaARN": "<ParallelDownloadStack.LambdaFunctionARN>", "num": 10, "strategy": "balanced",`	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"payload":
	{"repeat": 2000,
	"objectKey":
	"sample.json"}
	}</pre>
	Denken Sie daran, es `<ParallelDownloadStack.LambdaFunctionARN>` durch den Wert aus der AWS CDK Ausgabe zu ersetzen.
	
	Am Ende des Laufs wird das Ergebnis auf der Registerkarte Eingabe und Ausgabe der Ausführung angezeigt.	

Sehen Sie sich die AWS Lambda Power Tuning-Ergebnisse in einem Diagramm an.	Kopieren Sie auf der Registerkarte Eingabe und Ausgabe der Ausführung den `visualization` Eigenschaftenlink und fügen Sie ihn in eine neue Browser-Registerkarte ein.	Cloud-Architekt

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die Objekte aus dem S3-Bucket.	Bevor Sie die bereitgestellten Ressourcen zerstören, entfernen Sie alle Objekte aus dem S3-Bucket:	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws s3 rm s3://<ParallelDownloadStack.SampleS3BucketName> \ --recursive` Denken Sie daran, `<ParallelDownloadStack.SampleS3BucketName>` durch den Wert aus den AWS CDK Ausgaben zu ersetzen.	
Zerstöre die Ressourcen.	Führen Sie den folgenden Befehl aus, um alle Ressourcen zu löschen, die für dieses Pilotprojekt erstellt wurden: `cdk destroy`	Cloud-Architekt

Fehlerbehebung

Problem	Lösung
`'MemorySize' value failed to satisfy constraint: Member must have value less than or equal to 3008`	Für neue Konten können Sie möglicherweise nicht mehr als 3.008 MB in Ihren Lambda-Funktionen konfigurieren. Um mit AWS Lambda Power Tuning zu testen, fügen Sie der Eingabe-JSON die folgende Eigenschaft hinzu, wenn Sie die Ausführung von Step Functions starten: `"powerValues": [ 512, 1024,`

Problem	Lösung
	1536, 2048, 2560, 3008]

Zugehörige Ressourcen

- Python — konkurrierende.Futures. ThreadPoolExecutor
- Lambda-Kontingente — Konfiguration, Bereitstellung und Ausführung von Funktionen
- Arbeiten mit dem AWS CDK in Python
- Profilierungsfunktionen mit AWS Lambda Power Tuning

Zusätzliche Informationen

Code

Der folgende Codeausschnitt führt die parallel I/O-Verarbeitung durch:

```
with ThreadPoolExecutor(max_workers=MAX_WORKERS) as executor:
  for result in executor.map(a_function, (the_arguments)):
    ...
```

Der `ThreadPoolExecutor` verwendet die Threads wieder, sobald sie verfügbar sind.

Tests und Ergebnisse

Diese Tests wurden im Dezember 2024 durchgeführt.

Beim ersten Test wurden 2.500 Objektlesevorgänge verarbeitet, mit dem folgenden Ergebnis.

Ab 3.009 MB blieb die Verarbeitungszeit bei jeder Speichererweiterung fast gleich, aber die Kosten stiegen mit zunehmender Speichergröße.

In einem weiteren Test wurde der Bereich zwischen 1.536 MB und 3.072 MB Arbeitsspeicher untersucht, wobei Werte verwendet wurden, die ein Vielfaches von 256 MB waren, und es wurden 10.000 Objektlesevorgänge verarbeitet. Dabei wurden die folgenden Ergebnisse erzielt.

Das beste performance-to-cost Verhältnis wurde mit der Lambda-Konfiguration mit 2.304 MB Speicher erzielt.

Zum Vergleich: Ein sequentieller Prozess mit 2.500 Objektlesevorgängen dauerte 47 Sekunden. Der parallel Vorgang mit der Lambda-Konfiguration mit 2.304 MB dauerte 7 Sekunden, was 85 Prozent weniger ist.

Senden Sie Telemetriedaten von AWS Lambda zu OpenSearch für Analysen und Visualisierungen in Echtzeit

Erstellt von Tabby Ward (AWS), Guy Bachar (AWS) und David Kilzer (AWS)

Übersicht

Moderne Anwendungen werden zunehmend verteilt und ereignisgesteuert, was die Notwendigkeit einer Überwachung und Beobachtbarkeit in Echtzeit verstärkt. AWS Lambda ist ein serverloser Computerdienst, der eine entscheidende Rolle beim Aufbau skalierbarer und ereignisgesteuerter Architekturen spielt. Die Überwachung und Fehlerbehebung von Lambda-Funktionen kann jedoch schwierig sein, wenn Sie sich ausschließlich auf Amazon CloudWatch Logs verlassen, was zu Latenz und begrenzten Aufbewahrungsfristen führen kann.

Um dieser Herausforderung zu begegnen, AWS wurde die Lambda Telemetry API eingeführt, die es Lambda-Funktionen ermöglicht, Telemetriedaten direkt an Überwachungs- und Beobachtungstools von Drittanbietern zu senden. Diese API unterstützt das Echtzeit-Streaming von Protokollen, Metriken und Traces und bietet einen umfassenden und zeitnahen Überblick über die Leistung und den Zustand Ihrer Lambda-Funktionen.

Dieses Muster erklärt, wie die Lambda-Telemetrie-API OpenSearch, eine verteilte Open-Source-Such- und Analyse-Engine, integriert werden kann. OpenSearch bietet eine leistungsstarke und skalierbare Plattform für die Aufnahme, Speicherung und Analyse großer Datenmengen und ist damit die ideale Wahl für Lambda-Telemetriedaten. Insbesondere zeigt dieses Muster, wie Logs von einer in Python geschriebenen Lambda-Funktion direkt an einen OpenSearch Cluster gesendet werden, indem eine Lambda-Erweiterung verwendet wird, die von bereitgestellt wird. AWS Diese Lösung ist flexibel und anpassbar, sodass Sie Ihre eigene Lambda-Erweiterung erstellen oder den Beispielquellcode ändern können, um das Ausgabeformat nach Wunsch zu ändern.

Das Muster erklärt, wie die Lambda-Telemetrie-API-Integration eingerichtet und konfiguriert wird OpenSearch, und enthält bewährte Methoden für Sicherheit, Kostenoptimierung und Skalierbarkeit. Ziel ist es, Ihnen zu helfen, tiefere Einblicke in Ihre Lambda-Funktionen zu gewinnen und die allgemeine Beobachtbarkeit Ihrer serverlosen Anwendungen zu verbessern.

> **Note**
>
> Dieses Muster konzentriert sich auf die Integration der Lambda-Telemetrie-API mit Managed. OpenSearch Die besprochenen Prinzipien und Techniken gelten jedoch auch für Self-Managed OpenSearch und Elasticsearch.

Voraussetzungen und Einschränkungen

Bevor Sie mit dem Integrationsprozess beginnen, stellen Sie sicher, dass Sie die folgenden Voraussetzungen erfüllen:

AWS-Konto: Eine aktive AWS-Konto Person mit den entsprechenden Berechtigungen zum Erstellen und Verwalten der folgenden AWS Ressourcen:

- AWS Lambda
- AWS Identity and Access Management (ICH BIN)
- Amazon OpenSearch Service (wenn Sie einen verwalteten OpenSearch Cluster verwenden)

OpenSearch Cluster:

- Sie können einen vorhandenen selbstverwalteten OpenSearch Cluster oder einen verwalteten Dienst wie OpenSearch Service verwenden.
- Wenn Sie OpenSearch Service verwenden, richten Sie Ihren OpenSearch Cluster ein, indem Sie den Anweisungen unter Erste Schritte mit Amazon OpenSearch Service in der OpenSearch Service-Dokumentation folgen.
- Stellen Sie sicher, dass über Ihre Lambda-Funktion auf den OpenSearch Cluster zugegriffen werden kann und dass er mit den erforderlichen Sicherheitseinstellungen wie Zugriffsrichtlinien, Verschlüsselung und Authentifizierung konfiguriert ist.
- Konfigurieren Sie den OpenSearch Cluster mit den erforderlichen Indexzuordnungen und Einstellungen, um die Lambda-Telemetriedaten aufzunehmen. Weitere Informationen finden Sie in der Servicedokumentation unter Laden von Streaming-Daten in Amazon OpenSearch OpenSearch Service.

Netzwerkkonnektivität:

- Stellen Sie sicher, dass Ihre Lambda-Funktion über die erforderliche Netzwerkkonnektivität für den Zugriff auf den OpenSearch Cluster verfügt. Anleitungen zur Konfiguration der Virtual Private Cloud (VPC) -Einstellungen finden Sie in der Servicedokumentation unter Starten Ihrer Amazon OpenSearch Service-Domains innerhalb einer VPC. OpenSearch

IAM-Rollen und -Richtlinien:

- Erstellen Sie eine IAM-Rolle mit den erforderlichen Berechtigungen für Ihre Lambda-Funktion, um auf den OpenSearch Cluster und auf Ihre darin gespeicherten Anmeldeinformationen zuzugreifen. AWS Secrets Manager
- Fügen Sie der Rolle die entsprechenden IAM-Richtlinien hinzu, z. B. die `AWSLambdaBasicExecutionRole` Richtlinie und alle zusätzlichen Berechtigungen, die für die Interaktion erforderlich sind. OpenSearch
- Stellen Sie sicher, dass die Ihrer Lambda-Funktion erteilten IAM-Berechtigungen das Schreiben von Daten in den OpenSearch Cluster ermöglichen. Informationen zur Verwaltung von IAM-Berechtigungen finden Sie unter Definieren von Lambda-Funktionsberechtigungen mit einer Ausführungsrolle in der Lambda-Dokumentation.

Kenntnisse in der Programmiersprache:

- Sie benötigen Grundkenntnisse in Python (oder der Programmiersprache Ihrer Wahl), um den Beispielcode für die Lambda-Funktion und die Lambda-Erweiterung zu verstehen und zu ändern.

Entwicklungsumgebung:

- Richten Sie eine lokale Entwicklungsumgebung mit den erforderlichen Tools und Abhängigkeiten für die Erstellung und Bereitstellung von Lambda-Funktionen und -Erweiterungen ein.

AWS CLI oder AWS Management Console:

- Installieren und konfigurieren Sie das AWS Command Line Interface (AWS CLI) oder verwenden Sie das AWS Management Console mit den entsprechenden Anmeldeinformationen, um mit den erforderlichen zu interagieren AWS-Services.

Überwachung und Protokollierung:

- Machen Sie sich mit bewährten Methoden zur Überwachung und Protokollierung vertraut AWS, einschließlich Diensten wie Amazon CloudWatch und AWS CloudTrail zu Überwachungs- und Prüfungszwecken.
- Überprüfen Sie die CloudWatch Logs für Ihre Lambda-Funktion, um Fehler oder Ausnahmen im Zusammenhang mit der Lambda-Telemetrie-API-Integration zu identifizieren. Anleitungen zur Fehlerbehebung finden Sie in der Lambda Telemetry API-Dokumentation.

Architektur

Dieses Muster verwendet OpenSearch Service, um Protokolle und Telemetriedaten zu speichern, die von Lambda-Funktionen generiert werden. Mit diesem Ansatz können Sie Protokolle schnell direkt in Ihren OpenSearch Cluster streamen, wodurch die Latenz und die Kosten reduziert werden, die mit der Verwendung von CloudWatch Logs als Vermittler verbunden sind.

> **Note**
>
> Ihr Lambda-Erweiterungscode kann Telemetrie entweder direkt über die OpenSearch API oder über eine OpenSearch Clientbibliothek an den OpenSearch Service weiterleiten. Die Lambda-Erweiterung kann die von der OpenSearch API unterstützten Massenoperationen verwenden, um Telemetrieereignisse zu bündeln und sie in einer einzigen Anfrage an den OpenSearch Service zu senden.

Das folgende Workflow-Diagramm veranschaulicht den Log-Workflow für Lambda-Funktionen, wenn Sie einen OpenSearch Cluster als Endpunkt verwenden.

Die Architektur umfasst die folgenden Komponenten:

- Lambda-Funktion: Die serverlose Funktion, die während der Ausführung Protokolle und Telemetriedaten generiert.
- Lambda-Erweiterung: Eine Python-basierte Erweiterung, die die Lambda-Telemetrie-API verwendet, um direkt in den Cluster zu integrieren. OpenSearch Diese Erweiterung wird zusammen mit der Lambda-Funktion in derselben Ausführungsumgebung ausgeführt.

- Lambda-Telemetrie-API: Die API, die es Lambda-Erweiterungen ermöglicht, Telemetriedaten, einschließlich Logs, Metriken und Traces, direkt an Überwachungs- und Beobachtungstools von Drittanbietern zu senden.
- Amazon OpenSearch Service-Cluster: Ein verwalteter OpenSearch Cluster, der auf gehostet wird AWS. Dieser Cluster ist für die Aufnahme, Speicherung und Indizierung der Protokolldaten verantwortlich, die von der Lambda-Funktion über die Lambda-Erweiterung gestreamt werden.

Der Workflow besteht aus den folgenden Schritten:

1. Die Lambda-Funktion wird aufgerufen und generiert während ihrer Ausführung Protokolle und Telemetriedaten.
2. Die Lambda-Erweiterung wird zusammen mit der Funktion zur Erfassung der Protokolle und Telemetriedaten mithilfe der Lambda-Telemetrie-API ausgeführt.
3. Die Lambda-Erweiterung stellt eine sichere Verbindung mit dem OpenSearch Service-Cluster her und streamt die Protokolldaten in Echtzeit.
4. Der OpenSearch Service-Cluster erfasst, indexiert und speichert die Protokolldaten, um sie mithilfe von Tools wie Kibana oder anderen kompatiblen Anwendungen für die Suche, Analyse und Visualisierung verfügbar zu machen.

Durch die Umgehung von CloudWatch Protokollen und das direkte Senden von Protokolldaten an den OpenSearch Cluster bietet diese Lösung mehrere Vorteile:

- Protokollstreaming und -analyse in Echtzeit ermöglichen eine schnellere Fehlerbehebung und eine verbesserte Beobachtbarkeit.
- Geringere Latenz und potenzielle Aufbewahrungsbeschränkungen im Zusammenhang mit CloudWatch Protokollen.
- Flexibilität, um die Lambda-Erweiterung anzupassen oder Ihre eigene Erweiterung für bestimmte Ausgabeformate oder zusätzliche Verarbeitung zu erstellen.
- Integration mit den Such-, Analyse- und Visualisierungsfunktionen von OpenSearch Service für die Protokollanalyse und -überwachung.

Der Abschnitt Epics enthält step-by-step Anweisungen zur Einrichtung der Lambda-Erweiterung, zur Konfiguration der Lambda-Funktion und zur Integration in den OpenSearch Service-Cluster. Sicherheitsüberlegungen, Strategien zur Kostenoptimierung und Tipps zur Überwachung und Fehlerbehebung der Lösung finden Sie im Abschnitt Bewährte Methoden.

Tools

AWS-Services

- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon OpenSearch Service ist ein vollständig verwalteter Service von AWS , der die Bereitstellung, den Betrieb und die Skalierung von OpenSearch Clustern in der Cloud vereinfacht.
- Lambda-Erweiterungen erweitern die Funktionalität Ihrer Lambda-Funktionen, indem sie zusätzlich benutzerdefinierten Code ausführen. Sie können Lambda-Erweiterungen verwenden, um Lambda in verschiedene Überwachungs-, Beobachtungs-, Sicherheits- und Governance-Tools zu integrieren.
- AWS Lambda Mit der Telemetrie-API können Sie Erweiterungen verwenden, um erweiterte Überwachungs- und Beobachtbarkeitsdaten direkt von Lambda zu erfassen und an ein Ziel Ihrer Wahl zu senden.
- AWS CloudFormationhilft Ihnen dabei, Ihre AWS Ressourcen zu modellieren und einzurichten, sodass Sie weniger Zeit mit der Verwaltung dieser Ressourcen verbringen und sich mehr auf Ihre Anwendungen konzentrieren können.

Code-Repositorys

- AWS Lambda Extensions umfasst Demos und Beispielprojekte von AWS und AWS Partnern, die Ihnen den Einstieg in die Erstellung Ihrer eigenen Erweiterungen erleichtern.
- Example Lambda Telemetry Integrations for OpenSearch bietet ein Beispiel für eine Lambda-Erweiterung, die zeigt, wie Logs von einer Lambda-Funktion an einen Cluster gesendet werden. OpenSearch

Andere Tools

- OpenSearchist eine verteilte Open-Source-Such- und Analysemaschine, die eine leistungsstarke Plattform für die Erfassung, Speicherung und Analyse großer Datenmengen bietet.
- Kibana ist ein Open-Source-Tool zur Datenvisualisierung und -erkundung, das Sie mit verwenden können. OpenSearch Beachten Sie, dass die Implementierung von Visualisierung und Analyse den Rahmen dieses Musters sprengen würde. Weitere Informationen finden Sie in der Kibana-Dokumentation und in anderen Ressourcen.

Bewährte Methoden

Beachten Sie bei der Integration der Lambda-Telemetrie-API die folgenden bewährten Methoden. OpenSearch

Sicherheit und Zugriffskontrolle

- Sichere Kommunikation: Verschlüsseln Sie die gesamte Kommunikation zwischen Ihren Lambda-Funktionen und dem OpenSearch Cluster mithilfe von HTTPS. Konfigurieren Sie die erforderlichen SSL/TLS-Einstellungen in Ihrer Lambda-Erweiterung und -Konfiguration. OpenSearch
- IAM-Berechtigungen:
  - Erweiterungen werden in derselben Ausführungsumgebung wie die Lambda-Funktion ausgeführt, sodass sie dieselbe Zugriffsebene auf Ressourcen wie Dateisystem-, Netzwerk- und Umgebungsvariablen erben.
  - Gewähren Sie Ihren Lambda-Funktionen die mindestens erforderlichen IAM-Berechtigungen, um auf die Lambda-Telemetrie-API zuzugreifen und Daten in den Cluster zu schreiben. OpenSearch Verwenden Sie das Prinzip der geringsten Rechte, um den Umfang der Berechtigungen einzuschränken.
- OpenSearch Zugriffskontrolle: Implementieren Sie eine differenzierte Zugriffskontrolle in Ihrem OpenSearch Cluster, um den Zugriff auf sensible Daten zu beschränken. Verwenden Sie die integrierten Sicherheitsfunktionen wie Benutzerauthentifizierung, rollenbasierte Zugriffskontrolle und Berechtigungen auf Indexebene in. OpenSearch
- Vertrauenswürdige Erweiterungen: Installieren Sie immer nur Erweiterungen aus einer vertrauenswürdigen Quelle. Verwenden Sie Infrastructure-as-Code-Tools (IaC) AWS CloudFormation , um beispielsweise das Anhängen derselben Erweiterungskonfiguration, einschließlich IAM-Berechtigungen, an mehrere Lambda-Funktionen zu vereinfachen. IaC-Tools bieten auch ein Auditprotokoll der zuvor verwendeten Erweiterungen und Versionen.
- Umgang mit sensiblen Daten: Vermeiden Sie beim Erstellen von Erweiterungen die Protokollierung sensibler Daten. Bereinigen Sie Payloads und Metadaten, bevor Sie sie protokollieren oder zu Prüfungszwecken speichern.

Kostenoptimierung

- Überwachung und Alarmierung: Richten Sie Überwachungs- und Warnmechanismen ein, um die Datenmenge zu verfolgen, an die Ihre OpenSearch Lambda-Funktionen gesendet werden. Auf diese Weise können Sie potenzielle Kostenüberschreitungen erkennen und beheben.

- Aufbewahrung von Daten: Überlegen Sie sich sorgfältig, welche Aufbewahrungsfrist für Ihre Lambda-Telemetriedaten angemessen ist. OpenSearch Längere Aufbewahrungsfristen können die Speicherkosten in die Höhe treiben. Bringen Sie also Ihre Anforderungen an die Beobachtbarkeit mit der Kostenoptimierung in Einklang.
- Komprimierung und Indizierung: Aktivieren Sie die Datenkomprimierung und optimieren Sie Ihre OpenSearch Indexierungsstrategie, um den Speicherbedarf Ihrer Lambda-Telemetriedaten zu reduzieren.
- Geringere Abhängigkeit von CloudWatch: Durch die direkte Integration der Lambda-Telemetrie-API können Sie Ihre Abhängigkeit von CloudWatch Protokollen potenziell reduzieren, was zu Kosteneinsparungen führen kann. OpenSearch Dies liegt daran, dass Sie mit der Lambda-Telemetrie-API Protokolle direkt an senden können OpenSearch, sodass die Daten nicht gespeichert und verarbeitet werden müssen. CloudWatch

Skalierbarkeit und Zuverlässigkeit

- Asynchrone Verarbeitung: Verwenden Sie asynchrone Verarbeitungsmuster wie Amazon Simple Queue Service (Amazon SQS) oder Amazon Kinesis, um die Ausführung der Lambda-Funktion von der Datenaufnahme zu entkoppeln. OpenSearch Dies trägt dazu bei, die Reaktionsfähigkeit Ihrer Lambda-Funktionen aufrechtzuerhalten und die allgemeine Zuverlässigkeit des Systems zu verbessern.
- OpenSearch Cluster-Skalierung: Überwachen Sie die Leistung und die Ressourcennutzung Ihres OpenSearch Clusters und skalieren Sie ihn nach Bedarf nach oben oder unten, um das zunehmende Volumen an Lambda-Telemetrie-Daten zu bewältigen.
- Failover und Disaster Recovery: Implementieren Sie eine robuste Notfallwiederherstellungsstrategie für Ihren OpenSearch Cluster, einschließlich regelmäßiger Backups und der Möglichkeit, Daten im Falle eines Ausfalls schnell wiederherzustellen.

Beobachtbarkeit und Überwachung

- Dashboards und Visualisierungen: Verwenden Sie Kibana oder andere Dashboard-Tools, um benutzerdefinierte Dashboards und Visualisierungen zu erstellen, die auf der Grundlage der enthaltenen Telemetriedaten Einblicke in die Leistung und den Zustand Ihrer Lambda-Funktionen bieten. OpenSearch
- Warnmeldungen und Benachrichtigungen: Richten Sie Warnmeldungen und Benachrichtigungen ein, um Ihre Lambda-Funktionen proaktiv auf Anomalien, Fehler oder Leistungsprobleme zu

überwachen. Integrieren Sie diese Warnungen und Benachrichtigungen in Ihre bestehenden Incident-Management-Prozesse.

- Rückverfolgung und Korrelation: Stellen Sie sicher, dass Ihre Lambda-Telemetriedaten relevante Tracing-Informationen wie Anfrage IDs oder Korrelation enthalten IDs, um die end-to-end Beobachtbarkeit und Fehlerbehebung in Ihren verteilten serverlosen Anwendungen zu ermöglichen.

Wenn Sie diese bewährten Methoden befolgen, können Sie sicherstellen, dass Ihre Integration der Lambda-Telemetrie-API sicher, kostengünstig und skalierbar OpenSearch ist und umfassende Beobachtbarkeit für Ihre serverlosen Anwendungen bietet.

Epen

Erstellen und implementieren Sie die Lambda-Erweiterungsebene

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Quellcode herunter.	Laden Sie die Beispiele rweiterungen aus dem AWS Lambda Extensions Repository herunter.	App-Entwickler, Cloud-Architekt
Navigieren Sie zum Verzeichnis `python-example-telemetry-opensearch-extension` .	Das AWS Lambda Erweiterungs-Repository, das Sie heruntergeladen haben, enthält zahlreiche Beispiele für verschiedene Anwendungsfälle und Sprachlaufzeiten. Navigieren Sie zum Ordner python-example-telemetry-opensearch-extension, um die OpenSearch Python-Erweiterung zu verwenden, an die Protokolle gesendet OpenSearch werden.	App-Entwickler, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Berechtigungen hinzu, um den Erweiterungsendpunkt auszuführen.	Führen Sie den folgenden Befehl aus, um den Erweiterungsendpunkt ausführbar zu machen: `chmod +x python-example-telemetry-opensearch-extension/extension.py`	App-Entwickler, Cloud-Architekt
Installieren Sie die Abhängigkeiten der Erweiterungen lokal.	Führen Sie den folgenden Befehl aus, um lokale Abhängigkeiten für den Python-Code zu installieren: `pip3 install -r python-example-telemetry-opensearch-extension/requirements.txt -t ./python-example-telemetry-opensearch-extension/` Diese Abhängigkeiten werden zusammen mit dem Erweiterungscode bereitgestellt.	App-Entwickler, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie ein ZIP-Paket für die Erweiterung, um sie als Ebene bereitzustellen.	Die Erweiterung.zip-Datei sollte ein Stammverzeichnis mit dem Namen`extensions/` , in dem sich die ausführbare Datei der Erweiterung befindet, und ein weiteres Stammverzeichnis mit dem Namen enthalten `python-example-telemetry-opensearch-extension/` , in dem sich die Kernlogik der Erweiterung und ihre Abhängigkeiten befinden.
	
	Erstellen Sie das ZIP-Paket für die Erweiterung:
	
	`chmod +x extensions/python-example-telemetry-opensearch-extension`
	`zip -r extension.zip extensions python-example-telemetry-opensearch-extension`
		App-Entwickler, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Erweiterung als Lambda-Schicht bereit.	Veröffentlichen Sie den Layer mithilfe Ihrer Erweiterung.zip-Datei und dem folgenden Befehl: `aws lambda publish-layer-version \ --layer-name "python-example-telemetry-opensearch-extension" \ --zip-file "fileb://extension.zip"`	App-Entwickler, Cloud-Architekt

Integrieren Sie die Erweiterung in Ihre Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die Ebene zu Ihrer Funktion hinzu.	1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Funktionsseite der AWS Lambda Konsole. 2. Wählen Sie Ihre Funktion aus. 3. Wählen Sie unter Layers (Ebenen) die Option Add a layer (Ebene hinzufügen). 4. Wählen Sie unter Ebene auswählen die Option Benutzerdefinierte Ebenen als Ebenenquelle aus und fügen Sie Ihre Ebene hinzu.	App-Entwickler, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen zum Hinzufügen einer Ebene zu Ihrer Lambda-Funktion finden Sie in der Lambda-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie die Umgebungs variablen für die Funktion fest.	Wählen Sie auf der Funktions seite die Registerkarte Konfiguration und fügen Sie Ihrer Funktion die folgenden Umgebungsvariablen hinzu: • `URL`— Die URI Ihres OpenSearch Endpunkts, an den Ihre Logs gesendet werden. • `AUTH_SECRET` — Der ARN Ihrer OpenSearch Anmeldeinformationen ist in gespeichert AWS Secrets Manager. Dies sollte als Schlüssel-Wert-Paar gespeichert werden und zwei Schlüssel haben: `username` und. `password` • `PLATFORM_INDEX` `FUNCTION_INDEX` , und `EXTENSION_INDEX` — Die Namen der Indizes, in denen Ihre Telemetriedaten, Funktions protokolle und Erweiteru ngsprotokolle gespeiche rt werden. Stellen Sie sicher, dass sie die richtigen Benennungskriterien erfüllen. Andernfalls werden Ihre Indizes nicht erstellt. • `DISPATCH_MIN_BATCH_SIZE` — Die Anzahl der	App-Entwickler, Cloud-Arc hitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Protokollereignisse, die Sie stapeln möchten. Wenn die Funktion jedoch heruntergefahren wird, werden Ihre Protokolle unabhängig von dieser Einstellung versendet.	

Fügen Sie Protokollierungsanweisungen hinzu und testen Sie Ihre Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie Ihrer Funktion Protokollierungsanweisungen hinzu.	Fügen Sie Ihrer Funktion Protokollierungsanweisungen hinzu, indem Sie einen der integrierten Protokollierungsmechanismen oder das Logging-Modul Ihrer Wahl verwenden.
	
	Hier sind Beispiele für das Protokollieren von Nachrichten in Python:
	
	`print("Your Log Message Here")`
	`logger = logging.getLogger(__name__)`
	
	`logger.info("Test Info Log.")`
	`logger.error("Test Error Log.")`
		App-Entwickler, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie Ihre Funktion.	1. Wählen Sie auf der Funktionsseite die Registerkarte Test aus. 2. Erstellen Sie ein Testereignis für Ihre Funktion und führen Sie den Test aus. Weitere Informationen finden Sie in der Lambda-Dokumentation unter Testen von Lambda-Funktionen in der Konsole. Wenn alles ordnungsgemäß funktioniert, sollte die Meldung „Funktion ausgeführt: erfolgreich“ angezeigt werden.	App-Entwickler, Cloud-Architekt

Sehen Sie sich Ihre Logs an OpenSearch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fragen Sie Ihre Indizes ab.	Führen Sie in OpenSearch den folgenden Befehl aus, um Ihre Indizes abzufragen: `SELECT * FROM index-name` Ihre Protokolle sollten in den Abfrageergebnissen angezeigt werden.	Cloud-Architekt

Fehlerbehebung

Problem	Lösung
Probleme mit der Verbindung	• Vergewissern Sie sich, dass Ihre Lambda-Funktion über die erforderliche Netzwerkkonnektivität für den Zugriff auf den OpenSearch Cluster verfügt. Anleitungen zur Konfiguration der VPC-Einstellungen finden Sie in der OpenSearch Servicedokumentation. • Stellen Sie sicher, dass die Ihrer Lambda-Funktion erteilten IAM-Berechtigungen das Schreiben von Daten in den OpenSearch Cluster ermöglichen. Informationen zur Verwaltung von IAM-Berechtigungen finden Sie in der Lambda-Dokumentation.
Fehler bei der Datenaufnahme	• Überprüfen Sie die CloudWatch Logs für Ihre Lambda-Funktion, um Fehler oder Ausnahmen im Zusammenhang mit der Lambda-Telemetrie-API-Integration zu identifizieren. Anleitungen zur Fehlerbehebung finden Sie in der Dokumentation zur Lambda Telemetry API. • Stellen Sie sicher, dass der OpenSearch Cluster korrekt konfiguriert ist und über die erforderlichen Indexzuordnungen und Einstellungen verfügt, um die Lambda-Telemetriedaten aufzunehmen. Weitere Informationen finden Sie in der OpenSearch Dokumentation.

Zugehörige Ressourcen

- Beispiel für Lambda-Telemetrie-Integrationen für OpenSearch (Repository) GitHub

- Erweitern Sie Lambda-Funktionen mithilfe von Lambda-Erweiterungen (Lambda-Dokumentation)
- Lambda-Telemetrie-API (Lambda-Dokumentation)
- Vorstellung der AWS Lambda Telemetrie-API (Blogbeitrag)AWS
- Integration der AWS Lambda Telemetrie-API mit Prometheus und OpenSearch (Blogbeitrag)AWS

Zusätzliche Informationen

Änderung der Protokollstruktur

Die Erweiterung sendet Protokolle standardmäßig als verschachteltes Dokument OpenSearch an. Auf diese Weise können Sie verschachtelte Abfragen ausführen, um einzelne Spaltenwerte abzurufen.

Wenn die Standard-Protokollausgabe nicht Ihren spezifischen Anforderungen entspricht, können Sie sie anpassen, indem Sie den Quellcode der Lambda-Erweiterung ändern, die von bereitgestellt wird AWS. AWS ermutigt Kunden, die Ausgabe an ihre Geschäftsanforderungen anzupassen. Um die Protokollausgabe zu ändern, suchen Sie die `dispatch_to_opensearch` Funktion in der `telemetry_dispatcher.py` Datei im Quellcode der Erweiterung und nehmen Sie die erforderlichen Änderungen vor.

Richten Sie einen serverlosen Mobilfunkrouter für eine zellenbasierte Architektur ein

Erstellt von Mian Tariq (AWS) und Ioannis Lioupras (AWS)

Übersicht

Als Einstiegspunkt in das System einer globalen zellbasierten Anwendung ist der Mobilfunkrouter dafür verantwortlich, Benutzer effizient den entsprechenden Zellen zuzuweisen und den Benutzern die Endpunkte zur Verfügung zu stellen. Der Mobilfunkrouter übernimmt Funktionen wie das Speichern von user-to-cell Zuordnungen, die Überwachung der Zellkapazität und das Anfordern neuer Zellen bei Bedarf. Es ist wichtig, die Funktionalität des Mobilfunkrouters bei möglichen Störungen aufrechtzuerhalten.

Das Design-Framework für Mobilfunkrouter in diesem Muster konzentriert sich auf Stabilität, Skalierbarkeit und allgemeine Leistungsoptimierung. Das Muster verwendet statisches Routing, bei dem Clients Endpunkte bei der ersten Anmeldung zwischenspeichern und direkt mit Zellen kommunizieren. Diese Entkopplung erhöht die Ausfallsicherheit des Systems, indem sie dazu beiträgt, die unterbrechungsfreie Funktionalität der zellbasierten Anwendung bei einem Ausfall des Mobilfunkrouters sicherzustellen.

Dieses Muster verwendet eine AWS CloudFormation Vorlage für die Bereitstellung der Architektur. Einzelheiten dazu, was die Vorlage bereitstellt, oder dazu, wie dieselbe Konfiguration mithilfe von bereitgestellt wird AWS Management Console, finden Sie im Abschnitt Zusätzliche Informationen.

> **Important**
>
> Die Demonstration, der Code und die AWS CloudFormation Vorlage in diesem Muster dienen nur zur Erläuterung. Das zur Verfügung gestellte Material dient ausschließlich der Veranschaulichung des Entwurfsmusters und der Verständlichkeit. Die Demo und der Code sind nicht produktionsbereit und sollten nicht für Live-Produktionsaktivitäten verwendet werden. Von jedem Versuch, den Code oder die Demo in einer Produktionsumgebung zu verwenden, wird dringend abgeraten und erfolgt auf eigenes Risiko. Wir empfehlen, sich mit geeigneten Fachleuten in Verbindung zu setzen und gründliche Tests durchzuführen, bevor Sie dieses Muster oder eine seiner Komponenten in einer Produktionsumgebung implementieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS) -Konto
- Die neueste Version von AWS Command Line Interface (AWS CLI)
- AWS-Anmeldeinformationen mit den erforderlichen Berechtigungen zum Erstellen des AWS CloudFormation Stacks, der AWS Lambda Funktionen und der zugehörigen Ressourcen

Produktversionen

- Python 3.12

Architektur

Das folgende Diagramm zeigt ein allgemeines Design des Mobilfunkrouters.

Das Diagramm durchläuft den folgenden Arbeitsablauf:

1. Der Benutzer kontaktiert Amazon API Gateway, das als Schnittstelle für die Mobilfunk-Router-API-Endpunkte dient.
2. Amazon Cognito kümmert sich um die Authentifizierung und Autorisierung.
3. Der AWS Step Functions Workflow besteht aus den folgenden Komponenten:
   - Orchestrator – Wird `Orchestrator` verwendet AWS Step Functions , um einen Workflow oder eine Zustandsmaschine zu erstellen. Der Workflow wird durch die Cell-Router-API ausgelöst. Der `Orchestrator` führt Lambda-Funktionen basierend auf dem Ressourcenpfad aus.
   - Dispatcher – Die `Dispatcher` Lambda-Funktion identifiziert und weist jedem registrierten neuen Benutzer eine statische Zelle zu. Die Funktion sucht nach der Zelle mit der geringsten Anzahl von Benutzern, weist sie dem Benutzer zu und gibt die Endpunkte zurück.
   - Mapper – Der `Mapper` Vorgang verarbeitet die user-to-cell Zuordnungen innerhalb der `RoutingDB` Amazon DynamoDB DynamoDB-Datenbank, die mit der Vorlage erstellt wurde. AWS CloudFormation Wenn die `Mapper` Funktion ausgelöst wird, stellt sie den bereits zugewiesenen Benutzern ihre Endpunkte zur Verfügung.

- Scaler – Die `Scaler` Funktion verfolgt die Zellbelegung und die verfügbare Kapazität. Bei Bedarf kann die `Scaler` Funktion über Amazon Simple Queue Service (Amazon SQS) eine Anfrage an die Bereitstellungs- und Bereitstellungsebene senden, um neue Zellen anzufordern.
- Validator – Die `Validator` Funktion validiert die Zellenendpunkte und erkennt mögliche Probleme.

4. Die `RoutingDB` speichert Zellinformationen und Attribute (API-Endpunkte, Status AWS-Region, Metriken).
5. Wenn die verfügbare Kapazität von Zellen einen Schwellenwert überschreitet, fordert der Mobilfunkrouter Bereitstellungs- und Bereitstellungsdienste über Amazon SQS an, um neue Zellen zu erstellen.

Wenn neue Zellen erstellt werden, `RoutingDB` wird es aus der Bereitstellungs- und Bereitstellungsebene aktualisiert. Dieser Prozess würde jedoch den Rahmen dieses Musters sprengen. Einen Überblick über die Voraussetzungen für den Entwurf zellenbasierter Architekturen und Einzelheiten zum in diesem Muster verwendeten Mobilfunkrouter-Design finden Sie im Abschnitt Zusätzliche Informationen.

Tools

AWS-Services

- Amazon API Gateway unterstützt Sie bei der Erstellung, Veröffentlichung, Wartung, Überwachung und Sicherung von REST, HTTP und WebSocket APIs in jeder Größenordnung.
- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und zu verwalten AWS-Regionen.
- Amazon Cognito bietet Authentifizierung, Autorisierung und Benutzerverwaltung für Web- und mobile Apps.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.
- AWS Step Functionsist ein serverloser Orchestrierungsservice, mit dem Sie Lambda-Funktionen und andere Funktionen kombinieren können, um geschäftskritische Anwendungen AWS-Services zu erstellen.

Andere Tools

- Python ist eine Allzweck-Computerprogrammiersprache.

Code-Repository

Der Code für dieses Muster ist im GitHub Serverless-Cell-Router-Repository verfügbar.

Bewährte Methoden

Bewährte Methoden für den Aufbau zellenbasierter Architekturen finden Sie in der folgenden AWS Well-Architected-Anleitung:

- Verringerung des Ausmaßes der Auswirkungen durch zellenbasierte Architektur
- AWS Säule der Zuverlässigkeit von Well-Architected Frameworks: REL1 0-BP04 Verwenden Sie Schottarchitekturen, um das Ausmaß der Auswirkungen zu begrenzen

Epen

Bereiten Sie die Quelldateien vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Beispielcode-Repository.	Verwenden Sie den folgenden Befehl, um das Serverless-Cell-Router GitHub Repository auf Ihren Computer zu klonen: `git clone https://github.com/aws-samp`	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`les/Serverless-Cell-Router/`	
Richten Sie AWS CLI temporäre Anmeldein formationen ein.	Konfigurieren Sie die AWS CLI mit Anmeldeinformationen für Ihre AWS-Konto. In dieser exemplarischen Vorgehens weise werden temporäre Anmeldeinformationen verwendet, die über die AWS IAM Identity Center-Be fehlszeile oder die programma tische Zugriffsoption bereitges tellt werden. Dadurch werden den `AWS_SESSI ON_TOKEN` AWS Umgebungs variablen `AWS_ACCES S_KEY_ID` `AWS_SECRE T_ACCESS_KEY` , und die entsprechenden Anmeldein formationen für die Verwendun g mit dem zugewiesen. AWS CLI	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Erstellen Sie einen S3-Bucket, der zum Speichern und Zugreifen auf die Serverless-Cell-Router Lambda-Funktionen für die Bereitstellung durch die AWS CloudFormation Vorlage verwendet wird. Verwenden Sie den folgenden Befehl, um den S3-Bucket zu erstellen: `aws s3api create-bucket --bucket <bucket name> --region eu-central-1 --create-bucket-configuration LocationConstraint=eu-central-1`	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie ZIP-Dateien.	Erstellen Sie eine ZIP-Datei für jede Lambda-Funktion, die sich im Verzeichnis Functions befindet. Diese ZIP-Dateien werden zur Bereitstellung der Lambda-Funktionen verwendet. Verwenden Sie auf einem Mac die folgenden Befehle: `zip`
	`zip -j mapper-scr.zip Functions/Mapper.py`
	`zip -j dispatcher-scr.zip Functions/Dispatcher.py`
	`zip -j scaler-scr.zip Functions/Scaler.py`
	`zip -j cp validator-scr.zip Functions/Validator.py`
	`zip -j dynamodbDummyData-scr.zip Functions/DynamodbDummyData.py`
		Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Kopieren Sie die ZIP-Dateien in den S3-Bucket.	Verwenden Sie die folgenden Befehle, um alle ZIP-Dateien der Lambda-Funktion in den S3-Bucket zu kopieren:
	`aws s3 cp mapper-scr.zip s3://<bucket name>`
	`aws s3 cp dispatcher-scr.zip s3://<bucket name>`
	`aws s3 cp scaler-scr.zip s3://<bucket name>`
	`aws s3 cp validator-scr.zip s3://<bucket name>`
	`aws s3 cp dynamodbDummyData-scr.zip s3://<bucket name>`
		Developer

Erstellen Sie den Stack AWS CloudFormation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die AWS CloudFormation Vorlage bereit.	Führen Sie den folgenden AWS CLI Befehl aus, um die AWS CloudFormation Vorlage bereitzustellen:
	`aws cloudformation create-stack --stack-name serverless.cell-router \`
	`--template-body file://Serverless-Cell-Router-Stack-v10.yaml \`
		Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--capabilities CAPABILITY_IAM \ --parameters ParameterKey=LambdaFunctionMapperS3KeyParameterSCR,ParameterValue=mapper-scr.zip \ ParameterKey=LambdaFunctionDispatcherS3KeyParameterSCR,ParameterValue=dispatcher-scr.zip \ ParameterKey=LambdaFunctionScalerS3KeyParameterSCR,ParameterValue=scaler-scr.zip \ ParameterKey=LambdaFunctionAddDynamoDBDummyItemsS3KeyParameterSCR,ParameterValue=dynamodbDummyData-scr.zip \ ParameterKey=LambdaFunctionsS3BucketParameterSCR,ParameterValue=<S3 bucket storing lambda zip files> \ ParameterKey=CognitoDomain,ParameterValue=<Cognito Domain Name> \ --region <enter your aws region id, e.g. "eu-central-1">`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Fortschritt.	Melden Sie sich bei der an AWS Management Console, öffnen Sie die AWS CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation/und überprüfen Sie den Fortschritt der Stack-Entwicklung. Wenn der Status lautet`CREATE_COMPLETE` , wurde der Stack erfolgreich bereitgestellt.	Developer

Beurteilen und verifizieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Weisen Sie dem Benutzer Zellen zu.	Um das zu initiiere n`Orchestrator` , führen Sie den folgenden curl-Befehl aus: `curl -X POST \ -H "Authorization: Bearer {User id_token}" \ https://xxxxxx.execute-api.eu-central-1.amazonaws.com/Cell_Router_Development/cells` Der `Orchestrator` löst die Ausführung der `Dispatcher` Funktion aus. Das `Dispatcher` wiederum überprüft die Existenz des	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Benutzers. Wenn der Benutzer gefunden wird, `Dispatcher` gibt der die zugehörigen Zellen-ID und den zugehörigen Endpunkt URLs zurück. Wenn der Benutzer nicht gefunden wird, `Dispatcher` weist der dem Benutzer eine Zelle zu und sendet die Zellen-ID an die `Scaler` Funktion zur Bewertung der Restkapazität der zugewiesenen Zelle. Die Antwort der `Scaler` Funktion lautet wie folgt: `"cellID : cell-0002 , endPoint_1 : https://xxxxx.execute-api.eu-north-1.amazonaws.com/ , endPoint_2 : https://xxxxxxx.execute-api.eu-central-1.amazonaws.com/"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Ruft Benutzerzellen ab.	Führen Sie `Orchestrator` den folgenden Befehl aus, um die `Mapper` Funktion auszuführen:
	`curl -X POST \ -H "Authorization: Bearer {User id_token} " \ https://xxxxxxxx x.execute-api.eu-c entral-1.amazonaws .com/Cell_Router_D evelopment/mapper`
	Das `Orchestrator` sucht nach der Zelle, die dem Benutzer zugewiesen ist, und gibt die Zellen-ID und URLs die folgende Antwort zurück:
	`"cellID : cell-0002 , endPoint_1 : https:// xxxxx.execute- api.eu-north-1 .amazonaws.com/ , endPoint_2 : https:// xxxxxxx.execute-api .eu-central-1.amaz onaws.com/"`
		Developer

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen Sie die Ressourcen.	Gehen Sie wie folgt vor, um zusätzliche Gebühren auf Ihrem Konto zu vermeiden: 1. Leeren Sie den S3-Bucket, den Sie für die Lambda-Funktionen erstellt haben. 2. Löschen Sie den Bucket. 3. Löschen Sie den AWS CloudFormation Stack.	App-Developer

Zugehörige Ressourcen

Referenzen

- Statische Stabilität mithilfe von Availability Zones
- Grenzen der AWS-Fehlerisolierung: Statische Stabilität

Video

Physalia: Zellenbasierte Architektur für höhere Verfügbarkeit auf Amazon EBS

https://www.youtube-nocookie.com/embed/RZMFic6 Ich weiß es? Steuerungen = 0

Zusätzliche Informationen

Prämissen für den Entwurf zellbasierter Architektur

Dieses Muster konzentriert sich zwar auf den Mobilfunkrouter, es ist jedoch wichtig, die gesamte Umgebung zu verstehen. Die Umgebung ist in drei separate Schichten gegliedert:

- Die Routing-Schicht oder dünne Schicht, die den Mobilfunkrouter enthält
- Die Zellschicht, bestehend aus verschiedenen Zellen
- Die Bereitstellungs- und Bereitstellungsebene, die Zellen bereitstellt und die Anwendung bereitstellt

Jede Schicht behält ihre Funktionalität auch bei Beeinträchtigungen anderer Schichten bei. AWS-Konten dienen als Grenze zur Fehlerisolierung.

Das folgende Diagramm zeigt die Schichten auf einer hohen Ebene. Die Zellschicht und die Bereitstellungs- und Bereitstellungsschicht fallen nicht in den Geltungsbereich dieses Musters.

Weitere Informationen zur zellenbasierten Architektur finden Sie unter Reduzierung des Wirkungsbereichs durch zellenbasierte Architektur: Zellenrouting.

Entwurfsmuster für Mobilfunkrouter

Der Mobilfunkrouter ist eine von allen Zellen gemeinsam genutzte Komponente. Um mögliche Auswirkungen zu minimieren, ist es wichtig, dass die Routing-Ebene ein vereinfachtes und horizontal skalierbares Design verwendet, das so dünn wie möglich ist. Die Routing-Schicht dient als Einstiegspunkt des Systems und besteht nur aus den Komponenten, die für die effiziente Zuweisung von Benutzern zu den entsprechenden Zellen erforderlich sind. Komponenten innerhalb dieser Ebene sind nicht an der Verwaltung oder Erstellung von Zellen beteiligt.

Dieses Muster verwendet statisches Routing, was bedeutet, dass der Client die Endpunkte bei der ersten Anmeldung zwischenspeichert und anschließend eine direkte Kommunikation mit der Zelle herstellt. Regelmäßige Interaktionen zwischen dem Client und dem Mobilfunkrouter werden initiiert, um den aktuellen Status zu bestätigen oder Aktualisierungen abzurufen. Diese gezielte Entkopplung ermöglicht bestehenden Benutzern einen unterbrechungsfreien Betrieb bei einem Ausfall des Mobilfunkrouters und sorgt für kontinuierliche Funktionalität und Stabilität innerhalb des Systems.

In diesem Muster unterstützt der Mobilfunkrouter die folgenden Funktionen:

- Abrufen von Zellendaten aus der Zellendatenbank in der Bereitstellungs- und Bereitstellungsschicht und Speichern oder Aktualisieren der lokalen Datenbank.
- Zuweisen einer Zelle zu jedem neuen registrierten Benutzer der Anwendung mithilfe des Zellenzuweisungsalgorithmus.
- Speichern der user-to-cells Zuordnung in der lokalen Datenbank.
- Überprüfung der Kapazität der Zellen während der Benutzerzuweisung und Auslösen eines Ereignisses für den Automaten in der Bereitstellungs- und Bereitstellungsebene, um Zellen zu erstellen.
- Verwendung des Algorithmus für Kriterien zur Zellenerstellung, um diese Funktionalität bereitzustellen.

- Beantwortung der neu registrierten Benutzeranfragen durch Bereitstellung URLs der statischen Zellen. Diese URLs werden auf dem Client mit einer Gültigkeitsdauer (TTL) zwischengespeichert.
- Beantwortung vorhandener Benutzeranfragen nach einer ungültigen URL durch Angabe einer neuen oder aktualisierten URL.

Sehen Sie sich die folgenden Komponenten und Schritte an, um mehr über den Demonstrations-Cellrouter zu erfahren, der anhand der AWS CloudFormation Vorlage eingerichtet wurde:

1. Richten Sie den Amazon Cognito Cognito-Benutzerpool ein und konfigurieren Sie ihn.
2. Richten Sie die API Gateway für den Mobilfunkrouter ein und konfigurieren Sie sie.
3. Erstellen Sie eine DynamoDB-Tabelle.
4. Erstellen und konfigurieren Sie eine SQS-Warteschlange.
5. Implementieren Sie die`Orchestrator`.
6. Implementieren Sie die Lambda-Funktionen:`Dispatcher`,`Scaler`,`Mapper`,`Validator`.
7. Beurteilt und verifiziert.

Voraussetzung ist, dass die Bereitstellungs- und Bereitstellungsschicht bereits eingerichtet ist. Ihre Implementierungsdetails würden den Rahmen dieses Artefakts sprengen.

Da diese Komponenten anhand einer AWS CloudFormation Vorlage eingerichtet und konfiguriert werden, werden die folgenden Schritte anschaulich und allgemein dargestellt. Es wird davon ausgegangen, dass Sie über die erforderlichen AWS Fähigkeiten verfügen, um die Einrichtung und Konfiguration abzuschließen.

1. Einrichtung und Konfiguration des Amazon Cognito Cognito-Benutzerpools

Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon Cognito Cognito-Konsole unter https://console.aws.amazon.com/cognito/. Richten Sie einen Amazon Cognito Cognito-Benutzerpool mit dem Namen`CellRouterPool`, mit App-Integration, gehosteter Benutzeroberfläche und den erforderlichen Berechtigungen ein und konfigurieren Sie ihn.

2. Richten Sie die API Gateway für den Mobilfunkrouter ein und konfigurieren Sie sie

Öffnen Sie die API Gateway Gateway-Konsole unter https://console.aws.amazon.com/apigateway/. Richten Sie mithilfe eines Amazon Cognito-Autorisierers`CellRouter`, der in den Amazon Cognito-Benutzerpool integriert ist, eine API mit dem Namen, ein und konfigurieren Sie sie. `CellRouterPool` Implementieren Sie die folgenden Elemente:

- `CellRouter`API-Ressourcen, einschließlich `POST` Methoden
- Integration mit dem in Schritt 5 implementierten Step Functions-Workflow
- Autorisierung durch den Amazon Cognito Cognito-Autorisierer
- Zuordnungen von Integrationsanfragen und Antworten
- Zuweisung der erforderlichen Berechtigungen

3. Erstellen Sie eine DynamoDB-Tabelle

Öffnen Sie die DynamoDB-Konsole unter und erstellen Sie eine Standard-DynamoDB-Tabelle https://console.aws.amazon.com/dynamodb/, die `tbl_router` mit der folgenden Konfiguration aufgerufen wird:

- Partitionsschlüssel – `marketId`
- Schlüssel sortieren – `cellId`
- Kapazitätsmodus – Bereitgestellt
- Point-in-time Wiederherstellung (PITR) – Aus

Erstellen Sie auf der Registerkarte Indizes einen globalen sekundären Index mit dem Namen. `marketId-currentCapacity-index` Die `Scaler` Lambda-Funktion verwendet den Index, um effizient nach der Zelle mit der niedrigsten Anzahl zugewiesener Benutzer zu suchen.

Erstellen Sie die Tabellenstruktur mit den folgenden Attributen:

- `marketId`– Europa
- `cellId`– cell-0002
- `currentCapacity`– 2
- `endPoint_1`– <your endpoint for the first Region>
- `endPoint_2`– <your endpoint for the second Region>
- `IsHealthy`– Stimmt
- `maxCapacity`– 10
- `regionCode_1` – `eu-north-1`
- `regionCode_2` – `eu-central-1`
- `userIds`– <your email address>

4 Erstellen und konfigurieren Sie eine SQS-Warteschlange

Öffnen Sie die Amazon SQS SQS-Konsole unter https://console.aws.amazon.com/sqs/und erstellen Sie eine Standard-SQS-Warteschlange namens `CellProvisioning` konfiguriert mit Amazon SQS SQS-Schlüsselverschlüsselung.

5. Implementieren Sie den Orchestrator

Entwickeln Sie einen Step Functions Functions-Workflow, der als `Orchestrator` Grundlage für den Router dient. Der Workflow kann über die Cell-Router-API aufgerufen werden. Der Workflow führt die angegebenen Lambda-Funktionen basierend auf dem Ressourcenpfad aus. Integrieren Sie die Step-Funktion in die API-Gateway-API für den Mobilfunkrouter `CellRouter` und konfigurieren Sie die erforderlichen Berechtigungen zum Aufrufen der Lambda-Funktionen.

Das folgende Diagramm zeigt den Arbeitsablauf. Der Auswahlstatus ruft eine der Lambda-Funktionen auf. Wenn die Lambda-Funktion erfolgreich ist, endet der Workflow. Wenn die Lambda-Funktion fehlschlägt, wird fail state aufgerufen.

6. Implementieren Sie die Lambda-Funktionen

Implementieren Sie die `Validator` Funktionen `Dispatcher` `MapperScaler`,, und. Wenn Sie jede Funktion in der Demonstration einrichten und konfigurieren, definieren Sie eine Rolle für die Funktion und weisen Sie die erforderlichen Berechtigungen für die Ausführung der erforderlichen Operationen in der DynamoDB-Tabelle zu. `tbl_router` Integrieren Sie zusätzlich jede Funktion in den Workflow. `Orchestrator`

Dispatcher-Funktion

Die `Dispatcher` Funktion ist dafür verantwortlich, jedem neuen registrierten Benutzer eine einzelne statische Zelle zu identifizieren und zuzuweisen. Wenn sich ein neuer Benutzer bei der globalen Anwendung registriert, wird die Anfrage an die `Dispatcher` Funktion weitergeleitet. Die Funktion verarbeitet die Anfrage anhand vordefinierter Bewertungskriterien wie den folgenden:

1. Region – Wählen Sie die Zelle auf dem Markt aus, in der sich der Benutzer befindet. Wenn der Benutzer beispielsweise von Europa aus auf die globale Anwendung zugreift, wählen Sie eine Zelle aus, die AWS-Regionen in Europa verwendet wird.
2. Nähe oder Latenz – Wählen Sie die Zelle aus, die dem Benutzer am nächsten ist. Wenn der Benutzer beispielsweise von Holland aus auf die Anwendung zugreift, berücksichtigt die Funktion eine Zelle, die Frankfurt und Irland verwendet. Die Entscheidung, welche Zelle sich am nächsten

befindet, basiert auf Kennzahlen wie der Latenz zwischen dem Standort des Benutzers und den Zellenregionen. Bei diesem Beispielmuster werden die Informationen statisch aus der Bereitstellungs- und Bereitstellungsebene eingespeist.

3. Health – Die `Dispatcher` Funktion überprüft anhand des angegebenen Zellstatus (Gesund = wahr oder falsch), ob die ausgewählte Zelle gesund ist.
4. Kapazität – Die Benutzerverteilung basiert auf der geringsten Anzahl von Benutzern in einer Zellenlogik, sodass der Benutzer der Zelle mit der geringsten Benutzeranzahl zugewiesen wird.

> **Note**
>
> Diese Kriterien dienen lediglich der Erläuterung dieses Beispielmusters. Für eine realitätsnahe Implementierung eines Mobilfunkrouters können Sie verfeinerte und anwendungsfallorientierte Kriterien definieren.

`Orchestrator`Ruft die Dispatcher-Funktion auf, um Zellen Benutzer zuzuweisen. In dieser Demofunktion ist der Marktwert ein statischer Parameter, der als definiert ist. `europe`

Die `Dispatcher` Funktion bewertet, ob dem Benutzer bereits eine Zelle zugewiesen ist. Wenn die Zelle bereits zugewiesen ist, gibt die `Dispatcher` Funktion die Endpunkte der Zelle zurück. Wenn dem Benutzer keine Zelle zugewiesen ist, sucht die Funktion nach der Zelle mit der geringsten Anzahl von Benutzern, weist sie dem Benutzer zu und gibt die Endpunkte zurück. Die Effizienz der Zellensuchanfrage wird durch die Verwendung des globalen sekundären Indexes optimiert.

Mapper-Funktion

Die `Mapper` Funktion überwacht die Speicherung und Wartung von user-to-cell Zuordnungen in der Datenbank. Jedem registrierten Benutzer wird eine einzelne Zelle zugewiesen. Jede Zelle hat zwei unterschiedliche URLs — eine für jede AWS-Region. Diese dienen als API-Endpunkte, die auf API Gateway gehostet werden, und URLs fungieren als eingehende Punkte für die globale Anwendung.

Wenn die `Mapper` Funktion eine Anfrage von der Client-Anwendung empfängt, führt sie eine Abfrage in der DynamoDB-Tabelle aus, `tbl_router` um die user-to-cell Zuordnung abzurufen, die der angegebenen E-Mail-ID zugeordnet ist. Wenn sie eine zugewiesene Zelle findet, stellt die `Mapper` Funktion umgehend die beiden Zellen der Zelle bereit. URLs Die `Mapper` Funktion überwacht außerdem aktiv Änderungen an der Zelle URLs und veranlasst Benachrichtigungen oder Aktualisierungen der Benutzereinstellungen.

Scaler-Funktion

Die `Scaler` Funktion verwaltet die Restkapazität der Zelle. Bei jeder neuen Benutzerregistrierungsanfrage bewertet die `Scaler` Funktion die verfügbare Kapazität der Zelle, der die `Dispatcher` Funktion dem Benutzer zugewiesen hat. Wenn die Zelle ihr vorgegebenes Limit gemäß den angegebenen Bewertungskriterien erreicht hat, initiiert die Funktion eine Anfrage über eine Amazon SQS SQS-Warteschlange an die Bereitstellungs- und Bereitstellungsebene und fordert die Bereitstellung und Bereitstellung neuer Zellen an. Die Skalierung von Zellen kann auf der Grundlage einer Reihe von Bewertungskriterien wie den folgenden durchgeführt werden:

1. Maximale Benutzeranzahl – Jede Zelle kann eine maximale Anzahl von 500 Benutzern haben.
2. Pufferkapazität – Die Pufferkapazität jeder Zelle beträgt 20 Prozent, was bedeutet, dass jeder Zelle jederzeit 400 Benutzern zugewiesen werden kann. Die verbleibenden 20 Prozent der Pufferkapazität sind für future Anwendungsfälle und die Behandlung unerwarteter Szenarien reserviert (z. B. wenn die Dienste zur Zellenerstellung und -bereitstellung nicht verfügbar sind).
3. Zellenerstellung – Sobald eine bestehende Zelle 70 Prozent der Kapazität erreicht, wird eine Anforderung zur Erstellung einer zusätzlichen Zelle ausgelöst.

> **Note**
>
> Diese Kriterien dienen nur zur Erläuterung dieses Beispielmusters. Für eine realitätsnahe Implementierung eines Mobilfunkrouters können Sie verfeinerte und anwendungsfallorientierte Kriterien definieren.

Der `Scaler` Demonstrationscode wird ausgeführt, `Orchestrator` nachdem der dem neu registrierten Benutzer `Dispatcher` erfolgreich eine Zelle zugewiesen hat. Nach Erhalt der Zellen-ID von bewertet der anhand vordefinierter Bewertungskriterien`Dispatcher`, ob die angegebene Zelle über ausreichend Kapazität für weitere Benutzer verfügt. `Scaler` Wenn die Kapazität der Zelle nicht ausreicht, sendet die `Scaler` Funktion eine Nachricht an den Amazon SQS-Service. Diese Nachricht wird vom Service innerhalb der Bereitstellungs- und Bereitstellungsebene abgerufen, wodurch die Bereitstellung einer neuen Zelle eingeleitet wird.

Validator-Funktion

Die `Validator` Funktion identifiziert und behebt Probleme im Zusammenhang mit dem Zellzugriff. Wenn sich ein Benutzer bei der globalen Anwendung anmeldet, ruft die Anwendung die Zellen

URLs aus den Benutzerprofileinstellungen ab und leitet Benutzeranfragen an eine der beiden zugewiesenen Regionen innerhalb der Zelle weiter. Wenn auf sie nicht zugegriffen URLs werden kann, kann die Anwendung eine validierte URL-Anfrage an den Mobilfunkrouter senden. Der Mobilfunkrouter ruft die `Orchestrator` auf. `Validator` Das `Validator` initiiert den Validierungsprozess. Die Validierung kann neben anderen Prüfungen Folgendes umfassen:

- Querverweise auf die URLs in der Datenbank URLs gespeicherte Zelle in der Anfrage, um mögliche Aktualisierungen zu identifizieren und zu verarbeiten
- Durchführung einer gründlichen Zustandsprüfung (z. B. eine `HTTP GET` Anfrage an den Endpunkt der Zelle)

Zusammenfassend liefert die `Validator` Funktion Antworten auf Anfragen von Kundenanwendungen und gibt den Validierungsstatus sowie alle erforderlichen Korrekturmaßnahmen an.

Die wurde `Validator` entwickelt, um die Benutzererfahrung zu verbessern. Stellen Sie sich ein Szenario vor, in dem bestimmte Benutzer Schwierigkeiten haben, auf die globale Anwendung zuzugreifen, weil aufgrund eines Vorfalls Zellen vorübergehend nicht verfügbar sind. Anstatt generische Fehler anzuzeigen, kann die `Validator` Funktion aufschlussreiche Schritte zur Problembehebung bereitstellen. Diese Schritte können die folgenden Aktionen beinhalten:

- Informieren Sie die Benutzer über den Vorfall.
- Geben Sie eine ungefähre Wartezeit bis zur Verfügbarkeit des Dienstes an.
- Geben Sie eine Support-Kontaktnummer an, um weitere Informationen zu erhalten.

Der Demo-Code für die `Validator` Funktion überprüft, ob die vom Benutzer angegebene Zelle URLs in der Anfrage mit den in der Tabelle gespeicherten Datensätzen übereinstimmt. `tbl_router` Die `Validator` Funktion überprüft auch, ob die Zellen gesund sind.

Richten Sie den privaten Zugriff auf einen Amazon S3 S3-Bucket über einen VPC-Endpunkt ein

Erstellt von Martin Maritsch (AWS), Gabriel Rodriguez Garcia (AWS), Shukhrat Khodjaev (AWS), Nicolas Jacob Baer (AWS), Mohan Gowda Purushothama (AWS) und Joaquin Rinaudo (AWS)

Übersicht

In Amazon Simple Storage Service (Amazon S3) können Sie mit Presigned URLs Dateien beliebiger Größe für Zielbenutzer freigeben. Standardmäßig URLs sind vorsignierte Amazon S3 innerhalb eines Ablaufzeitfensters über das Internet zugänglich, sodass sie bequem zu verwenden sind. In Unternehmensumgebungen ist jedoch häufig der Zugriff auf Amazon S3 erforderlich, der so vorkonfiguriert ist URLs , dass er nur auf ein privates Netzwerk beschränkt ist.

Dieses Muster stellt eine serverlose Lösung für die sichere Interaktion mit S3-Objekten dar, indem vorsignierte Daten URLs aus einem privaten Netzwerk ohne Internetdurchquerung verwendet werden. In der Architektur greifen Benutzer über einen internen Domainnamen auf einen Application Load Balancer zu. Der Datenverkehr wird intern über Amazon API Gateway und einen Virtual Private Cloud (VPC) -Endpunkt für den S3-Bucket geleitet. Die AWS Lambda Funktion generiert vorsignierte URLs Dateidownloads über den privaten VPC-Endpunkt, wodurch die Sicherheit und der Datenschutz für sensible Daten verbessert werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine VPC, die ein Subnetz umfasst AWS-Konto , das in einem mit dem Unternehmensnetzwerk verbunden ist (z. B. über AWS Direct Connect).

Einschränkungen

- Der S3-Bucket muss denselben Namen wie die Domain haben. Wir empfehlen daher, die Amazon S3 S3-Bucket-Namensregeln zu überprüfen.
- Diese Beispielarchitektur beinhaltet keine Überwachungsfunktionen für die bereitgestellte Infrastruktur. Wenn Ihr Anwendungsfall eine Überwachung erfordert, sollten Sie das Hinzufügen von AWS Überwachungsdiensten in Betracht ziehen.

- Diese Beispielarchitektur beinhaltet keine Eingabevalidierung. Wenn Ihr Anwendungsfall eine Eingabevalidierung und ein erhöhtes Sicherheitsniveau erfordert, sollten Sie dies AWS WAF zum Schutz Ihrer API in Betracht ziehen.
- Diese Beispielarchitektur beinhaltet keine Zugriffsprotokollierung mit dem Application Load Balancer. Wenn Ihr Anwendungsfall eine Zugriffsprotokollierung erfordert, sollten Sie die Aktivierung der Load Balancer-Zugriffsprotokolle in Betracht ziehen.

Versionen

- Python-Version 3.11 oder höher
- Terraform Version 1.6 oder höher

Architektur

Zieltechnologie-Stack

Die folgenden AWS-Services werden im Zieltechnologie-Stack verwendet:

- Amazon S3 ist der zentrale Speicherservice, der für das sichere Hochladen, Herunterladen und Speichern von Dateien verwendet wird.
- Amazon API Gateway stellt Ressourcen und Endpunkte für die Interaktion mit dem S3-Bucket zur Verfügung. Dieser Service spielt eine Rolle bei der Generierung von Daten, die URLs für das Herunterladen oder Hochladen vorkonfiguriert sind.
- AWS Lambdageneriert vorsignierte Dateien URLs für das Herunterladen von Dateien von Amazon S3. Die Lambda-Funktion wird von API Gateway aufgerufen.
- Amazon VPC stellt Ressourcen innerhalb einer VPC bereit, um das Netzwerk zu isolieren. Die VPC umfasst Subnetze und Routingtabellen zur Steuerung des Datenverkehrs.
- Der Application Load Balancer leitet eingehenden Datenverkehr entweder an API Gateway oder an den VPC-Endpunkt des S3-Buckets weiter. Es ermöglicht Benutzern aus dem Unternehmensnetzwerk den internen Zugriff auf Ressourcen.
- Der VPC-Endpunkt für Amazon S3 ermöglicht die direkte, private Kommunikation zwischen Ressourcen in der VPC und Amazon S3, ohne das öffentliche Internet zu durchqueren.
- AWS Identity and Access Management (IAM) steuert den Zugriff auf Ressourcen. AWS Berechtigungen werden eingerichtet, um sichere Interaktionen mit der API und anderen Diensten zu gewährleisten.

Zielarchitektur

Das Diagramm veranschaulicht folgende Vorgänge:

1. Benutzer aus dem Unternehmensnetzwerk können über einen internen Domainnamen auf den Application Load Balancer zugreifen. Wir gehen davon aus, dass eine Verbindung zwischen dem Unternehmensnetzwerk und dem Intranet-Subnetz im besteht AWS-Konto (z. B. über eine AWS Direct Connect Verbindung).
2. Der Application Load Balancer leitet eingehenden Datenverkehr entweder an API Gateway weiter, um Daten zu generieren, die für das Herunterladen oder Hochladen von Daten auf Amazon S3 vorsigniert URLs sind, oder an den VPC-Endpunkt des S3-Buckets. In beiden Szenarien werden Anfragen intern weitergeleitet und müssen nicht über das Internet geleitet werden.
3. API Gateway stellt Ressourcen und Endpunkte für die Interaktion mit dem S3-Bucket zur Verfügung. In diesem Beispiel stellen wir einen Endpunkt zum Herunterladen von Dateien aus dem S3-Bucket bereit. Dieser könnte jedoch erweitert werden, um auch Upload-Funktionen bereitzustellen.
4. Die Lambda-Funktion generiert die vorsignierte URL zum Herunterladen einer Datei von Amazon S3, indem sie den Domainnamen des Application Load Balancer anstelle der öffentlichen Amazon S3 S3-Domain verwendet.
5. Der Benutzer erhält die vorsignierte URL und verwendet sie, um die Datei mithilfe des Application Load Balancer von Amazon S3 herunterzuladen. Der Load Balancer enthält eine Standardroute, um Traffic, der nicht für die API bestimmt ist, an den VPC-Endpunkt des S3-Buckets zu senden.
6. Der VPC-Endpunkt leitet die vorsignierte URL mit dem benutzerdefinierten Domainnamen an den S3-Bucket weiter. Der S3-Bucket muss denselben Namen wie die Domain haben.

Automatisierung und Skalierung

Dieses Muster verwendet Terraform, um die Infrastruktur aus dem Code-Repository in einem bereitzustellen. AWS-Konto

Tools

Tools

- Python ist eine Allzweck-Computerprogrammiersprache.

- Terraform ist ein IaC-Tool (Infrastructure as Code) HashiCorp , mit dem Sie Cloud- und lokale Ressourcen erstellen und verwalten können.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer AWS Befehlszeilen-Shell mit Diensten interagieren können.

Code-Repository

Der Code für dieses Muster ist in einem GitHub Repository unter https://github.com/aws-samples/private-s3-vpce verfügbar.

Bewährte Methoden

Die Beispielarchitektur für dieses Muster verwendet IAM-Berechtigungen, um den Zugriff auf die API zu steuern. Jeder, der über gültige IAM-Anmeldeinformationen verfügt, kann die API aufrufen. Wenn Ihr Anwendungsfall ein komplexeres Autorisierungsmodell erfordert, möchten Sie möglicherweise einen anderen Zugriffskontrollmechanismus verwenden.

Epen

Stellen Sie die Lösung in einem bereit AWS-Konto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Besorgen Sie sich AWS Anmeldeinformationen.	Überprüfen Sie Ihre AWS Anmeldeinformationen und Ihren Zugang zu Ihrem Konto. Anweisungen finden Sie in der AWS CLI Dokumentation unter Konfiguration und Einstellungen für die Anmeldeinformationsdatei.	AWS DevOps, Allgemeines AWS
Klonen Sie das Repository	Klonen Sie das mit diesem Muster bereitgestellte GitHub Repository:	AWS DevOps, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`git clone https://github.com/aws-samples/private-s3-vpce`	
Variablen konfigurieren.	1. Öffnen Sie auf Ihrem Computer im GitHub Repository den `terraform` Ordner: `cd terraform` 2. Öffnen Sie die `example.tfvars` Datei und passen Sie die Parameter an Ihre Bedürfnisse an.	AWS DevOps, Allgemeines AWS
Lösung bereitstellen.	1. Führen Sie im `terraform` Ordner Terraform aus und übergeben Sie die Variablen, die Sie angepasst haben: `terraform apply -var-file="example.tfvars"` 2. Vergewissern Sie sich, dass die im Architekturdiagramm angezeigten Ressourcen erfolgreich bereitgestellt wurden.	AWS DevOps, Allgemeines AWS

Testen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Testdatei.	Laden Sie eine Datei auf Amazon S3 hoch, um ein Testszenario für den Dateidownload zu erstellen . Sie können die Amazon S3 S3-Konsole oder den folgenden AWS CLI Befehl verwenden: `aws s3 cp /path/to/ testfile s3://your- bucket-name/testfile`	AWS DevOps, Allgemeines AWS
Testen Sie die Funktionalität vordefinierter URLs.	1. Senden Sie mithilfe von awscurl eine Anfrage an den Application Load Balancer, um eine vorsignierte URL für die Testdatei zu erstellen: `awscurl https://your- domain-name/api/ get_url?key=testfile` In diesem Schritt wird aus Ihren Anmeldeinformationen eine gültige Signatur erstellt, die von API Gateway validiert wird. 2. Analysieren Sie den Link aus der Antwort, die Sie im vorherigen Schritt erhalten haben, und öffnen Sie die	AWS DevOps, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	vorsignierte URL, um die Datei herunterzuladen.	
Bereinigen Sie.	Stellen Sie sicher, dass Sie die Ressourcen entfernen, wenn sie nicht mehr benötigt werden: `terraform destroy`	AWS DevOps, Allgemeines AWS

Fehlerbehebung

Problem	Lösung
S3-Objektschlüsselnamen mit Sonderzeichen wie Nummernzeichen (#) unterbrechen URL-Parameter und führen zu Fehlern.	Codieren Sie die URL-Parameter ordnungsgemäß und stellen Sie sicher, dass der Name des S3-Objektschlüssels den Amazon S3 S3-Richtlinien entspricht.

Zugehörige Ressourcen

Amazon S3:

- Objekte mit vorsignierten teilen URLs
- Steuern des Zugriffs von VPC-Endpunkten aus mit Bucket-Richtlinien

Amazon API Gateway:

- Verwenden Sie VPC-Endpunktrichtlinien für private Zwecke APIs in API Gateway

Application Load Balancer:

- Hosten interner statischer HTTPS-Websites mit ALB, S3 und PrivateLink (AWS Blogbeitrag)

Problembehebung bei Zuständen AWS Step Functions mithilfe von Amazon Bedrock

Erstellt von Aniket Kurzadkar (AWS) und Sangam Kushwaha (AWS)

Übersicht

AWS Step Functions Funktionen zur Fehlerbehandlung können Ihnen helfen, einen Fehler zu erkennen, der während eines bestimmten Status in einem Workflow auftritt, aber es kann dennoch schwierig sein, die Ursache eines Fehlers zu finden und zu debuggen. Dieses Muster adressiert diese Herausforderung und zeigt, wie Amazon Bedrock Ihnen helfen kann, Fehler zu beheben, die während Status in Step Functions auftreten.

Step Functions bietet Workflow-Orchestrierung und erleichtert es Entwicklern, Prozesse zu automatisieren. Step Functions bietet auch Funktionen zur Fehlerbehandlung, die folgende Vorteile bieten:

- Entwickler können robustere Anwendungen entwickeln, die nicht komplett ausfallen, wenn etwas schief geht.
- Workflows können bedingte Logik enthalten, um verschiedene Arten von Fehlern unterschiedlich zu behandeln.
- Das System kann fehlgeschlagene Operationen automatisch wiederholen, möglicherweise mit exponentiellem Backoff.
- Für Fehlerszenarien können alternative Ausführungspfade definiert werden, sodass der Workflow angepasst und die Verarbeitung fortgesetzt werden kann.

Wenn in einem Step Functions-Workflow ein Fehler auftritt, zeigt dieses Muster, wie die Fehlermeldung und der Kontext an ein Foundation Model (FM) wie Claude 3 gesendet werden können, das von Step Functions unterstützt wird. Das FM kann den Fehler analysieren, ihn kategorisieren und mögliche Schritte zur Behebung vorschlagen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Grundlegendes Verständnis von AWS Step Functions und Arbeitsabläufen
- Amazon Bedrock API-Konnektivität

Einschränkungen

- Sie können den Ansatz dieses Musters für verschiedene AWS-Services Zwecke verwenden. Die Ergebnisse können jedoch je nach der von AWS Lambda Amazon Bedrock erstellten Aufforderung variieren.
- Einige AWS-Services sind nicht in allen AWS-Regionen verfügbar. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie unter AWS-Services nach Regionen. Informationen zu bestimmten Endpunkten finden Sie unter Service-Endpunkte und Kontingente. Wählen Sie dort den Link für den Service aus.

Architektur

Das folgende Diagramm zeigt den Workflow und die Architekturkomponenten für dieses Muster.

Das Diagramm zeigt den automatisierten Workflow für die Fehlerbehandlung und Benachrichtigung in einer Step Functions Functions-Zustandsmaschine:

1. Der Entwickler startet die Ausführung einer Zustandsmaschine.
2. Die Step Functions Functions-Zustandsmaschine beginnt mit der Verarbeitung ihrer Zustände. Es gibt zwei mögliche Ergebnisse:
   - (a) Wenn alle Staaten erfolgreich ausgeführt wurden, wird der Workflow direkt an Amazon SNS weitergeleitet, wo eine E-Mail-Erfolgsmeldung gesendet wird.
   - (b) Wenn ein Status ausfällt, wechselt der Workflow zur Lambda-Funktion zur Fehlerbehandlung.
3. Im Falle eines Fehlers passiert Folgendes:
   - (a) Die Lambda-Funktion (Fehlerhandler) wird ausgelöst. Die Lambda-Funktion extrahiert die Fehlermeldung aus den Ereignisdaten, die ihr von der Step Functions Functions-Zustandsmaschine übergeben wurden. Anschließend bereitet die Lambda-Funktion eine Aufforderung auf der Grundlage dieser Fehlermeldung vor und sendet die Aufforderung an Amazon Bedrock. In der Aufforderung werden Lösungen und Vorschläge für den spezifischen aufgetretenen Fehler angefordert.
   - (b) Amazon Bedrock, das das generative KI-Modell hostet, verarbeitet die Eingabeaufforderung. (Dieses Muster verwendet das Anthropic Claude 3 Foundation Model (FM), eines von vielen, FMs die Amazon Bedrock unterstützt.) Das KI-Modell analysiert den Fehlerkontext. Anschließend generiert das Modell eine Antwort, die Erklärungen zur Ursache des Fehlers,

mögliche Lösungen zur Behebung des Fehlers und Vorschläge zur Vermeidung future Fehler enthalten kann.

Amazon Bedrock gibt seine KI-generierte Antwort an die Lambda-Funktion zurück. Die Lambda-Funktion verarbeitet die Antwort und formatiert sie möglicherweise oder extrahiert wichtige Informationen. Dann sendet die Lambda-Funktion die Antwort an die Ausgabe der Zustandsmaschine.

4. Nach der Fehlerbehandlung oder erfolgreicher Ausführung wird der Workflow abgeschlossen, indem Amazon SNS veranlasst wird, eine E-Mail-Benachrichtigung zu senden.

Tools

AWS-Services

- Amazon Bedrock ist ein vollständig verwalteter Service, der Ihnen leistungsstarke Basismodelle (FMs) von führenden KI-Startups und Amazon über eine einheitliche API zur Verfügung stellt.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.
- AWS Step Functionsist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Funktionen und andere Funktionen kombinieren können, um geschäftskritische Anwendungen AWS-Services zu erstellen.

Bewährte Methoden

- Angesichts der Tatsache, dass Amazon Bedrock ein generatives KI-Modell ist, das aus trainierten Daten lernt, verwendet es diese Daten auch, um Kontext zu trainieren und zu generieren. Es hat sich bewährt, alle privaten Informationen zu verbergen, die zu Problemen mit Datenlecks führen könnten.
- Obwohl generative KI wertvolle Erkenntnisse liefern kann, sollten kritische Entscheidungen zur Fehlerbehandlung immer noch unter menschlicher Aufsicht getroffen werden, insbesondere in Produktionsumgebungen.

Epen

Erstellen Sie eine Zustandsmaschine für Ihren Workflow

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen -Zustands automaten.	Gehen Sie wie folgt vor, um eine Zustandsmaschine zu erstellen, die für Ihren Workflow geeignet ist: 1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Step Functions Konsole. 2. Wählen Sie im linken Navigationsbereich State Machines aus. 3. Wählen Sie Create State Machine (Zustands automaten erstellen). 4. Wählen Sie eine Vorlage, die Ihrem Anwendung sfall entspricht, oder wählen Sie Leer, um eine Vorlage entsprechend Ihren Anforderungen zu erstellen.	AWS DevOps

Erstellen einer Lambda-Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Lambda-Fu nktion.	Gehen Sie wie folgt vor, um eine Lambda-Funktion zu erstellen:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Navigieren Sie in der AWS Management Console zur AWS Lambda Konsole. 2. Wählen Sie im linken Navigationsbereich Funktionen und dann Funktion anlegen. 3. Wählen Sie auf der Seite Funktion erstellen eine der Optionen aus, um eine Funktion zu erstellen . Geben Sie dann einen Namen in das Feld Funktionsname ein und wählen Sie die entsprech ende Sprache aus der Dropdownliste in Runtime aus. 4. Wählen Sie Funktion erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die erforderliche Logik im Lambda-Code ein.	• Verwenden Sie den folgenden Code, um mithilfe von eine Verbindung zur AWS SDK für Python (Boto3)Amazon Bedrock-API herzustellen. Dieser Code richtet einen Client für Amazon Bedrock ein, bereitet die erforderlichen Parameter vor und sendet dann eine Anfrage mit einer bestimmten Aufforderung an das Claude 3-Modell. Dieses Muster ruft das Claude 3-Modell auf. Weitere Informationen zu allen unterstützten Foundation-Modellen, einschließlich verwandter Modelle IDs, finden Sie unter Unterstützte Foundation-Modelle in Amazon Bedrock in der Amazon Bedrock-Dokumentation. `client = boto3.client( service_name="bedrock-runtime", region_name="selected-region" )`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> # Invoke Claude 3
	 with the text prompt
	    model_id = "your-mod
	el-id" # Select your
	 Model ID, Based on the
	 Model Id, Change the
	 body format
	
	    try:
	        response =
	 client.invoke_model(
	            modelId=m
	odel_id,
	            body=json
	.dumps(
	                {
	
	 "anthropic_version":
	 "bedrock-2023-05-31",
	
	 "max_tokens": 1024,
	
	 "messages": [
	
	 {
	
	    "role": "user",
	
	          "content"
	: [{"type": "text",
	 "text": prompt}],
	
	 }
	                    ],
	                }
	            ),
	        )</pre>
	• (Optional) Ersetzen Sie das AWS-Konto IDs Konto durch einen Platzhalter. IDs Aus	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Sicherheitsgründen kann dieser Ansatz nützlich sein, um Protokolle, Fehlermeldungen oder andere Ausgaben zu bereinigen, die möglicherweise vertrauliche Kontoinformationen enthalten.
	
	Der folgende Code findet jedes Vorkommen einer 12-stelligen Zahl in Doppelpunkten (was dem Format AWS-Konto IDs in Amazon Resource Names (ARNs) und einigen anderen AWS Identifikatoren entspricht) und ersetzt sie durch die Platzhalter-Konto-ID. `":123456789012:"`
	
	`def replace_account_id(input_string):`
	`  # Use a regular expression to find the AWS account ID pattern`
	`  account_id_pattern = r'(:\d{12}:)'`
	`  # Replace the matched pattern with ":123456789012:"`
	`  modified_string = re.sub(account_id_`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`pattern, ":1234567 89012:", input_str ing)`
	
	`return modified_ string`	

Integrieren Sie Step Functions mit Lambda

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Lambda für die Behandlung von Fehlern in Step Functions ein.	Gehen Sie wie folgt vor, um Step Functions so einzurich ten, dass Fehler behandelt werden, ohne den Arbeitsab lauf zu unterbrechen: 1. Navigieren Sie in der Step Functions Functions-Konsole zu der Zustandsm aschine, die Sie zuvor erstellt haben. 2. Wählen Sie Bearbeiten und wählen Sie dann den Dienst aus, für den Sie die Fehlerbehandlung einrichte n möchten, und wählen Sie Fehlerbehandlung aus. 3. Wählen Sie Neuen Catcher hinzufügen und als Fallback-Status die Option Lambda und dann die Lambda-Funktion aus, die Sie zuvor erstellt haben. Weitere Informationen	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	finden Sie unter Fehler abfangen in der Dokumentation zu Step Functions.	

Fehlerbehebung

Problem	Lösung
Lambda kann nicht auf die Amazon Bedrock API zugreifen (nicht zur Ausführung autorisiert)	Dieser Fehler tritt auf, wenn die Lambda-Rolle nicht berechtigt ist, auf die Amazon Bedrock-API zuzugreifen. Um dieses Problem zu beheben, fügen Sie die `AmazonBedrockFullAccess` Richtlinie für die Lambda-Rolle hinzu. Weitere Informationen finden Sie AmazonBedrockFullAccessim Referenzhandbuch für AWS verwaltete Richtlinien.
Lambda-Timeout-Fehler	Manchmal kann es je nach Aufforderung mehr als 30 Sekunden dauern, bis eine Antwort generiert und zurückgesendet wird. Erhöhen Sie die Konfigurationszeit, um dieses Problem zu beheben. Weitere Informationen finden Sie unter Configure Lambda function timeout im AWS Lambda Developer Guide.

Zugehörige Ressourcen

- Amazon Bedrock
- Amazon Bedrock API-Zugriff
- Erstellen Sie Ihre erste Lambda-Funktion
- Entwicklung von Workflows mit Step Functions
- AWS Step Functions

Verketten Sie AWS-Services mithilfe eines serverlosen Ansatzes

Erstellt von Aniket Braganza (AWS)

Übersicht

Dieses Muster veranschaulicht einen skalierbaren, serverlosen Ansatz für die Verarbeitung einer hochgeladenen Datei, indem Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon SNS), Amazon Simple Queue Service (Amazon SQS) und AWS Lambda miteinander verkettet werden. Das Beispiel für eine hochgeladene Datei dient zu Demonstrationszwecken. Sie können einen serverlosen Ansatz verwenden, um andere Aufgaben zu erledigen, indem Sie die Kombination der AWS-Services, die zur Erreichung Ihrer Geschäftsziele erforderlich sind, miteinander verknüpfen. Der serverlose Ansatz verwendet einen asynchronen Workflow, der auf ereignisgesteuerten Benachrichtigungen, robustem Speicher und Function-as-a-Service (FaaS) -Computing zur Bearbeitung von Anfragen basiert. Sie können den serverlosen Ansatz verwenden, um bedarfsgerecht zu skalieren und gleichzeitig die Kosten zu minimieren.

> **Note**
>
> Es gibt mehrere Optionen, um AWS-Services über einen serverlosen Ansatz miteinander zu verknüpfen. Sie können beispielsweise einen Ansatz verwenden, der Lambda mit Amazon S3 anstelle von Amazon SNS und Amazon SQS kombiniert. Dieses Muster verwendet jedoch Amazon SNS und Amazon SQS, da dieser Ansatz es ermöglicht, dem Lambda-Aufrufprozess während einer Ereignisbenachrichtigung mehrere Integrationspunkte hinzuzufügen und die Implementierung auf mehrere Listener in einer serverlosen Orchestrierung auszudehnen und gleichzeitig den Verarbeitungsaufwand zu minimieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Programmatischer Zugriff auf das AWS-Konto. Weitere Informationen finden Sie unter:
  - Voraussetzungen in der Dokumentation zum AWS Cloud Development Kit (AWS CDK)
  - Voraussetzungen in der Dokumentation zur AWS-Befehlszeilenschnittstelle (AWS CLI)
- AWS CDK, installiert

- AWS CLI, installiert und konfiguriert
- Python 3.9

Produktversionen

- AWS CDK 2.x
- Python 3.9

Architektur

Das folgende Diagramm zeigt, wie verkettete AWS-Services es einem Benutzer ermöglichen können, eine Datei zur Verarbeitung in einen S3-Bucket hochzuladen.

Das Diagramm zeigt den folgenden Workflow:

1. Ein Benutzer lädt eine Datei in den S3-Bucket hoch.
2. Der Upload löst ein S3-Ereignis aus, das eine Nachricht zu einem SNS-Thema veröffentlicht. Die Nachricht enthält die Details des S3-Ereignisses.
3. Die unter dem SNS-Thema veröffentlichte Nachricht wird in eine SQS-Warteschlange eingefügt, die abonniert ist und Benachrichtigungen zu diesem Thema erhält.
4. Eine Lambda-Funktion fragt die SQS-Warteschlange (als Ereignisquelle) ab und wartet auf die Verarbeitung von Nachrichten.
5. Wenn die Lambda-Funktion Nachrichten aus der SQS-Warteschlange empfängt, verarbeitet sie sie und bestätigt den Empfang dieser Nachrichten.
6. Wenn eine Nachricht nicht von Lambda verarbeitet wird, wird diese Nachricht an die SQS-Warteschlange zurückgegeben und schließlich in eine SQS-Warteschlange mit unzustellbaren Buchstaben übertragen.

Technologie-Stack

- Amazon S3
- Amazon SNS
- Amazon SQS
- AWS Lambda

Tools

AWS-Services

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.
- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.

Andere Tools

- Das AWS Cloud Development Kit (AWS CDK) ist das wichtigste Tool für die Interaktion mit Ihrer AWS CDK-App. Es führt Ihre App aus, fragt das von Ihnen definierte Anwendungsmodell ab und erstellt und stellt die vom AWS-CDK generierten CloudFormation AWS-Vorlagen bereit.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Python ist eine interpretierte Mehrzweck-Programmiersprache auf hohem Niveau.

Code

Der Code für dieses Muster ist im Repository GitHub Chaining S3 to SNS to SQS to Lambda verfügbar.

Epen

Entwickeln Sie Ihre serverlose Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Klonen Sie das Repository und navigieren Sie zum `python/s3-sns-sqs-lambda-chain` Ordner.	App-Developer
Richten Sie eine virtuelle Umgebung ein.	1. Führen Sie im AWS-CDK den `python3 -m venv .venv` Befehl aus. 2. Führen Sie den `source .venv/bin/activate` Befehl unter MacOS/Linux oder `.venv\Scripts\activate.bat` Windows aus.	App-Developer
Installieren Sie die Abhängigkeiten.	Führen Sie den Befehl `pip install -r requirements.txt` aus.	App-Developer

Testen Sie den Stack CloudFormation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie Komponententests durch.	1. Führen Sie den Befehl `pip install -r requirements-dev.txt` aus. 2. **Important** (Optional) Führen Sie den `cdk`	App-Entwickler, Testingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`synth --no-staging > template.yml` Befehl aus, um den CloudFormation Stack zu generiere n. Sie können den Stapel untersuch en, aber vermeiden , die bereitges tellten Ressource n und Artefakte zu generieren. 3. Führen Sie den `pytest` Befehl aus, um alle Komponententests auszuführen. 4. (Optional) Führen Sie den `pytest tests/uni t/<test_filename>` Befehl aus, um Tests für eine bestimmte Datei auszuführen.	

Stellen Sie den CloudFormation Stack bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Bootstrap-Umgebung ein.	Folgen Sie den Anweisung en unter Bootstrapping in der AWS-Dokumentation, um die Umgebung für die AWS-CDK-Bereitstellung in jeder AWS-	App-Entwickler, DevOps Ingenieur, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Region, in der der CloudFormation Stack bereitgestellt wird, zu booten. **Note** Für diesen Schritt benötigen Sie Anmeldeinformationen mit programmatischem Zugriff.	
Stellen Sie den CloudFormation Stack bereit.	Führen Sie den `cdk deploy` Befehl aus, um den Stack zu erstellen und für das AWS-Konto bereitzustellen.	App-Entwickler, DevOps Ingenieur, AWS DevOps

Bereinigen Sie die Ressourcen Ihrer Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie den CloudFormation Stapel und entfernen Sie die zugehörigen Ressourcen.	Um den erstellten CloudFormation Stack zu löschen und alle zugehörigen Ressourcen zu entfernen, führen Sie den Befehl `run cdk` destroy aus.	App-Developer

Mehr Muster

- Mit Athena auf Amazon DynamoDB-Tabellen zugreifen, diese abfragen und verbinden
- Aggregieren Sie Daten in Amazon DynamoDB für ML-Prognosen in Athena
- Automatisieren Sie CodeGuru Amazon-Rezensionen für AWS CDK Python-Anwendungen mithilfe von GitHub Aktionen
- Automatisieren Sie die AWS-Ressourcenbewertung
- Automatisieren Sie die Bereitstellung verschachtelter Anwendungen mit AWS SAM
- Automatisieren Sie die Replikation von Amazon RDS-Instances auf AWS-Konten
- Automatisches Archivieren von Elementen in Amazon S3 mithilfe von DynamoDB TTL
- Automatische Erkennung von Änderungen und Initiierung verschiedener CodePipeline Pipelines für ein Monorepo in CodeCommit
- Erstellen Sie eine lose gekoppelte Architektur mit Microservices mithilfe von DevOps Praktiken und AWS Cloud9
- Erstellen Sie eine serverlose Architektur mit mehreren Mandanten in Amazon Service OpenSearch
- Erstellen Sie einen fortschrittlichen Mainframe-Dateiviewer in der AWS-Cloud
- Value at Risk (VaR) mithilfe von AWS-Services berechnen
- Kopieren Sie AWS Service Catalog-Produkte zwischen verschiedenen AWS-Konten und AWS-Regionen
- Automatisches Erstellen dynamischer CI-Pipelines für Java- und Python-Projekte
- Zerlegen Sie Monolithen mithilfe von CQRS und Event Sourcing in Microservices
- Stellen Sie eine React-basierte Einzelseitenanwendung auf Amazon S3 bereit und CloudFront
- Stellen Sie eine Amazon API Gateway Gateway-API auf einer internen Website mithilfe von privaten Endpunkten und einem Application Load Balancer bereit
- Bereitstellen und Debuggen von Amazon EKS-Clustern
- Bereitstellen und verwalten Sie einen serverlosen Data Lake in der AWS-Cloud, indem Sie Infrastruktur als Code verwenden
- Stellen Sie mithilfe AWS von Terraform und Amazon Bedrock einen RAG-Anwendungsfall bereit
- Entwickeln Sie mithilfe von Amazon Bedrock-Agenten und Wissensdatenbanken einen vollautomatischen Chat-basierten Assistenten
- Entwickeln Sie mithilfe von RAG und Prompting fortschrittliche, auf KI basierende Chat-Assistenten ReAct

- Dynamisches Generieren einer IAM-Richtlinie mit IAM Access Analyzer mithilfe von Step Functions
- Stellen Sie sicher, dass die Amazon EMR-Protokollierung bei Amazon S3 beim Start aktiviert ist
- Schätzen Sie die Kosten einer DynamoDB-Tabelle für On-Demand-Kapazität
- Generieren Sie mit Amazon Personalize personalisierte und neu eingestufte Empfehlungen
- Generieren Sie Testdaten mit einem AWS Glue Glue-Job und Python
- Implementieren Sie SHA1 Hashing für PII-Daten bei der Migration von SQL Server zu PostgreSQL
- Implementieren Sie das serverlose Saga-Muster mithilfe von AWS Step Functions
- Verbessern Sie die Betriebsleistung, indem Sie Amazon DevOps Guru in mehreren AWS-Regionen, Konten und OUs mit dem AWS CDK aktivieren
- Starten Sie mithilfe von Step Functions und einer Lambda-Proxyfunktion ein CodeBuild Projekt für alle AWS-Konten
- Migrieren Sie Apache Cassandra-Workloads mithilfe von AWS Glue zu Amazon Keyspaces
- Überwachen Sie die Nutzung eines gemeinsam genutzten Amazon Machine Image über mehrere AWS-Konten
- Optimieren Sie serverlose Bereitstellungen mit mehreren Konten mithilfe der AWS CDK Workflows und Aktionen GitHub
- Orchestrieren Sie eine ETL-Pipeline mit Validierung, Transformation und Partitionierung mithilfe von AWS Step Functions
- Abfragen von Amazon DynamoDB-Tabellen mit SQL mithilfe von Amazon Athena
- Führen Sie ereignisgesteuerte und geplante Workloads in großem Umfang mit AWS Fargate aus
- Statische Inhalte in einem Amazon S3 S3-Bucket über eine VPC mithilfe von Amazon bereitstellen CloudFront
- Optimieren Sie die Entwicklung und Bereitstellung von Amazon Lex Lex-Bot mithilfe eines automatisierten Workflows
- Strukturieren Sie ein Python-Projekt in hexagonaler Architektur mit AWS Lambda
- Translate natürliche Sprache in Abfragen, DSL für OpenSearch und Elasticsearch-Abfragen
- Deaktivieren Sie die Sicherheitsstandardkontrollen für alle Security Hub Hub-Mitgliedskonten in einer Umgebung mit mehreren Konten
- Daten aus einem Amazon Redshift Redshift-Cluster kontenübergreifend nach Amazon S3 entladen
- Koordinieren Sie die Ressourcenabhängigkeit und die Aufgabenausführung mithilfe des AWS Fargate WaitCondition Hook-Konstrukts

- Verwenden Sie Amazon Bedrock-Agenten, um die Erstellung von Zugriffskontrollen in Amazon EKS durch textbasierte Eingabeaufforderungen zu automatisieren

Netzwerk

Themen

- Automatisieren Sie die Einrichtung von regionsübergreifendem Peering mit AWS Transit Gateway
- Zentralisieren Sie die Netzwerkkonnektivität mit AWS Transit Gateway
- Konfigurieren Sie die HTTPS-Verschlüsselung für Oracle JD Edwards EnterpriseOne auf Oracle WebLogic mithilfe eines Application Load Balancer
- Stellen Sie über ein privates Netzwerk eine Connect zu Daten- und Steuerungsebenen des Application Migration Service her
- Erstellen Sie Infoblox-Objekte mithilfe von CloudFormation benutzerdefinierten AWS-Ressourcen und Amazon SNS
- Passen Sie CloudWatch Amazon-Benachrichtigungen an für AWS Network Firewall
- Bereitstellen von Ressourcen in einer AWS Wavelength Zone mithilfe von Terraform
- Massenmigrieren von DNS-Einträgen in eine private gehostete Zone von Amazon Route 53
- Ändern Sie HTTP-Header, wenn Sie von F5 zu einem Application Load Balancer auf AWS migrieren
- Greifen Sie privat von mehreren aus auf einen zentralen AWS-Serviceendpunkt zu VPCs
- Erstellen Sie einen Bericht mit den Ergebnissen von Network Access Analyzer für eingehenden Internetzugang in mehreren AWS-Konten
- Richten Sie die DNS-Auflösung für Hybridnetzwerke in einer Umgebung mit mehreren Konten AWS ein
- Stellen Sie sicher, dass ELB-Load Balancer eine TLS-Terminierung erfordern
- AWS-Netzwerk-Firewall-Protokolle und -Metriken mithilfe von Splunk anzeigen
- Mehr Muster

Automatisieren Sie die Einrichtung von regionsübergreifendem Peering mit AWS Transit Gateway

Erstellt von Ram Kandaswamy (AWS)

Übersicht

AWS Transit Gateway verbindet virtuelle private Clouds (VPCs) und lokale Netzwerke über einen zentralen Hub. Der Transit Gateway Gateway-Verkehr bleibt immer auf dem globalen Amazon Web Services (AWS) -Backbone und durchquert nicht das öffentliche Internet, wodurch Bedrohungsvektoren wie häufige Exploits und verteilte Denial-of-Service (DDoS) -Angriffe reduziert werden.

Wenn Sie zwischen zwei oder mehr AWS-Regionen kommunizieren müssen, können Sie regionsübergreifendes Transit Gateway Gateway-Peering verwenden, um Peering-Verbindungen zwischen Transit-Gateways in verschiedenen Regionen herzustellen. Die manuelle Konfiguration von regionsübergreifendem Peering mit Transit Gateway kann jedoch ein zeitaufwändiger Prozess sein, der mehrere Schritte umfasst. Dieses Muster bietet einen automatisierten Prozess zum Entfernen dieser manuellen Schritte, indem das Peering mithilfe von Code durchgeführt wird. Sie können diesen Ansatz verwenden, wenn Sie während der Einrichtung einer Organisation mit mehreren Regionen wiederholt mehrere Regionen und AWS-Konten konfigurieren müssen.

Dieses Muster verwendet einen CloudFormation AWS-Stack, der den AWS Step Functions-Workflow, AWS Lambda Lambda-Funktionen, AWS Identity and Access Management (IAM) -Rollen und Protokollgruppen in Amazon CloudWatch Logs umfasst. Anschließend können Sie eine Step Functions Functions-Ausführung starten und die regionsübergreifende Peering-Verbindung für Ihre Transit-Gateways erstellen. Informationen zur manuellen Einrichtung von regionsübergreifendem Peering finden Sie unter Peer VPCs in verschiedenen AWS-Regionen mithilfe von AWS Transit Gateway.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein vorhandener Amazon Simple Storage Service (Amazon S3) -Bucket.
- Transit-Gateways, die in der anfordernden Region und den akzeptierenden Regionen erstellt und konfiguriert wurden. Die Region des Anforderers ist der Ort, an dem eine Peering-Anfrage gestellt wird, und die akzeptierenden Regionen akzeptieren die Peering-Anfrage. Weitere Informationen

dazu finden Sie unter Erstellen und Akzeptieren einer VPC-Peering-Verbindung in der Amazon VPC-Dokumentation.

- VPCs, wurde in den Regionen Acceptor und Requester installiert und konfiguriert. Schritte zum Erstellen einer VPC finden Sie unter Erstellen der VPC von Get Started with Amazon VPC in der Amazon VPC-Dokumentation.
- Sie VPCs müssen das Tag und den `addToTransitGateway` Wert verwenden. `true`
- Sicherheitsgruppen und Netzwerkzugriffskontrolllisten (ACLs) für Sie VPCs, konfiguriert nach Ihren Anforderungen. Weitere Informationen dazu finden Sie unter Sicherheitsgruppen für Ihre VPC und Ihr Netzwerk ACLs in der Amazon VPC-Dokumentation.

AWS-Regionen und Einschränkungen

- Nur bestimmte AWS-Regionen unterstützen regionsübergreifendes Peering. Eine vollständige Liste der Regionen, die regionsübergreifendes Peering unterstützen, finden Sie im AWS Transit Gateway. FAQs
- Im beigefügten Beispielcode wird davon ausgegangen, dass die Region des Anforderers und die Region des Akzeptors dies ist. `us-east-2` `us-west-2` Wenn Sie verschiedene Regionen konfigurieren möchten, müssen Sie diese Werte in allen Python-Dateien bearbeiten. Um ein komplexeres Setup zu implementieren, das mehr als zwei Regionen umfasst, können Sie die Step-Funktion so ändern, dass die Regions als Parameter an die Lambda-Funktion übergeben und die Funktion für jede Kombination ausgeführt werden.

Architektur

Das Diagramm zeigt einen Workflow mit den folgenden Schritten:

1. Der Benutzer erstellt einen CloudFormation AWS-Stack.
2. AWS CloudFormation erstellt eine Step Functions Functions-Zustandsmaschine, die eine Lambda-Funktion verwendet. Weitere Informationen dazu finden Sie in der AWS Step Functions Step Functions-Dokumentation unter Erstellen einer Step Functions-Zustandsmaschine, die Lambda verwendet.
3. Step Functions ruft eine Lambda-Funktion für das Peering auf.
4. Die Lambda-Funktion stellt eine Peering-Verbindung zwischen Transit-Gateways her.

5. Step Functions ruft eine Lambda-Funktion für Änderungen an Routentabellen auf.
6. Die Lambda-Funktion ändert die Routentabellen, indem sie den CIDR-Block (Classless Inter-Domain Routing) von hinzufügt. VPCs

Arbeitsablauf für Step Functions

Das Diagramm zeigt den folgenden Step Functions Functions-Arbeitsablauf:

1. Der Step Functions Functions-Workflow ruft die Lambda-Funktion für das Transit-Gateway-Peering auf.
2. Es erfolgt ein Timer-Anruf, um eine Minute zu warten.
3. Der Peering-Status wird abgerufen und an den Condition-Block gesendet. Der Block ist für das Looping verantwortlich.
4. Wenn die Erfolgsbedingung nicht erfüllt ist, ist der Workflow so codiert, dass er in die Timer-Phase übergeht.
5. Wenn die Erfolgsbedingung erfüllt ist, wird eine Lambda-Funktion aufgerufen, um die Routentabellen zu ändern. Nach diesem Aufruf endet der Step Functions Functions-Workflow.

Tools

- AWS CloudFormation — AWS CloudFormation ist ein Service, der Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen unterstützt.
- Amazon CloudWatch Logs — CloudWatch Logs hilft Ihnen dabei, die Protokolle all Ihrer Systeme, Anwendungen und AWS-Services, die Sie verwenden, zu zentralisieren.
- AWS Identity and Access Management (IAM) — IAM ist ein Webservice zur sicheren Steuerung des Zugriffs auf AWS-Services.
- AWS Lambda — Lambda führt Ihren Code auf einer hochverfügbaren Recheninfrastruktur aus und übernimmt die gesamte Verwaltung der Rechenressourcen.
- AWS Step Functions — Step Functions macht es einfach, die Komponenten verteilter Anwendungen als eine Reihe von Schritten in einem visuellen Workflow zu koordinieren.

Epen

Automatisieren Sie das Peering

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die angehängten Dateien in Ihren S3-Bucket hoch.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon S3 S3-Konsole und laden Sie dann die (angehängten) `get-transit-gateway-peering-status.zip` Dateien `modify-transit-gateway-routes.zip` `peer-transit-gateway.zip` , und in Ihren S3-Bucket hoch.	Allgemeines AWS
Erstellen Sie den CloudFormation AWS-Stack.	Führen Sie den folgenden Befehl aus, um mithilfe der `transit-gateway-peering.json` Datei (angehängt) einen CloudFormation AWS-Stack zu erstellen: `aws cloudformation create-stack --stack-name myteststack --template-body file://sampletemplate.json` Der CloudFormation AWS-Stack erstellt den Step Functions Functions-Workflow , die Lambda-Funktionen, IAM-Rollen und CloudWatch Protokollgruppen.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Stellen Sie sicher, dass sich die CloudFormation AWS-Vorlage auf den S3-Bucket bezieht, der die zuvor hochgeladenen Dateien enthält. **Note** Sie können einen Stack auch mithilfe der CloudFormation AWS-Konsole erstellen. Weitere Informationen dazu finden Sie in der CloudFormation AWS-Dokumentation unter Erstellen eines Stacks auf der CloudFormation AWS-Konsole.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie eine neue Ausführung in Step Functions.	Öffnen Sie die Step Functions Functions-Konsole und starten Sie eine neue Ausführung. Step Functions ruft die Lambda-Funktion auf und erstellt die Peering-Verbindung für die Transit-Gateways. Sie benötigen keine JSON-Eingabedatei. Stellen Sie sicher, dass ein Anhang verfügbar ist und ob der Verbindungstyp Peering ist. Weitere Informationen dazu finden Sie unter Starten einer neuen Ausführung unter Erste Schritte mit AWS Step Functions in der Dokumentation zu AWS Steps Functions.	DevOps Ingenieur, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Routen in den Routentabellen.	Zwischen den Transit-G ateways wird regionsüb ergreifendes Peering eingerich tet. Die Routentabellen werden mit dem CIDR-Bloc kbereich der VPC der Peer-Region aktualisiert. IPv4 Öffnen Sie die Amazon VPC-Konsole und wählen Sie in der Routentabelle, die dem Transit-Gateway-Anhang entspricht, die Registerk arte Verknüpfungen aus. Überprüfen Sie den VPC-CIDR-Blockbereich der Peering-Regionen. Ausführliche Schritte und Anweisungen finden Sie unter Zuordnen einer Transit-G ateway-Routentabelle in der Amazon VPC-Dokumentation.	Netzwerkadministrator

Zugehörige Ressourcen

- Ausführungen in Step Functions
- Peering-Anlagen des Transit-Gateways
- Peer VPCs in verschiedenen AWS-Regionen mithilfe von AWS Transit Gateway
- Verbindung zwischen VPCs AWS-Regionen mithilfe von AWS Transit Gateway herstellen — Demo (Video)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Zentralisieren Sie die Netzwerkkonnektivität mit AWS Transit Gateway

Erstellt von Mydhili Palagummi (AWS) und Nikhil Marrapu (AWS)

Übersicht

Dieses Muster beschreibt die einfachste Konfiguration, in der AWS Transit Gateway verwendet werden kann, um ein lokales Netzwerk mit virtuellen privaten Clouds (VPCs) in mehreren AWS-Konten innerhalb einer AWS-Region zu verbinden. Mit diesem Setup können Sie ein Hybridnetzwerk einrichten, das mehrere VPC-Netzwerke in einer Region und ein lokales Netzwerk verbindet. Dies wird durch die Verwendung eines Transit-Gateways und einer VPN-Verbindung (Virtual Private Network) zum lokalen Netzwerk erreicht.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein Konto für das Hosten von Netzwerkdiensten, das als Mitgliedskonto einer Organisation in AWS Organizations verwaltet wird
- VPCs in mehreren AWS-Konten, ohne sich überlappende Classless Inter-Domain Routing (CIDR) -Blöcke

Einschränkungen

Dieses Muster unterstützt nicht die Isolierung des Datenverkehrs zwischen bestimmten Netzwerken VPCs oder dem lokalen Netzwerk. Alle an das Transit-Gateway angeschlossenen Netzwerke können sich gegenseitig erreichen. Um den Verkehr zu isolieren, müssen Sie benutzerdefinierte Routentabellen auf dem Transit-Gateway verwenden. Dieses Muster verbindet das Netzwerk VPCs und das lokale Netzwerk nur mithilfe einer einzigen Standard-Routentabelle für das Transit-Gateway, was die einfachste Konfiguration darstellt.

Architektur

Zieltechnologie-Stack

- AWS Transit Gateway
- Site-to-SiteAWS-VPN
- VPC

- AWS Resource Access Manager (AWS RAM)

Zielarchitektur

Tools

AWS-Services

- Mit AWS Resource Access Manager (AWS RAM) können Sie Ihre Ressourcen sicher über Ihre AWS-Konten, Organisationseinheiten oder Ihre gesamte Organisation von AWS Organizations aus teilen.
- AWS Transit Gateway ist ein zentraler Hub, der virtuelle private Clouds (VPCs) und lokale Netzwerke verbindet.

Epen

Erstellen Sie ein Transit-Gateway im Netzwerkdienstkonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Transit-Gateway.	Erstellen Sie in dem AWS-Konto, in dem Sie Netzwerkdienste hosten möchten, ein Transit-Gateway in der AWS-Zielregion. Anweisungen finden Sie unter Ein Transit-Gateway erstellen. Beachten Sie Folgendes: • Wählen Sie Standard-Routing-Tabellenzuordnung aus. • Wählen Sie Standardweiterleitung für Routing-Tabellen aus.	Netzwerkadministrator

Connect das Transit-Gateway mit Ihrem lokalen Netzwerk

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie ein Kunden-Gateway-Gerät für die VPN-Verbindung ein.	Das Kunden-Gateway-Gerät ist an der lokalen Seite der Site-to-Site VPN-Verbindung zwischen dem Transit-Gateway und Ihrem lokalen Netzwerk angeschlossen. Weitere Informationen finden Sie in der Site-to-Site AWS-VPN-Dokumentation unter Ihr Kunden-Gateway-Gerät. Identifizieren oder starten Sie ein unterstütztes lokales Kundengerät und notieren Sie sich dessen öffentliche IP-Adresse. Die VPN-Konfiguration wird später in diesem Epos abgeschlossen.	Netzwerkadministrator
Erstellen Sie im Netzwerkdienstkonto einen VPN-Anhang zum Transit-Gateway.	Um eine Verbindung einzurichten, erstellen Sie einen VPN-Anhang für das Transit-Gateway. Anweisungen finden Sie unter VPN-Anlagen für das Transit-Gateway.	Netzwerkadministrator
Konfigurieren Sie das VPN auf dem Kunden-Gateway-Gerät in Ihrem lokalen Netzwerk.	Laden Sie die Konfigurationsdatei für die Site-to-Site VPN-Verbindung herunter, die dem Transit-Gateway zugeordnet ist, und konfigurieren Sie die VPN-Einstellungen auf dem Kunden-Gateway-Gerät. Anweisungen	Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	finden Sie unter Laden Sie die Konfigurationsdatei herunter.	

Teilen Sie das Transit-Gateway im Netzwerk-Services-Konto mit anderen AWS-Konten oder Ihrer Organisation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie im Verwaltungskonto von AWS Organizations die Option Teilen.	Um das Transit-Gateway mit Ihrer Organisation oder mit bestimmten Organisationseinheiten zu teilen, aktivieren Sie die gemeinsame Nutzung in AWS Organizations. Andernfalls müssten Sie das Transit-Gateway für jedes Konto einzeln teilen. Anweisungen finden Sie unter Aktivieren der gemeinsamen Nutzung von Ressourcen innerhalb von AWS Organizations.	AWS-Systemadministrator
Erstellen Sie die Transit-Gateway-Ressourcenfreigabe im Netzwerkdienstkonto.	VPCs Damit andere AWS-Konten innerhalb Ihrer Organisation eine Verbindung zum Transit-Gateway herstellen können, verwenden Sie im Netzwerk-Services-Konto die AWS-RAM-Konsole, um die Transit-Gateway-Ressource gemeinsam zu nutzen. Anweisungen finden Sie unter Eine gemeinsam	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	e Nutzung von Ressourcen erstellen.	

Connect VPCs zum Transit-Gateway her

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie VPC-Anhänge in einzelnen Konten.	Erstellen Sie in den Konten, für die das Transit-Gateway gemeinsam genutzt wurde, Transit-Gateway-VPC-Anlagen. Anweisungen finden Sie unter Erstellen eines Transit-Gateway-Anhangs zu einer VPC.	Netzwerkadministrator
Akzeptieren Sie die VPC-Anhangsanfragen.	Akzeptieren Sie im Netzwerkdienstkonto die VPC-Anhangsanforderungen des Transit-Gateways. Anweisungen finden Sie unter Akzeptieren eines gemeinsamen Anhangs.	Netzwerkadministrator

Routing konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Routen in einem individuellen Konto VPCs.	Fügen Sie in jeder einzelnen Konto-VPC Routen zum lokalen Netzwerk und zu anderen VPC-Netzwerken hinzu, wobei Sie das Transit-Gateway als Ziel verwenden. Anweisungen finden Sie unter	Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinzufügen und Entfernen von Routen aus einer Routentabelle.	
Konfigurieren Sie Routen in der Transit-Gateway-Routentabelle.	Routen von VPCs und die VPN-Verbindung sollten weitergegeben werden und in der Standardroutentabelle des Transit-Gateways erscheinen. Erstellen Sie bei Bedarf statische Routen (ein Beispiel sind statische Routen für die statische VPN-Verbindung) in der Standardroutentabelle des Transit-Gateways. Anweisungen finden Sie unter Erstellen einer statischen Route.	Netzwerkadministrator
Fügen Sie Regeln für Sicherheitsgruppen und Netzwerkzugriffskontrolllisten (Network Access Control List, ACL) hinzu.	Stellen Sie für die EC2 Instances und andere Ressourcen in der VPC sicher, dass die Sicherheitsgruppenregeln und die Netzwerk-ACL-Regeln den Datenverkehr sowohl zwischen dem lokalen Netzwerk VPCs als auch zwischen dem lokalen Netzwerk zulassen. Anweisungen finden Sie unter Steuern des Datenverkehrs zu Ressourcen mithilfe von Sicherheitsgruppen und Hinzufügen und Löschen von Regeln aus einer ACL.	Netzwerkadministrator

Testen Sie die Konnektivität

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Konnektivität zwischen VPCs.	Stellen Sie sicher, dass Netzwerk-ACL und Sicherheitsgruppen ICMP-Verkehr (Internet Control Message Protocol) zulassen, und pingen Sie dann von Instances in einer VPC an eine andere VPC, die ebenfalls mit dem Transit-Gateway verbunden ist.	Netzwerkadministrator
Testen Sie die Konnektivität zwischen VPCs und dem lokalen Netzwerk.	Stellen Sie sicher, dass Netzwerk-ACL-Regeln, Sicherheitsgruppenregeln und alle Firewalls ICMP-Verkehr zulassen, und pingen Sie dann zwischen dem lokalen Netzwerk und den EC2 Instanzen im. VPCs Die Netzwerkkommunikation muss zuerst vom lokalen Netzwerk aus initiiert werden, um die VPN-Verbindung in den Status zu versetzen. UP	Netzwerkadministrator

Zugehörige Ressourcen

- Aufbau einer skalierbaren und sicheren AWS-Netzwerkinfrastruktur mit mehreren VPC (AWS-Whitepaper)
- Arbeiten mit gemeinsam genutzten Ressourcen (AWS-RAM-Dokumentation)
- Arbeiten mit Transit-Gateways (AWS Transit Gateway Gateway-Dokumentation)

Konfigurieren Sie die HTTPS-Verschlüsselung für Oracle JD Edwards EnterpriseOne auf Oracle WebLogic mithilfe eines Application Load Balancer

Erstellt von Thanigaivel Thirumalai (AWS)

Übersicht

Dieses Muster erklärt, wie die HTTPS-Verschlüsselung für SSL-Offloading in Oracle JD Edwards auf Oracle-Workloads konfiguriert wird. EnterpriseOne WebLogic Bei diesem Ansatz wird der Datenverkehr zwischen dem Browser des Benutzers und einem Load Balancer verschlüsselt, um die Server von der Verschlüsselungslast zu entlasten. EnterpriseOne

Viele Benutzer skalieren die Stufe der EnterpriseOne JAVA Virtual Machine (JVM) horizontal, indem sie einen AWS Application Load Balancer verwenden.Der Load Balancer dient als zentrale Anlaufstelle für Kunden und verteilt den eingehenden Datenverkehr auf mehrere. JVMs Optional kann der Load Balancer den Datenverkehr auf mehrere Availability Zones verteilen und die Verfügbarkeit von erhöhen. EnterpriseOne

Der in diesem Muster beschriebene Prozess konfiguriert die Verschlüsselung zwischen dem Browser und dem Load Balancer, anstatt den Datenverkehr zwischen dem Load Balancer und dem zu verschlüsseln. EnterpriseOne JVMs Dieser Ansatz wird als SSL-Offloading bezeichnet. Die Auslagerung des SSL-Entschlüsselungsprozesses vom EnterpriseOne Web- oder Anwendungsserver auf den Application Load Balancer reduziert die Belastung der Anwendungsseite. Nach der SSL-Terminierung am Load Balancer wird der unverschlüsselte Datenverkehr an die Anwendung auf AWS weitergeleitet.

Oracle JD Edwards EnterpriseOne ist eine ERP-Lösung (Enterprise Resource Planning) für Unternehmen, die Produkte oder Sachanlagen herstellen, konstruieren, vertreiben, warten oder verwalten. JD Edwards EnterpriseOne unterstützt verschiedene Hardware, Betriebssysteme und Datenbankplattformen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine AWS Identity and Access Management (IAM) -Rolle, die berechtigt ist, AWS-Serviceanrufe zu tätigen und AWS-Ressourcen zu verwalten

- Ein SSL-Zertifikat

Produktversionen

- Dieses Muster wurde mit Oracle WebLogic 12c getestet, Sie können aber auch andere Versionen verwenden.

Architektur

Es gibt mehrere Ansätze, um SSL-Offloading durchzuführen. Dieses Muster verwendet einen Application Load Balancer und einen Oracle HTTP Server (OHS), wie in der folgenden Abbildung dargestellt.

Das folgende Diagramm zeigt das JVM-Layout von JD Edwards EnterpriseOne, Application Load Balancer und Java Application Server (JAS).

Tools

AWS-Services

- Application Load Balancer verteilen den eingehenden Anwendungsdatenverkehr auf mehrere Ziele, z. B. Amazon Elastic Compute Cloud (EC2 Amazon-Instances), in mehreren Availability Zones.
- AWS Certificate Manager (ACM) unterstützt Sie bei der Erstellung, Speicherung und Erneuerung von öffentlichen und privaten SSL/TLS X.509-Zertifikaten und Schlüsseln, die Ihre AWS-Websites und -Anwendungen schützen.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.

Bewährte Methoden

- Bewährte Methoden für ACM finden Sie in der ACM-Dokumentation.

Epen

Einrichtung WebLogic und Arbeitsschutz

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren und konfigurieren Sie Oracle-Komponenten.	1. Installieren Sie Fusion Middleware Infrastructure, indem Sie dem Standardinstallationsprozess folgen. Dieses Programm hilft Ihnen bei der Installation und Konfiguration einer WebLogic Domain. Anweisungen finden Sie in der Oracle-Dokumentation. 2. Installieren Sie OHS, indem Sie dem Standardinstallationsprozess folgen. Anweisungen finden Sie in der Oracle-Dokumentation. 3. Wenn die Installation abgeschlossen ist, starten Sie den Konfigurationsassistenten (`config.sh` Datei), um OHS zu konfigurieren. • Sie können eine bestehende Domain aktualisieren oder eine neue Domain erstellen. Bei diesem Muster wird davon ausgegangen, dass Sie eine bestehende Domain aktualisieren.	JDE CNC, Administrator WebLogic

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wählen Sie für Verfügbare Vorlagen Oracle Enterprise Manager-Restricted JRF und Oracle HTTP Server (Restricted JRF). Wenn Sie diese Optionen für Java Required Files (JRF) auswählen, entfällt die Verbindung zu einer externen Datenbank. • Akzeptieren Sie für Verwaltete Server, Cluster, Servervorlagen, Coherence Clusters, Machines, Assign Servers to Machines, Virtuelle Ziele und Partitionen die Standardkonfigurationswerte und wählen Sie Weiter, um zur nächsten Kategorie zu wechseln. • Vervollständigen Sie die Konfigurationsdetails (z. B. Administratorhost und Port, Listenadresse und Port, Servername) für die OHS-Instanz (z. B.`ohs1`).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie das WebLogic Plugin auf Domainebene.	Das WebLogic Plugin ist für den Lastenausgleich erforderl ich. Um das Plugin zu aktiviere n: 1. Melden Sie sich über den WebLogic folgenden Link bei der Verwaltungskonsole an: `http://<WeblogicSe rver>:<Adminport>/ console` 2. Wählen Sie Sperren und Bearbeiten und anschließend Konfiguration, Webanwendungen. 3. Wählen Sie das WebLogic Plugin aktiviert (Kontroll kästchen oder Drop-down-Option). 4. Wählen Sie Änderungen speichern und aktivieren.	JDE CNC, Administrator WebLogic

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bearbeiten Sie die Konfigura tionsdatei.	Die `mod_wl_ohs.conf` Datei konfiguriert Proxy-Anf ragen von OHS an. WebLogic
	
	1. Bearbeiten Sie diese Datei. Sie befindet sich in:
	
	`$ORACLE_HOME/user_ projects/domains/`
	
	Zum Beispiel:
	
	`/home/oracle/Oracl e/Middleware/Oracl e_Home/user_projec ts/domains/base_do main/config/fmwcon fig/components/OHS /instances/ohs1`
	2. Fügen Sie die Werte WebLogic host (`WebLogicHost`) und port (`WebLogicPort`) hinzu (Dieses Muster geht von localhost und Port 8000 aus.)
	3. Fügen Sie die `WLProxySS LPassThrough` Werte `WLProxySSL` und wie folgt hinzu:
	
	`<VirtualHost *:8000>`
	`<Location /jde>`
	`WLSRequest On`
		JDE CNC, Administrator WebLogic

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>SetHandler weblogic-
	handler
	WebLogicHost
	 localhost
	WebLogicPort 8000
	WLProxySSL On
	WLProxySSLPassThrough
	 On
	</Location>
	</VirtualHost></pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie OHS mit dem Enterprise Manager.	1. Melden Sie sich über den folgenden Link bei Enterprise Manager Fusion Middleware an: `http://<WeblogicServer>:<Adminport>/em/` 2. Wählen Sie in Target Navigation unter HTTP-Server die OHS-Instanz aus (z. B.). `ohs1` 3. Wählen Sie Herunterfahren und Starten, um die OHS-Instanz neu zu starten. 4. Wenn das OHS-Setup abgeschlossen ist, können Sie eine Verbindung zum EnterpriseOne HTML-Client herstellen, indem Sie Ihren HTTP-Server-Hostnamen mit Port 8000 anstelle des EnterpriseOne Server-Hostnamens verwenden. • Alter Link: `http://<Webserver>:80/jde/owhtml` • Neuer Link: `http://<HTTP server or web server>:8000/jde/owhtml` Wenn Sie einen anderen Port als den standardm	JDE CNC, Administrator WebLogic

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	äßigen Oracle-HTTP-Port verwenden, bearbeiten Sie die `httpd.conf` Datei, um an zwei Stellen einen Listener für diesen Port hinzuzufügen:
	`#[Listen] OHS_LISTEN_PORT`
	`Listen 8000`
	und:
	`#`
	`ServerName <Weblogic Server1>:8000`	

Den Application Load Balancer konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine Zielgruppe ein.	1. Erstellen Sie eine Zielgruppe für den HTTP-Server-Port 8000. 2. Registrieren Sie die Ziele unter der Zielgruppe mit demselben Port. 3. Überprüfen Sie den Status der Ziele, um sicherzustellen, dass sie fehlerfrei sind. 4. Konfigurieren Sie die Einstellungen für die	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Integritätsprüfung nach Bedarf. Eine ausführliche Anleitung finden Sie in der Elastic Load Balancing Balancing-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie den Load Balancer ein.	1. Erstellen Sie einen Application Load Balancer mit Standardattributen und der erforderlichen Virtual Private Cloud (VPC), Sicherheitsgruppen und Subnetzen. Anweisungen finden Sie in der Elastic Load Balancing Balancing-Dokumentation. 2. Fügen Sie einen Listener-Eintrag für HTTPS 443 hinzu und leiten Sie ihn an die Zielgruppe weiter, die Sie im vorherigen Schritt erstellt haben. (Anweisungen finden Sie in der Elastic Load Balancing Balancing-Dokumentation.) Ein HTTPS-Listener benötigt ein SSL-Zertifikat. Sie können ein Zertifikat von ACM auswählen oder eines hochladen. 3. Aktivieren Sie für beide Listener Stickiness, indem Sie den Anweisungen in der Elastic Load Balancing Balancing-Dokumentation folgen.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie einen Route 53 53-Eintrag (DNS) hinzu.	(Optional) Sie können einen Amazon Route 53 53-DNS-Eintrag für die Subdomain hinzufügen. Dieser Datensatz würde auf Ihren Application Load Balancer verweisen. Anweisungen finden Sie in der Dokumentation zu Route 53	AWS-Administrator

Fehlerbehebung

Problem	Lösung
Der HTTP-Server wird nicht angezeigt.	Wenn der HTTP-Server nicht in der Zielnavig ationsliste der Enterprise Manager-Konsole erscheint, gehen Sie wie folgt vor: 1. Wählen Sie unter WebLogic Domain, Administration die Option OHS-Instances aus. 2. Wählen Sie Create, um eine neue OHS-Insta nz zu erstellen. 3. Geben Sie einen Instanznamen ein und wählen Sie dann OK, um die Instanz zu erstellen. Wenn die Instanz erstellt und die Änderungen aktiviert wurden, können Sie den HTTP-Server im Zielnavigationsbereich sehen.

Zugehörige Ressourcen

AWS-Dokumentation

- Application Load Balancer
- Arbeiten mit öffentlich gehosteten Zonen
- Arbeiten mit privaten Hosting-Zonen

Oracle-Dokumentation:

- Überblick über das Oracle WebLogic Server Proxy Plug-In
- WebLogic Server mit dem Infrastructure Installer installieren
- Installation und Konfiguration des Oracle HTTP-Servers

Stellen Sie über ein privates Netzwerk eine Connect zu Daten- und Steuerungsebenen des Application Migration Service her

Erstellt von Dipin Jain (AWS) und Mike Kuznetsov (AWS)

Übersicht

Dieses Muster erklärt, wie Sie mithilfe von VPC-Schnittstellen-Endpunkten eine Verbindung zu einer AWS Application Migration Service Daten- und Steuerungsebene in einem privaten, sicheren Netzwerk herstellen können.

Der Application Migration Service ist eine hochautomatisierte lift-and-shift (Rehost-) Lösung, die die Migration von Anwendungen nach vereinfacht, beschleunigt und die Kosten senkt. AWS Es ermöglicht Unternehmen, eine große Anzahl von physischen, virtuellen oder Cloud-Servern ohne Kompatibilitätsprobleme, Leistungsunterbrechungen oder lange Umstellungsfenster neu zu hosten. Der Anwendungsmigrationsdienst ist verfügbar unter. AWS Management Console Dies ermöglicht eine nahtlose Integration mit anderen AWS-Services Anbietern wie AWS CloudTrail Amazon CloudWatch und AWS Identity and Access Management (IAM).

Sie können über eine private Verbindung eine Verbindung von einem Quelldatencenter zu einer Datenebene herstellen, d. h. zu einem Subnetz, das als Staging-Bereich für die Datenreplikation in der Ziel-VPC dient AWS Direct Connect, indem Sie AWS VPN Dienste oder VPC-Peering im Application Migration Service verwenden. Sie können auch Schnittstellen-VPC-Endpunkte verwenden, AWS PrivateLink um über ein privates Netzwerk eine Verbindung zu einer Application Migration Service-Kontrollebene herzustellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Subnetz für den Staging-Bereich — Bevor Sie den Application Migration Service einrichten, erstellen Sie ein Subnetz, das als Staging-Bereich für Daten verwendet werden soll, auf die von Ihren Quellservern repliziert werden AWS (d. h. auf eine Datenebene). Sie müssen dieses Subnetz in der Vorlage für die Replikationseinstellungen angeben, wenn Sie zum ersten Mal auf die Application Migration Service-Konsole zugreifen. Sie können dieses Subnetz für bestimmte Quellserver in der Vorlage für Replikationseinstellungen überschreiben. Sie können zwar ein vorhandenes Subnetz in Ihrem verwenden AWS-Konto, wir empfehlen jedoch, zu diesem Zweck ein neues, dediziertes Subnetz zu erstellen.

- Netzwerkanforderungen — Die Replikationsserver, die vom Application Migration Service in Ihrem Staging-Bereich-Subnetz gestartet werden, müssen in der Lage sein, Daten an den API-Endpunkt des Application Migration Service zu sendenhttps://mgn.<region>.amazonaws.com/, auf den AWS-Region Sie replizieren (z. B.). <region> https://mgn.us-east-1.amazonaws.com Zum Herunterladen der Application Migration Service-Software ist der Amazon Simple Storage Service URLs (Amazon S3) -Service erforderlich.
  - Das AWS Replication Agent-Installationsprogramm sollte Zugriff auf die Amazon Simple Storage Service (Amazon S3) -Bucket-URL haben, die AWS-Region Sie mit dem Application Migration Service verwenden.
  - Das Staging-Area-Subnetz sollte Zugriff auf Amazon S3 haben.
  - Die Quellserver, auf denen der AWS Replication Agent installiert ist, müssen in der Lage sein, Daten an die Replikationsserver im Staging-Bereich-Subnetz und an den API-Endpunkt des Application Migration Service unter zu senden. https://mgn.<region>.amazonaws.com/

In der folgenden Tabelle sind die erforderlichen Ports aufgeführt.

Quelle	Zieladresse	Port	Weitere Informationen finden Sie unter
Quellrechenzentrum	Amazon S3 S3-Dienst URLs	443 (TCP)	Kommunikation über TCP-Port 443
Quellrechenzentrum	AWS-Region-spezifische Konsolenadresse für den Application Migration Service	443 (TCP)	Kommunikation zwischen den Quellservern und dem Application Migration Service über TCP-Port 443
Quellrechenzentrum	Subnetz für den Bereitstellungsbereich	1500 (TCP)	Kommunikation zwischen den Quellservern und dem Staging-Area-Subnetz über TCP-Port 1500
Subnetz des Staging-Bereichs	AWS-Region-spezifische Konsolena	443 (TCP)	Kommunikation zwischen dem

	dresse für den Application Migration Service		Staging-Area-Subnetz und dem Application Migration Service über TCP-Port 443
Subnetz des Staging-Bereichs	Amazon S3 S3-Dienst URLs	443 (TCP)	Kommunikation über TCP-Port 443
Subnetz des Staging-Bereichs	Amazon Elastic Compute Cloud (Amazon EC2) -Endpunkt des Subnetzes AWS-Region	443 (TCP)	Kommunikation über TCP-Port 443

-Einschränkungen

Der Anwendungsmigrationsdienst ist derzeit nicht in allen AWS-Regionen Betriebssystemen verfügbar.

- Wird unterstützt AWS-Regionen
- Unterstützte Betriebssysteme

Architektur

Das folgende Diagramm zeigt die Netzwerkarchitektur für eine typische Migration. Weitere Informationen zu dieser Architektur finden Sie in der Dokumentation zum Application Migration Service und im Video zur Architektur und Netzwerkarchitektur des Application Migration Service.

Die folgende detaillierte Ansicht zeigt die Konfiguration der Schnittstellen-VPC-Endpunkte im Staging-Bereich VPC zur Verbindung von Amazon S3 und Application Migration Service.

Tools

- AWS Application Migration Servicevereinfacht, beschleunigt und reduziert die Kosten für das Rehosten von Anwendungen auf. AWS

- Mit Schnittstellen-VPC-Endpunkten können Sie eine Verbindung zu Diensten herstellen, die von bereitgestellt werden, AWS PrivateLink ohne dass ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder AWS Direct Connect eine Verbindung erforderlich ist. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit den Ressourcen in dem Service zu kommunizieren. Der Datenverkehr zwischen Ihrer VPC und dem anderen Service verlässt das Amazon-Netzwerk nicht.

Epen

Endpunkte für Application Migration Service EC2, Amazon und Amazon S3 erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Schnittstellenendpunkt für den Application Migration Service.	Das Quellrechenzentrum und die Staging-Bereichs-VPC stellen über den Schnittst ellenendpunkt, den Sie in der Ziel-Staging-Bereichs-VPC erstellen, eine private Verbindung mit der Application Migration Service-Kontrolleb ene her. So erstellen Sie den Endpunkt: 1. Öffnen Sie die Amazon Virtual Private Cloud (Amazon VPC) -Konsole. 2. Wählen Sie im Navigatio nsbereich Endpoints und klicken Sie auf Create Endpoint. 3. Wählen Sie für Serviceka tegorie die Option AWS-Services aus. 4. Geben Sie `com.amazonaws.<region>.mgn`	Leiter der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	als Dienstname ein. Wählen Sie als Typ die Option Interface aus. 5. Wählen Sie für VPC eine Ziel-Staging-Bereichs-VPC aus, um den Endpunkt zu erstellen. 6. Wählen Sie für Subnetze die Subnetze aus, in denen die Endpunkt-Netzwerks chnittstellen erstellt werden sollen. 7. Um privates DNS für den Schnittstellenendpunkt zu aktivieren, wählen Sie im Abschnitt Zusätzliche Einstellungen die Option DNS-Name aktivieren aus. 8. Wählen Sie eine Sicherhei tsgruppe aus, die den Zugriff aus dem VPC-Subne tz des Staging-Bereichs über TCP 443 ermöglicht. 9. Wählen Sie Endpunkt erstellen aus. Weitere Informationen finden Sie unter Zugreifen und AWS-Service Verwenden eines VPC-Schnittstellen-Endpunkt s in der Amazon VPC-Dokum entation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Schnittstellenendpunkt für Amazon EC2.	Die Staging-Bereichs-VPC stellt über den Schnittstellenendpunkt, den Sie in der Ziel-Staging-Bereichs-VPC erstellen, eine private Verbindung zur EC2 Amazon-API her. Folgen Sie den Anweisungen in der vorherigen Geschichte, um den Endpunkt zu erstellen. • Geben Sie als Dienstnamen ein `com.amazonaws.<region>.ec2` . Wählen Sie für Typ die Option Interface aus. • Die Sicherheitsgruppe muss eingehenden HTTPS-Verkehr aus dem VPC-Subnetz des Staging-Bereichs über Port 443 zulassen. • Wählen Sie im Abschnitt Zusätzliche Einstellungen die Option DNS-Namen aktivieren aus.	Leiter der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Schnittstellenendpunkt für Amazon S3.	Das Quellrechenzentrum und die Staging-Bereichs-VPC stellen über den Schnittstellenendpunkt, den Sie in der Ziel-Staging-Bereichs-VPC erstellen, privat eine Verbindung zur Amazon S3 S3-API her. Folgen Sie den Anweisungen in der ersten Geschichte, um den Endpunkt zu erstellen. • Geben Sie als Dienstname ein `com.amazonaws.<region>.s3` . Wählen Sie als Typ die Option Interface aus. • Die VPC-Sicherheitsgruppe muss eingehenden HTTPS-Verkehr aus dem VPC-Subnetz des Staging-Bereichs über Port 443 zulassen. • Deaktivieren Sie im Abschnitt Zusätzliche Einstellungen die Option DNS-Namen aktivieren. Amazon S3 S3-Schnittstellenendpunkte unterstützen keine privaten DNS-Namen.	Leiter der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Sie verwenden einen Schnittstellenendpunkt, da Gateway-Endpunktverbindungen nicht von einer VPC aus erweitert werden können. (Einzelheiten finden Sie in der AWS PrivateLink Dokumentation.)	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Amazon S3 Gateway-Endpunkt.	Während der Konfigurationsphase muss der Replikationsserver eine Verbindung zu einem S3-Bucket herstellen, um die Softwareupdates des AWS Replication Servers herunterzuladen. Amazon S3 S3-Schnittstellenendpunkte unterstützen jedoch keine privaten DNS-Namen, und es gibt keine Möglichkeit, einem Replikationsserver einen Amazon S3 S3-Endpunkt-DNS-Namen zur Verfügung zu stellen. Um dieses Problem zu beheben, erstellen Sie einen Amazon S3 S3-Gateway-Endpunkt in der VPC, zu der das Staging-Bereichs-Subnetz gehört, und aktualisieren die Routing-Tabellen des Staging-Subnetzes mit den entsprechenden Routen. Weitere Informationen finden Sie in der Dokumentation unter Einen Gateway-Endpunkt erstellen. AWS PrivateLink	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie lokales DNS, um private DNS-Namen für Endgeräte aufzulösen.	Die Schnittstellenendpunkte für Application Migration Service und Amazon EC2 haben private DNS-Namen , die in der VPC aufgelöst werden können. Sie müssen jedoch auch lokale Server konfigurieren, um private DNS-Namen für diese Schnittstellenendpunkte aufzulösen. Es gibt mehrere Möglichke iten, diese Server zu konfiguri eren. In diesem Muster haben wir diese Funktiona lität getestet, indem wir lokale DNS-Abfragen an den Amazon Route 53 Resolver eingehenden Endpunkt im Staging-Bereich VPC weitergeleitet haben. Weitere Informationen finden Sie unter Auflösen von DNS-Abfragen zwischen VPCs und Ihrem Netzwerk in der Route 53-Dokumentation.	Ingenieur für Migration

Stellen Sie über eine private Connect eine Verbindung zur Kontrollebene des Application Migration Service her

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie AWS Replication Agent mithilfe von AWS PrivateLink.	1. Laden Sie den AWS Replication Agent in einen privaten S3-Bucket in der Zielregion herunter. 2. Melden Sie sich bei den Quellservern an, die migriert werden sollen. Das AWS Replication Agent-Installationsprogramm benötigt Netzwerkzugriff auf den Application Migration Service und die Amazon S3 S3-Endpoints. Da Ihr lokales Netzwerk nicht für Application Migration Service und öffentliche Amazon S3 S3-Endpunkte geöffnet ist, müssen Sie den Agenten mithilfe der Schnittstellenendpunkte installieren, die Sie in den vorherigen Schritten erstellt haben, indem Sie AWS PrivateLink Hier ist ein Beispiel für Linux: 1. Laden Sie den Agenten mit dem folgenden Befehl herunter:	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`wget -O ./aws-replication-installer-init.py \ https://aws-application-migration-service-<aws_region>.bucket.<s3-endpoint-DNS-name>/latest/linux/aws-replication-installer-init.py`
	
	Wenn der DNS-Name des Amazon S3 S3-Schnittstellenendpunkts beispielsweise lautet `vpce-009c8b07adb052a11-qgf8q50y.s3.us-west-1.vpce.amazonaws.com` und der AWS-Region ist `us-west-1`, würden Sie den folgenden Befehl verwenden:
	
	`wget -O ./aws-replication-installer-init.py \ https://aws-application-migration-service-us-west-1.bucket.vpce-009c8b07adb052a11-qgf8q50y.s3.us-west-1.vpce.amazonaws.com/latest/linux/aws-replication-installer-init.py`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note `bucket`ist ein statisches Schlüsselwort, das Sie vor dem DNS-Namen des Endpunkts der Amazon S3 S3-Schnittstelle hinzufügen müssen. Weitere Informationen finden Sie in der Amazon S3-Dokumentation. 2. Installieren Sie den Agenten: • Wenn Sie beim Erstellen eines Schnittstellenendpunkts für den Application Migration Service die Option DNS-Namen aktivieren ausgewählt haben, führen Sie den folgenden Befehl aus: `sudo python3 aws-replication-installer-init.py \ --region <aws_region> \ --aws-access-key-id <access-key> \`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>--aws-secret-access-key <secret-key> \
	--no-prompt \
	--s3-endpoint <s3-endpoint-DNS-name></pre>
	• Wenn Sie bei der Erstellung des Schnittstellenendpunkts für den Application Migration Service nicht die Option DNS-Namen aktivieren ausgewählt haben, führen Sie den folgenden Befehl aus:
	<pre>sudo python3 aws-replication-installer-init.py \
	--region <aws_region> \
	--aws-access-key-id <access-key> \
	--aws-secret-access-key <secret-key> \
	--no-prompt \
	--s3-endpoint <s3-endpoint-DNS-name> \
	--endpoint <mgn-endpoint-DNS-name></pre>
	Weitere Informationen finden Sie in den Installat	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ionsanweisungen für den AWS Replication Agent in der Dokumentation zum Application Migration Service. Nachdem Sie Ihre Verbindung mit Application Migration Service hergestellt und den AWS Replication Agent installiert haben, folgen Sie den Anweisungen in der Dokumentation zum Application Migration Service, um Ihre Quellserver auf Ihre Ziel-VPC und Ihr Zielsubnetz zu migrieren.	

Zugehörige Ressourcen

Dokumentation zum Anwendungsmigrationsdienst

- Konzepte
- Arbeitsablauf bei der Migration
- Schnellstart-Anleitung
- HÄUFIG GESTELLTE FRAGEN
- Fehlersuche

Weitere Ressourcen

- Rehosten Ihrer Anwendungen in einer Architektur mit mehreren Konten unter Verwendung AWS von VPC-Schnittstellenendpunkten (AWS Prescriptive Guidance Guide Guide)

- AWS Application Migration Service — Eine technische Einführung (Komplettlösung für Schulung und Zertifizierung)AWS
- AWS Application Migration Service Architektur und Netzwerkarchitektur (Video)

Zusätzliche Informationen

Problembehandlung bei AWS Replication Agent-Installationen auf Linux-Servern

Wenn Sie auf einem Amazon Linux-Server einen gcc-Fehler erhalten, konfigurieren Sie das Paket-Repository und verwenden Sie den folgenden Befehl:

```
## sudo yum groupinstall "Development Tools"
```

Erstellen Sie Infoblox-Objekte mithilfe von CloudFormation benutzerdefinierten AWS-Ressourcen und Amazon SNS

Erstellt von Tim Sutton (AWS)

Übersicht

Hinweis: AWS Cloud9 ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS Cloud9 können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Mit dem Infoblox Domain Name System (DNS), dem Dynamic Host Configuration Protocol (DHCP) und der IP-Adressverwaltung (Infoblox DDI) können Sie eine komplexe Hybridumgebung zentralisieren und effizient steuern. Mit Infoblox DDI können Sie alle Netzwerkressourcen in einer autoritativen IP-Adressverwaltungsdatenbank (IPAM) ermitteln und aufzeichnen. Darüber hinaus können Sie DNS vor Ort und in der Amazon Web Services (AWS) Cloud verwalten, indem Sie dieselben Appliances verwenden.

Dieses Muster beschreibt, wie eine CloudFormation benutzerdefinierte AWS-Ressource verwendet wird, um Infoblox-Objekte (z. B. DNS-Einträge oder IPAM-Objekte) zu erstellen, indem die Infoblox WAPI-API aufgerufen wird. Weitere Informationen zur Infoblox-WAPI finden Sie in der WAPI-Dokumentation in der Infoblox-Dokumentation.

Durch die Verwendung des Ansatzes dieses Musters erhalten Sie eine einheitliche Ansicht der DNS-Einträge und IPAM-Konfigurationen für Ihre AWS- und lokalen Umgebungen. Außerdem müssen Sie keine manuellen Prozesse mehr durchführen, die Datensätze erstellen und Ihre Netzwerke bereitstellen. Sie können den Ansatz dieses Musters für die folgenden Anwendungsfälle verwenden:

- Hinzufügen eines A-Eintrags nach dem Erstellen einer Amazon Elastic Compute Cloud (Amazon EC2) -Instanz
- Hinzufügen eines CNAME-Eintrags nach der Erstellung eines Application Load Balancer
- Hinzufügen eines Netzwerkobjekts nach dem Erstellen einer Virtual Private Cloud (VPC)
- Bereitstellung des nächsten Netzwerkbereichs und Verwendung dieses Bereichs zur Erstellung von Subnetzen

Sie können dieses Muster auch erweitern und andere Infoblox-Gerätefunktionen verwenden, z. B. das Hinzufügen verschiedener DNS-Eintragstypen oder die Konfiguration von Infoblox vDiscovery.

Das Muster verwendet ein hub-and-spoke Design, bei dem der Hub Konnektivität zur Infoblox-Appliance in der AWS-Cloud oder vor Ort benötigt und AWS Lambda verwendet, um die Infoblox-API aufzurufen. Der Spoke befindet sich in demselben oder einem anderen Konto in derselben Organisation in AWS Organizations und ruft die Lambda-Funktion mithilfe einer CloudFormation benutzerdefinierten AWS-Ressource auf.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine bestehende Infoblox-Appliance oder ein Infoblox-Grid, das in der AWS-Cloud, vor Ort oder in beiden installiert und mit einem Admin-Benutzer konfiguriert ist, der IPAM- und DNS-Aktionen verwalten kann. Weitere Informationen dazu finden Sie unter Über Administratorkonten in der Infoblox-Dokumentation.
- Eine bestehende autoritative DNS-Zone, der Sie Datensätze auf der Infoblox-Appliance hinzufügen möchten. Weitere Informationen dazu finden Sie unter Konfiguration autoritativer Zonen in der Infoblox-Dokumentation.
- Zwei aktive AWS-Konten in AWS Organizations. Ein Konto ist das Hub-Konto und das andere Konto ist das Spoke-Konto.
- Die Hub- und Spoke-Konten müssen sich in derselben AWS-Region befinden.
- Die VPC des Hub-Kontos muss eine Verbindung zur Infoblox-Appliance herstellen, beispielsweise mithilfe von AWS Transit Gateway oder VPC-Peering.
- AWS Serverless Application Model (AWS SAM), lokal installiert und konfiguriert mit AWS Cloud9 oder AWS. CloudShell
- Die `ClientTest.yaml` Dateien `Infoblox-Hub.zip` und (angehängt), die in die lokale Umgebung heruntergeladen wurden, die AWS SAM enthält.

Einschränkungen

- Das Service-Token der CloudFormation benutzerdefinierten AWS-Ressource muss aus derselben Region stammen, in der der Stack erstellt wurde. Wir empfehlen, dass Sie in jeder Region ein Hub-Konto verwenden, anstatt in einer Region ein Amazon Simple Notification Service (Amazon SNS) -Thema zu erstellen und die Lambda-Funktion in einer anderen Region aufzurufen.

Produktversionen

- Infoblox WAPI-Version 2.7

Architektur

Die folgenden Diagramme zeigen den Arbeitsablauf dieses Musters.

Das Diagramm zeigt die folgenden Komponenten für die Lösung dieses Musters:

1. Mit CloudFormation benutzerdefinierten AWS-Ressourcen können Sie benutzerdefinierte Bereitstellungslogik in Vorlagen schreiben, die AWS CloudFormation ausführt, wenn Sie Stacks erstellen, aktualisieren oder löschen. Wenn Sie einen Stack erstellen, CloudFormation sendet AWS eine `create` Anfrage an ein SNS-Thema, das von einer Anwendung überwacht wird, die auf einer EC2 Instance ausgeführt wird.
2. Die Amazon SNS SNS-Benachrichtigung von der CloudFormation benutzerdefinierten AWS-Ressource wird mit einem bestimmten AWS Key Management Service (AWS KMS) -Schlüssel verschlüsselt, und der Zugriff ist auf Konten in Ihrer Organisation in Organizations beschränkt. Das SNS-Thema initiiert die Lambda-Ressource, die die Infoblox WAPI-API aufruft.
3. Amazon SNS ruft die folgenden Lambda-Funktionen auf, die die Infoblox-WAPI-URL, den Benutzernamen und das Passwort AWS Secrets Manager Amazon Resource Names () als Umgebungsvariablen verwenden: ARNs
   - `dnsapi.lambda_handler`— Empfängt die `DNSName` `DNSType` ,- und `DNSValue` -Werte von der CloudFormation benutzerdefinierten AWS-Ressource und verwendet diese, um DNS-A-Einträge und CNAMES zu erstellen.
   - `ipaddr.lambda_handler`— Empfängt die`VPCCIDR`, `TypeSubnetPrefix`, und `Network Name` Werte von der CloudFormation benutzerdefinierten AWS-Ressource und verwendet diese, um die Netzwerkdaten zur Infoblox IPAM-Datenbank hinzuzufügen oder die benutzerdefinierte Ressource mit dem nächsten verfügbaren Netzwerk bereitzustellen, das zum Erstellen neuer Subnetze verwendet werden kann.
   - `describeprefixes.lambda_handler`— Ruft die `describe_managed_prefix_lists` AWS-API auf, indem der `"com.amazonaws."+Region+".s3"` Filter verwendet wird, um die erforderlichen Daten abzurufen`prefix ID`.

> **Important**
>
> Diese Lambda-Funktionen sind in Python geschrieben und ähneln sich, rufen aber unterschiedlich APIs auf.

4. Sie können das Infoblox-Grid als physische, virtuelle oder cloudbasierte Netzwerk-Appliances bereitstellen. Es kann vor Ort oder als virtuelle Appliance mithilfe einer Reihe von Hypervisoren bereitgestellt werden, darunter Microsoft Hyper-V VMware ESXi, Linux KVM und Xen. Sie können das Infoblox-Grid auch mit einem Amazon Machine Image (AMI) in der AWS-Cloud bereitstellen.
5. Das Diagramm zeigt eine Hybridlösung für das Infoblox-Grid, die DNS und IPAM für Ressourcen in der AWS-Cloud und vor Ort bereitstellt.

Technologie-Stack

- AWS CloudFormation
- IAM
- AWS KMS
- AWS Lambda
- AWS SAM
- AWS Secrets Manager
- Amazon SNS
- Amazon VPC

Tools

- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Key Management Service (AWS KMS) unterstützt Sie bei der Erstellung und Kontrolle kryptografischer Schlüssel, um Ihre Daten zu schützen.

- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten.
- AWS Secrets Manager hilft Ihnen dabei, hartcodierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Geheimnis programmgesteuert abzurufen.
- Das AWS Serverless Application Model (AWS SAM) ist ein Open-Source-Framework, mit dem Sie serverlose Anwendungen in der AWS-Cloud erstellen können.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.

Code

Sie können die `ClientTest.yaml` CloudFormation AWS-Beispielvorlage (beigefügt) verwenden, um den Infoblox-Hub zu testen. Sie können die CloudFormation AWS-Vorlage so anpassen, dass sie die benutzerdefinierten Ressourcen aus der folgenden Tabelle enthält.

Erstellen Sie einen A-Datensatz mithilfe der benutzerdefinierten Infoblox-Spoke-Ressource	Rückgabewerte:
	`infobloxref` — Infoblox-Referenzen
	Beispielressource:
	`ARECORDCustomResource:`
	`  Type: "Custom::InfobloxAPI"`
	`  Properties:`

```
    ServiceToken: !Sub  arn:aws:sns:
${AWS::Region}:${HubAccountID}:Ru
nInfobloxDNSFunction

    DNSName: 'arecordtest.compa
ny.com'

    DNSType: 'ARecord'

    DNSValue: '10.0.0.1'
```

Erstellen Sie einen CNAME-Eintrag mit der benutzerdefinierten Infoblox Spoke-Ressource

Rückgabewerte:

`infobloxref` — Infoblox-Referenzen

Beispielressource:

```
CNAMECustomResource:

  Type: "Custom::InfobloxAPI"

  Properties:

    ServiceToken: !Sub arn:aws:sns:
${AWS::Region}:${HubAccountID}:Ru
nInfoblox

    DNSFunction

    DNSName: 'cnametest.company.com'

    DNSType: 'cname'

    DNSValue: 'aws.amazon.com'
```

Erstellen Sie ein Netzwerkobjekt mithilfe der benutzerdefinierten Infoblox Spoke-Ressource	Rückgabewerte:
	`infobloxref` — Infoblox-Referenzen
	`network`— Netzwerkreichweite (dieselbe wie) `VPCCIDR`
	Beispielressource:
	`VPCCustomResource:`
	`  Type: 'Custom::InfobloxAPI'`
	`  Properties:`
	`  ServiceToken: !Sub  arn:aws:sns:${AWS::Region}:${HubAccountID}:RunInfobloxNextSubnetFunction`
	`  VPCCIDR: !Ref VpcCIDR`
	`  Type: VPC`
	`  NetworkName: My-VPC`

Rufen Sie das nächste verfügbare Subnetz mithilfe der benutzerdefinierten Infoblox-Spoke-Ressource ab	Rückgabewerte:
	`infobloxref` — Infoblox-Referenzen
	`network` — Die Netzwerkreichweite des Subnetzes
	Beispielressource:
	`Subnet1CustomResource:`
	`  Type: 'Custom::InfobloxAPI'`
	`  DependsOn: VPCCustomResource`
	`  Properties:`
	`  ServiceToken: !Sub arn:aws:sns:${AWS::Region}:${HubAccountID}:RunInfobloxNextSubnetFunction`
	`  VPCCIDR: !Ref VpcCIDR`
	`  Type: Subnet`
	`  SubnetPrefix: !Ref SubnetPrefix`
	`NetworkName: My-Subnet`

Epen

Erstellen und konfigurieren Sie die VPC des Hub-Kontos

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC mit einer Verbindung zur Infoblox-Appliance.	Melden Sie sich bei der AWS-Managementkonsole für Ihr Hub-Konto an und erstellen Sie eine VPC, indem Sie den Schritten in der Referenzb	Netzwerkadministrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ereitstellung Amazon VPC on the AWS Cloud Quick Start von AWS Quick Starts folgen. **Important** Die VPC muss über eine HTTPS-Kon nektivität zur Infoblox-Appliance verfügen. Wir empfehlen, für diese Verbindung ein privates Subnetz zu verwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Erstellen Sie die VPC-Endpoints für private Subnetze.	VPC-Endpunkte bieten Konnektivität zu öffentlichen Diensten für Ihre privaten Subnetze. Die folgenden Endpunkte sind erforderlich: • Ein Gateway-Endpunkt für Amazon Simple Storage Service (Amazon S3), der es Lambda ermöglicht, mit AWS zu kommunizieren CloudFormation • Ein Schnittstellenendpunkt für Secrets Manager zur Aktivierung der Konnektivität mit Secrets Manager • Ein Schnittstellenendp unkt für AWS KMS, der die Verschlüsselung des SNS-Themas und des Secrets Manager Manager-Geheimnisses ermöglicht Weitere Informationen zum Erstellen von Endpunkten für private Subnetze finden Sie unter VPC-Endpunkte in der Amazon VPC-Dokumentation.	Netzwerkadministrator, Systemadministrator

Stellen Sie den Infoblox-Hub bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die AWS-SAM-Vorlage.	1. Führen Sie den `unzip Infoblox-Hub.zip` Befehl in der Umgebung aus, die AWS SAM enthält. 2. Führen Sie den `cd Hub/` Befehl aus, um Ihr Verzeichnis in das Hub Verzeichnis zu ändern. 3. Führen Sie den `sam build` Befehl aus, um die AWS-SAM-Vorlagendatei, den Anwendungscode und alle sprachspezifischen Dateien und Abhängigkeiten zu verarbeiten. Der `sam build` Befehl kopiert auch Build-Artefakte in dem Format und an dem Speicherort, die für die folgende Geschichte erwartet werden.	Entwickler, Systemadministrator
Stellen Sie die AWS-SAM-Vorlage bereit.	Der `sam deploy` Befehl verwendet die erforderlichen Parameter und speichert sie in der `samconfig.toml` Datei, speichert die CloudFormation AWS-Vorlage und die Lambda-Funktionen in einem S3-Bucket und stellt dann die CloudFormation AWS-Vorlage in Ihrem Hub-Konto bereit.	Entwickler, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Der folgende Beispielcode zeigt, wie die AWS-SAM-V orlage bereitgestellt wird:
	
	`$ sam deploy --guided`
	
	`Configuring SAM deploy`
	`==========`
	`==`
	`Looking for config file [samconfig.toml] : Found`
	`Reading default arguments : Success`
	`Setting default arguments for 'sam deploy'`
	`==========`
	`==========`
	`Stack Name [Infoblox-Hub]:`
	`AWS Region [eu-west-1]:`
	`Parameter InfobloxUsername:`
	`Parameter InfobloxPassword:`
	`Parameter InfobloxIPAddress [xxx.xxx.xx.xxx]:`
	`Parameter AWSOrganisationID [o-xxxxxxxxx]:`
	`Parameter VPCID [vpc-xxxxxxxxx]:`
	`Parameter VPCCIDR [xxx.xxx.xxx.xxx/16]:`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>Parameter VPCSubnetID1 [subnet-xxx]:
	Parameter VPCSubnetID2 [subnet-xxx]:
	Parameter VPCSubnetID3 [subnet-xxx]:
	Parameter VPCSubnetID4 []:
	#Shows you resources changes to be deployed and require a 'Y' to initiate deploy
	Confirm changes before deploy [Y/n]: y
	#SAM needs permission to be able to create roles to connect to the resources in your template
	Allow SAM CLI IAM role creation [Y/n]: n
	Capabilities [['CAPABILITY_NAMED_IAM']]:
	Save arguments to configuration file [Y/n]: y
	SAM configuration file [samconfig.toml]:
	SAM configuration environment [default]:</pre>
	⚠ Important
	Sie müssen die `--guided` Option jedes	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Mal verwenden, da die Infoblox-Anmeldein formationen nicht in der Datei gespeiche rt sind. `samconfig .toml`	

Zugehörige Ressourcen

- Erste Schritte mit der WAPIs Verwendung von Postman (Infoblox Blog)
- Bereitstellung von VNIOs für AWS mithilfe des BYOL-Modells (Infoblox-Dokumentation)
- quickstart-aws-vpc(GitHub Repo)
- describe_managed_prefix_lists (Dokumentation zum AWS-SDK für Python)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Passen Sie CloudWatch Amazon-Benachrichtigungen an für AWS Network Firewall

Erstellt von Jason Owens (AWS)

Übersicht

Das Muster hilft Ihnen dabei, die CloudWatch Amazon-Benachrichtigungen anzupassen, die von generiert werden AWS Network Firewall. Sie können vordefinierte Regeln verwenden oder benutzerdefinierte Regeln erstellen, die die Nachricht, die Metadaten und den Schweregrad der Benachrichtigungen bestimmen. Sie können dann auf diese Benachrichtigungen reagieren oder die Antworten anderer Amazon-Dienste wie Amazon automatisieren EventBridge.

In diesem Muster generieren Sie Suricata-kompatible Firewall-Regeln. Suricata ist eine Open-Source-Engine zur Erkennung von Bedrohungen. Sie erstellen zunächst einfache Regeln und testen sie dann, um sicherzustellen, dass die CloudWatch Warnungen generiert und protokolliert wurden. Nachdem Sie die Regeln erfolgreich getestet haben, ändern Sie sie, um benutzerdefinierte Meldungen, Metadaten und Schweregrade zu definieren. Anschließend testen Sie erneut, um die Aktualisierungen zu bestätigen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto.
- AWS Command Line Interface (AWS CLI) auf Ihrer Linux-, macOS- oder Windows-Workstation installiert und konfiguriert. Weitere Informationen finden Sie unter Installieren oder Aktualisierung auf die neueste Version von AWS CLI.
- AWS Network Firewall für die Verwendung von CloudWatch Logs installiert und konfiguriert. Weitere Informationen finden Sie unter Protokollieren des Netzwerkverkehrs von AWS Network Firewall.
- Eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance in einem privaten Subnetz einer Virtual Private Cloud (VPC), die durch eine Network Firewall geschützt ist.

Produktversionen

- Verwenden Sie für Version 1 von AWS CLI 1.18.180 oder höher. Verwenden Sie für Version 2 von AWS CLI 2.1.2 oder höher.

- Die Datei classification.config aus Suricata Version 5.0.2. Eine Kopie dieser Konfigurationsdatei finden Sie im Abschnitt Zusätzliche Informationen.

Architektur

Das Architekturdiagramm zeigt den folgenden Arbeitsablauf:

1. Eine EC2 Amazon-Instance in einem privaten Subnetz stellt eine Anfrage entweder mit curl oder Wget.
2. Die Network Firewall verarbeitet den Datenverkehr und generiert eine Warnung.
3. Die Network Firewall sendet die protokollierten Warnungen an CloudWatch Logs.

Tools

AWS-Services

- Amazon CloudWatch hilft Ihnen dabei, die Kennzahlen Ihrer AWS Ressourcen und der Anwendungen, auf denen Sie laufen, AWS in Echtzeit zu überwachen.
- Amazon CloudWatch Logs hilft Ihnen dabei, die Protokolle all Ihrer Systeme und Anwendungen zu zentralisieren, AWS-Services sodass Sie sie überwachen und sicher archivieren können.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie AWS-Services über Befehle in Ihrer Befehlszeilen-Shell interagieren können.
- AWS Network Firewallist ein zustandsorientierter, verwalteter Dienst zur Netzwerk-Firewall sowie zur Erkennung und Verhinderung von Eindringlingen für virtuelle private Clouds () in der. VPCs AWS Cloud

Andere Tools

- curl ist ein Open-Source-Befehlszeilentool und eine Bibliothek.
- GNU Wget ist ein kostenloses Befehlszeilentool.

Epen

Erstellen Sie die Firewallregeln und die Regelgruppe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen von Regeln.	1. Erstellen Sie in einem Texteditor eine Liste von Regeln, die Sie der Firewall hinzufügen möchten. Jede Regel muss sich in einer separaten Zeile befinden. Der Wert im `classtype` Parameter stammt aus der standardmäßigen Konfigurationsdatei für die Suricata-Klassifikation. Den vollständigen Inhalt der Konfigurationsdatei finden Sie im Abschnitt Zusätzliche Informationen. Im Folgenden finden Sie zwei Beispiele für Regeln.
	`alert http any any -> any any (content:"badstuff"; classtype:misc-activity; sid:3; rev:1;)`
	`alert http any any -> any any (content:"morebadstuff"; classtype:bad-unknown; sid:4; rev:1;)`
	2. Speichern Sie die Regeln in einer Datei mit dem Namen `custom.rules` .
		AWS-Systemadministrator, Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Regelgruppe.	Geben Sie im AWS CLI den folgenden Befehl ein. Dadurch wird die Regelgruppe erstellt.
	
	`# aws network-firewall create-rule-group \ --rule-group-name custom --type STATEFUL \ --capacity 10 --rules file://custom.rules \ --tags Key=environment,Value=development`
	
	Im Folgenden finden Sie eine Beispielausgabe. Notieren Sie sich die`RuleGroupArn` , die Sie in einem späteren Schritt benötigen.
	
	`{ "UpdateToken": "4f998d72-973c-490a-bed2-fc3460547e23", "RuleGroupResponse": { "RuleGroupArn": "arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom", "RuleGroupName": "custom", "RuleGroupId": "238a8259-9eaf-48bb-90af-5e690cf8c48b",`
		AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"Type": "STATEFUL", "Capacity": 10, "RuleGroupStatus": "ACTIVE", "Tags": [{ "Key": "environment", "Value": "development" }] }	

Aktualisieren Sie die Firewall-Richtlinie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie den ARN der Firewall-Richtlinie ab.	Geben Sie im AWS CLI den folgenden Befehl ein. Dadurch wird der Amazon-Ressourcenname (ARN) der Firewall-Richtlinie zurückgegeben. Notieren Sie den ARN für die spätere Verwendung in diesem Muster. `# aws network-firewall describe-firewall \ --firewall-name aws-network-firewall-anfw \ --query 'Firewall.FirewallPolicyArn'`	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Im Folgenden finden Sie ein Beispiel für einen ARN, der von diesem Befehl zurückgeg eben wird. `"arn:aws:network-firewall:us-east-2:1234567890:firewall-policy/firewall-policy-anfw"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Firewall-Richtlinie.	Kopieren Sie in einem Texteditor den folgenden Code und fügen Sie ihn ein. Ersetze ihn `<RuleGroupArn>` durch den Wert, den du im vorherigen Epos aufgezeichnet hast. Speichern Sie die Datei als `firewall-policy-anfw.json` . `{ "StatelessDefaultActions": [ "aws:forward_to_sfe" ], "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ], "StatefulRuleGroupReferences": [ { "ResourceArn": "<RuleGroupArn>" } ] }` Geben Sie den folgenden Befehl in die ein AWS CLI. Für diesen Befehl ist ein Aktualisierungstoken erforderlich, um die neuen Regeln hinzuzufügen. Das Token wird verwendet, um zu bestätige	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	n, dass sich die Richtlinie seit dem letzten Abruf nicht geändert hat.
	
	`UPDATETOKEN=(`aws network-firewall describe-firewall-policy \ --firewall-policy-name firewall-policy-anfw \ --output text --query UpdateToken`)`
	
	`aws network-firewall update-firewall-policy \ --update-token $UPDATETOKEN \ --firewall-policy-name firewall-policy-anfw \ --firewall-policy file://firewall-policy-anfw.json`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bestätigen Sie die Richtlini enaktualisierungen.	(Optional) Wenn Sie überprüfe n möchten, ob die Regeln hinzugefügt wurden, und das Richtlinienformat anzeigen möchten, geben Sie den folgenden Befehl in die Datei ein AWS CLI.
	`# aws network-firewall describe-firewall-policy \ --firewall-policy-name firewall-policy-anfw \ --query FirewallPolicy`
	Im Folgenden finden Sie eine Beispielausgabe.
	`{ "StatelessDefaultActions": [ "aws:forward_to_sfe" ], "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ], "StatefulRuleGroupReferences": [ { "ResourceArn": "arn:aws:network-firewall:us-east-2:123456789`
		AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>0:stateful-rulegroup/
	custom"
	        }
	    ]
	}</pre>	

Testen Sie die Alarmfunktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Generieren Sie Benachric htigungen zum Testen.	1. Melden Sie sich bei einer Test-Workstation im Firewall-Subnetz an.
	2. Geben Sie Befehle ein, die Warnmeldungen generiere n sollen. Sie können beispielsweise `wget` oder verwenden`curl`.
	<pre>wget -U "badstuff"
	 http://www.amazon.
	com -o /dev/null</pre>
	<pre>curl -A "morebads
	tuff" http://ww
	w.amazon.com -o /
	dev/null</pre>
		AWS-Systemadministrator

Stellen Sie sicher, dass die Warnungen protokolliert wurden.	1. Öffnen Sie die CloudWatch -Konsole. 2. Navigieren Sie zur richtigen Protokollgruppe und zum richtigen Stream. Weitere Informationen finden Sie unter An Logs gesendete	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Protokolldaten anzeigen (CloudWatch CloudWatch Logs-Dokumentation).
	3. Vergewissern Sie sich, dass die protokollierten Ereignisse den folgenden Beispielen ähneln. Die Beispiele zeigen nur den relevanten Teil der Warnung.
	
	Beispiel 1
	
	`"alert": { "action": "allowed", "signature_id": 3, "rev": 1, "signature": "", "category": "Misc activity", "severity": 3 }`
	
	Beispiel 2
	
	`"alert": { "action": "allowed", "signature_id": 4, "rev": 1, "signature": "", "category": "Potentially Bad Traffic",`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"severity ": 2 } </pre>	

Aktualisieren Sie die Firewall-Regeln und die Regelgruppe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Firewall-Regeln.	1. Öffnen Sie die Datei `custom.rules` in einem Texteditor. 2. Ändern Sie die erste Regel so, dass sie der folgenden ähnelt. Diese Regel muss in einer einzigen Zeile in der Datei eingegeben werden. <pre>alert http any any -> any any (msg:"Watch out - Bad Stuff!!"; content:"badstuff" ; classtype:misc-activity; priority: 2; sid:3; rev:2; metadata:custom-field-2 Danger!, custom-field More Info;)</pre> Dadurch werden die folgenden Änderungen an der Regel vorgenommen: • Fügt eine Zeichenfolge vom Typ msg (Suricata -Website) hinzu, die Textinformationen zur	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Signatur oder Warnung enthält. In der generierten Warnung wird dies der Signatur zugeordnet. • Passt die Standardpriorität (Suricata-Website) `misc-activity` von 3 auf 2 an. Die Standardwerte der verschiedenen Optionen finden Sie im `classtypes` Abschnitt Zusätzliche Informationen. • Fügt der Warnung benutzerdefinierte Metadaten (Suricata-Website) hinzu. Dies sind zusätzliche Informationen, die der Signatur hinzugefügt werden. Es wird empfohlen, Schlüssel-Wert-Paare zu verwenden. • Ändert die Version (Suricata-Website) von 1 auf 2. Dies stellt die Version der Signatur dar.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Regelgruppe.	Führen Sie in der AWS CLI die folgenden Befehle aus. Verwenden Sie den ARN Ihrer Firewall-Richtlinie. Diese Befehle rufen ein Aktualisierungstoken ab und aktualisieren die Regelgruppe mit den Regeländerungen. `# UPDATETOKEN=(`aws network-firewall \ describe-rule-group \ --rule-group-arn arn:aws:network-firewall:us-east-2:123457890:stateful-rulegroup/custom \ --output text --query UpdateToken`)` `# aws network-firewall update-rule-group \ --rule-group-arn arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom \ --rules file://custom.rules \ --update-token $UPDATETOKEN` Im Folgenden finden Sie eine Beispielausgabe. `{`	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"UpdateToken": "7536939f-6a1d-414c-96d1-bb28110996ed", "RuleGroupResponse": { "RuleGroupArn": "arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom", "RuleGroupName": "custom", "RuleGroupId": "238a8259-9eaf-48bb-90af-5e690cf8c48b", "Type": "STATEFUL", "Capacity": 10, "RuleGroupStatus": "ACTIVE", "Tags": [{ "Key": "environment", "Value": "development" }] } }	

Testen Sie die aktualisierte Warnfunktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie eine Warnung zum Testen.	1. Melden Sie sich bei einer Test-Workstation im Firewall-Subnetz an.	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Geben Sie einen Befehl ein, der eine Warnung auslösen soll. Sie können beispielsweise die Datei `curl` verwenden. `curl -A "badstuff" http://www.amazon.com -o /dev/null`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie, dass die Warnung geändert wurde.	1. Öffnen Sie die CloudWatch -Konsole. 2. Navigieren Sie zur richtigen Protokollgruppe und zum richtigen Stream. 3. Vergewissern Sie sich, dass das protokollierte Ereignis dem folgenden Beispiel ähnelt. Das Beispiel zeigt nur den relevanten Teil der Warnung. `"alert": { "action": "allowed", "signature_id": 3, "rev": 2, "signature": "Watch out - Bad Stuff!!", "category": "Misc activity", "severity": 2, "metadata": { "custom-field": [ "More Info" ], "custom-field-2": [ "Danger!" ] } }`	AWS-Systemadministrator

Zugehörige Ressourcen

Referenzen

- Senden Sie Benachrichtigungen von AWS Network Firewall an einen Slack-Channel (AWS Prescriptive Guidance)
- Skalierung der Bedrohungsabwehr AWS mit Suricata (Blogbeitrag)AWS
- Bereitstellungsmodelle für AWS Network Firewall (AWS Blogbeitrag)
- Suricata-Meta-Schlüsselwerke (Suricata-Dokumentation)

Anleitungen und Videos

- AWS Network Firewall Werkstatt

Zusätzliche Informationen

Im Folgenden finden Sie die Konfigurationsdatei für die Klassifizierung von Suricata 5.0.2. Diese Klassifizierungen werden bei der Erstellung der Firewallregeln verwendet.

```
# config classification:shortname,short description,priority

config classification: not-suspicious,Not Suspicious Traffic,3
config classification: unknown,Unknown Traffic,3
config classification: bad-unknown,Potentially Bad Traffic, 2
config classification: attempted-recon,Attempted Information Leak,2
config classification: successful-recon-limited,Information Leak,2
config classification: successful-recon-largescale,Large Scale Information Leak,2
config classification: attempted-dos,Attempted Denial of Service,2
config classification: successful-dos,Denial of Service,2
config classification: attempted-user,Attempted User Privilege Gain,1
config classification: unsuccessful-user,Unsuccessful User Privilege Gain,1
config classification: successful-user,Successful User Privilege Gain,1
config classification: attempted-admin,Attempted Administrator Privilege Gain,1
config classification: successful-admin,Successful Administrator Privilege Gain,1

# NEW CLASSIFICATIONS
config classification: rpc-portmap-decode,Decode of an RPC Query,2
config classification: shellcode-detect,Executable code was detected,1
config classification: string-detect,A suspicious string was detected,3
config classification: suspicious-filename-detect,A suspicious filename was detected,2
```

```
config classification: suspicious-login,An attempted login using a suspicious username
 was detected,2
config classification: system-call-detect,A system call was detected,2
config classification: tcp-connection,A TCP connection was detected,4
config classification: trojan-activity,A Network Trojan was detected, 1
config classification: unusual-client-port-connection,A client was using an unusual
 port,2
config classification: network-scan,Detection of a Network Scan,3
config classification: denial-of-service,Detection of a Denial of Service Attack,2
config classification: non-standard-protocol,Detection of a non-standard protocol or
 event,2
config classification: protocol-command-decode,Generic Protocol Command Decode,3
config classification: web-application-activity,access to a potentially vulnerable web
 application,2
config classification: web-application-attack,Web Application Attack,1
config classification: misc-activity,Misc activity,3
config classification: misc-attack,Misc Attack,2
config classification: icmp-event,Generic ICMP event,3
config classification: inappropriate-content,Inappropriate Content was Detected,1
config classification: policy-violation,Potential Corporate Privacy Violation,1
config classification: default-login-attempt,Attempt to login by a default username and
 password,2

# Update
config classification: targeted-activity,Targeted Malicious Activity was Detected,1
config classification: exploit-kit,Exploit Kit Activity Detected,1
config classification: external-ip-check,Device Retrieving External IP Address
 Detected,2
config classification: domain-c2,Domain Observed Used for C2 Detected,1
config classification: pup-activity,Possibly Unwanted Program Detected,2
config classification: credential-theft,Successful Credential Theft Detected,1
config classification: social-engineering,Possible Social Engineering Attempted,2
config classification: coin-mining,Crypto Currency Mining Activity Detected,2
config classification: command-and-control,Malware Command and Control Activity
 Detected,1
```

Bereitstellen von Ressourcen in einer AWS Wavelength Zone mithilfe von Terraform

Erstellt von Zahoor Chaudhrey (AWS) und Luca Iannario (AWS)

Übersicht

AWS Wavelengthhilft Ihnen beim Aufbau einer Infrastruktur, die für Multi-Access Edge Computing (MEC) -Anwendungen optimiert ist. Wellenlängenzonen sind AWS Infrastrukturbereitstellungen, die AWS Rechen- und Speicherdienste in die 5G-Netzwerke von Kommunikationsdienstanbietern (CSP) einbetten. Der Anwendungsverkehr von 5G-Geräten erreicht Anwendungsserver, die in Wellenlängenzonen laufen, ohne das Telekommunikationsnetz zu verlassen. Folgendes erleichtert die Netzwerkkonnektivität über Wavelength:

- Virtuelle private Clouds (VPCs) — AWS-Konto können VPCs sich über mehrere Availability Zones erstrecken, einschließlich Wellenlängenzonen. Amazon Elastic Compute Cloud (Amazon EC2) -Instances und zugehörige Services werden als Teil Ihrer regionalen VPC angezeigt. VPCs werden in Amazon Virtual Private Cloud (Amazon VPC) erstellt und verwaltet.
- Carrier-Gateway — Ein Carrier-Gateway ermöglicht die Konnektivität vom Subnetz in der Wellenlängenzone zum CSP-Netzwerk, zum Internet oder AWS-Region über das Netzwerk des CSP. Das Carrier-Gateway dient zwei Zwecken. Es ermöglicht eingehenden Verkehr von einem CSP-Netzwerk an einem bestimmten Standort und ausgehenden Verkehr zum Telekommunikationsnetz und zum Internet.

Dieses Muster und der zugehörige Terraform-Code helfen Ihnen dabei, Ressourcen wie EC2 Amazon-Instances, Amazon Elastic Block Store (Amazon EBS) -Volumes VPCs, Subnetze und ein Carrier-Gateway in einer Wellenlängenzone zu starten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Eine integrierte Entwicklungsumgebung (IDE)
- Wählen Sie die Ziel-Wellenlängenzone aus
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert
- Terraform Version 1.8.4 oder höher, installiert (Terraform-Dokumentation)

- Terraform AWS Provider Version 5.32.1 oder höher, konfiguriert (Terraform-Dokumentation)
- Git, installiert (GitHub)
- Berechtigungen zum Erstellen von Amazon VPC-, Wavelength- und Amazon-Ressourcen EC2

Einschränkungen

Nicht alle AWS-Regionen unterstützen Wellenlängenzonen. Weitere Informationen finden Sie unter Verfügbare Wellenlängenzonen in der Wellenlängen-Dokumentation.

Architektur

Das folgende Diagramm zeigt, wie Sie ein Subnetz und AWS Ressourcen in einer Wellenlängenzone erstellen können. VPCs die ein Subnetz in einer Wellenlängenzone enthalten, können eine Verbindung zu einem Carrier-Gateway herstellen. Mit einem Carrier-Gateway können Sie eine Verbindung zu den folgenden Ressourcen herstellen:

- 4G/LTE- und 5G-Geräte im Netzwerk des Telekommunikationsanbieters.
- Fester drahtloser Zugang für ausgewählte Wavelength Zone-Partner. Weitere Informationen finden Sie unter Multi-Access AWS Wavelength.
- Ausgehender Verkehr zu öffentlichen Internetressourcen.

Tools

AWS-Services

- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk bereitzustellen. Dieses virtuelle Netzwerk entspricht einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben würden, mit den Vorteilen der Verwendung der skalierbaren Infrastruktur von AWS.
- AWS Wavelengtherweitert die AWS Cloud Infrastruktur auf die 5G-Netzwerke von Telekommunikationsanbietern. Auf diese Weise können Sie Anwendungen entwickeln, die Mobilgeräten und Endbenutzern extrem niedrige Latenzen bieten.

Andere Tools

- Terraform ist ein IaC-Tool (Infrastructure as Code) HashiCorp , mit dem Sie Cloud- und lokale Ressourcen erstellen und verwalten können.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub Creating AWS Wavelength Infrastructure using Terraform verfügbar. Der Terraform-Code stellt die folgende Infrastruktur und Ressourcen bereit:

- Eine VPC
- Eine Wellenlängenzone
- Ein öffentliches Subnetz in der Wellenlängenzone
- Ein Carrier-Gateway in der Wellenlängenzone
- Eine EC2 Amazon-Instance in der Wavelength Zone

Bewährte Methoden

- Vergewissern Sie sich vor der Bereitstellung, dass Sie die neuesten Versionen von Terraform und dem verwenden. AWS CLI
- Verwenden Sie eine CI/CD-Pipeline (Continuous Integration and Continuous Delivery), um IaC bereitzustellen. Weitere Informationen finden Sie in Blogs unter Bewährte Methoden für die Verwaltung von Terraform State-Dateien in AWS der CI/CD-Pipeline. AWS

Epen

Stellen Sie die Infrastruktur bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Geben Sie den folgenden Befehl ein, um das Repository Creating AWS Wavelength Infrastructure using Terraform in Ihre Umgebung zu klonen. `git clone git@github.com:aws-samples/`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`terraform-wavelength-infrastructure.git`	
Aktualisieren Sie die Variablen.	1. Navigieren Sie zum geklonten Repository. `cd terraform-wavelength-infrastructure` 2. Erstellen Sie mit einem beliebigen Texteditor eine Datei namens terraform.tfvars im Stammverzeichnis. 3. Erstellen Sie die folgenden Variablen und geben Sie ihre Werte ein: • `region = <enter Region name>` • `vpc_cidr = <enter CIDR block used by VPC>` • `wavelength_subnet_cidr = <enter CIDR block for the subnet in the Wavelength Zone>` • `availabilityzone_wavelength = <enter Wavelength Zone name>` 4. Speichern Sie die Datei terraform.tfvars.	DevOps Ingenieur, Terraform

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initialisieren Sie die Konfiguration.	Geben Sie den folgenden Befehl ein, um das Arbeitsverzeichnis zu initialisieren. `terraform init`	DevOps Ingenieur, Terraform
Sehen Sie sich eine Vorschau des Terraform-Plans an.	Geben Sie den folgenden Befehl ein, um den Zielstatus mit dem aktuellen Status Ihrer AWS Umgebung zu vergleichen. Dieser Befehl generiert eine Vorschau der Ressourcen, die konfiguriert werden. `terraform plan`	DevOps Ingenieur, Terraform

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verifizieren und bereitstellen.	1. Überprüfen Sie die Konfigurationsänderungen im Terraform-Plan und bestätigen Sie, dass Sie diese Änderungen implementieren möchten. 2. Geben Sie den folgenden Befehl ein, um den Plan anzuwenden und die Infrastruktur zu erstellen. `terraform apply` 3. Geben Sie ein`yes`, um fortzufahren. Terraform erstellt die Architektur, die in den Konfigurationsdate ien deklariert ist. Weitere Informationen zur Architekt ur finden Sie im Abschnitt Zielarchitektur dieses Musters.	DevOps Ingenieur, Terraform

Validieren und bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Bereitste llung der Infrastruktur.	1. Wenn Sie noch keine EC2 Amazon-Instance in einem öffentlichen Subnetz in Ihrem haben AWS-Region, erstellen Sie eine. Anweisungen finden Sie unter Starten Sie	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ihre Linux-Instance oder Starten Sie Ihre Windows-Instance. Sie werden diese Instanz verwenden, um die Konnektivität von der AWS-Region zur Wellenlängenzone zu testen. 2. Testen Sie die Konnektivität von der Instanz in der AWS-Region zur Instanz in der Wellenlängenzone. Anweisungen finden Sie unter Testen der Konnektivität in der Wellenlängen-Dokumentation.	
(Optional) Bereinigen Sie die Infrastruktur.	Wenn Sie alle Ressourcen löschen müssen, die von Terraform bereitgestellt wurden, gehen Sie wie folgt vor: 1. Geben Sie den folgenden Befehl ein. `terraform destroy` 2. Geben Sie `yes` zur Bestätigung ein.	DevOps Ingenieur, Terraform

Fehlerbehebung

Problem	Lösung
Konnektivität zu EC2 Amazon-Instances in der AWS-Region.	Weitere Informationen finden Sie unter Problembehandlung bei der Verbindung mit Ihrer Linux-Instance oder Problembehandlung bei der Verbindung mit Ihrer Windows-Instance.
Konnektivität zu EC2 Amazon-Instances in der Wavelength Zone.	Weitere Informationen finden Sie unter Fehlerbehebung bei der SSH- oder RDP-Konnektivität zu meinen EC2 Instances, die in einer Wellenlängenzone gestartet wurden.
Kapazität in der Wellenlängenzone.	Siehe Kontingente und Überlegungen für Wellenlängenzonen.
Mobil- oder Mobilfunkanbieterkonnektivität vom Mobilfunknetz zum AWS-Region.	1. Stellen Sie sicher, dass das Carrier-Gateway betriebsbereit ist. Gehen Sie wie folgt vor: a. Öffnen Sie die Amazon VPC-Konsole. b. Wählen Sie im Navigationsbereich Ihr aus VPCs. c. Wählen Sie die VPC aus, die die Wellenlängenzone enthält. d. Vergewissern Sie sich im Detailbereich für Carrier Gateway, dass der Wert angehängt ist. 2. Stellen Sie sicher, dass alle elastischen IP-Adressen, die an Instances in der Wavelength Zone angeschlossen sind, betriebsbereit sind. Gehen Sie wie folgt vor: a. Öffnen Sie die EC2 Amazon-Konsole. b. Wählen Sie im Navigationsbereich Instances aus. c. Wählen Sie die Instanz in der Wellenlängenzone aus.

Problem	Lösung
	d. Wählen Sie die Registerkarte Network (Netzwerk) aus. e. Vergewissern Sie sich, dass an die elastic network interface eine Elastic IP-Adresse angehängt ist. 3. Wenden Sie sich an das Carrier Network-Supportteam.

Zugehörige Ressourcen

- Was ist AWS Wavelength?
- Wie AWS Wavelength funktioniert
- Resilienz in AWS Wavelength

Massenmigrieren von DNS-Einträgen in eine private gehostete Zone von Amazon Route 53

Erstellt von Ram Kandaswamy (AWS)

Übersicht

Netzwerktechniker und Cloud-Administratoren benötigen eine effiziente und einfache Möglichkeit, DNS-Einträge (Domain Name System) zu privaten Hosting-Zonen in Amazon Route 53 hinzuzufügen. Das manuelle Kopieren von Einträgen aus einem Microsoft Excel-Arbeitsblatt an die entsprechenden Stellen in der Route 53 53-Konsole ist mühsam und fehleranfällig. Dieses Muster beschreibt einen automatisierten Ansatz, der den Zeit- und Arbeitsaufwand für das Hinzufügen mehrerer Datensätze reduziert. Es bietet auch eine wiederholbare Reihe von Schritten für die Erstellung mehrerer gehosteter Zonen.

Dieses Muster verwendet Amazon Simple Storage Service (Amazon S3) zum Speichern von Datensätzen. Um effizient mit Daten zu arbeiten, verwendet das Muster aufgrund seiner Einfachheit und der Fähigkeit, ein Python-Wörterbuch (`dict`Datentyp) zu unterstützen, das JSON-Format.

> **Note**
>
> Wenn Sie eine Zonendatei von Ihrem System aus generieren können, sollten Sie stattdessen die Route 53 53-Importfunktion verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein Excel-Arbeitsblatt, das private, gehostete Zonendatensätze enthält
- Vertrautheit mit verschiedenen Typen von DNS-Einträgen wie A-Eintrag, NAPTR-Datensatz (Name Authority Pointer) und SRV-Eintrag (siehe Unterstützte DNS-Eintragstypen)
- Vertrautheit mit der Sprache Python und ihren Bibliotheken

Einschränkungen

- Das Muster deckt nicht alle Anwendungsszenarien umfassend ab. Beispielsweise verwendet der Aufruf change_resource_record_sets nicht alle verfügbaren Eigenschaften der API.

- Im Excel-Arbeitsblatt wird davon ausgegangen, dass der Wert in jeder Zeile eindeutig ist. Es wird erwartet, dass mehrere Werte für jeden vollqualifizierten Domänennamen (FQDN) in derselben Zeile erscheinen. Wenn das nicht der Fall ist, sollten Sie den in diesem Muster bereitgestellten Code ändern, um die erforderliche Verkettung durchzuführen.
- Das Muster verwendet das AWS-SDK SDK for Python (Boto3), um den Route 53-Service direkt aufzurufen. Sie können den Code so erweitern, dass er einen CloudFormation AWS-Wrapper für die `update_stack` Befehle `create_stack` und verwendet und die JSON-Werte zum Auffüllen von Vorlagenressourcen verwenden.

Architektur

Technologie-Stack

- Route 53 private, gehostete Zonen für die Weiterleitung des Datenverkehrs
- Amazon S3 zum Speichern der JSON-Ausgabedatei

Der Workflow besteht aus den folgenden Schritten, wie im vorherigen Diagramm dargestellt und im Abschnitt Epics beschrieben:

1. Laden Sie ein Excel-Arbeitsblatt mit den Datensatzinformationen in einen S3-Bucket hoch.
2. Erstellen Sie ein Python-Skript, das die Excel-Daten in das JSON-Format konvertiert, und führen Sie es aus.
3. Lesen Sie die Datensätze aus dem S3-Bucket und bereinigen Sie die Daten.
4. Erstellen Sie Datensätze in Ihrer privaten gehosteten Zone.

Tools

- Route 53 — Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Webservice, der die Domainregistrierung, das DNS-Routing und die Zustandsprüfung übernimmt.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen.

Epen

Bereiten Sie Daten für die Automatisierung vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Excel-Datei für Ihre Unterlagen.	Verwenden Sie die Datensätze, die Sie aus Ihrem aktuellen System exportiert haben, um ein Excel-Arbeitsblatt zu erstellen, das die erforderlichen Spalten für einen Datensatz enthält, z. B. den vollqualifizierten Domänennamen (FQDN), den Datensatztyp, die Gültigkeitsdauer (TTL) und den Wert. Bei NAPTR- und SRV-Datensätzen ist der Wert eine Kombination aus mehreren Eigenschaften. Verwenden Sie daher die `concat` Excel-Methode, um diese Eigenschaften zu kombinieren. FqdnN Recor e Wert TTL somet .exam org A 1.1.1.1 900	Dateningenieur, Excel-Kenntnisse
Überprüfen Sie die Arbeitsumgebung.	Erstellen Sie in Ihrer IDE eine Python-Datei, um das Excel-Eingabearbeitsblatt in das JSON-Format zu konvertieren. (Anstelle einer IDE können Sie	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	auch ein SageMaker Amazon-Notebook verwenden, um mit Python-Code zu arbeiten.)
	
	Stellen Sie sicher, dass die von Ihnen verwendete Python-Version Version 3.7 oder höher ist.
	
	`python3 --version`
	
	Installieren Sie das Pandas-Paket.
	
	`pip3 install pandas --user`	

Konvertiert die Excel-Arbeitsblattdaten in JSON.	Erstellen Sie eine Python-Datei, die den folgenden Code für die Konvertierung von Excel nach JSON enthält.
	
	`import pandas as pd`
	`data=pd.read_excel('./Book1.xls')`
	`data.to_json(path_or_buf='my.json', orient='records')`
	
	wobei `Book1` der Name des Excel-Arbeitsblatts und der Name der JSON-Ausgabedatei `my.json` steht.
		Dateningenieur, Python-Kenntnisse

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die JSON-Datei in einen S3-Bucket hoch.	Laden Sie die Datei `my.json` zu einem S3-Bucket hoch. Weitere Informationen finden Sie unter Bucket erstellen in der Amazon S3 S3-Dokumentation.	App-Developer

Fügen Sie Datensätze ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine private gehostete Zone.	Verwenden Sie die API create_hosted_zone und den folgenden Python-Beispielcode, um eine private gehostete Zone zu erstellen. Ersetzen Sie die Parameter und `vpcId` durch `hostedZoneName` Ihre `vpcRegion` eigenen Werte.
	`import boto3`
	`import random`
	`hostedZoneName ="xxx"`
	`vpcRegion = "us-east-1"`
	`vpcId="vpc-xxxx"`
	`route53_client = boto3.client('route53')`
	`response = route53_client.create_hosted_zone(`
	`Name= hostedZoneName,`
	`VPC={`
		Cloud-Architekt, Netzwerkadministrator, Python-Kenntnisse

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>'VPCRegion': vpcRegion,
	'VPCId': vpcId
	},
	CallerReference=str(random.random()*100000),
	HostedZoneConfig={
	'Comment': "private hosted zone created by automation",
	'PrivateZone': True
	}
	)
	print(response)</pre>
	Sie können auch ein IaC-Tool (Infrastructure as Code) wie AWS verwenden, CloudFormation um diese Schritte durch eine Vorlage zu ersetzen, die einen Stack mit den entsprechenden Ressourcen und Eigenschaften erstellt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie Details als Wörterbuch von Amazon S3 ab.	Verwenden Sie den folgenden Code, um aus dem S3-Bucket zu lesen und die JSON-Werte als Python-Wörterbuch abzurufen. `fileobj = s3_client.get_object( Bucket=bucket_name, Key='my.json' ) filedata = fileobj['Body'].read() contents = filedata.decode('utf-8') json_content=json.loads(contents) print(json_content)` wo `json_content` enthält das Python-Wörterbuch.	App-Entwickler, Python-Kenntnisse

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Saubere Datenwerte für Leerzeichen und Unicode-Zeichen.	Verwenden Sie als Sicherheitsmaßnahme zur Sicherstellung der Richtigkeit der Daten den folgenden Code, um eine Operation mit den Werten in durchzuführen`json_content` . Dieser Code entfernt die Leerzeichen am Anfang und Ende jeder Zeichenfolge. Außerdem wird die `replace` Methode verwendet, um harte (geschützte) Leerzeichen (die `\xa0` Zeichen) zu entfernen.
	`for item in json_content:`
	`  fqn_name = unicodedata.normalize("NFKD",item["FqdnName"].replace("u'", "'").replace('\xa0', '').strip())`
	`  rec_type = item["RecordType"].replace('\xa0', '').strip()`
	`  res_rec = {`
	`  'Value': item["Value"].replace('\xa0', '').strip()`
	`  }`
		App-Entwickler, Python-Kenntnisse

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Datensätze ein.	Verwenden Sie den folgenden Code als Teil der vorherigen `for` Schleife. `change_response = route53_client.change_resource_record_sets( HostedZoneId="xxxxxxxx", ChangeBatch={ 'Comment': 'Created by automation', 'Changes': [ { 'Action': 'UPSERT', 'ResourceRecordSet': { 'Name': fqn_name, 'Type': rec_type, 'TTL': item["TTL"], 'ResourceRecords': res_rec } } ] } )`	App-Entwickler, Python-Kenntnisse

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wo xxxxxxx ist die Hosting-Zonen-ID aus dem ersten Schritt dieses Epos?	

Zugehörige Ressourcen

Referenzen

- Erstellen von Datensätzen durch Import einer Zonendatei (Amazon Route 53 53-Dokumentation)
- Methode create_hosted_zone (Boto3-Dokumentation)
- Methode change_resource_record_sets (Boto3-Dokumentation)

Tutorials und Videos

- Das Python-Tutorial (Python-Dokumentation)
- DNS-Design mit Amazon Route 53 (YouTube Video, AWS Online Tech Talks)

Ändern Sie HTTP-Header, wenn Sie von F5 zu einem Application Load Balancer auf AWS migrieren

Erstellt von Sachin Trivedi (AWS)

Übersicht

Wenn Sie eine Anwendung, die einen F5 Load Balancer verwendet, zu Amazon Web Services (AWS) migrieren und einen Application Load Balancer auf AWS verwenden möchten, ist die Migration von F5-Regeln für Header-Änderungen ein häufiges Problem. Ein Application Load Balancer unterstützt keine Header-Änderungen, aber Sie können Amazon CloudFront als Content Delivery Network (CDN) und Lambda @Edge verwenden, um Header zu ändern.

Dieses Muster beschreibt die erforderlichen Integrationen und bietet Beispielcode für die Header-Änderung mithilfe von AWS CloudFront und Lambda @Edge.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine lokale Anwendung, die einen F5-Load Balancer mit einer Konfiguration verwendet, die den HTTP-Header-Wert ersetzt durch `if, else` Weitere Informationen zu dieser Konfiguration finden Sie unter HTTP: :header in der F5-Produktdokumentation.

Einschränkungen

- Dieses Muster gilt für die Anpassung des F5-Load Balancer-Headers. Informationen zur Unterstützung anderer Load Balancer von Drittanbietern finden Sie in der Load Balancer-Dokumentation.
- Die Lambda-Funktionen, die Sie für Lambda @Edge verwenden, müssen sich in der Region USA Ost (Nord-Virginia) befinden.

Architektur

Das folgende Diagramm zeigt die Architektur auf AWS, einschließlich des Integrationsflusses zwischen dem CDN und anderen AWS-Komponenten.

Tools

AWS-Services

- Application Load Balancer – Ein Application Load Balancer ist ein vollständig verwalteter AWS-Load-Balancing-Service, der auf der siebten Ebene des Open Systems Interconnection (OSI) -Modells funktioniert. Er verteilt den Datenverkehr auf mehrere Ziele und unterstützt erweiterte Routing-Anfragen, die auf HTTP-Headern und -Methoden, Abfragezeichenfolgen und host- oder pfadbasiertem Routing basieren.
- Amazon CloudFront — Amazon CloudFront ist ein Webservice, der die Verteilung Ihrer statischen und dynamischen Webinhalte wie .html-, .css-, .js- und Bilddateien an Ihre Benutzer beschleunigt. CloudFront stellt Ihre Inhalte über ein weltweites Netzwerk von Rechenzentren bereit, die als Edge-Standorte bezeichnet werden, um die Latenz zu verringern und die Leistung zu verbessern.
- Lambda @Edge – Lambda @Edge ist eine Erweiterung von AWS Lambda, mit der Sie Funktionen ausführen können, um den bereitgestellten Inhalt anzupassen. CloudFront Sie können Funktionen in der Region USA Ost (Nord-Virginia) erstellen und die Funktion dann einer CloudFront Distribution zuordnen, um Ihren Code automatisch auf der ganzen Welt zu replizieren, ohne Server bereitstellen oder verwalten zu müssen. Dies reduziert die Latenz und verbessert die Benutzererfahrung.

Code

Der folgende Beispielcode bietet einen Blueprint zum Ändern von CloudFront Antwort-Headern. Folgen Sie den Anweisungen im Abschnitt Epics, um den Code bereitzustellen.

```
exports.handler = async (event, context) => {
    const response = event.Records[0].cf.response;
    const headers = response.headers;


    const headerNameSrc = 'content-security-policy';
    const headerNameValue = '*.xyz.com';


    if (headers[headerNameSrc.toLowerCase()]) {
        headers[headerNameSrc.toLowerCase()] = [{
            key: headerNameSrc,
            value: headerNameValue,
        }];
```

```
        console.log(`Response header "${headerNameSrc}" was set to ` +
                    `"${headers[headerNameSrc.toLowerCase()][0].value}"`);
    }
    else {
            headers[headerNameSrc.toLowerCase()] = [{
            key: headerNameSrc,
            value: headerNameValue,
            }];
    }
    return response;
};
```

Epen

Erstellen Sie eine CDN-Distribution

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CloudFront Webdistribution.	In diesem Schritt erstellen Sie eine CloudFront Verteilung, in der Sie angeben, von CloudFront wo aus Inhalte bereitgestellt werden sollen. Außerdem erfahren Sie, wie Sie die Inhaltsbereitstellung nachverfolgen und verwalten können. Um eine Verteilung mithilfe der Konsole zu erstellen, melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die CloudFront Konsole und folgen Sie dann den Schritten in der CloudFront Dokumentation.	Cloud-Administrator

Lambda @Edge -Funktion erstellen und bereitstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Lambda @Edge -Funktion und stellen Sie sie bereit.	Sie können eine Lambda @Edge -Funktion erstellen , indem Sie einen Blueprint zum Ändern von CloudFron t Antwortheadern verwenden . (Andere BluePrints sind für verschiedene Anwendung sfälle verfügbar; weitere Informationen finden Sie in der CloudFront Dokumenta tion unter Lambda @Edge - Beispielfunktionen.) Um eine Lambda @Edge -Funktion zu erstellen: 1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS Lambda-Konsole unter https://console.aws.amazon .com/lambda/. 2. Stellen Sie sicher, dass Sie sich in der Region USA Ost (Nord-Virginia) befinden. CloudFront Blueprints sind nur in dieser Region verfügbar. 3. Wählen Sie Funktion erstellen. 4. Wählen Sie Blueprint verwenden aus und geben	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie dann Cloudfront in das Blueprints-Suchfeld ein. 5. Wählen Sie den cloudfront-modify-response-headerBlueprint aus und wählen Sie dann Konfigurieren aus. 6. Geben Sie auf der Seite mit den Basisinformationen die folgenden Informationen ein: a. Geben Sie einen Funktionsnamen ein. b. Wählen Sie unter Execution Role (Ausführungsrolle) die Option Create a new role from AWS policy templates (Neue Rolle aus AWS-Richtlinienvorlagen erstellen). c. Ordnen Sie den erforderlichen Rollennamen für AWS Identity and Access Management (IAM) zu. 7. Wählen Sie Funktion erstellen. 8. Wählen Sie im Bereich Designer der Seite Ihren Funktionsnamen aus. 9. Ersetzen Sie im Abschnitt Funktionscode den Vorlagencode durch den	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Beispielcode, der zuvor in diesem Muster im Abschnitt Code bereitgestellt wurde. 10. Ersetzen Sie ihn im Beispielcode `xyz.com` durch Ihren Domainnamen. 11. Wählen Sie Speichern.	
Stellen Sie die Lambda @Edge -Funktion bereit.	Folgen Sie den Anweisungen in Schritt 4 des Tutorials : Erstellen einer einfachen Lambda @Edge -Funktion in der CloudFront Amazon-Dokumentation, um den CloudFront Trigger zu konfigurieren und die Funktion bereitzustellen.	AWS-Administrator

Zugehörige Ressourcen

CloudFront Dokumentation

- Anfrage- und Antwortverhalten für benutzerdefinierte Ursprünge
- Mit Distributionen arbeiten
- Lambda @Edge -Beispielfunktionen
- Anpassung an der Peripherie mit Lambda @Edge
- Tutorial: Eine einfache Lambda @Edge -Funktion erstellen

Greifen Sie privat von mehreren aus auf einen zentralen AWS-Serviceendpunkt zu VPCs

Erstellt von Martin Guenthner (AWS) und Samuel Gordon (AWS)

Übersicht

Die Sicherheits- und Compliance-Anforderungen für Ihre Umgebung können vorsehen, dass der Datenverkehr zu Amazon Web Services (AWS) -Services oder Endpunkten nicht über das öffentliche Internet erfolgen darf. Dieses Muster ist eine Lösung, die für eine hub-and-spokeTopologie konzipiert ist, bei der eine zentrale Hub-VPC mit mehreren verteilten Spokes verbunden ist. VPCs In dieser Lösung verwenden Sie AWS, PrivateLink um einen VPC-Schnittstellen-Endpunkt für den AWS-Service im Hub-Konto zu erstellen. Anschließend verwenden Sie Transit-Gateways und eine DNS-Regel (Distributed Domain Name System), um Anfragen an die private IP-Adresse des Endpunkts über das verbundene Netzwerk zu lösen. VPCs

Dieses Muster beschreibt, wie AWS Transit Gateway, ein eingehender Amazon Route 53 Resolver Resolver-Endpunkt und eine gemeinsam genutzte Route 53-Weiterleitungsregel verwendet werden, um die DNS-Abfragen von den verbundenen Ressourcen aufzulösen. VPCs Sie erstellen den Endpunkt, das Transit-Gateway, den Resolver und die Weiterleitungsregel im Hub-Konto. Anschließend verwenden Sie AWS Resource Access Manager (AWS RAM), um das Transit-Gateway und die Weiterleitungsregel mit dem Spoke zu teilen VPCs. Die bereitgestellten CloudFormation AWS-Vorlagen helfen Ihnen bei der Bereitstellung und Konfiguration der Ressourcen in der Hub-VPC und Spoke VPCs.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein Hub-Konto und ein oder mehrere Spoke-Konten, die in derselben Organisation in AWS Organizations verwaltet werden. Weitere Informationen finden Sie unter Organisation erstellen und verwalten.
- AWS Resource Access Manager (AWS RAM) ist als vertrauenswürdiger Service in AWS Organizations konfiguriert. Weitere Informationen finden Sie unter Verwenden von AWS Organizations mit anderen AWS-Services.
- Die DNS-Auflösung muss im Hub-and-Spoke-Modus aktiviert sein VPCs. Weitere Informationen finden Sie unter DNS-Attribute für Ihre VPC (Amazon Virtual Private Cloud Cloud-Dokumentation).

Einschränkungen

- Dieses Muster verbindet Hub- und Spoke-Konten in derselben AWS-Region. Bei Bereitstellungen in mehreren Regionen müssen Sie dieses Muster für jede Region wiederholen.
- Der AWS-Service muss PrivateLink als Schnittstelle in den VPC-Endpunkt integriert werden. Eine vollständige Liste finden Sie unter AWS-Services, die in AWS integriert sind PrivateLink (PrivateLink Dokumentation).
- Die Affinität zur Availability Zone ist nicht garantiert. Beispielsweise könnten Anfragen aus Availability Zone A mit einer IP-Adresse aus Availability Zone B antworten.
- Die dem VPC-Endpunkt zugeordnete elastic network interface hat ein Limit von 10.000 Abfragen pro Sekunde.

Architektur

Zieltechnologie-Stack

- Eine Hub-VPC im Hub-AWS-Konto
- Ein oder mehrere Spoke VPCs in einem Spoke-AWS-Konto
- Ein oder mehrere Schnittstellen-VPC-Endpunkte im Hub-Konto
- Route 53 53-Resolver für eingehenden und ausgehenden Datenverkehr im Hub-Konto
- Eine Route 53 Resolver-Weiterleitungsregel, die im Hub-Konto bereitgestellt und mit dem Spoke-Konto geteilt wird
- Ein Transit-Gateway, das im Hub-Konto bereitgestellt und mit dem Spoke-Konto geteilt wird
- AWS Transit Gateway verbindet den Hub und Spoke VPCs

Zielarchitektur

Die folgende Abbildung zeigt eine Beispielarchitektur für diese Lösung. In dieser Architektur hat die Route 53 Resolver-Weiterleitungsregel im Hub-Konto die folgende Beziehung zu den anderen Architekturkomponenten:

1. Die Weiterleitungsregel wird mithilfe von AWS-RAM mit der Spoke-VPC geteilt.
2. Die Weiterleitungsregel ist dem Outbound-Resolver in der Hub-VPC zugeordnet.
3. Die Weiterleitungsregel zielt auf den Resolver für eingehende Anrufe in der Hub-VPC ab.

Die folgende Abbildung zeigt den Verkehrsfluss durch die Beispielarchitektur:

1. Eine Ressource, z. B. eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance, in der Spoke-VPC stellt eine DNS-Anfrage an`<service>.<region>.amazonaws.com`. Die Anfrage wird vom Spoke Amazon DNS Resolver empfangen.
2. Die Route 53 53-Weiterleitungsregel, die vom Hub-Konto gemeinsam genutzt und der Spoke-VPC zugeordnet wird, fängt die Anfrage ab.
3. In der Hub-VPC verwendet der Outbound-Resolver die Weiterleitungsregel, um die Anfrage an den Inbound-Resolver weiterzuleiten.
4. Der Inbound Resolver verwendet den Hub-VPC Amazon DNS Resolver, um die IP-Adresse für `<service>.<region>.amazonaws.com` die private IP-Adresse eines VPC-Endpunkts aufzulösen. Wenn kein VPC-Endpunkt vorhanden ist, wird er in die öffentliche IP-Adresse aufgelöst.

Tools

AWS-Tools und -Services

- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server starten, wie Sie benötigen, und diese schnell nach oben oder unten skalieren.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie kontrollieren, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Mit AWS Resource Access Manager (AWS RAM) können Sie Ihre Ressourcen sicher für mehrere AWS-Konten gemeinsam nutzen, um den betrieblichen Aufwand zu reduzieren und für Transparenz und Überprüfbarkeit zu sorgen.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer Domain Name System (DNS)-Web-Service.

- AWS Systems Manager unterstützt Sie bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der AWS-Cloud ausgeführt werden. Es vereinfacht das Anwendungs- und Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme und hilft Ihnen, Ihre AWS-Ressourcen sicher und skalierbar zu verwalten.
- AWS Transit Gateway ist ein zentraler Knotenpunkt, der lokale Netzwerke verbindet VPCs .
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.

Andere Tools und Dienste

- nslookup ist ein Befehlszeilentool zum Abfragen von DNS-Einträgen. In diesem Muster verwenden Sie dieses Tool, um die Lösung zu testen.

Code-Repository

Der Code für dieses Muster ist im vpc-endpoint-sharingRepository verfügbar. GitHub Dieses Muster bietet zwei CloudFormation AWS-Vorlagen:

- Eine Vorlage für die Bereitstellung der folgenden Ressourcen im Hub-Konto:
  - `rSecurityGroupEndpoints`— Die Sicherheitsgruppe, die den Zugriff auf den VPC-Endpunkt steuert.
  - `rSecurityGroupResolvers`— Die Sicherheitsgruppe, die den Zugriff auf den Route 53 Resolver steuert.
  - `rKMSEndpoint`, `rSSMMessagesEndpointrSSMEndpoint`, und `rEC2MessagesEndpoint` — Beispiel für VPC-Endpunkte mit Schnittstelle im Hub-Konto. Passen Sie diese Endpunkte an Ihren Anwendungsfall an.
  - `rInboundResolver`— Ein Route 53 53-Resolver, der DNS-Anfragen an den Hub Amazon DNS Resolver löst.
  - `r0utboundResolver`— Ein ausgehender Route 53 53-Resolver, der Anfragen an den eingehenden Resolver weiterleitet.
  - `rAWSApiResolverRule`— Die Route 53 Resolver-Weiterleitungsregel, die für alle Spoke VPCs gilt.

  - `rRamShareAWSResolverRule`— Die AWS-RAM-Freigabe, die es dem Spoke ermöglicht, die `rAWSApiResolverRule` Weiterleitungsregel VPCs zu verwenden.
  - * `rVPC` — Die Hub-VPC, die zur Modellierung der gemeinsamen Dienste verwendet wird.
  - * `rSubnet1` — Ein privates Subnetz, das zur Unterbringung der Hub-Ressourcen verwendet wird.
  - * `rRouteTable1` — Die Routentabelle für die Hub-VPC.
  - * `rRouteTableAssociation1` — Für die `rRouteTable1` Routentabelle in der Hub-VPC die Zuordnung für das private Subnetz.
  - * `rRouteSpoke` — Die Route von der Hub-VPC zur Spoke-VPC.
  - * `rTgw` — Das Transit-Gateway, das von allen Spoke gemeinsam genutzt wird. VPCs
  - * `rTgwAttach` — Der Anhang, der es der Hub-VPC ermöglicht, den Verkehr an das `rTgw` Transit-Gateway weiterzuleiten.
  - * `rTgwShare` — Die AWS-RAM-Freigabe, die es den Spoke-Konten ermöglicht, das `rTgw` Transit-Gateway zu verwenden.
- Eine Vorlage für die Bereitstellung der folgenden Ressourcen in den Spoke-Konten:
  - `rAWSApiResolverRuleAssociation`— Eine Zuordnung, die es der Spoke-VPC ermöglicht, die gemeinsame Weiterleitungsregel im Hub-Konto zu verwenden.
  - * `rVPC` — Die Spoke-VPC.
  - * `rSubnet1, rSubnet2, rSubnet3` — Ein Subnetz für jede Availability Zone, das zur Unterbringung der privaten Spoke-Ressourcen verwendet wird.
  - * `rTgwAttach` — Der Anhang, der es der Spoke-VPC ermöglicht, den Verkehr an das `rTgw` Transit-Gateway weiterzuleiten.
  - * `rRouteTable1` — Die Routentabelle für die Spoke-VPC.
  - * `rRouteEndpoints` — Die Route von den Ressourcen in der Spoke-VPC zum Transit-Gateway.
  - * `rRouteTableAssociation1/2/3` — Für die `rRouteTable1` Routentabelle in der Spoke-VPC die Zuordnungen für die privaten Subnetze.
  - * `rInstanceRole` — Die IAM-Rolle, die zum Testen der Lösung verwendet wurde.
  - * `rInstancePolicy` — Die IAM-Richtlinie, die zum Testen der Lösung verwendet wurde.
  - * `rInstanceSg` — Die Sicherheitsgruppe, die zum Testen der Lösung verwendet wurde.
  - * `rInstanceProfile` — Das zum Testen der Lösung verwendete IAM-Instanzprofil.

- * `rInstance` — Eine EC2 Instanz, die für den Zugriff über AWS Systems Manager vorkonfiguriert ist. Verwenden Sie diese Instanz, um die Lösung zu testen.

* Diese Ressourcen unterstützen die Beispielarchitektur und sind möglicherweise nicht erforderlich, wenn dieses Muster in einer vorhandenen landing zone implementiert wird.

Epen

Bereite die Vorlagen vor CloudFormation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Code-Repo sitory.	1. Ändern Sie in einer Befehlszeilenschnittstelle Ihr Arbeitsverzeichnis in das Verzeichnis, in dem Sie die Beispieldateien speichern möchten. 2. Geben Sie den folgenden Befehl ein: `git clone https://github.com/aws-samples/vpc-endpoint-sharing.git`	Netzwerkadministrator, Cloud-Architekt
Ändern Sie die Vorlagen.	1. Öffnen Sie im geklonten Repository die Dateien hub.yml und spoke.yml. 2. Überprüfen Sie die mit diesen Vorlagen erstellte n Ressourcen und passen Sie die Vorlagen nach Bedarf an Ihre Umgebung an. Eine vollständige Liste finden Sie im Abschnitt Code-Repository unter	Netzwerkadministrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Tools. Wenn Ihre Konten bereits über einige dieser Ressourcen verfügen, entfernen Sie sie aus der CloudFormation Vorlage. Weitere Informationen finden Sie unter Arbeiten mit Vorlagen (CloudFormation Dokumentation). 3. Speichern und schließen Sie die Dateien hub.yml und spoke.yml.	

Stellen Sie die Ressourcen in den Zielkonten bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Hub-Ressourcen bereit.	Erstellen Sie mithilfe der hub.yml-Vorlage einen Stack. CloudFormation Wenn Sie dazu aufgefordert werden, geben Sie Werte für die Parameter in der Vorlage ein. Weitere Informationen finden Sie unter Einen Stack erstellen (CloudFormation Dokumentation).	Cloud-Architekt, Netzwerkadministrator
Stellen Sie die Spoke-Ressourcen bereit.	Erstellen Sie mithilfe der Vorlage spoke.yml einen Stack. CloudFormation Wenn Sie dazu aufgefordert werden, geben Sie Werte für die Parameter in der Vorlage an.	Cloud-Architekt, Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter Einen Stack erstellen (CloudFormation Dokumentation).	

Testen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie private DNS-Abfragen an den AWS-Service.	1. Stellen Sie mithilfe von Session Manager, einer Funktion von AWS Systems Manager, eine Connect zur `rInstance` EC2 Instance her. Weitere Informationen finden Sie unter Connect zu Ihrer Linux-Instance mithilfe von Session Manager (EC2 Amazon-Dokumentation). 2. Verwenden Sie für einen AWS-Service, der einen VPC-Endpunkt im Hub-Konto hat, `nslookup` um zu bestätigen, dass die privaten IP-Adressen für den eingehenden Route 53 53-Resolver zurückgegeben werden. Im Folgenden finden Sie ein Beispiel für die Verwendun `gnslookup`, um einen Amazon Systems Manager	Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Manager-Endpunkt zu erreichen.
	
	`nslookup ssm.<region>.amazonaws.com`
	
	3. Geben Sie in der AWS-Befehlszeilenschnittstelle (AWS CLI) einen Befehl ein, mit dessen Hilfe Sie überprüfen können, ob die Änderungen die Servicefunktionalität nicht beeinträchtigt haben. Eine Liste der Befehle finden Sie unter AWS CLI Command Reference.
	
	Der folgende Befehl sollte beispielsweise eine Liste von Amazon Systems Manager Manager-Dokumenten zurückgeben.
	
	`aws ssm list-documents`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie öffentliche DNS-Abfragen an einen AWS-Service.	1. Verwenden Sie für einen AWS-Service, der keinen VPC-Endpunkt im Hub-Konto hat, `nslookup` um zu bestätigen, dass die öffentlichen IP-Adressen zurückgegeben werden. Im Folgenden finden Sie ein Beispiel für die Verwendung `nslookup`, um einen Amazon Simple Notification Service (Amazon SNS) -Endpunkt zu erreichen. `nslookup sns.<region>.amazonaws.com` 2. Geben Sie in der AWS-CLI einen Befehl ein, mit dessen Hilfe Sie bestätigen können, dass die Änderungen die Servicefunktionalität nicht beeinträchtigt haben. Eine Liste der Befehle finden Sie unter AWS CLI Command Reference. Wenn beispielsweise Amazon SNS SNS-Themen im Hub-Konto vorhanden sind, sollte der folgende Befehl eine Themenliste zurückgeben.	Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws sns list-topics`	

Zugehörige Ressourcen

- Aufbau einer skalierbaren und sicheren AWS-Netzwerkinfrastruktur mit mehreren VPC (AWS-Whitepaper)
- Arbeiten mit gemeinsam genutzten Ressourcen (AWS-RAM-Dokumentation)
- Arbeiten mit Transit-Gateways (AWS Transit Gateway Gateway-Dokumentation)

Erstellen Sie einen Bericht mit den Ergebnissen von Network Access Analyzer für eingehenden Internetzugang in mehreren AWS-Konten

Erstellt von Mike Virgilio (AWS)

Übersicht

Unbeabsichtigter eingehender Internetzugriff auf AWS Ressourcen kann Risiken für den Datenperimeter eines Unternehmens darstellen. Network Access Analyzer ist eine Funktion von Amazon Virtual Private Cloud (Amazon VPC), mit der Sie unbeabsichtigte Netzwerkzugriffe auf Ihre Ressourcen auf Amazon Web Services (AWS) identifizieren können. Sie können Network Access Analyzer verwenden, um Ihre Netzwerkzugriffsanforderungen zu spezifizieren und potenzielle Netzwerkpfade zu identifizieren, die Ihren angegebenen Anforderungen nicht entsprechen. Sie können Network Access Analyzer verwenden, um Folgendes zu tun:

1. Identifizieren Sie AWS Ressourcen, auf die über Internet-Gateways über das Internet zugegriffen werden kann.
2. Stellen Sie sicher, dass Ihre virtuellen privaten Clouds (VPCs) angemessen segmentiert sind, z. B. durch die Isolierung von Produktions- und Entwicklungsumgebungen und die Trennung von Transaktionsworkloads.

Network Access Analyzer analysiert die Bedingungen der end-to-end Netzwerkerreichbarkeit und nicht nur eine einzelne Komponente. Um festzustellen, ob eine Ressource über das Internet zugänglich ist, bewertet Network Access Analyzer das Internet-Gateway, VPC-Routentabellen, Netzwerkzugriffskontrolllisten (ACLs), öffentliche IP-Adressen auf elastischen Netzwerkschnittstellen und Sicherheitsgruppen. Wenn eine dieser Komponenten den Internetzugang verhindert, generiert Network Access Analyzer kein Ergebnis. Wenn eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance beispielsweise über eine offene Sicherheitsgruppe verfügt, die Datenverkehr zulässt, sich die Instance `0/0` aber in einem privaten Subnetz befindet, das von keinem Internet-Gateway aus routbar ist, würde Network Access Analyzer kein Ergebnis generieren. Dies liefert qualitativ hochwertige Ergebnisse, sodass Sie Ressourcen identifizieren können, auf die wirklich über das Internet zugegriffen werden kann.

Wenn Sie Network Access Analyzer ausführen, verwenden Sie Network Access Scopes, um Ihre Netzwerkzugriffsanforderungen festzulegen. Diese Lösung identifiziert Netzwerkpfade zwischen einem Internet-Gateway und einer elastic network interface. Bei diesem Muster stellen Sie die Lösung in einer zentralen Umgebung Ihrer Organisation bereit, die von allen Konten AWS-Konto in der

Organisation verwaltet wird AWS Organizations, und sie analysiert alle Konten in der Organisation. AWS-Region

Bei der Entwicklung dieser Lösung wurde Folgendes berücksichtigt:

- Die AWS CloudFormation Vorlagen reduzieren den Aufwand, der für die Bereitstellung der AWS Ressourcen in diesem Muster erforderlich ist.
- Sie können die Parameter in den CloudFormation Vorlagen und im Skript naa-script.sh zum Zeitpunkt der Bereitstellung anpassen, um sie an Ihre Umgebung anzupassen.
- Bash-Scripting stellt automatisch die Network Access Scopes für mehrere Konten parallel bereit und analysiert sie.
- Ein Python-Skript verarbeitet die Ergebnisse, extrahiert die Daten und konsolidiert dann die Ergebnisse. Sie können wählen, ob Sie den konsolidierten Bericht mit den Ergebnissen von Network Access Analyzer im CSV-Format oder in AWS Security Hubüberprüfen möchten. Ein Beispiel für den CSV-Bericht finden Sie im Abschnitt Zusätzliche Informationen dieses Musters.
- Sie können Ergebnisse korrigieren oder sie von future Analysen ausschließen, indem Sie sie der Datei naa-exclusions.csv hinzufügen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein AWS-Konto zum Hosten von Sicherheitsdiensten und -tools, das als Mitgliedskonto einer Organisation in AWS Organizations verwaltet wird. In diesem Muster wird dieses Konto als Sicherheitskonto bezeichnet.
- Im Sicherheitskonto müssen Sie über ein privates Subnetz mit ausgehendem Internetzugang verfügen. Anweisungen finden Sie unter Erstellen eines Subnetzes in der Amazon VPC-Dokumentation. Sie können den Internetzugang mithilfe eines NAT-Gateways oder eines VPC-Schnittstellen-Endpunkts einrichten.
- Zugriff auf das AWS Organizations Verwaltungskonto oder ein Konto, für das Administratorrechte delegiert wurden. CloudFormation Anweisungen finden Sie in der Dokumentation unter Registrieren eines delegierten Administrators. CloudFormation
- Aktivieren Sie den vertrauenswürdigen Zugriff zwischen AWS Organizations und CloudFormation. Anweisungen finden Sie AWS Organizations in der CloudFormation Dokumentation unter Vertrauenswürdigen Zugriff aktivieren mit.

- Wenn Sie die Ergebnisse auf Security Hub hochladen, muss Security Hub für das Konto und den Ort aktiviert sein, AWS-Region an dem die EC2 Amazon-Instance bereitgestellt wird. Weitere Informationen finden Sie unter Einrichtung. AWS Security Hub

Einschränkungen

- Kontoübergreifende Netzwerkpfade werden derzeit aufgrund von Einschränkungen der Network Access Analyzer-Funktion nicht analysiert.
- Das Ziel AWS-Konten muss als Organisation in AWS Organizations verwaltet werden. Wenn Sie das nicht verwenden AWS Organizations, können Sie die CloudFormation Vorlage naa-execrole.yaml und das Skript naa-script.sh für Ihre Umgebung aktualisieren. Stattdessen geben Sie eine Liste der Regionen an, in denen Sie das AWS-Konto IDs Skript ausführen möchten.
- Die CloudFormation Vorlage ist für die Bereitstellung der EC2 Amazon-Instance in einem privaten Subnetz mit ausgehendem Internetzugang konzipiert. Der AWS Systems Manager Agent (SSM-Agent) benötigt ausgehenden Zugriff, um den Systems Manager-Dienstendpunkt zu erreichen, und Sie benötigen ausgehenden Zugriff, um das Code-Repository zu klonen und Abhängigkeiten zu installieren. Wenn Sie ein öffentliches Subnetz verwenden möchten, müssen Sie die Vorlage naa-resources.yaml ändern, um der Amazon-Instance eine Elastic IP-Adresse zuzuordnen. EC2

Architektur

Zielarchitektur

Option 1: Greifen Sie auf Ergebnisse in einem Amazon S3 S3-Bucket zu

Das Diagramm zeigt den folgenden Prozess:

1. Wenn Sie die Lösung manuell ausführen, authentifiziert sich der Benutzer mit Session Manager bei der EC2 Amazon-Instance und führt dann das Skript naa-script.sh aus. Dieses Shell-Skript führt die Schritte 2—7 aus.

   Wenn Sie die Lösung automatisch ausführen, wird das Skript naa-script.sh automatisch nach dem Zeitplan gestartet, den Sie im Cron-Ausdruck definiert haben. Dieses Shell-Skript führt die Schritte 2 bis 7 aus. Weitere Informationen finden Sie unter Automatisierung und Skalierung am Ende dieses Abschnitts.

2. Die EC2 Amazon-Instance lädt die neueste Datei naa-exception.csv aus dem Amazon S3-Bucket herunter. Diese Datei wird später im Prozess verwendet, wenn das Python-Skript die Ausnahmen verarbeitet.
3. Die EC2 Amazon-Instance übernimmt die Rolle `NAAEC2Role` AWS Identity and Access Management (IAM), die Berechtigungen für den Zugriff auf den Amazon S3-Bucket und für die Übernahme der `NAAExecRole` IAM-Rollen in den anderen Konten in der Organisation gewährt.
4. Die EC2 Amazon-Instance übernimmt die `NAAExecRole` IAM-Rolle im Verwaltungskonto der Organisation und generiert eine Liste der Konten in der Organisation.
5. Die EC2 Amazon-Instance übernimmt die `NAAExecRole` IAM-Rolle in den Mitgliedskonten der Organisation (im Architekturdiagramm als Workload-Konten bezeichnet) und führt für jedes Konto eine Sicherheitsbewertung durch. Die Ergebnisse werden als JSON-Dateien auf der EC2 Amazon-Instance gespeichert.
6. Die EC2 Amazon-Instance verwendet ein Python-Skript, um die JSON-Dateien zu verarbeiten, die Datenfelder zu extrahieren und einen CSV-Bericht zu erstellen.
7. Die EC2 Amazon-Instance lädt die CSV-Datei in den Amazon S3-Bucket hoch.
8. Eine EventBridge Amazon-Regel erkennt den Datei-Upload und verwendet ein Amazon SNS-Thema, um eine E-Mail zu senden, die den Benutzer darüber informiert, dass der Bericht abgeschlossen ist.
9. Der Benutzer lädt die CSV-Datei aus dem Amazon S3 S3-Bucket herunter. Der Benutzer importiert die Ergebnisse in die Excel-Vorlage und überprüft die Ergebnisse.

Option 2: Zugriff auf die Ergebnisse in AWS Security Hub

Das Diagramm zeigt den folgenden Prozess:

1. Wenn Sie die Lösung manuell ausführen, authentifiziert sich der Benutzer mit Session Manager bei der EC2 Amazon-Instance und führt dann das Skript naa-script.sh aus. Dieses Shell-Skript führt die Schritte 2—7 aus.

   Wenn Sie die Lösung automatisch ausführen, wird das Skript naa-script.sh automatisch nach dem Zeitplan gestartet, den Sie im Cron-Ausdruck definiert haben. Dieses Shell-Skript führt die Schritte 2 bis 7 aus. Weitere Informationen finden Sie unter Automatisierung und Skalierung am Ende dieses Abschnitts.

2. Die EC2 Amazon-Instance lädt die neueste Datei naa-exception.csv aus dem Amazon S3-Bucket herunter. Diese Datei wird später im Prozess verwendet, wenn das Python-Skript die Ausnahmen verarbeitet.
3. Die EC2 Amazon-Instance übernimmt die `NAAEC2Role` IAM-Rolle, die Berechtigungen für den Zugriff auf den Amazon S3-Bucket und für die Übernahme der `NAAExecRole` IAM-Rollen in den anderen Konten in der Organisation gewährt.
4. Die EC2 Amazon-Instance übernimmt die `NAAExecRole` IAM-Rolle im Verwaltungskonto der Organisation und generiert eine Liste der Konten in der Organisation.
5. Die EC2 Amazon-Instance übernimmt die `NAAExecRole` IAM-Rolle in den Mitgliedskonten der Organisation (im Architekturdiagramm als Workload-Konten bezeichnet) und führt für jedes Konto eine Sicherheitsbewertung durch. Die Ergebnisse werden als JSON-Dateien auf der EC2 Amazon-Instance gespeichert.
6. Die EC2 Amazon-Instance verwendet ein Python-Skript, um die JSON-Dateien zu verarbeiten und die Datenfelder für den Import in Security Hub zu extrahieren.
7. Die EC2 Amazon-Instance importiert die Ergebnisse von Network Access Analyzer in Security Hub.
8. Eine EventBridge Amazon-Regel erkennt den Import und verwendet ein Amazon SNS-Thema, um eine E-Mail zu senden, die den Benutzer darüber informiert, dass der Vorgang abgeschlossen ist.
9. Der Benutzer sieht sich die Ergebnisse im Security Hub an.

Automatisierung und Skalierung

Sie können diese Lösung so planen, dass das Skript naa-script.sh automatisch nach einem benutzerdefinierten Zeitplan ausgeführt wird. Um einen benutzerdefinierten Zeitplan festzulegen, ändern Sie in der CloudFormation Vorlage naa-resources.yaml den Parameter. `CronScheduleExpression` Der Standardwert von `0 0 * * 0` führt die Lösung beispielsweise jeden Sonntag um Mitternacht aus. Ein Wert von `0 0 * 1-12 0` würde die Lösung jeden ersten Sonntag im Monat um Mitternacht ausführen. Weitere Informationen zur Verwendung von Cron-Ausdrücken finden Sie unter Cron- und Rate-Ausdrücke in der Systems Manager Manager-Dokumentation.

Wenn Sie den Zeitplan nach der Bereitstellung des `NAA-Resources` Stacks anpassen möchten, können Sie den Cron-Zeitplan unter manuell bearbeiten. `/etc/cron.d/naa-schedule`

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS Lambda Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen. AWS-Konten
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Organizationsist ein Kontoverwaltungsservice, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie erstellen und zentral verwalten.
- AWS Security Hubbietet einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS. Es hilft Ihnen auch dabei, Ihre AWS Umgebung anhand von Industriestandards und Best Practices im Bereich Sicherheit zu überprüfen.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Systems Managerhilft Ihnen bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der AWS Cloud ausgeführt werden. Es vereinfacht das Anwendungs- und Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme und hilft Ihnen, Ihre AWS Ressourcen sicher und in großem Umfang zu verwalten. Dieses Muster verwendet Session Manager, eine Funktion von Systems Manager.

Code-Repository

Der Code für dieses Muster ist im GitHub Network Access Analyzer Multi-Account Analysis-Repository verfügbar. Das Code-Repository enthält die folgenden Dateien:

- naa-script.sh — Dieses Bash-Skript wird verwendet, um eine Network Access Analyzer-Analyse mehrerer AWS-Konten parallel zu starten. Wie in der CloudFormation Vorlage naa-resources.yaml definiert, wird dieses Skript automatisch im `/usr/local/naa` Ordner auf der Amazon-Instance bereitgestellt. EC2
- naa-resources.yaml — Sie verwenden diese CloudFormation Vorlage, um einen Stack im Sicherheitskonto der Organisation zu erstellen. Diese Vorlage stellt alle erforderlichen Ressourcen für dieses Konto bereit, um die Lösung zu unterstützen. Dieser Stack muss vor der Vorlage naa-execrole.yaml bereitgestellt werden.

> **Note**
>
> Wenn dieser Stack gelöscht und erneut bereitgestellt wird, müssen Sie den `NAAExecRole` Stacksatz neu erstellen, um die kontenübergreifenden Abhängigkeiten zwischen den IAM-Rollen wiederherzustellen.

- naa-execrole.yaml — Sie verwenden diese CloudFormation Vorlage, um ein Stack-Set zu erstellen, das die `NAAExecRole` IAM-Rolle in allen Konten der Organisation, einschließlich des Verwaltungskontos, bereitstellt.
- naa-processfindings.py — Das Skript naa-script.sh ruft dieses Python-Skript automatisch auf, um die JSON-Ausgaben von Network Access Analyzer zu verarbeiten, alle zweifelsfrei funktionierenden Ressourcen in der Datei naa-exclusions.csv auszuschließen und dann entweder eine CSV-Datei mit den konsolidierten Ergebnissen zu generieren oder die Ergebnisse in Security Hub zu importieren.

Epen

Bereite dich auf den Einsatz vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Code-Repo sitory.	1. Ändern Sie in einer Befehlszeilenschnittstelle Ihr Arbeitsverzeichnis in das Verzeichnis, in dem Sie die Beispieldateien speichern möchten.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Geben Sie den folgenden Befehl ein: `git clone https://github.com/aws-samples/network-access-analyzer-multi-account-analysis.git`	
Überprüfen Sie die Vorlagen.	1. Öffnen Sie im geklonten Repository die Dateien naa-resources.yaml und naa-execrole.yaml. 2. Überprüfen Sie die mit diesen Vorlagen erstellten Ressourcen und passen Sie die Vorlagen nach Bedarf an Ihre Umgebung an. Weitere Informationen finden Sie in der CloudFormation Dokumentation unter Arbeiten mit Vorlagen. 3. Speichern und schließen Sie die Dateien naa-resources.yaml und naa-execrole.yaml.	AWS DevOps

Erstellen Sie die CloudFormation Stapel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Ressourcen im Sicherheitskonto bereit.	Mithilfe der Vorlage naa-resources.yaml erstellen Sie einen	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CloudFormation Stack, der alle erforderlichen Ressourcen im Sicherheitskonto bereitstellt. Anweisungen finden Sie in der Dokumentation unter Einen Stack erstellen. CloudFormation Beachten Sie bei der Bereitstellung dieser Vorlage Folgendes: 1. Wählen Sie auf der Seite „Vorlage angeben“ die Option Vorlage ist bereit aus und laden Sie dann die Datei naa-resources.yaml hoch. 2. Geben Sie auf der Seite „Stack-Details angeben“ im Feld Stack-Name Folgendes ein. `NAA-Resources` 3. Geben Sie im Abschnitt Parameter Folgendes ein: • `VPCId`— Wählen Sie eine VPC im Konto aus. • `SubnetId`— Wählen Sie ein privates Subnetz mit Internetzugang aus. **Note** Wenn Sie ein öffentliches Subnetz auswählen,	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wird der EC2 Amazon-Instance möglicherweise keine öffentlic he IP-Adresse zugewiesen, da die CloudForm ation Vorlage standardmäßig keine Elastic IP-Adresse bereitste llt und anfügt. • `InstanceType` — Behalten Sie den Standard-Instance-Typ bei. • `InstanceImageId` — Behält die Standarde instellung bei. • `KeyPairName` — Wenn Sie SSH für den Zugriff verwenden, geben Sie den Namen eines vorhandenen key pair an. • `PermittedSSHInboun d` — Wenn Sie SSH für den Zugriff verwenden , geben Sie einen zulässigen CIDR-Block an. Wenn Sie SSH nicht verwenden, behalten Sie den Standardwert von bei. `127.0.0.1`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `BucketName` — Der Standardwert ist `naa-<accountID>-<region>` . Sie können dies nach Bedarf ändern. Wenn Sie einen benutzerdefinierten Wert angeben, werden die Konto-ID und die Region automatisch an den angegebenen Wert angehängt. • `EmailAddress` — Geben Sie eine E-Mail-Adresse für eine Amazon SNS SNS-Benachrichtigung an, wenn die Analyse abgeschlossen ist. **Note** Die Amazon SNS SNS-Abonnementkonfiguration muss vor Abschluss der Analyse bestätigt werden, andernfalls wird keine Benachrichtigung gesendet. • `NAAEC2Role` — Behalten Sie die Standardeinstellung	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bei, es sei denn, Ihre Benennungskonventionen erfordern einen anderen Namen für diese IAM-Rolle. • `NAAExecRole` — Behalten Sie die Standardeinstellung bei, es sei denn, bei der Bereitstellung von naa-execrole.yaml wird ein anderer Name verwendet • `Parallelism` — Geben Sie die Anzahl der parallel Prüfungen an, die durchgeführt werden sollen. • `Regions`— Geben Sie an AWS-Regionen , was Sie analysieren möchten. • `ScopeNameValue` — Geben Sie das Tag an, das dem Bereich zugewiesen werden soll. Dieses Tag wird verwendet, um den Netzwerkzugriffsbereich zu bestimmen. • `ExclusionFile` — Geben Sie den Namen der Ausschlussdatei an. Einträge in dieser Datei werden von den	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ergebnissen ausgeschl ossen. • `FindingsToCSV` — Geben Sie an, ob die Ergebnisse als CSV ausgegeben werden sollen. Zulässige Werte sind `true` und`false`. • `FindingsToSecurity Hub` — Geben Sie an, ob Ergebnisse in Security Hub importiert werden sollen. Zulässige Werte sind `true` und`false`. • `EmailNotifications ForSecurityHub` — Geben Sie an, ob beim Import von Ergebniss en in Security Hub E-Mail-Benachrichtigungen generiert werden sollen. Zulässige Werte sind `true` und`false`. • `Scheduled Analysis` — Wenn die Lösung automatisch nach einem Zeitplan ausgeführ t werden soll`true`, geben Sie den Zeitplan in den `CronScheduleExpres sion` Parameter ein und passen Sie ihn an. Wenn Sie die Lösung nicht automatisch ausführen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	möchten, geben Sie ein`false`. • `CronScheduleExpression` — Wenn Sie die Lösung automatisch ausführen, geben Sie einen Cron-Ausdruck ein, um den Zeitplan zu definieren. Weitere Informationen finden Sie unter Automatisierung und Skalierung im Abschnitt Architektur dieses Musters. 1. Wählen Sie auf der Seite Überprüfen die Option Die folgenden Ressourcen erfordern Fähigkeiten: [AWS::IAM::Role] und wählen Sie dann Stack erstellen aus. 2. Nachdem der Stack erfolgreich erstellt wurde, kopieren Sie in der CloudFormation Konsole auf der Registerkarte Outputs den `NAAEC2Role` Amazon-Ressourcennamen (ARN). Sie verwenden diesen ARN später, wenn Sie die Datei naa-execrole.yaml bereitstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die IAM-Rolle in den Mitgliedskonten bereit.	Verwenden Sie im AWS Organizations Verwaltungskonto oder einem Konto mit delegierten Administratorrechten für die Vorlage naa-execrole.yaml CloudFormation, um ein Stack-Set zu erstellen. CloudFormation Das Stack-Set stellt die `NAAExecRole` IAM-Rolle in allen Mitgliedskonten der Organisation bereit. Anweisungen finden Sie in der Dokumentation unter Erstellen eines Stack-Sets mit vom Service verwalteten Berechtigungen. CloudFormation Beachten Sie bei der Bereitstellung dieser Vorlage Folgendes: 1. Wählen Sie unter Vorlage vorbereiten die Option Vorlage ist bereit aus und laden Sie dann die Datei naa-execrole.yaml hoch. 2. Geben Sie auf der Seite „StackSet Details angeben“ dem Stack-Set einen Namen. `NAA-ExecRole` 3. Geben Sie im Abschnitt Parameter Folgendes ein: • `AuthorizedARN` — Geben Sie den `NAAEC2Role` ARN ein,	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den Sie bei der Erstellung des `NAA-Resources` Stacks kopiert haben. • `NAARoleName` — Behalten Sie den Standardwert von bei, `NAAExecRole` sofern bei der Bereitstellung der Datei naa-resources.yaml kein anderer Name verwendet wurde. 4. Wählen Sie unter Permissions (Berechtigungen) die Option Service-managed permissions (Servicev erwaltete Berechtigungen) aus. 5. Wählen Sie auf der Seite Bereitstellungsoptionen festlegen unter Bereitstellungsziele die Option Für die Organisation bereitstellen aus und akzeptieren Sie alle Standardeinstellungen. **Note** Wenn Sie möchten, dass die Stacks für alle Mitgliedskonten gleichzeitig bereitgestellt werden, legen Sie „Maximale	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anzahl gleichzeitiger Konten“ und „Fehlertoleranz“ auf einen hohen Wert fest, z. B. `100` 6. Wählen Sie unter Bereitstellungsregionen die Region aus, in der die EC2 Amazon-Instance für Network Access Analyzer bereitgestellt wird. Da es sich bei den IAM-Ressourcen um globale und nicht um regionale Ressourcen handelt, wird dadurch die IAM-Rolle in allen aktiven Regionen bereitgestellt. 7. Wählen Sie auf der Seite Überprüfen die Option Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen mit benutzerdefinierten Namen erstellt werden, und wählen Sie dann Erstellen aus. StackSet 8. Überwachen Sie die Registerkarte Stack-Instances (für den Status einzelner Konten) und die Registerkarte Operationen (für den Gesamtstatus), um festzustellen, wann die	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bereitstellung abgeschlossen ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die IAM-Rolle im Verwaltungskonto bereit.	Mithilfe der Vorlage naa-execrole.yaml erstellen Sie einen CloudFormation Stack, der die `NAAExecRole` IAM-Rolle im Verwaltungskonto der Organisation bereitstellt. Das StackSet, das Sie zuvor erstellt haben, stellt die IAM-Rolle nicht im Verwaltungskonto bereit. Anweisungen finden Sie in der CloudFormation Dokumentation unter Einen Stack erstellen. Beachten Sie bei der Bereitstellung dieser Vorlage Folgendes: 1. Wählen Sie auf der Seite „Vorlage angeben“ die Option Vorlage ist bereit aus und laden Sie dann die Datei naa-execrole.yaml hoch. 2. Geben Sie auf der Seite „Stack-Details angeben“ im Feld Stackname Folgendes ein. `NAA-ExecRole` 3. Geben Sie im Abschnitt Parameter Folgendes ein: • `AuthorizedARN` — Geben Sie den `NAAEC2Role` ARN ein, den Sie bei der Erstellun	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	g des `NAA-Resources` Stacks kopiert haben. • `NAARoleName` — Behalten Sie den Standardwert von bei, `NAAExecRole` sofern bei der Bereitstellung der Datei naa-resources.yaml kein anderer Name verwendet wurde. 4. Wählen Sie auf der Seite Überprüfen die Option Die folgenden Ressourcen erfordern Fähigkeiten: [AWS::IAM::Role] und wählen Sie dann Create Stack aus.	

Führen Sie die Analyse durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie das Shell-Skript an.	1. Melden Sie sich mit dem Sicherheitskonto in der Organisation an. 2. Stellen Sie mithilfe von Session Manager eine Verbindung zu der EC2 Amazon-Instance für Network Access Analyzer her, die Sie zuvor bereitgestellt haben. Anweisungen finden Sie unter Connect zu Ihrer Linux-Instance mithilfe	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	von Session Manager. Wenn Sie keine Verbindung herstellen können, lesen Sie den Abschnitt zur Fehlerbehebung in diesem Muster.
	3. Geben Sie die folgenden Befehle ein, um die Datei naa-script.sh zur Bearbeitung zu öffnen:
	`sudo -i`
	`cd /usr/local/naa`
	`vi naa-script.sh`
	4. Überprüfen und ändern Sie die einstellbaren Parameter und Variablen in diesem Skript nach Bedarf für Ihre Umgebung. Weitere Informationen zu Anpassungsoptionen finden Sie in den Kommentaren am Anfang des Skripts.
	Anstatt beispielsweise eine Liste aller Mitglieds konten in der Organisation aus dem Verwaltungskonto abzurufen, können Sie das Skript ändern, um das AWS-Konto IDs oder anzugeben, AWS-Regionen das Sie scannen möchten, oder Sie können auf eine	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	externe Datei verweisen, die diese Parameter enthält. 5. Speichern und schließen Sie die Datei naa-script.sh.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Analysieren Sie die Zielkonten.	1. Geben Sie die folgenden Befehle ein. Dadurch wird das Skript naa-script.sh ausgeführt:
	`sudo -i`
	`cd /usr/local/naa`
	`screen`
	`./naa-script.sh`
	Beachten Sie Folgendes:
	• Der `screen` Befehl ermöglicht die weitere Ausführung des Skripts für den Fall, dass die Verbindung unterbrochen wird oder Sie den Konsolenzugriff verlieren.
	• Nach dem Start des Scans können Sie das Trennen des Bildschirms erzwingen, indem Sie Strg+A D drücken. Der Bildschirm wird getrennt, und Sie können die Instanzverbindung schließen, während die Analyse fortgesetzt wird.
	• Um eine getrennte Sitzung wieder aufzunehmen, stellen Sie eine Verbindung zur Instanz her, geben Sie ein und geben Sie `sudo`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`-i` dann die Eingabetaste ein`screen -r`. 2. Überwachen Sie die Ausgabe auf Fehler, um sicherzustellen, dass das Skript ordnungsg emäß funktioniert. Eine Beispielausgabe finden Sie im Abschnitt Zusätzlic he Informationen dieses Musters. 3. Warten Sie, bis die Analyse abgeschlossen ist. Wenn Sie E-Mail-Benachricht igungen konfiguriert haben, erhalten Sie eine E-Mail, wenn die Ergebnisse in den Amazon S3 S3-Bucket hochgeladen oder in Security Hub importiert wurden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 1 — Rufen Sie die Ergebnisse aus dem Amazon S3 S3-Bucket ab.	1. Laden Sie die CSV-Datei aus dem `naa-<accountID>-<region>` Bucket herunter. Anweisungen finden Sie in der Amazon S3 S3-Dokumentation unter Objekt herunterladen. 2. Löschen Sie die CSV-Datei aus dem Amazon S3 S3-Bucket. Dies ist eine bewährte Methode zur Kostenoptimierung. Anweisungen finden Sie in der Amazon S3 S3-Dokumentation unter Objekte löschen.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 2 — Überprüfen Sie die Ergebnisse in Security Hub.	1. Öffnen Sie die Security Hub Hub-Konsole. 2. Wählen Sie im Navigationsbereich Findings aus. 3. Überprüfen Sie die Ergebnisse von Network Access Analyzer. Anweisungen finden Sie in der Security Hub Hub-Dokumentation unter Ergebnislisten und Details anzeigen. **Note** Sie können nach Ergebnissen suchen, indem Sie einen Titel, der mit einem Filter beginnt, hinzufügen und eingeben `Network Access Analyzer`.	AWS DevOps

Ergebnisse korrigieren und ausschließen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Korrigieren Sie die Ergebnisse.	Korrigieren Sie alle Ergebnisse, die Sie korrigieren möchten. Weitere Informationen und	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bewährte Methoden zur Einrichtung eines Perimeters rund um Ihre AWS Identitäten, Ressourcen und Netzwerke finden Sie unter Building a data perimeter on AWS (Whitepaper).AWS	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schließen Sie Ressourcen mit zweifelsfrei funktionierenden Netzwerkpfaden aus.	Wenn Network Access Analyzer Ergebnisse für Ressourcen generiert, auf die über das Internet zugegriff en werden sollte, können Sie diese Ressourcen zu einer Ausschlussliste hinzufüge n. Wenn Network Access Analyzer das nächste Mal ausgeführt wird, wird kein Ergebnis für diese Ressource generiert. 1. Navigieren Sie zu dem Skript naa-script.sh **`/usr/local/naa`** , und öffnen Sie es. Notieren Sie sich den Wert der `S3_EXCLUSION_FILE` Variablen. 2. Wenn der Wert der `S3_EXCLUSION_FILE` Variablen ist `true`, laden Sie die Datei naa-exclu sions.csv aus dem `naa-<accountID>-<region>` Bucket herunter. Anweisungen finden Sie in der Amazon S3 S3-Dokumentation unter Objekt herunterladen. Wenn der Wert der `S3_EXCLUSION_FILE` Variablen lautet `false`, navigieren Sie zu der Datei	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	naa-exclusions.csv **`/usr/local/naa`** und öffnen Sie sie. **Note** Wenn der Wert der `S3_EXCLUSION_FILE` Variablen lautet`false`, verwendet das Skript eine lokale Version der Ausschlussdatei. Wenn Sie den Wert später auf ändern`true`, überschreibt das Skript die lokale Version mit der Datei im Amazon S3 S3-Bucket. 3. Geben Sie in der Datei naa-exclusions.csv die Ressourcen ein, die Sie ausschließen möchten. Geben Sie in jeder Zeile eine Ressource ein, und verwenden Sie das folgende Format. `<resource_id>,<secgroup_id>,<sgrule_`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`cidr>,<sgrule_port range>,<sgrule_pro tocol>`
	
	Im Folgenden finden Sie ein Beispiel für eine Ressource.
	
	`eni-1111aaaaa2222b bbb,sg-3333cccc44 44dddd,0.0.0.0/0,8 0 to 80,tcp`
	4. Speichern und schließen Sie die Datei naa-exclu sions.csv.
	5. Wenn Sie die Datei naa-exclusions.csv aus dem Amazon S3 S3-Bucket heruntergeladen haben, laden Sie die neue Version hoch. Anweisungen finden Sie unter Objekte hochladen in der Amazon S3 S3-Dokumentation.	

(Optional) Aktualisieren Sie das Skript naa-script.sh

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie das Skript naa-script.sh.	Wenn Sie das Skript naa-scrip t.sh auf die neueste Version im Repository aktualisieren möchten, gehen Sie wie folgt vor:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	1. Stellen Sie mithilfe des Session Managers eine Connect zur EC2 Amazon-Instance her. Anweisungen finden Sie unter Connect zu Ihrer Linux-Instance mithilfe von Session Manager.
	2. Geben Sie den folgenden Befehl ein:
	`sudo -i`
	3. Navigieren Sie zum Skriptverzeichnis naa-script.sh:
	`cd /usr/local/naa`
	4. Geben Sie den folgenden Befehl ein, um das lokale Skript zu speichern, sodass Sie benutzerdefinierte Änderungen in der neuesten Version zusammenführen können:
	`git stash`
	5. Geben Sie den folgenden Befehl ein, um die neueste Version des Skripts abzurufen:
	`git pull`
	6. Geben Sie den folgenden Befehl ein, um das	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	benutzerdefinierte Skript mit der neuesten Version des Skripts zusammenzuführen: `git stash pop`	

(Optional) Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie alle bereitgestellten Ressourcen.	Sie können die bereitgestellten Ressourcen in den Konten belassen. Wenn Sie die Bereitstellung aller Ressourcen aufheben möchten, gehen Sie wie folgt vor: 1. Löschen Sie den `NAA-ExecRole` Stack, der im Verwaltungskonto bereitgestellt wurde. Anweisungen finden Sie in der CloudFormation Dokumentation unter Löschen eines Stacks. 2. Löschen Sie das `NAA-ExecRole` Stack-Set, das im Verwaltungskonto der Organisation oder im delegierten Administratorkonto bereitgestellt wurde. Anweisungen finden Sie in der Dokumentation	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	unter Löschen eines Stack-Sets. CloudFormation 3. Löschen Sie alle Objekte im `naa-<accountID>-<region>` Amazon S3 S3-Bucket. Anweisungen finden Sie in der Amazon S3 S3-Dokumentation unter Objekte löschen. 4. Löschen Sie den `NAA-Resources` Stack, der im Sicherheitskonto bereitgestellt wurde. Anweisungen finden Sie in der CloudFormation Dokumentation unter Löschen eines Stacks.	

Fehlerbehebung

Problem	Lösung
Es konnte keine Verbindung mit der EC2 Amazon-Instance mithilfe des Sitzungsmanagers hergestellt werden.	Der SSM-Agent muss in der Lage sein, mit dem Systems Manager Manager-Endpunkt zu kommunizieren. Gehen Sie wie folgt vor: 1. Stellen Sie sicher, dass das Subnetz, in dem die EC2 Amazon-Instance bereitgestellt wird, über Internetzugang verfügt. 2. Starten Sie die EC2 Amazon-Instance neu.
Bei der Bereitstellung des Stack-Sets werden Sie von der CloudFormation Konsole dazu aufgefordert. `Enable trusted access`	Dies weist darauf hin, dass der vertrauen swürdige Zugriff zwischen AWS Organizations und CloudFormation nicht aktiviert wurde. Für die Bereitstellung des vom Service verwaltet

Problem	Lösung
`with AWS Organizations to use service-managed permissions`	en Stack-Sets ist ein vertrauenswürdiger Zugriff erforderlich. Wählen Sie die Schaltfläche, um den vertrauenswürdigen Zugriff zu aktivieren. Weitere Informationen finden Sie in der CloudFormation Dokumentation unter Vertrauenswürdigen Zugriff aktivieren.

Zugehörige Ressourcen

- Neu — Amazon VPC Network Access Analyzer (AWS Blogbeitrag)
- AWS re:INFORCE 2022 — Validieren Sie effektive Netzwerkzugriffskontrollen auf AWS (NIS202) (Video)
- Demo — Unternehmensweite Analyse von eingehenden Internetdaten mithilfe des Network Access Analyzer (Video)

Zusätzliche Informationen

Beispiel für eine Konsolenausgabe

Das folgende Beispiel zeigt die Ausgabe der Generierung der Liste der Zielkonten und der Analyse der Zielkonten.

```
[root@ip-10-10-43-82 naa]# ./naa-script.sh
download: s3://naa-<account ID>-us-east-1/naa-exclusions.csv to ./naa-exclusions.csv

AWS Management Account: <Management account ID>

AWS Accounts being processed...
<Account ID 1> <Account ID 2> <Account ID 3>

Assessing AWS Account: <Account ID 1>, using Role: NAAExecRole
Assessing AWS Account: <Account ID 2>, using Role: NAAExecRole
Assessing AWS Account: <Account ID 3>, using Role: NAAExecRole
Processing account: <Account ID 1> / Region: us-east-1
Account: <Account ID 1> / Region: us-east-1 - Detecting Network Analyzer scope...
Processing account: <Account ID 2> / Region: us-east-1
Account: <Account ID 2> / Region: us-east-1 - Detecting Network Analyzer scope...
```

```
Processing account: <Account ID 3> / Region: us-east-1
Account: <Account ID 3> / Region: us-east-1 - Detecting Network Analyzer scope...
Account: <Account ID 1> / Region: us-east-1 - Network Access Analyzer scope detected.
Account: <Account ID 1> / Region: us-east-1 - Continuing analyses with Scope ID.
 Accounts with many resources may take up to one hour
Account: <Account ID 2> / Region: us-east-1 - Network Access Analyzer scope detected.
Account: <Account ID 2> / Region: us-east-1 - Continuing analyses with Scope ID.
 Accounts with many resources may take up to one hour
Account: <Account ID 3> / Region: us-east-1 - Network Access Analyzer scope detected.
Account: <Account ID 3> / Region: us-east-1 - Continuing analyses with Scope ID.
 Accounts with many resources may take up to one hour
```

Beispiele für CSV-Berichte

Die folgenden Bilder sind Beispiele für die CSV-Ausgabe.

Richten Sie die DNS-Auflösung für Hybridnetzwerke in einer Umgebung mit mehreren Konten AWS ein

Erstellt von Anvesh Koganti (AWS)

Übersicht

Dieses Muster bietet eine umfassende Lösung für die Einrichtung der DNS-Auflösung in hybriden Netzwerkumgebungen, die mehrere Amazon Web Services (AWS) -Konten umfassen. Es ermöglicht die bidirektionale DNS-Auflösung zwischen lokalen Netzwerken und der AWS Umgebung über Amazon Route 53 Resolver Endpunkte. Das Muster bietet zwei Lösungen, um die DNS-Auflösung in einer zentralisierten Architektur mit mehreren Konten zu ermöglichen:

- Bei der Grundkonfiguration werden keine Route 53 53-Profile verwendet. Es hilft, die Kosten für kleine bis mittlere Bereitstellungen mit geringerer Komplexität zu optimieren.
- Das erweiterte Setup verwendet Route 53 53-Profile, um den Betrieb zu vereinfachen. Es eignet sich am besten für größere oder komplexere DNS-Bereitstellungen.

> **Note**
>
> Informieren Sie sich vor der Implementierung im Abschnitt Einschränkungen über Diensteinschränkungen und Kontingente. Berücksichtigen Sie bei Ihrer Entscheidung Faktoren wie Verwaltungsaufwand, Kosten, betriebliche Komplexität und Teamkompetenz.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Umgebung mit AWS mehreren Konten mit Amazon Virtual Private Cloud (Amazon VPC), die für Shared Services- und Workload-Konten bereitgestellt wird (vorzugsweise über AWS Control Tower eingerichtet, wobei AWS bewährte Methoden für die Kontostruktur befolgt werden).
- Bestehende hybride Konnektivität (AWS Direct Connect oder AWS Site-to-Site VPN) zwischen Ihrem lokalen Netzwerk und der Umgebung. AWS
- Amazon VPC-Peering oder AWS Cloud WAN für Layer-3-Netzwerkkonnektivität zwischen. AWS Transit Gateway VPCs (Diese Konnektivität ist für den Anwendungsdatenverkehr erforderlich.

Sie ist nicht erforderlich, damit die DNS-Auflösung funktioniert. Die DNS-Auflösung funktioniert unabhängig von der Netzwerkkonnektivität zwischen den VPCs.)

- DNS-Server, die in der lokalen Umgebung ausgeführt werden.

Einschränkungen

- Die Endpunkte, Regeln und Profile von Route 53 Resolver sind regionale Konstrukte und erfordern für globale Organisationen möglicherweise mehrere AWS-Regionen Replikationen.
- Eine umfassende Liste der Dienstkontingente für Route 53 Resolver, private gehostete Zonen und Profile finden Sie in der Route 53-Dokumentation unter Kontingente.

Architektur

Zieltechnologie-Stack

- Routet 53 ausgehende und eingehende Endpunkte
- Route 53 Resolver-Regeln für die bedingte Weiterleitung
- AWS Resource Access Manager (AWS RAM)
- Private gehostete Zone von Route 53

Zielarchitektur

Endpunkte für ausgehenden und eingehenden Datenverkehr

Das folgende Diagramm zeigt den DNS-Auflösungsfluss von AWS zu vor Ort. Dies ist das Konnektivitäts-Setup für ausgehende Auflösungen, bei denen die Domäne lokal gehostet wird. Im Folgenden finden Sie einen allgemeinen Überblick über den Prozess, der bei der Einrichtung erforderlich ist. Einzelheiten finden Sie im Abschnitt Epics.

1. Stellen Sie ausgehende Route 53-Resolver-Endpunkte in der Shared Services-VPC bereit.
2. Erstellen Sie Route 53 Resolver-Regeln (Weiterleitungsregeln) im Shared Services-Konto für Domänen, die lokal gehostet werden.
3. Teilen und verknüpfen Sie die Regeln mit VPCs anderen Konten, die Ressourcen hosten, die für die Auflösung lokal gehosteter Domänen erforderlich sind. Dies kann je nach Anwendungsfall auf unterschiedliche Weise geschehen, wie später in diesem Abschnitt beschrieben wird.

Nachdem Sie die Konnektivität eingerichtet haben, sind die folgenden Schritte für die Lösung ausgehender Nachrichten erforderlich:

1. Die Amazon Elastic Compute Cloud (Amazon EC2) -Instance sendet eine DNS-Auflösungsanfrage `db.onprem.example.com` an den Route 53-Resolver der VPC an der VPC+2-Adresse.
2. Route 53 Resolver überprüft die Resolver-Regeln und leitet die Anfrage mithilfe des ausgehenden Endpunkts an den lokalen DNS-Server weiter. IPs
3. Der ausgehende Endpunkt leitet die Anfrage an den lokalen DNS weiter. IPs Der Datenverkehr wird über die etablierte hybride Netzwerkkonnektivität zwischen der Shared Services-VPC und dem lokalen Rechenzentrum übertragen.
4. Der lokale DNS-Server antwortet auf den ausgehenden Endpunkt, der die Antwort dann zurück an den Route 53-Resolver der VPC weiterleitet. Der Resolver gibt die Antwort an die Instanz zurück. EC2

Das nächste Diagramm zeigt den DNS-Auflösungsfluss von der lokalen Umgebung zur. AWS Dies ist das Konnektivitäts-Setup für eingehende Auflösungen, auf denen die Domain gehostet wird. AWS Hier finden Sie einen allgemeinen Überblick über den Prozess, der bei der Einrichtung erforderlich ist. Einzelheiten finden Sie im Abschnitt Epics.

1. Stellen Sie Resolver-Endpoints für eingehende Anfragen in der Shared Services-VPC bereit.
2. Erstellen Sie private gehostete Zonen im Shared Services-Konto (zentralisierter Ansatz).
3. Ordnen Sie die privat gehosteten Zonen der Shared Services-VPC zu. Teilen Sie diese Zonen und ordnen Sie sie VPCs für die VPC-to-VPC DNS-Auflösung kontoübergreifend zu. Dies kann je nach Anwendungsfall auf unterschiedliche Weise geschehen, wie später in diesem Abschnitt beschrieben wird.

Nachdem Sie die Konnektivität eingerichtet haben, sind die folgenden Schritte für die Auflösung eingehender E-Mails erforderlich:

1. Die lokale Ressource sendet eine DNS-Auflösungsanforderung für `ec2.prod.aws.example.com` an den lokalen DNS-Server.
2. Der lokale DNS-Server leitet die Anfrage über die hybride Netzwerkverbindung an den eingehenden Resolver-Endpunkt in der Shared Services-VPC weiter.

3. Der eingehende Resolver-Endpunkt sucht mithilfe des VPC Route 53 Resolvers nach der Anfrage in der zugehörigen privaten gehosteten Zone und erhält die entsprechende IP-Adresse.
4. Diese IP-Adressen werden an den lokalen DNS-Server zurückgesendet, der die Antwort an die lokale Ressource zurückgibt.

Diese Konfiguration ermöglicht es lokalen Ressourcen, AWS private Domainnamen aufzulösen, indem sie Abfragen über die eingehenden Endpunkte an die entsprechende private gehostete Zone weiterleiten. In dieser Architektur sind private gehostete Zonen in einer Shared Services-VPC zentralisiert, was eine zentrale DNS-Verwaltung durch ein einzelnes Team ermöglicht. Diese Zonen können vielen Zonen zugeordnet werden VPCs , um den Anwendungsfall der VPC-to-VPC DNS-Auflösung zu lösen. Alternativ können Sie den Besitz und die Verwaltung der DNS-Domäne an beide delegieren. AWS-Konto In diesem Fall verwaltet jedes Konto seine eigenen privaten gehosteten Zonen und ordnet jede Zone der zentralen Shared Services-VPC zu, um eine einheitliche Lösung mit der lokalen Umgebung zu erreichen. Dieser dezentrale Ansatz würde den Rahmen dieses Musters sprengen. Weitere Informationen finden Sie unter Skalierung der DNS-Verwaltung auf mehrere Konten und VPCs im Whitepaper Hybrid Cloud DNS-Optionen für Amazon VPC.

Wenn Sie die grundlegenden DNS-Auflösungsabläufe mithilfe von Resolver-Endpunkten einrichten, müssen Sie festlegen, wie Sie die gemeinsame Nutzung und Zuordnung von Resolver-Regeln und privaten Hosting-Zonen in Ihrem System verwalten. AWS-Konten Sie können dies auf zwei Arten angehen: durch selbstverwaltetes Teilen, indem AWS RAM Sie Resolver-Regeln und direkte private Hosting-Zonenzuordnungen verwenden, wie im Abschnitt Grundeinstellungen beschrieben, oder über Route 53 53-Profile, wie im Abschnitt Erweiterte Konfiguration beschrieben. Die Wahl hängt von den DNS-Verwaltungseinstellungen und den betrieblichen Anforderungen Ihres Unternehmens ab. Die folgenden Architekturdiagramme veranschaulichen eine skalierte Umgebung, die mehrere VPCs verschiedene Konten umfasst, was einer typischen Unternehmensumgebung entspricht.

Grundlegende Einrichtung

In der Grundkonfiguration werden bei der Implementierung der Hybrid-DNS-Auflösung in einer AWS Umgebung mit mehreren Konten Resolver-Weiterleitungsregeln und private Hosting-Zonenzuordnungen gemeinsam genutzt AWS RAM , um DNS-Abfragen zwischen lokalen Standorten und Ressourcen zu verwalten. AWS Bei dieser Methode werden zentralisierte Route 53 Resolver-Endpunkte in einer Shared Services-VPC verwendet, die mit Ihrem lokalen Netzwerk verbunden ist, um sowohl eingehende als auch ausgehende DNS-Auflösungen effizient zu handhaben.

- Für die Auflösung ausgehender Nachrichten werden Resolver-Weiterleitungsregeln im Shared Services-Konto erstellt und dann mit anderen Benutzern gemeinsam genutzt. AWS-Konten AWS

RAM Diese gemeinsame Nutzung ist auf Konten innerhalb derselben Region beschränkt. Die Zielkonten können diese Regeln dann ihren eigenen zuordnen VPCs und den Ressourcen in diesen Regeln ermöglichen VPCs , lokale Domainnamen aufzulösen.

- Für die eingehende Auflösung werden private Hosting-Zonen im Shared Services-Konto erstellt und der Shared Services-VPC zugeordnet. Diese Zonen können dann mithilfe VPCs der Route 53-API oder der AWS Command Line Interface ()AWS CLI anderen Konten zugeordnet werden. AWS SDKs Die zugewiesenen Ressourcen VPCs können dann DNS-Einträge auflösen, die in den privaten gehosteten Zonen definiert sind, wodurch eine einheitliche DNS-Ansicht in Ihrer gesamten AWS Umgebung entsteht.

Das folgende Diagramm zeigt die DNS-Auflösungsflüsse in dieser Basiskonfiguration.

Dieses Setup funktioniert gut, wenn Sie in begrenztem Umfang mit einer DNS-Infrastruktur arbeiten. Die Verwaltung kann jedoch schwierig werden, wenn Ihre Umgebung wächst. Der betriebliche Aufwand für die Verwaltung der gemeinsamen Nutzung und Zuordnung von Regeln für private gehostete Zonen und Resolver nimmt mit VPCs der Skalierung erheblich zu. Darüber hinaus können Dienstkontingente wie das Zuweisungslimit von 300 VPC pro privat gehosteter Zone bei groß angelegten Bereitstellungen zu einschränkenden Faktoren werden. Das verbesserte Setup bewältigt diese Herausforderungen.

Verbessertes Setup

Route 53 53-Profile bieten eine optimierte Lösung für die Verwaltung der DNS-Auflösung in hybriden Netzwerken über mehrere AWS-Konten Netzwerke hinweg. Anstatt private Hosting-Zonen und Resolver-Regeln einzeln zu verwalten, können Sie DNS-Konfigurationen in einem einzigen Container gruppieren, der problemlos gemeinsam genutzt und auf mehrere Konten in einer VPCs Region angewendet werden kann. Dieses Setup behält die zentralisierte Resolver-Endpunktarchitektur in einer Shared Services-VPC bei und vereinfacht gleichzeitig die Verwaltung von DNS-Konfigurationen erheblich.

Das folgende Diagramm zeigt DNS-Auflösungsflüsse in einer erweiterten Konfiguration.

Mit Route 53 53-Profilen können Sie private Hosting-Zonenzuordnungen, Resolver-Weiterleitungsregeln und DNS-Firewallregeln in einer einzigen, gemeinsam nutzbaren Einheit zusammenfassen. Sie können Profile im Shared Services-Konto erstellen und sie mit Mitgliedskonten teilen, indem Sie AWS RAM Wenn ein Profil geteilt und auf Target angewendet wird VPCs, werden

alle erforderlichen Verknüpfungen und Konfigurationen automatisch vom Dienst verarbeitet. Dadurch wird der betriebliche Aufwand für die DNS-Verwaltung erheblich reduziert und eine hervorragende Skalierbarkeit für wachsende Umgebungen gewährleistet.

Automatisierung und Skalierung

Verwenden Sie Infrastructure-as-Code-Tools (IaC) wie AWS CloudFormation oder Terraform, um Route 53 Resolver-Endpunkte, Regeln, private gehostete Zonen und Profile automatisch bereitzustellen und zu verwalten. Integrieren Sie die DNS-Konfiguration in CI/CD-Pipelines (Continuous Integration and Continuous Delivery), um Konsistenz, Wiederholbarkeit und schnelle Updates zu gewährleisten.

Tools

AWS-Services

- AWS Resource Access Manager (AWS RAM) hilft Ihnen dabei, Ihre Ressourcen sicher gemeinsam zu nutzen, um den betrieblichen Aufwand AWS-Konten zu reduzieren und für Transparenz und Überprüfbarkeit zu sorgen.
- Amazon Route 53 Resolverreagiert rekursiv auf DNS-Abfragen von AWS Ressourcen und ist standardmäßig in allen verfügbar. VPCs Sie können Resolver-Endpunkte und Regeln für bedingte Weiterleitungen erstellen, um DNS-Namespaces zwischen Ihrem lokalen Rechenzentrum und Ihrem aufzulösen. VPCs
- Die private gehostete Zone von Amazon Route 53 ist ein Container, der Informationen darüber enthält, wie Route 53 auf DNS-Anfragen für eine Domain und deren Subdomains reagieren soll.
- Mit Amazon Route 53 53-Profilen können Sie DNS-bezogene Route 53-Konfigurationen für viele VPCs und unterschiedliche AWS-Konten Konfigurationen auf vereinfachte Weise anwenden und verwalten.

Bewährte Methoden

Dieser Abschnitt enthält einige der bewährten Methoden zur Optimierung von Route 53 Resolver. Diese stellen einen Teil der bewährten Methoden für Route 53 dar. Eine umfassende Liste finden Sie unter Bewährte Methoden für Amazon Route 53.

Vermeiden Sie Loop-Konfigurationen mit Resolver-Endpunkten

- Entwerfen Sie Ihre DNS-Architektur so, dass rekursives Routing verhindert wird, indem Sie VPC-Zuordnungen sorgfältig planen. Wenn eine VPC einen eingehenden Endpunkt hostet, vermeiden Sie es, ihn mit Resolver-Regeln zu verknüpfen, die Zirkelverweise erzeugen könnten.
- Verwenden Sie diese AWS RAM Option strategisch, wenn Sie DNS-Ressourcen für mehrere Konten gemeinsam nutzen, um saubere Routingpfade aufrechtzuerhalten.

Weitere Informationen finden Sie in der Route 53-Dokumentation unter Vermeiden von Schleifenkonfigurationen mit Resolver-Endpunkten.

Skalieren Sie Resolver-Endpunkte

- Beachten Sie bei Umgebungen, die eine hohe Anzahl von Abfragen pro Sekunde (QPS) erfordern, dass auf einem Endpunkt ein Limit von 10.000 QPS pro ENI gilt. Einem Endpunkt ENIs können weitere hinzugefügt werden, um DNS QPS zu skalieren.
- Amazon CloudWatch stellt `InboundQueryVolume` `OutboundQueryVolume` Metriken zur Verfügung (siehe CloudWatch Dokumentation). Wir empfehlen Ihnen, Überwachungsregeln einzurichten, die Sie benachrichtigen, wenn der Schwellenwert einen bestimmten Wert überschreitet (z. B. 80 Prozent von 10.000 QPS).
- Konfigurieren Sie statusbehaftete Sicherheitsgruppenregeln für Resolver-Endpunkte, um zu verhindern, dass Grenzwerte für die Verbindungsverfolgung bei hohem Datenvolumen zu einer Drosselung von DNS-Abfragen führen. Weitere Informationen darüber, wie die Verbindungsverfolgung in Sicherheitsgruppen funktioniert, finden Sie unter Amazon EC2 Security Group Connection Tracking in der EC2 Amazon-Dokumentation.

Weitere Informationen finden Sie unter Resolver Endpoint Scaling in der Route 53-Dokumentation.

Stellen Sie eine hohe Verfügbarkeit für Resolver-Endpunkte bereit

- Erstellen Sie aus Redundanzgründen eingehende Endpunkte mit IP-Adressen in mindestens zwei Availability Zones.
- Stellen Sie zusätzliche Netzwerkschnittstellen bereit, um die Verfügbarkeit bei Wartungsarbeiten oder bei hohem Datenaufkommen sicherzustellen.

Weitere Informationen finden Sie unter Hochverfügbarkeit für Resolver-Endpunkte in der Route 53-Dokumentation.

Epen

Stellen Sie Route 53 Resolver-Endpunkte bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie einen Endpunkt für eingehenden Datenverkehr bereit.	Route 53 Resolver verwendet den eingehenden Endpunkt, um DNS-Anfragen von lokalen DNS-Resolvern zu empfangen . Anweisungen finden Sie in der Route 53-Dokumentation unter Weiterleiten eingehender DNS-Abfragen VPCs an Ihren. Notieren Sie sich die IP-Adresse des eingehenden Endpunkts.	AWS-Administrator, Cloud-Administrator
Stellen Sie einen ausgehenden Endpunkt bereit.	Route 53 Resolver verwendet den ausgehenden Endpunkt, um DNS-Abfragen an lokale DNS-Resolver zu senden. Anweisungen finden Sie in der Route 53-Dokumentation unter Weiterleiten ausgehender DNS-Abfragen an Ihr Netzwerk. Notieren Sie sich die ID des Ausgabeendpunkts.	AWS-Administrator, Cloud-Administrator

Private Hosting-Zonen von Route 53 konfigurieren und gemeinsam nutzen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine private Hosting-Zone für eine Domain, die auf gehostet wird AWS.	Diese Zone enthält die DNS-Einträge für Ressourcen in einer AWS-gehosteten Domäne (z. B.`prod.aws.`	AWS-Administrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`example.com`), die von der lokalen Umgebung aus aufgelöst werden sollten. Anweisungen finden Sie in der Route 53-Dokumentation unter Erstellen einer privaten gehosteten Zone. Wenn Sie eine private gehostete Zone erstellen, müssen Sie der Hosting-Zone, die demselben Konto gehört, eine VPC zuordnen. Wählen Sie die Shared Services-VPC für diesen Zweck aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Grundlegende Einrichtung: Ordnen Sie die privat gehostete VPCs Zone anderen Konten zu.	Wenn Sie die Basiskonfiguration verwenden (siehe Abschnitt Architektur): Damit Ressourcen im Mitgliedskonto VPCs DNS-Einträge in dieser privaten Hosting-Zone auflösen können, müssen Sie Ihre VPCs mit der Hosting-Zone verknüpfen. Sie müssen die Zuordnung autorisieren und die Zuordnung dann programmgesteuert vornehmen. Anweisungen finden Sie in der Route 53-Dokumentation unter Zuordnen einer Amazon-VPC und einer privaten gehosteten Zone, die Sie mit different AWS-Konten erstellt haben.	AWS-Administrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verbessertes Setup: Konfiguration und gemeinsame Nutzung von Route 53 53-Profilen.	Wenn Sie das erweiterte Setup verwenden (siehe Abschnitt Architektur): 1. Erstellen Sie ein Route 53-Profil und ordnen Sie ihm die entsprechenden privaten Hosting-Zonen zu. Anweisungen finden Sie in der Route 53 53-Dokumentation unter Erstellen von Route 53-Profilen. 2. Wird verwendet AWS RAM , um das Profil für Mitgliedskonten freizugeben und das geteilte Profil anschließend mit Target zu verknüpfen VPCs. Anweisungen finden Sie in der Route 53-Dokumentation unter Freigeben eines Route 53-Profils und Zuordnen eines Route 53-Profils zu VPCs. **Note** Je nach Struktur und DNS-Anforderungen Ihrer Organisation müssen Sie möglicher weise mehrere Profile für unterschi edliche Konten oder	AWS-Administrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Workloads erstellen und verwalten.	

Konfigurieren und teilen Sie die Route 53 Resolver-Weiterleitungsregeln

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Weiterleitungsregel für eine Domain, die lokal gehostet wird.	Diese Regel weist Route 53 Resolver an, alle DNS-Abfragen für lokale Domänen (z. B. `onprem.example.com`) an lokale DNS-Resolver weiterzuleiten. Um diese Regel zu erstellen, benötigen Sie die IP-Adressen der lokalen DNS-Resolver und die ausgehende Endpunkt-ID. Anweisungen finden Sie in der Route 53-Dokumentation unter Erstellen von Weiterleitungsregeln.	AWS-Administrator, Cloud-Administrator
Grundlegende Einrichtung: Teilen Sie die Weiterleitungsregel und verknüpfen Sie sie mit Ihren Konten VPCs in anderen Konten.	Wenn du die Basiskonfiguration verwendest: Damit die Weiterleitungsregel wirksam wird, müssen Sie die Regel mit Ihren VPCs anderen Konten teilen und sie mit ihnen verknüpfen. Route 53 Resolver berücksichtigt die Regel dann bei der Auflösung einer Domäne. Anweisungen finden Sie unter Resolver-	AWS-Administrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Regeln mit anderen teilen AWS-Konten und gemeinsam genutzte Regeln verwenden und Weiterleitungsregeln mit einer VPC verknüpfen in der Route 53-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verbessertes Setup: Konfiguration und gemeinsame Nutzung von Route 53 53-Profilen.	Wenn Sie das erweiterte Setup verwenden: 1. Wenn Sie in den vorherigen Schritten bereits ein Route 53-Profil erstellt haben, können Sie dasselbe Profil verwenden. Wenn nicht, erstellen Sie ein Route 53-Profil und ordnen Sie ihm die entsprechenden Resolver-Weiterleitungsregeln zu. Anweisungen finden Sie in der Route 53 53-Dokumentation unter Erstellen von Route 53-Profilen. 2. Wird verwendet AWS RAM , um das Profil für Mitgliedskonten freizugeben und das geteilte Profil anschließend mit Target zu verknüpfen VPCs. Anweisungen finden Sie in der Route 53-Dokumentation unter Freigeben eines Route 53-Profils und Zuordnen eines Route 53-Profils zu VPCs. **Note** Je nach Struktur und DNS-Anforderungen	AWS-Administrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ihrer Organisation müssen Sie möglicher weise mehrere Profile für unterschi edliche Konten oder Workloads erstellen und verwalten.	

Konfigurieren Sie lokale DNS-Resolver für die Integration AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die bedingte Weiterleitung in den lokalen DNS-Resolvern.	Damit DNS-Abfragen zur Auflösung AWS von der lokalen Umgebung aus gesendet werden können, müssen Sie die bedingte Weiterleitung in den lokalen DNS-Resolvern so konfiguri eren, dass sie auf die IP-Adresse des eingehenden Endpunkts verweist. Dadurch werden die DNS-Resolver angewiesen, alle DNS-Abfra gen für die AWS-gehostete Domäne (z. B. für`prod.aws.example.com`) an die IP-Adresse des eingehenden Endpunkts weiterzuleiten, damit sie vom Route 53-Resolver aufgelöst werden.	Netzwerkadministrator

Überprüfen Sie die end-to-end DNS-Auflösung in einer Hybridumgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die DNS-Auflösung AWS von der lokalen Umgebung aus.	Führen Sie von einer Instanz in einer VPC aus, der die Weiterleitungsregel zugeordnet ist, eine DNS-Abfrage für eine lokal gehostete Domäne (z. B. für`db.onprem.example.com`).	Netzwerkadministrator
Testen Sie die DNS-Auflösung von der lokalen Umgebung bis. AWS	Führen Sie von einem lokalen Server aus die DNS-Auflösung für eine AWS-gehostete Domäne durch (z. B. für). `ec2.prod.aws.example.com`	Netzwerkadministrator

Zugehörige Ressourcen

- Hybrid-Cloud-DNS-Optionen für Amazon VPC (AWS Whitepaper)
- Arbeiten mit privat gehosteten Zonen (Route 53-Dokumentation)
- Erste Schritte mit Route 53 Resolver (Route 53-Dokumentation)
- Vereinfachen Sie die DNS-Verwaltung in einer Umgebung mit mehreren Konten mit Route 53 Resolver (Blogbeitrag)AWS
- Vereinheitlichen Sie die DNS-Verwaltung mithilfe von Amazon Route 53 53-Profilen mit mehreren VPCs und AWS-Konten (AWS Blogbeitrag)
- Migration Ihrer DNS-Umgebung mit mehreren Konten zu Amazon Route 53 Profiles (AWS Blogbeitrag)
- Verwendung von Amazon Route 53 53-Profilen für skalierbare AWS Umgebungen mit mehreren Konten (AWS Blogbeitrag)

Stellen Sie sicher, dass ELB-Load Balancer eine TLS-Terminierung erfordern

Erstellt von Priyanka Chaudhary (AWS)

Übersicht

In der Amazon Web Services (AWS) -Cloud verteilt Elastic Load Balancing (ELB) den eingehenden Anwendungsdatenverkehr automatisch auf mehrere Ziele, z. B. Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Container, IP-Adressen und AWS Lambda Lambda-Funktionen. Die Load Balancer verwenden Listener, um die Ports und Protokolle zu definieren, die der Load Balancer verwendet, um Traffic von Benutzern anzunehmen. Application Load Balancer treffen Routing-Entscheidungen auf Anwendungsebene und verwenden die. HTTP/HTTPS protocols. Classic Load Balancers make routing decisions at either the transport layer, by using TCP or Secure Sockets Layer (SSL) protocols, or at the application layer, by using HTTP/HTTPS

Dieses Muster bietet eine Sicherheitskontrolle, die mehrere Ereignistypen für Application Load Balancers und Classic Load Balancers untersucht. Wenn die Funktion aufgerufen wird, überprüft AWS Lambda das Ereignis und stellt sicher, dass der Load Balancer konform ist.

Die Funktion initiiert ein Amazon CloudWatch Events-Ereignis bei den folgenden API-Aufrufen: CreateLoadBalancerCreateLoadBalancerListeners, DeleteLoadBalancerListeners, CreateLoadBalancerPolicy, SetLoadBalancerPoliciesOfListener, CreateListenerDeleteListener, und ModifyListener. Wenn das Ereignis eines davon erkennt APIs, ruft es AWS Lambda auf, das ein Python-Skript ausführt. Das Python-Skript überprüft, ob der Listener ein SSL-Zertifikat enthält und ob die angewendete Richtlinie Transport Layer Security (TLS) verwendet. Wenn festgestellt wird, dass es sich bei der SSL-Richtlinie um etwas anderes als TLS handelt, sendet die Funktion eine Amazon Simple Notification Service (Amazon SNS) -Benachrichtigung mit den entsprechenden Informationen an den Benutzer.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

Einschränkungen

- Diese Sicherheitskontrolle sucht nicht nach vorhandenen Load Balancers, es sei denn, die Load Balancer-Listener werden aktualisiert.
- Diese Sicherheitskontrolle ist regional. Sie müssen es in jeder AWS-Region bereitstellen, die Sie überwachen möchten.

Architektur

Zielarchitektur

Automatisierung und Skalierung

- Wenn Sie AWS Organizations verwenden, können Sie AWS Cloudformation verwenden, StackSets um diese Vorlage in mehreren Konten bereitzustellen, die Sie überwachen möchten.

Tools

AWS-Services

- AWS CloudFormation — AWS CloudFormation hilft Ihnen dabei, Ihre AWS-Ressourcen zu modellieren und einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus zu verwalten. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben und sie zusammen als Stack zu starten und zu konfigurieren, anstatt Ressourcen einzeln zu verwalten.
- Amazon CloudWatch Events — Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit.
- AWS Lambda — AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice, der für eine Vielzahl von Speicherlösungen verwendet werden kann, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Code

Dieses Muster umfasst die folgenden Anlagen:

- `ELBRequirestlstermination.zip`— Der Lambda-Code für die Sicherheitskontrolle.
- `ELBRequirestlstermination.yml`— Die CloudFormation Vorlage, die das Ereignis und die Lambda-Funktion einrichtet.

Epen

Richten Sie den S3-Bucket ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Wählen oder erstellen Sie in der Amazon S3 S3-Konsole einen S3-Bucket, um die Lambda-Code-ZIP-Datei zu hosten. Dieser S3-Bucket muss sich in derselben AWS-Region befinden wie der Load Balancer, den Sie auswerten möchten. Ein S3-Bucket-Name ist weltweit eindeutig, und der Namespace wird von allen AWS-Konten gemeinsam genutzt. Der S3-Bucket-Name darf keine führenden Schrägstriche enthalten.	Cloud-Architekt
Laden Sie den Lambda-Code hoch.	Laden Sie den Lambda-Code (`ELBRequirestlstermination.zip` Datei), der im Abschnitt Anlagen bereitgestellt wird, in den S3-Bucket hoch.	Cloud-Architekt

Stellen Sie die CloudFormation Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die CloudFormation AWS-Vorlage.	Öffnen Sie die CloudFormation AWS-Konsole in derselben AWS-Region wie Ihr S3-Bucket und stellen Sie die angehängte Vorlage bereit `ELBRequirestlstermination.yml`. Weitere Informationen zur Bereitstellung von CloudFormation AWS-Vorlagen finden Sie in der CloudFormation Dokumentation unter Erstellen eines Stacks auf der CloudFormation AWS-Konsole.	Cloud-Architekt
Vervollständigen Sie die Parameter in der Vorlage.	Wenn Sie die Vorlage starten, werden Sie zur Eingabe der folgenden Informationen aufgefordert: • S3-Bucket: Geben Sie den Bucket an, den Sie im ersten Epic erstellt oder ausgewählt haben. Hier haben Sie den angehängten Lambda-Code (`ELBRequirestlstermination.zip` Datei) hochgeladen. • S3-Schlüssel: Geben Sie den Speicherort der Lambda-ZIP-Datei in Ihrem S3-Bucket	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	an (z. B. `ELBRequirestlstermination.zip odercontrols/ELBRequirestlstermination.zip`). Fügen Sie keine führenden Schrägstriche ein. • Benachrichtigungs-E-Mail: Geben Sie eine aktive E-Mail-Adresse an, unter der Sie Amazon SNS SNS-Benachrichtigungen erhalten möchten. • Lambda-Protokollierungsebene: Geben Sie die Protokollierungsebene und die Häufigkeit für die Lambda-Funktion an. Verwenden Sie Info, um detaillierte Informationsmeldungen über den Fortschritt, Fehler für Fehlerereignisse, die die Fortsetzung der Bereitstellung dennoch ermöglichen würden, und Warnmeldungen für potenziell schädliche Situationen zu protokollieren.	

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die CloudFormation Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail an die von Ihnen angegebene E-Mail-Adresse. Sie müssen dieses E-Mail-Abonnement bestätigen, um Benachrichtigungen über Verstöße zu erhalten.	Cloud-Architekt

Zugehörige Ressourcen

- Einen Stack auf der CloudFormation AWS-Konsole erstellen (CloudFormation AWS-Dokumentation)
- Was ist AWS Lambda? (AWS Lambda Lambda-Dokumentation)
- Was ist ein Classic Load Balancer? (ELB-Dokumentation)
- Was ist ein Application Load Balancer? (ELB-Dokumentation)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

AWS-Netzwerk-Firewall-Protokolle und -Metriken mithilfe von Splunk anzeigen

Erstellt von Ivo Pinto

Übersicht

Viele Unternehmen verwenden Splunk Enterprise als zentralisiertes Aggregations- und Visualisierungstool für Logs und Metriken aus verschiedenen Quellen. Dieses Muster hilft Ihnen, Splunk so zu konfigurieren, dass mithilfe des Splunk-Add-Ons für AWS Protokolle und Metriken der AWS Network Firewall von Amazon CloudWatch Logs abgerufen werden.

Um dies zu erreichen, erstellen Sie eine schreibgeschützte AWS Identity and Access Management (IAM) -Rolle. Splunk Add-On für AWS verwendet diese Rolle für den Zugriff. CloudWatch Sie konfigurieren das Splunk Add-On für AWS zum Abrufen von Metriken und Protokollen von. CloudWatch Schließlich erstellen Sie Visualisierungen in Splunk aus den abgerufenen Protokolldaten und Metriken.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein Splunk-Konto
- Eine Splunk Enterprise-Instanz, Version 8.2.2 oder höher
- Ein aktives AWS-Konto
- Network Firewall, eingerichtet und konfiguriert, um Protokolle an Logs zu CloudWatch senden

Einschränkungen

- Splunk Enterprise muss als Cluster von Amazon Elastic Compute Cloud (Amazon EC2) -Instances in der AWS-Cloud bereitgestellt werden.
- Das Sammeln von Daten mithilfe einer automatisch erkannten IAM-Rolle für Amazon EC2 wird in den AWS-Regionen China nicht unterstützt.

Architektur

Das Diagramm veranschaulicht folgende Vorgänge:

1. Die Network Firewall veröffentlicht CloudWatch Protokolle in Logs.
2. Splunk Enterprise ruft Metriken und Protokolle von ab. CloudWatch

Um Beispielmetriken und Logs in dieser Architektur aufzufüllen, generiert ein Workload Traffic, der über den Netzwerk-Firewall-Endpunkt ins Internet geleitet wird. Dies wird durch die Verwendung von Routentabellen erreicht. Obwohl dieses Muster eine einzelne EC2 Amazon-Instance als Workload verwendet, kann dieses Muster für jede Architektur gelten, sofern die Network Firewall so konfiguriert ist, dass sie CloudWatch Protokolle an Logs sendet.

Diese Architektur verwendet auch eine Splunk Enterprise-Instanz in einer anderen Virtual Private Cloud (VPC). Die Splunk-Instance kann sich jedoch an einem anderen Standort befinden, z. B. in derselben VPC wie der Workload, sofern sie den erreichen kann. CloudWatch APIs

Tools

AWS-Services

- Amazon CloudWatch Logs hilft Ihnen dabei, die Protokolle all Ihrer Systeme, Anwendungen und AWS-Services zu zentralisieren, sodass Sie sie überwachen und sicher archivieren können.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Die AWS Network Firewall ist ein zustandsbehafteter, verwalteter Netzwerk-Firewall sowie Service zur Erkennung und Verhinderung von Eindringlingen VPCs in der AWS-Cloud.

Andere Tools

- Splunk unterstützt Sie bei der Überwachung, Visualisierung und Analyse von Protokolldaten.

Epen

Erstellen einer IAM-Rolle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Richtlinie.	Folgen Sie den Anweisungen unter Richtlinien mit dem	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	JSON-Editor erstellen, um die IAM-Richtlinie zu erstellen , die nur Lesezugriff auf die CloudWatch Logdaten und -Metriken gewährt. CloudWatch Fügen Sie die folgende -Richtlinie in den JSON-Editor ein. `{ "Statement": [ { "Action": [ "cloudwatch:List*", "cloudwatch:Get*", "network-firewall:List*", "logs:Describe*", "logs:Get*", "logs:List*", "logs:StartQuery", "logs:StopQuery", "logs:TestMetricFilter", "logs:FilterLogEvents", "network-firewall:Describe*" ],`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"Effect": "Allow", "Resource": "*" }], "Version": "2012-10-17" }</pre>	
Erstellen Sie eine neue IAM-Rolle.	Folgen Sie den Anweisungen unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service, um die IAM-Rolle zu erstellen, auf die das Splunk Add-On für AWS zugreift. CloudWatch Wählen Sie für Berechtigungsrichtlinien die Richtlinie aus, die Sie zuvor erstellt haben.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Weisen Sie den EC2 Instances im Splunk-Cluster die IAM-Rolle zu.	1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/. 2. Wählen Sie im Navigationsbereich Instances aus. 3. Wählen Sie die EC2 Instances im Splunk-Cluster aus. 4. Wählen Sie Aktionen, Sicherheit und dann IAM-Rolle ändern aus. 5. Wählen Sie die IAM-Rolle aus, die Sie zuvor erstellt haben, und klicken Sie dann auf Speichern.	AWS-Administrator

Installieren Sie das Splunk-Add-On für AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie das Add-on.	1. Navigieren Sie im Splunk-Dashboard zu Splunk Apps. 2. Suchen Sie nach dem Splunk-Add-on für Amazon Web Services. 3. Wählen Sie Installieren aus. 4. Geben Sie Ihre Splunk-Anmeldeinformationen ein.	Splunk-Administrator
Konfigurieren Sie die AWS-Anmeldeinformationen.	1. Navigieren Sie im Splunk-Dashboard zu Splunk Add-on for AWS.	Splunk-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie Konfiguration. 3. Wählen Sie in der Spalte Autodiscovered IAM Role die IAM-Rolle aus, die Sie zuvor erstellt haben. Weitere Informationen finden Sie in der Splunk-Dokumentation unter Suchen Sie eine IAM-Rolle in Ihrer Splunk-Plattform-Instance.	

Konfigurieren Sie den Splunk-Zugriff auf CloudWatch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Abruf von Netzwerk-Firewall-Protokollen aus CloudWatch Protokollen.	1. Navigieren Sie im Splunk-Dashboard zu Splunk Add-on for AWS. 2. Wählen Sie Eingabe. 3. Wählen Sie „Neue Eingabe erstellen“. 4. Wählen Sie in der Liste Benutzerdefinierter Datentyp und dann CloudWatch Protokolle aus. 5. Geben Sie den Namen, das AWS-Konto, die AWS-Region und die Protokoll gruppe für Ihre Netzwerk-Firewall-Protokolle an. 6. Wählen Sie Speichern.	Splunk-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Standardmäßig ruft Splunk die Protokolldaten alle 10 Minuten ab. Dies ist ein konfigurierbarer Parameter unter Erweiterte Einstellungen. Weitere Informationen finden Sie in der Splunk-Dokumentation unter Konfiguration einer CloudWatch Log-Eingabe mit Splunk Web.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Abruf von Netzwerk-Firewall-Metriken von CloudWatch.	1. Navigieren Sie im Splunk-Dashboard zu Splunk Add-on for AWS. 2. Wählen Sie Eingabe. 3. Wählen Sie „Neue Eingabe erstellen“. 4. Wählen Sie in der Liste CloudWatch. 5. Geben Sie den Namen, das AWS-Konto und die AWS-Region für Ihre Netzwerk-Firewall-Metriken an. 6. Wählen Sie neben Metric Configuration die Option Im erweiterten Modus bearbeiten aus. 7. (Optional) Löschen Sie alle vorkonfigurierten Namespaces. 8. Wählen Sie Add Namespace und nennen Sie ihn dann NetworkFirewallAWS/. 9. Fügen Sie unter Dimensionswert Folgendes hinzu. `[{"AvailabilityZone":[".*"],"Engine":[".*"],"FirewallName":[".*"]}]` 10. Wählen Sie für Metriken die Option Alle aus.	Splunk-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	11. Wählen Sie für Metrische Statistiken die Option Summe aus. 12. Wählen Sie OK aus. 13. Wählen Sie Speichern. Standardmäßig ruft Splunk die Metrikdaten alle 5 Minuten ab. Dies ist ein konfigurierbarer Parameter unter Erweitert e Einstellungen. Weitere Informationen finden Sie in der Splunk-Dokumentati on unter Eine CloudWatch Eingabe mithilfe von Splunk Web konfigurieren.	

Erstellen Sie Splunk-Visualisierungen mithilfe von Abfragen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich die wichtigsten Quell-IP-Adressen an.	1. Navigieren Sie im Splunk-Dashboard zu Search & Reporting. 2. Geben Sie im Feld „Suche hier eingeben“ Folgendes ein. `sourcetype="aws:cl oudwatchlogs" | top event.src_ip` Diese Abfrage zeigt eine Tabelle mit den Quell-IP-	Splunk-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Adressen mit dem meisten Verkehr in absteigender Reihenfolge an. 3. Für eine grafische Darstellung wählen Sie Visualization.	
Paketstatistiken anzeigen.	1. Navigieren Sie im Splunk-Dashboard zu Search & Reporting. 2. Geben Sie im Feld „Suche hier eingeben“ Folgendes ein. `sourcetype="aws:cloudwatch"| timechart sum(Sum) by metric_name` Diese Abfrage zeigt eine Tabelle mit den Metriken `DroppedPackets` `PassedPackets` , und `ReceivedPackets` pro Minute an. 3. Für eine grafische Darstellung wählen Sie Visualisierung.	Splunk-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich die am häufigsten verwendeten Quellports an.	1. Navigieren Sie im Splunk-Dashboard zu Search & Reporting. 2. Geben Sie im Feld „Suche hier eingeben“ Folgendes ein. `sourcetype="aws:cloudwatchlogs" | top event.dest_port` Diese Abfrage zeigt eine Tabelle der Quellports mit dem meisten Verkehr in absteigender Reihenfolge an. 3. Für eine grafische Darstellung wählen Sie Visualisierung.	Splunk-Administrator

Zugehörige Ressourcen

AWS-Dokumentation

- Eine Rolle erstellen, um Berechtigungen an einen AWS-Service zu delegieren (IAM-Dokumentation)
- IAM-Richtlinien erstellen (IAM-Dokumentation)
- Protokollierung und Überwachung in der AWS-Netzwerk-Firewall (Netzwerk-Firewall-Dokumentation)
- Routentabellenkonfigurationen für die AWS-Netzwerk-Firewall (Netzwerk-Firewall-Dokumentation)

AWS-Blogbeiträge

- Bereitstellungsmodelle für AWS-Netzwerk-Firewalls

AWS Marketplace

- Splunk Enterprise Amazon Machine Image (AMI)

Mehr Muster

- Greifen Sie mithilfe von Session Manager und Amazon EC2 Instance Connect auf einen Bastion-Host zu
- Greifen Sie privat auf Container-Anwendungen auf Amazon ECS zu, indem Sie AWS Fargate PrivateLink, AWS und einen Network Load Balancer verwenden
- Greifen Sie mithilfe von AWS PrivateLink und einem Network Load Balancer privat auf Container-Anwendungen auf Amazon ECS zu
- Zentralisieren Sie die DNS-Auflösung mithilfe von AWS Managed Microsoft AD und vor Ort von Microsoft Active Directory
- Suchen Sie in den Eingangsregeln für Sicherheitsgruppen nach Einzelhost-Netzwerkeinträgen für und IPv4 IPv6
- Erstellen Sie ein Portal für Mikro-Frontends mithilfe AWS Amplify von Angular und Module Federation
- Stellen Sie eine Firewall mit AWS Network Firewall und AWS Transit Gateway bereit
- Stellen Sie eine Amazon API Gateway Gateway-API auf einer internen Website mithilfe von privaten Endpunkten und einem Application Load Balancer bereit
- Stellen Sie detektivattributebasierte Zugriffskontrollen für öffentliche Subnetze bereit, indem Sie AWS Config
- Implementieren Sie präventive attributebasierte Zugriffskontrollen für öffentliche Subnetze
- Verschlüsselte Verbindungen für PostgreSQL-DB-Instances in Amazon RDS aktivieren
- Mit AWS Transit Gateway Connect auf AWS erweitern VRFs
- Migrieren Sie einen F5 BIG-IP-Workload zu F5 BIG-IP VE in der AWS-Cloud
- Migrieren Sie NGINX Ingress Controller, wenn Sie den Amazon EKS Auto Mode aktivieren
- Beibehaltung von routingfähigem IP-Speicherplatz in VPC-Designs mit mehreren Konten für Subnetze ohne Arbeitslast
- Verhindern Sie den Internetzugang auf Kontoebene mithilfe einer Dienststeuerungsrichtlinie
- Benachrichtigungen von der AWS-Netzwerk-Firewall an einen Slack-Channel senden
- Statische Inhalte in einem Amazon S3 S3-Bucket über eine VPC mithilfe von Amazon bereitstellen CloudFront
- Richten Sie die Notfallwiederherstellung für Oracle JD Edwards EnterpriseOne mit AWS Elastic Disaster Recovery ein

- Verwenden Sie BMC Discovery-Abfragen, um Migrationsdaten für die Migrationsplanung zu extrahieren
- Verwenden Sie die Network Firewall, um die DNS-Domänennamen aus der Servernamenanzeige für ausgehenden Datenverkehr zu erfassen

Bereitstellung von Inhalten

Themen

- AWS WAF Logs mithilfe AWS Firewall Manager von Amazon Data Firehose an Splunk senden
- Statische Inhalte in einem Amazon S3 S3-Bucket über eine VPC mithilfe von Amazon bereitstellen CloudFront
- Mehr Muster

AWS WAF Logs mithilfe AWS Firewall Manager von Amazon Data Firehose an Splunk senden

Erstellt von Michael Friedenthal (AWS), Aman Kaur Gandhi (AWS) und JJ Johnson (AWS)

Übersicht

In der Vergangenheit gab es zwei Möglichkeiten, Daten in Splunk zu verschieben: eine Push- oder eine Pull-Architektur. Eine Pull-Architektur bietet garantierte Lieferdaten durch Wiederholungsversuche, erfordert jedoch spezielle Ressourcen in Splunk, die Daten abfragen. Pull-Architekturen funktionieren aufgrund des Pollings in der Regel nicht in Echtzeit. Eine Push-Architektur hat in der Regel eine geringere Latenz, ist skalierbarer und reduziert die betriebliche Komplexität und die Kosten. Sie garantiert jedoch nicht die Lieferung und erfordert in der Regel Agenten.

Die Splunk-Integration mit Amazon Data Firehose liefert Streaming-Daten in Echtzeit über einen HTTP Event Collector (HEC) an Splunk. Diese Integration bietet die Vorteile von Push- und Pull-Architekturen: Sie garantiert die Datenübermittlung durch Wiederholungsversuche, erfolgt nahezu in Echtzeit und zeichnet sich durch geringe Latenz und geringe Komplexität aus. Die HEC sendet Daten schnell und effizient über HTTP oder HTTPS direkt an Splunk. HECs sind tokenbasiert, wodurch die Notwendigkeit entfällt, Anmeldeinformationen in einer Anwendung oder in unterstützenden Dateien fest zu codieren.

In einer AWS Firewall Manager Richtlinie können Sie die Protokollierung für den gesamten AWS WAF Web-ACL-Verkehr in all Ihren Konten konfigurieren. Anschließend können Sie einen Firehose-Zustellungsstream verwenden, um diese Protokolldaten zur Überwachung, Visualisierung und Analyse an Splunk zu senden. Diese Lösung bietet die folgenden Vorteile:

- Zentrale Verwaltung und Protokollierung des AWS WAF Web-ACL-Datenverkehrs in all Ihren Konten
- Splunk-Integration mit einem einzigen AWS-Konto
- Skalierbarkeit
- Bereitstellung von Protokolldaten nahezu in Echtzeit
- Kostenoptimierung durch den Einsatz einer serverlosen Lösung, sodass Sie nicht für ungenutzte Ressourcen bezahlen müssen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine aktive Person AWS-Konto , die Teil einer Organisation in AWS Organizations ist.
- Sie benötigen die folgenden Berechtigungen, um die Protokollierung mit Firehose zu aktivieren:
  - `iam:CreateServiceLinkedRole`
  - `firehose:ListDeliveryStreams`
  - `wafv2:PutLoggingConfiguration`
- AWS WAF und sein Web ACLs muss konfiguriert sein. Anweisungen finden Sie unter Erste Schritte mit AWS WAF.
- AWS Firewall Manager muss eingerichtet sein. Anweisungen finden Sie unter AWS Firewall Manager Voraussetzungen.
- Die Firewall Manager Manager-Sicherheitsrichtlinien für AWS WAF müssen konfiguriert werden. Anweisungen finden Sie unter Erste Schritte mit AWS Firewall ManagerAWS WAF Richtlinien.
- Splunk muss mit einem öffentlichen HTTP-Endpunkt eingerichtet werden, der von Firehose erreicht werden kann.

Einschränkungen

- Der AWS-Konten muss in einer einzigen Organisation verwaltet werden. AWS Organizations
- Die Web-ACL muss sich in derselben Region wie der Lieferstream befinden. Wenn Sie Protokolle für Amazon erfassen CloudFront, erstellen Sie den Firehose-Lieferstream in der Region USA Ost (Nord-Virginia),`us-east-1`.
- Das Splunk-Add-on für Firehose ist für kostenpflichtige Splunk Cloud-Implementierungen, verteilte Splunk Enterprise-Bereitstellungen und Splunk Enterprise-Implementierungen mit einer einzigen Instanz verfügbar. Dieses Add-on wird für kostenlose Testversionen von Splunk Cloud nicht unterstützt.

Architektur

Zieltechnologie-Stack

- Firewall Manager
- Firehose

- Amazon Simple Storage Service (Amazon-S3)
- AWS WAF
- Splunk

Zielarchitektur

Die folgende Abbildung zeigt, wie Sie den Firewall Manager verwenden können, um alle AWS WAF Daten zentral zu protokollieren und über Firehose an Splunk zu senden.

1. Das AWS WAF Web ACLs sendet Firewall-Protokolldaten an Firewall Manager.
2. Firewall Manager sendet die Protokolldaten an Firehose.
3. Der Firehose-Lieferstream leitet die Protokolldaten an Splunk und an einen S3-Bucket weiter. Der S3-Bucket dient als Backup im Falle eines Fehlers im Firehose-Lieferstream.

Automatisierung und Skalierung

Diese Lösung ist so konzipiert, dass sie skaliert werden kann und alle AWS WAF Websites ALCs innerhalb des Unternehmens berücksichtigt. Sie können alle Websites so konfigurieren ACLs , dass sie dieselbe Firehose-Instanz verwenden. Wenn Sie jedoch mehrere Firehose-Instanzen einrichten und verwenden möchten, können Sie dies tun.

Tools

AWS-Services

- AWS Firewall Managerist ein Sicherheitsverwaltungsdienst, mit dem Sie Firewallregeln für Ihre Konten und Anwendungen zentral konfigurieren und verwalten können. AWS Organizations
- Amazon Data Firehose unterstützt Sie bei der Bereitstellung von Echtzeit-Streaming-Daten an andere AWS-Services, benutzerdefinierte HTTP-Endpunkte und HTTP-Endpunkte, die von unterstützten Drittanbietern wie Splunk betrieben werden.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS WAFist eine Firewall für Webanwendungen, mit der Sie HTTP- und HTTPS-Anfragen überwachen können, die an Ihre geschützten Webanwendungsressourcen weitergeleitet werden.

Andere Tools

- Splunk unterstützt Sie bei der Überwachung, Visualisierung und Analyse von Protokolldaten.

Epen

Splunk konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die Splunk-App für. AWS	1. Melden Sie sich bei Ihrem Splunk Heavy Forwarder an. Die Standard-URL ist. `http://<IP address>:8000` 2. Wählen Sie in der linken Navigationsleiste neben Apps die Zahnradtaste aus. 3. Wähle „Weitere Apps durchsuchen“. 4. Suchen Sie nach AWS. 5. Wählen Sie für Splunk App for die Option AWS Installieren. 6. Geben Sie Ihre Splunk.com-Anmeldedaten ein, akzeptieren Sie die Allgemeinen Geschäftsbedingungen und wählen Sie dann Anmelden und Installieren. 7. Wählen Sie Erledigt aus.	Sicherheitsadministrator, Splunk-Administrator
Installieren Sie das Add-on für. AWS WAF	Wiederholen Sie die vorherigen Anweisungen, um das AWS	Sicherheitsadministrator, Splunk-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Web Application Firewall Add-on für Splunk zu installieren.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren und konfigurieren Sie das Splunk-Add-on für Firehose.	1. Installieren und konfiguri eren Sie das Splunk-Add-on für Firehose. Im Rahmen der Installation und Konfiguration richten Sie, falls dies für Ihre Splunk-Plattform erforderl ich ist, einen HTTP Event Collector ein und bereiten die Infrastruktur vor, um die Protokolldaten an Ihre Indexer zu senden. Sehen Sie sich die Anweisung en an, die Ihrer Splunk-Be reitstellung entsprechen: • Bereitstellung von Splunk Cloud (Splunk-D okumentation) • Verteilte Splunk Enterpris e-Bereitstellung (Splunk-Dokumentation) • Bereitstellung von Splunk Enterprise in einer einzigen Instanz (Splunk-Dokumentation) **Important** Beenden Sie diesen Vorgang, nachdem Sie das Splunk-Ad d-on installiert und konfiguriert haben. Fahren Sie nicht	Sicherheitsadministrator, Splunk-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	mit den Anweisungen zur Konfiguration von Firehose für das Senden von Daten an die Splunk-Plattform fort. 2. Notieren Sie sich das HTTP-Event-Collector-Token und den HTTP-Endpunkt. Sie benötigen diesen Wert später, wenn Sie den Delivery Stream konfigurieren.	

Erstellen Sie den Firehose-Lieferstream

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gewähren Sie Firehose Zugriff auf ein Splunk-Ziel.	Konfigurieren Sie die Zugriffsrichtlinie, die es Firehose ermöglicht, auf ein Splunk-Ziel zuzugreifen und die Protokolldaten in einem S3-Bucket zu sichern. Weitere Informationen finden Sie unter Firehose Zugriff auf ein Splunk-Ziel gewähren.	Sicherheitsadministrator
Erstellen Sie einen Firehose-Lieferstream.	Erstellen Sie in demselben Konto AWS WAF, ACLs für das Sie das Web verwalten, einen Lieferstream in Firehose. Sie müssen eine	Sicherheitsadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	IAM-Rolle besitzen, wenn Sie einen Bereitstellungsdatenstrom erstellen. Firehose nimmt diese IAM-Rolle an und erhält Zugriff auf den angegebenen S3-Bucket. Anweisungen finden Sie unter Einen Lieferstream erstellen. Beachten Sie Folgendes: • Der Name des Lieferdatenstroms muss mit beginnen `aws-waf-logs-` . • Wählen Sie als Quelle Direct PUT aus. • Wählen Sie für den S3-Backup-Modus Alle Ereignisse sichern und wählen Sie dann einen vorhandenen Bucket aus oder erstellen Sie einen neuen. • Folgen Sie für das Ziel den Anweisungen unter Wählen Sie Splunk für Ihr Ziel in der Firehose-Dokumentation. Informationen zu den Werten für Splunk-Endpunkte und Endpunkttypen finden Sie unter Amazon Data Firehose konfigurieren in der Splunk-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wiederholen Sie diesen Vorgang für jedes Token, das Sie im HTTP-Event-Collector konfiguriert haben.	
Testen Sie den Lieferstream.	Testen Sie den Lieferstr eam, um sicherzustellen, dass er richtig konfiguriert ist. Anweisungen finden Sie unter Testen mit Splunk als Ziel in der Firehose-Dokumentation.	Sicherheitsadministrator

Konfigurieren Sie den Firewall Manager für die Protokollierung von Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Firewall Manager Manager-Richtlinien.	Die Firewall Manager Manager-Richtlinien müssen so konfiguriert sein, dass sie die Protokollierung aktiviere n und Protokolle an den richtigen Firehose-Lieferstr eam weiterleiten. Weitere Informationen und Anweisung en finden Sie unter Konfigura tion der Protokollierung für eine AWS WAF Richtlinie.	Sicherheitsadministrator

Zugehörige Ressourcen

AWS Ressourcen

- Web-ACL-Verkehr protokollieren (AWS WAF Dokumentation)
- Konfiguration der Protokollierung für eine AWS WAF Richtlinie (AWS WAF Dokumentation)

- Tutorial: Mit Amazon Data Firehose VPC-Flow-Logs an Splunk senden (Firehose-Dokumentation)
- Wie übertrage ich VPC-Flow-Logs mit Amazon Data Firehose an Splunk? (Wissenszentrum)AWS
- Optimieren Sie die Datenaufnahme in Splunk mithilfe von Amazon Data Firehose (Blogbeitrag)AWS

Splunk-Dokumentation

- Splunk-Add-on für Amazon Data Firehose

Statische Inhalte in einem Amazon S3 S3-Bucket über eine VPC mithilfe von Amazon bereitstellen CloudFront

Erstellt von Angel Emmanuel Hernandez Cebrian

Übersicht

Wenn Sie statische Inhalte bereitstellen, die auf Amazon Web Services (AWS) gehostet werden, wird empfohlen, einen Amazon Simple Storage Service (S3) -Bucket als Quelle zu verwenden und Amazon für die Verteilung der Inhalte CloudFront zu verwenden. Diese Lösung bietet zwei Hauptvorteile: die Bequemlichkeit, statische Inhalte an Edge-Standorten zwischenzuspeichern, und die Möglichkeit, Web-Zugriffskontrolllisten (Web ACLs) für die CloudFront Verteilung zu definieren, was Ihnen hilft, Anfragen zu den Inhalten mit minimalem Konfigurations- und Verwaltungsaufwand zu sichern.

Der empfohlene Standardansatz weist jedoch häufig eine architektonische Einschränkung auf. In einigen Umgebungen möchten Sie, dass virtuelle Firewall-Appliances, die in einer Virtual Private Cloud (VPC) bereitgestellt werden, den gesamten Inhalt überprüfen, einschließlich statischer Inhalte. Der Standardansatz leitet den Datenverkehr nicht zur Inspektion durch die VPC. Dieses Muster bietet eine alternative architektonische Lösung. Sie verwenden immer noch eine CloudFront Distribution, um statische Inhalte in einem S3-Bucket bereitzustellen, aber der Datenverkehr wird mithilfe eines Application Load Balancer über die VPC geleitet. Eine AWS-Lambda-Funktion ruft dann den Inhalt aus dem S3-Bucket ab und gibt ihn zurück.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Statischer Website-Inhalt, der in einem S3-Bucket gehostet wird.

Einschränkungen

- Die Ressourcen in diesem Muster müssen sich in einer einzigen AWS-Region befinden, sie können jedoch in verschiedenen AWS-Konten bereitgestellt werden.
- Es gelten Grenzwerte für die maximale Anfrage- und Antwortgröße, die die Lambda-Funktion empfangen bzw. senden kann. Weitere Informationen finden Sie unter Grenzwerte in Lambda-Funktionen als Ziele (Elastic Load Balancing Balancing-Dokumentation).

- Bei der Verwendung dieses Ansatzes ist es wichtig, ein ausgewogenes Verhältnis zwischen Leistung, Skalierbarkeit, Sicherheit und Kosteneffektivität zu finden. Trotz der hohen Skalierbarkeit von Lambda werden einige Anfragen gedrosselt, wenn die Anzahl gleichzeitiger Lambda-Aufrufe das maximale Kontingent überschreitet. Weitere Informationen finden Sie unter Lambda-Kontingente (Lambda-Dokumentation). Bei der Verwendung von Lambda müssen Sie auch die Preisgestaltung berücksichtigen. Um Lambda-Aufrufe zu minimieren, stellen Sie sicher, dass Sie den Cache für die Distribution richtig definieren. CloudFront Weitere Informationen finden Sie unter Optimierung von Caching und Verfügbarkeit (Dokumentation). CloudFront

Architektur

Zieltechnologie-Stack

- CloudFront
- Amazon Virtual Private Cloud (Amazon VPC)
- Application Load Balancer
- Lambda
- Amazon S3

Zielarchitektur

Die folgende Abbildung zeigt die vorgeschlagene Architektur, wenn Sie statische Inhalte aus einem S3-Bucket über eine VPC bereitstellen müssen. CloudFront

1. Der Client fordert die URL der CloudFront Verteilung an, um eine bestimmte Website-Datei im S3-Bucket abzurufen.
2. CloudFront sendet die Anfrage an AWS WAF. AWS WAF filtert die Anfrage mithilfe des Webs, das auf die CloudFront Verteilung ACLs angewendet wurde. Wenn sich herausstellt, dass die Anfrage gültig ist, wird der Ablauf fortgesetzt. Wenn sich herausstellt, dass die Anfrage ungültig ist, erhält der Client einen 403-Fehler.
3. CloudFront überprüft seinen internen Cache. Wenn es einen gültigen Schlüssel gibt, der der eingehenden Anfrage entspricht, wird der zugehörige Wert als Antwort an den Client zurückgesendet. Ist dies nicht der Fall, wird der Datenfluss fortgesetzt.
4. CloudFront leitet die Anfrage an die URL des angegebenen Application Load Balancer weiter.

5. Der Application Load Balancer hat einen Listener, der auf einer Lambda-Funktion einer Zielgruppe zugeordnet ist. Der Application Load Balancer ruft die Lambda-Funktion auf.
6. Die Lambda-Funktion stellt eine Verbindung zum S3-Bucket her, führt eine `GetObject` Operation darauf aus und gibt den Inhalt als Antwort zurück.

Automatisierung und Skalierung

Um die Bereitstellung statischer Inhalte mit diesem Ansatz zu automatisieren, erstellen Sie CI/CD-Pipelines zur Aktualisierung der Amazon S3 S3-Buckets, die Websites hosten.

Die Lambda-Funktion skaliert automatisch, um die gleichzeitigen Anfragen innerhalb der Kontingente und Einschränkungen des Dienstes zu verarbeiten. Weitere Informationen finden Sie unter Lambda-Funktionsskalierung und Lambda-Kontingente (Lambda-Dokumentation). Für die anderen AWS-Services und -Funktionen wie CloudFront den Application Load Balancer skaliert AWS diese automatisch.

Tools

- Amazon CloudFront beschleunigt die Verteilung Ihrer Webinhalte, indem es sie über ein weltweites Netzwerk von Rechenzentren bereitstellt, was die Latenz senkt und die Leistung verbessert.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. In diesem Muster verwenden Sie einen Application Load Balancer, der über Elastic Load Balancing bereitgestellt wird, um den Datenverkehr an die Lambda-Funktion weiterzuleiten.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.

Epen

Wird verwendet CloudFront , um statische Inhalte von Amazon S3 über eine VPC bereitzustellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC.	Erstellen Sie eine VPC zum Hosten der in diesem Muster bereitgestellten Ressourcen, z. B. des Application Load Balancer und der Lambda-Funktion. Anweisungen finden Sie unter Erstellen einer VPC (Amazon VPC-Dokumentation).	Cloud-Architekt
Erstellen Sie eine AWS WAF WAF-Web-ACL.	Erstellen Sie eine AWS WAF WAF-Web-ACL. Später in diesem Muster wenden Sie diese Web-ACL auf die CloudFront Distribution an. Anweisungen finden Sie unter Erstellen einer Web-ACL (AWS-WAF-Dokumentation).	Cloud-Architekt
So erstellen Sie die Lambda-Funktion:	Erstellen Sie die Lambda-Funktion, die den im S3-Bucket gehosteten statischen Inhalt als Website bereitstellt. Verwenden Sie den Code, der im Abschnitt Zusätzliche Informationen dieses Musters bereitgestellt wird. Passen Sie den Code an, um Ihren Ziel-S3-Bucket zu identifizieren.	Allgemeines AWS
Laden Sie die Lambda-Funktion hoch.	Geben Sie den folgenden Befehl ein, um den Lambda-	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Funktionscode in ein ZIP-Datei archiv in Lambda hochzulad en. `aws lambda update-fu nction-code \ --function-name \ --zip-file fileb://l ambda-alb-s3-websi te.zip`	
Erstellen Sie einen Application Load Balancer.	Erstellen Sie einen mit dem Internet verbundenen Applicati on Load Balancer, der auf die Lambda-Funktion verweist. Anweisungen finden Sie unter Eine Zielgruppe für die Lambda-Funktion erstellen (Elastic Load Balancing Balancing-Dokumentation). Für eine Hochverfügbarkeits konfiguration erstellen Sie den Application Load Balancer und fügen ihn privaten Subnetzen in verschiedenen Availability Zones hinzu.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CloudFront Distribution.	Erstellen Sie eine CloudFront Verteilung, die auf den von Ihnen erstellten Application Load Balancer verweist. 1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudFront Konsole unter https://console.aws.amazon.com/cloudfront/v3/home. 2. Wählen Sie Create Distribution. 3. Wählen Sie auf der ersten Seite des Assistenten Create Distribution Wizard im Abschnitt Web die Option Get Started. 4. Geben Sie die Einstellungen für Ihre Distribution an. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Aktualisieren einer Verteilung angeben. Beachten Sie Folgendes: a. Legen Sie den Application Load Balancer als Ursprung fest. b. Wählen Sie in den Vertriebseinstellungen die vorhandene Website aus ACLs , die Sie über AWS WAF anwenden	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	möchten. Weitere Informationen finden Sie unter AWS WAF Web ACL. 5. Speichern Sie Ihre Änderungen. 6. Nachdem Sie Ihre Distribution CloudFront erstellt haben, ändert sich der Wert der Status-Spalte für Ihre Distribution von InProgress zu Deployed. Wenn Sie die Verteilung aktivieren, kann sie sofort Anfragen verarbeiten, nachdem der Status auf Deployed (Bereitgestellt) gewechselt hat.	

Zugehörige Ressourcen

AWS-Dokumentation

- Optimierung von Caching und Verfügbarkeit (CloudFront Dokumentation)
- Lambda-Funktionen als Ziele (Dokumentation zu Elastic Load Balancing)
- Lambda-Kontingente (Lambda-Dokumentation)

AWS-Servicewebsites

- Application Load Balancer
- Lambda
- CloudFront
- Amazon S3

- AWS WAF
- Amazon VPC

Zusätzliche Informationen

Code

Die folgende Lambda-Beispielfunktion ist in Node.js geschrieben. Diese Lambda-Funktion fungiert als Webserver, der eine `GetObject` Operation für einen S3-Bucket ausführt, der die Website-Ressourcen enthält.

```
/**

 * This is an AWS Lambda function created for demonstration purposes.

 * It retrieves static assets from a defined Amazon S3 bucket.

 * To make the content available through a URL, use an Application Load Balancer with a
 Lambda integration.
 *
 * Set the S3_BUCKET environment variable in the Lambda function definition.
 */

var AWS = require('aws-sdk');

exports.handler = function(event, context, callback) {

    var bucket = process.env.S3_BUCKET;
    var key = event.path.replace('/', '');

    if (key == '') {
        key = 'index.html';
    }

    // Fetch from S3
    var s3 = new AWS.S3();
    return s3.getObject({Bucket: bucket, Key: key},
       function(err, data) {

           if (err) {
               return err;
           }
```

```
            var isBase64Encoded = false;
            var encoding = 'utf8';

            if (data.ContentType.indexOf('image/') > -1) {
                isBase64Encoded = true;
                encoding = 'base64'
            }

            var resp = {
                statusCode: 200,
                headers: {
                    'Content-Type': data.ContentType,
                },
                body: new Buffer(data.Body).toString(encoding),
                isBase64Encoded: isBase64Encoded
            };

            callback(null, resp);
        }
    );
};
```

Mehr Muster

- Suchen Sie in einer CloudFront Amazon-Distribution nach Zugriffsprotokollierung, HTTPS- und TLS-Version
- Stellen Sie eine GRPC-basierte Anwendung auf einem Amazon EKS-Cluster bereit und greifen Sie mit einem Application Load Balancer darauf zu
- Implementieren Sie präventive attributebasierte Zugriffskontrollen für öffentliche Subnetze
- Bereitstellen von Ressourcen in einer AWS Wavelength Zone mithilfe von Terraform
- Stellen Sie die Security Automations for AWS WAF Solution mithilfe von Terraform bereit
- Richten Sie einen serverlosen Mobilfunkrouter für eine zellenbasierte Architektur ein
- Verwenden Sie Amazon Q Developer als Programmierassistenten, um Ihre Produktivität zu steigern
- AWS-Netzwerk-Firewall-Protokolle und -Metriken mithilfe von Splunk anzeigen

Datenbanken und Speicher

Themen

- Datenbanken
- Speicher und Backup

Datenbanken

Themen

- Greifen Sie von Microsoft SQL Server auf Amazon EC2 mithilfe von Verbindungsservern auf lokale Microsoft SQL Server-Tabellen zu
- Fügen Sie HA mithilfe einer Read Replica zu Oracle PeopleSoft auf Amazon RDS Custom hinzu
- Beurteilen Sie die Abfrageleistung für die Migration von SQL Server-Datenbanken zu MongoDB Atlas auf AWS
- Automatisieren Sie blaue/grüne Bereitstellungen globaler Amazon Aurora Aurora-Datenbanken mithilfe von IaC-Prinzipien
- Automatisieren Sie Datenbankaufgaben in der SQL Server Express Edition, die auf Amazon ausgeführt wird, EC2 mithilfe eines AWS Lambda Taskplaners
- Automatisieren Sie regionsübergreifendes Failover und Failback mithilfe des DR Orchestrator Framework
- Automatisieren Sie die Replikation von Amazon RDS-Instances auf AWS-Konten
- Automatisches Backup von SAP HANA-Datenbanken mit Systems Manager und EventBridge
- Automatisches Generieren eines PynamoDB-Modells und CRUD-Funktionen für Amazon DynamoDB mithilfe einer Python-Anwendung
- Blockieren Sie den öffentlichen Zugriff auf Amazon RDS mithilfe von Cloud Custodian
- Kontenübergreifenden Zugriff auf Amazon DynamoDB konfigurieren
- Konfigurieren Sie das schreibgeschützte Routing in einer Always-On-Verfügbarkeitsgruppe in SQL Server auf AWS
- Stellen Sie eine Connect über einen SSH-Tunnel in pgAdmin her
- JSON-Oracle-Abfragen in PostgreSQL-Datenbank-SQL konvertieren
- Kopieren Sie Amazon DynamoDB-Tabellen zwischen Konten mit AWS Backup
- Amazon DynamoDB-Tabellen mithilfe einer benutzerdefinierten Implementierung kontenübergreifend kopieren
- Erstellen Sie detaillierte Kosten- und Nutzungsberichte für Amazon RDS und Amazon Aurora
- Stellen Sie mithilfe von Terraform SQL Server-Failover-Cluster-Instances auf Amazon EC2 und Amazon FSx bereit
- Emulieren Sie Oracle RAC-Workloads mithilfe benutzerdefinierter Endpunkte in Aurora PostgreSQL

- Verschlüsselte Verbindungen für PostgreSQL-DB-Instances in Amazon RDS aktivieren
- Verschlüsseln Sie eine bestehende Amazon RDS for PostgreSQL PostgreSQL-DB-Instance
- Automatisches Tagging von Amazon RDS-Datenbanken beim Start erzwingen
- Schätzen Sie die Kosten einer DynamoDB-Tabelle für On-Demand-Kapazität
- Schätzung der Speicherkosten für eine Amazon DynamoDB-Tabelle
- Schätzen Sie die Größe der Amazon RDS-Engine für eine Oracle-Datenbank mithilfe von AWR-Berichten
- Exportieren Sie Amazon RDS for SQL Server-Tabellen mithilfe von AWS DMS in einen S3-Bucket
- Behandeln Sie anonyme Blöcke in dynamischen SQL-Anweisungen in Aurora PostgreSQL
- Behandeln Sie überladene Oracle-Funktionen in Aurora PostgreSQL-kompatibel
- Helfen Sie mit, DynamoDB-Tagging durchzusetzen
- Implementieren Sie regionsübergreifende Notfallwiederherstellung mit AWS DMS und Amazon Aurora
- Migrieren Sie Oracle-Funktionen und -Prozeduren mit mehr als 100 Argumenten nach PostgreSQL
- Migrieren Sie Amazon RDS for Oracle DB-Instances zu anderen Konten, die AMS verwenden
- Migrieren Sie Oracle OUT-Bind-Variablen in eine PostgreSQL-Datenbank
- Migrieren Sie SAP HANA zu AWS mithilfe von SAP HSR mit demselben Hostnamen
- Migrieren Sie SQL Server mithilfe verteilter Verfügbarkeitsgruppen zu AWS
- Migrieren Sie mithilfe von AWS DMS von Oracle 8i oder 9i zu Amazon RDS for Oracle SharePlex
- Überwachen Sie Amazon Aurora auf Instances ohne Verschlüsselung
- Überwachen Sie GoldenGate Oracle-Protokolle mithilfe von Amazon CloudWatch
- Replatform Oracle Database Enterprise Edition auf Standard Edition 2 auf Amazon RDS for Oracle
- Replizieren Sie Mainframe-Datenbanken mithilfe von Precisely Connect nach AWS
- Planen Sie Jobs für Amazon RDS for PostgreSQL und Aurora PostgreSQL mithilfe von Lambda und Secrets Manager
- Senden Sie Benachrichtigungen für eine Amazon RDS for SQL Server Server-Datenbank-Instance mithilfe eines lokalen SMTP-Servers und Datenbank-E-Mail
- Disaster Recovery für SAP auf IBM Db2 auf AWS einrichten
- Richten Sie mithilfe von Terraform eine CI/CD-Pipeline für die Datenbankmigration ein
- Richten Sie eine HA/DR-Architektur für Oracle E-Business Suite auf Amazon RDS Custom mit einer aktiven Standby-Datenbank ein

- Richten Sie die Datenreplikation zwischen Amazon RDS for MySQL und MySQL auf Amazon EC2 mithilfe von GTID ein
- Rollen für eine PeopleSoft Oracle-Anwendung auf Amazon RDS Custom for Oracle wechseln
- Daten aus einem Amazon Redshift Redshift-Cluster kontenübergreifend nach Amazon S3 entladen
- Datenbankmigrationsmuster nach Workload
- Mehr Muster

Greifen Sie von Microsoft SQL Server auf Amazon EC2 mithilfe von Verbindungsservern auf lokale Microsoft SQL Server-Tabellen zu

Erstellt von Tirumala Dasari (AWS) und Eduardo Valentim (AWS)

Übersicht

Dieses Muster beschreibt, wie Sie auf lokale Microsoft SQL Server-Datenbanktabellen zugreifen, die unter Microsoft Windows ausgeführt werden, von Microsoft SQL Server-Datenbanken aus, die auf Amazon Elastic Compute Cloud (Amazon EC2) Windows- oder Linux-Instances ausgeführt oder gehostet werden, mithilfe von Verbindungsservern.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Amazon EC2 mit Microsoft SQL Server, der auf Amazon Linux AMI (Amazon Machine Image) läuft
- AWS Direct Connect zwischen dem lokalen Microsoft SQL Server (Windows) -Server und der Windows- oder Linux-Instance EC2

Produktversionen

- SQL Server 2016 oder höher

Architektur

Quelltechnologie-Stack

- Lokale Microsoft SQL Server-Datenbank, die unter Windows ausgeführt wird
- Amazon EC2 mit Microsoft SQL Server, der auf Windows AMI oder Linux AMI läuft

Zieltechnologie-Stack

- Amazon EC2 mit Microsoft SQL Server, der auf Amazon Linux AMI läuft
- Amazon EC2 mit Microsoft SQL Server, der auf Windows AMI läuft

Quell- und Zieldatenbankarchitektur

Tools

- Microsoft SQL Server Management Studio (SSMS) ist eine integrierte Umgebung für die Verwaltung einer SQL Server-Infrastruktur. Es bietet eine Benutzeroberfläche und eine Gruppe von Tools mit umfangreichen Skripteditoren, die mit SQL Server interagieren.

Epen

Ändern Sie den Authentifizierungsmodus in Windows SQL Server auf Windows für SQL Server

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie über SSMS eine Connect zu Windows SQL Server her.		DBA
Ändern Sie den Authentif izierungsmodus in SQL Server über das Kontextmenü (Rechtsklick) für die Windows SQL Server-Instanz auf Windows.		DBA

Starten Sie den Windows MSSQL-Dienst neu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den SQL-Dienst neu.	1. Wählen Sie im SSMS Object Explorer die SQL Server-Instanz aus. 2. Öffnen Sie das Kontextme nü (Rechtsklick). 3. Wählen Sie Neu starten.	DBA

Erstellen Sie ein neues Login und wählen Sie Datenbanken aus, auf die Sie in Windows SQL Server zugreifen möchten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Öffnen Sie auf der Registerkarte Sicherheit das Kontextmenü (Rechtsklick) für Login und wählen Sie ein neues Login aus.		DBA
Wählen Sie auf der Registerkarte Allgemein die Option SQL Server-Authentifizierung aus, geben Sie einen Benutzernamen und das Kennwort ein, bestätigen Sie das Kennwort und deaktivieren Sie die Option zum Ändern des Kennworts bei der nächsten Anmeldung.		DBA
Wählen Sie auf der Registerkarte Serverrollen die Option Öffentlich aus.		DBA
Wählen Sie auf der Registerkarte Benutzerzuordnung die Datenbank und das Schema aus, auf das Sie zugreifen möchten, und markieren Sie dann die Datenbank, um Datenbankrollen auszuwählen.	Wählen Sie public und db_datareader aus, um auf Daten aus den Datenbanktabellen zuzugreifen.	DBA
Wählen Sie OK, um einen Benutzer zu erstellen.		DBA

Fügen Sie die Windows SQL Server-IP zur Linux SQL Server-Hostdatei hinzu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie über das Terminalfenster eine Connect zur Linux SQL Server-Box her.		DBA
Öffnen Sie die the /etc/hosts Datei und fügen Sie die IP-Adresse des Windows-Computers mit SQL Server hinzu.		DBA
Speichern Sie die Hosts-Datei.		DBA

Verbindungsserver auf Linux SQL Server erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Verbindungsserver mithilfe der gespeicherten Prozeduren master.sys.sp_addlinkedserver und master.dbo.sp_addlinkedsrvlogin.	Weitere Informationen zur Verwendung dieser gespeicherten Prozeduren finden Sie im Abschnitt Zusätzliche Informationen.	DBA, Entwickler

Überprüfen Sie den erstellten Verbindungsserver und die Datenbanken in SSMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gehen Sie in Linux SQL Server in SSMS zu Linked Servers und aktualisieren Sie die Datei.		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erweitern Sie die erstellte n Verbindungsserver und Kataloge im linken Bereich.	Sie sehen die ausgewählten SQL Server-Datenbanken mit Tabellen und Ansichten.	DBA

Stellen Sie sicher, dass Sie auf Windows SQL Server-Datenbanktabellen zugreifen können

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie im SSMS-Abfragefenster die folgende Abfrage aus: „select top 3 * from [sqllin] .dms_sample_win.dbo.mlb_data“.	Beachten Sie, dass die FROM-Klausel eine vierteilige Syntax verwendet: computer. database.schema.table (z. B. SELECT-Name „databases“ FROM [sqllin] .master.sys.databases). SQL2 In unserem Beispiel haben wir SQL2 in der Hosts-Datei einen Alias für erstellt, sodass Sie den tatsächlichen NetBIOS-Namen nicht zwischen den eckigen Klammern eingeben müssen. Wenn Sie die tatsächlichen NetBIOS-Namen verwenden, beachten Sie, dass AWS standardmäßig NetBIOS-Namen wie Win-XXXX verwendet und SQL Server eckige Klammern für Namen mit Bindestrichen benötigt.	DBA, Entwickler

Zugehörige Ressourcen

- Versionshinweise für SQL Server unter Linux

Zusätzliche Informationen

Verwenden von gespeicherten Prozeduren zum Erstellen von Verbindungsservern

SSMS unterstützt die Erstellung von Verbindungsservern für Linux SQL Server nicht, daher müssen Sie diese gespeicherten Prozeduren verwenden, um sie zu erstellen:

```
EXEC master.sys.sp_addlinkedserver @server= N'SQLLIN' , @srvproduct= N'SQL Server'
EXEC master.dbo.sp_addlinkedsrvlogin
 @rmtsrvname=N'SQLLIN',@useself=N'False',@locallogin=NULL,@rmtuser=N'username',@rmtpassword='Te
```

Hinweis 1: Geben Sie die Anmeldeinformationen, die Sie zuvor in Windows SQL Server erstellt haben, in die gespeicherte Prozedur ein. `master.dbo.sp_addlinkedsrvlogin`

Hinweis 2: `@server` Name `SQLLIN` und Name des Eintrags in der Hostdatei `172.12.12.4 SQLLIN` sollten identisch sein.

Sie können diesen Prozess verwenden, um Verbindungsserver für die folgenden Szenarien zu erstellen:

- Linux SQL Server zu Windows SQL Server über einen Verbindungsserver (wie in diesem Muster angegeben)
- Windows SQL Server zu Linux SQL Server über einen Verbindungsserver
- Linux SQL Server zu einem anderen Linux SQL Server über einen Verbindungsserver

Fügen Sie HA mithilfe einer Read Replica zu Oracle PeopleSoft auf Amazon RDS Custom hinzu

Erstellt von sampath kathirvel (AWS)

Übersicht

Um die Oracle PeopleSoft Enterprise Resource Planning (ERP) -Lösung auf Amazon Web Services (AWS) auszuführen, können Sie Amazon Relational Database Service (Amazon RDS) oder Amazon RDS Custom for Oracle verwenden, das ältere, benutzerdefinierte und verpackte Anwendungen unterstützt, die Zugriff auf das zugrunde liegende Betriebssystem und die Datenbankumgebung benötigen. Wichtige Faktoren, die bei der Planung einer Migration zu berücksichtigen sind, finden Sie unter Strategien zur Oracle-Datenbankmigration in AWS Prescriptive Guidance.

Zum jetzigen Zeitpunkt unterstützt RDS Custom for Oracle die Multi-AZ-Option nicht, die für Amazon RDS for Oracle als HA-Lösung mit Speicherreplikation verfügbar ist. Stattdessen wird mit diesem Muster HA erreicht, indem eine Standby-Datenbank verwendet wird, die eine physische Kopie der Primärdatenbank erstellt und verwaltet. Das Muster konzentriert sich auf die Schritte zum Ausführen einer PeopleSoft Anwendungsdatenbank auf Amazon RDS Custom mit HA, indem Oracle Data Guard zum Einrichten einer Read Replica verwendet wird.

Dieses Muster versetzt die Read Replica auch in den Nur-Lese-Modus. Wenn sich Ihre Read Replica im schreibgeschützten Modus befindet, bietet dies zusätzliche Vorteile:

- Auslagern von schreibgeschützten Workloads aus der Primärdatenbank
- Aktivierung der automatischen Reparatur beschädigter Blöcke durch Abrufen fehlerfreier Blöcke aus der Standby-Datenbank mithilfe der Oracle Active Data Guard-Funktion
- Verwendung der Far Sync-Funktion, um die Remote-Standby-Datenbank synchron zu halten, ohne den Leistungsaufwand, der mit der Redo-Log-Übertragung über große Entfernungen verbunden ist.

Für die Verwendung eines Replikats im schreibgeschützten Modus ist die Option Oracle Active Data Guard erforderlich, die mit zusätzlichen Kosten verbunden ist, da es sich um eine separat lizenzierte Funktion der Oracle Database Enterprise Edition handelt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine bestehende PeopleSoft Anwendung auf Amazon RDS Custom. Wenn Sie keine Anwendung haben, sehen Sie sich das Muster Migrate Oracle PeopleSoft to Amazon RDS Custom an.
- Eine einzige PeopleSoft Anwendungsebene. Sie können dieses Muster jedoch so anpassen, dass es mit mehreren Anwendungsebenen funktioniert.
- Amazon RDS Custom ist mit mindestens 8 GB Swap-Speicherplatz konfiguriert.
- Eine Oracle Active Data Guard-Datenbanklizenz für die Konvertierung der Read Replica in den Nur-Lese-Modus und deren Verwendung zum Auslagern von Berichtsaufgaben in den Standby-Modus. Weitere Informationen finden Sie in der kommerziellen Preisliste von Oracle Technology.

Einschränkungen

- Allgemeine Einschränkungen und nicht unterstützte Konfigurationen für RDS Custom for Oracle
- Einschränkungen im Zusammenhang mit Amazon RDS Custom for Oracle Read Replicas

Produktversionen

- Informationen zu Oracle-Datenbankversionen, die von Amazon RDS Custom unterstützt werden, finden Sie unter RDS Custom for Oracle.
- Informationen zu Oracle-Datenbankinstanzklassen, die von Amazon RDS Custom unterstützt werden, finden Sie unter DB-Instance-Klassenunterstützung für RDS Custom for Oracle.

Architektur

Zieltechnologie-Stack

- Amazon RDS Custom für Oracle
- AWS Secrets Manager
- Oracle Active Data Guard
- PeopleSoft Oracle-Anwendung

Zielarchitektur

Das folgende Diagramm zeigt eine Amazon RDS Custom DB-Instance und eine Amazon RDS Custom Read Replica. Die Read Replica verwendet Oracle Active Data Guard, um in eine andere

Availability Zone zu replizieren. Sie können die Read Replica auch verwenden, um den Lesetraffic auf die Primärdatenbank auszulagern und zu Berichtszwecken.

Eine repräsentative Architektur mit Oracle PeopleSoft auf AWS finden Sie unter Eine hochverfügbare PeopleSoft Architektur auf AWS einrichten.

Tools

AWS-Services

- Amazon RDS Custom for Oracle ist ein verwalteter Datenbankservice für ältere, benutzerdefinierte und verpackte Anwendungen, die Zugriff auf das zugrunde liegende Betriebssystem und die Datenbankumgebung benötigen.
- AWS Secrets Manager hilft Ihnen dabei, hartcodierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Geheimnis programmgesteuert abzurufen. In diesem Muster rufen Sie die Datenbankbenutzerkennwörter aus Secrets Manager für `RDS_DATAGUARD` mit dem geheimen Namen ab`do-not-delete-rds-custom-+<<RDS Resource ID>>+-dg`.

Andere Tools

- Oracle Data Guard unterstützt Sie bei der Erstellung, Wartung, Verwaltung und Überwachung von Standby-Datenbanken.

Bewährte Methoden

Um ein Ziel ohne Datenverlust (RPO=0) zu erreichen, verwenden Sie den `MaxAvailability` Data Guard-Schutzmodus mit der `SYNC+NOAFFIRM` Redo-Transport-Einstellung für eine bessere Leistung. Weitere Informationen zur Auswahl des Datenbankschutzmodus finden Sie im Abschnitt Zusätzliche Informationen.

Epen

Erstellen Sie die Read Replica

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Read Replica.	Um eine Read Replica der Amazon RDS Custom DB-Instance zu erstellen, folgen Sie den Anweisungen in der Amazon RDS-Dokumentation und verwenden Sie die Amazon RDS Custom DB-Instance, die Sie erstellt haben (siehe Abschnitt Voraussetzungen), als Quelldatenbank. Standardmäßig wird die Amazon RDS Custom Read Replica als physisches Standby erstellt und befindet sich im gemounteten Zustand. Dies dient dazu, die Einhaltung der Oracle Active Data Guard-Lizenz sicherzustellen. Dieses Muster enthält Code für die Einrichtung einer Multitenant-Container-Datenbank (CDB) oder einer Nicht-CDB-Instance.	DBA

Ändern Sie den Oracle Data Guard-Schutzmodus auf MaxAvailability

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Greifen Sie auf die Data Guard-Broker-Konfiguration in der Primärdatenbank zu.	In diesem Beispiel ist die Amazon RDS Custom Read Replica `RDS_CUSTOM_ORCL_D` für die Nicht-CDB-Instance und `RDS_CUSTOM_RDSCDB_B` für die CDB-Instance. Die Datenbanken für Nicht-CDB sind `orcl_a` (primär) und (Standby). `orcl_d` Die Datenbanknamen für CDB lauten `rdscdb_a` (primär) und `rdscdb_b` (Standby). Sie können direkt oder über die Primärdatenbank eine Verbindung zur RDS Custom Read Replica herstellen. Den Net Service Name für Ihre Datenbank finden Sie in der `tnsnames.ora` Datei im `$ORACLE_HOME/network/admin` Verzeichnis. RDS Custom for Oracle füllt diese Einträge automatisch für Ihre Primärdatenbank und Ihre Read Replicas aus. Das Passwort für den `RDS_DATAGUARD` Benutzer wird in AWS Secrets Manager mit einem geheimen Namen gespeichert`do-not-de`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`lete-rds-custom-+<<RDS Resource ID>>+-dg`. Weitere Informationen dazu, wie Sie mithilfe des von Secrets Manager abgerufenen SSH-Schlüssels (Secure Shell) eine Verbindung zu einer benutzerdefinierten RDS-Instance herstellen können, finden Sie unter Herstellen einer Verbindung zu Ihrer benutzerdefinierten RDS-DB-Instance mithilfe von SSH.
	
	Verwenden Sie den folgenden Code, um über die Data Guard-Befehlszeile (`dgmgrl`) auf die Oracle Data Guard-Broker-Konfiguration zuzugreifen.
	
	Nicht-CDB
	
	`$ dgmgrl RDS_DATAGUARD@RDS_CUSTOM_ORCL_D`
	`DGMGRL for Linux: Release 19.0.0.0.0 - Production on Fri Sep 30 22:44:49 2022`
	`Version 19.10.0.0.0`
	`Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved.`
	`Welcome to DGMGRL, type "help" for information.`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Password: Connected to "ORCL_D" Connected as SYSDG. DGMGRL> DGMGRL> show database orcl_d Database - orcl_d Role: PHYSICAL STANDBY Intended State: APPLY- ON Transport Lag: 0 seconds (computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Average Apply Rate: 11.00 KByte/s Instance(s): ORCL SUCCESS DGMGRL> CDB -bash-4.2$ dgmgrl C##RDS_DATAGUARD@R DS_CUSTOM_RDSCDB_B DGMGRL for Linux: Release 19.0.0.0.0 - Production on Wed Jan 11 20:24:11 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Welcome to DGMGRL, type "help" for informati on. Password:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Connected to "RDSCDB_B " Connected as SYSDG. DGMGRL> DGMGRL> show database rdscdb_b Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: 2.00 KByte/s Real Time Query: OFF Instance(s): RDSCDB Database Status: SUCCESS DGMGRL>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Ändern Sie die Einstellung für den Protokolltransport, indem Sie vom Primärknoten aus eine Verbindung zu DGMGRL herstellen.	Ändern Sie den Protokoll transportmodus auf`FastSync`, der der Redo-Transport-Ein stellung entspricht. `SYNC +NOAFFIRM` Um sicherzus tellen, dass Sie nach dem Rollenwechsel über gültige Einstellungen verfügen, ändern Sie diese Einstellu ngen sowohl für die Primärdat enbank als auch für die Standby-Datenbank.
	
	Nicht-CDB
	
	`DGMGRL>`
	`DGMGRL> edit database orcl_d set property logxptmode=fastsync;`
	`Property "logxptmode" updated`
	`DGMGRL> show database orcl_d LogXptMode;`
	`LogXptMode = 'fastsync'`
	`DGMGRL> edit database orcl_a set property logxptmode=fastsync;`
	`Property "logxptmode" updated`
	`DGMGRL> show database orcl_a logxptmode;`
	`LogXptMode = 'fastsync'`
	`DGMGRL>`
	
	CDB
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`DGMGRL> edit database rdscdb_b set property logxptmode=fastsyn c;DGMGRL> edit database rdscdb_b set property logxptmode=fastsync; Property "logxptmode" updated DGMGRL> show database rdscdb_b LogXptMode; LogXptMode = 'fastsync' DGMGRL> edit database rdscdb_a set property logxptmode=fastsync; Property "logxptmode" updated DGMGRL> show database rdscdb_a logxptmode; LogXptMode = 'fastsync' DGMGRL>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Ändern Sie den Schutzmodus auf MaxAvailability.	Ändern Sie den Schutzmodus auf, `MaxAvailability` indem Sie DGMGRL vom primären Knoten aus eine Verbindung herstellen.
	
	Nicht-CDB
	
	`DGMGRL> edit configuration set protection mode as maxavailability;`
	`Succeeded.`
	`DGMGRL> show configuration;`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
	`orcl_a - Primary database`
	`orcl_d - Physical standby database`
	`Fast-Start Failover: Disabled`
	`Configuration Status:`
	`SUCCESS (status updated 38 seconds ago)`
	`DGMGRL>`
	
	CDB
	
	`DGMGRL> show configuration`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	rdscdb_a - Primary database rdscdb_b - Physical standby database Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 57 seconds ago) DGMGRL>	

Ändern Sie den Replikatstatus von Mount in Read-Only und aktivieren Sie Redo Apply

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beenden Sie die Redo-Anwendung für die Standby-Datenbank.	Die Read Replica wird standardmäßig im `MOUNT` Modus erstellt. Um es im schreibgeschützten Modus zu öffnen, müssen Sie zuerst Redo Apply deaktivieren, indem Sie vom Primär- oder Standby-Knoten `DGMGRL` aus eine Verbindung zu herstellen. Kein CDB DGMGRL> show database orcl_dDGMGRL> show database orcl_d Database - orcl_d Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 1 second ago)	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: 11.00 KByte/s Real Time Query: OFF Instance(s): ORCL Database Status: SUCCESS DGMGRL> edit database orcl_d set state=app ly-off; Succeeded. DGMGRL> show database orcl_d Database - orcl_d Role: PHYSICAL STANDBY Intended State: APPLY- OFF Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 42 seconds (computed 1 second ago) Average Apply Rate: (unknown) Real Time Query: OFF Instance(s): ORCL Database Status: SUCCESS DGMGRL> CDB DGMGRL> show configura tionDGMGRL> show configuration Configuration - rds_dg Protection Mode: MaxAvailability	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Members: rdscdb_a - Primary database rdscdb_b - Physical standby database Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 57 seconds ago) DGMGRL> show database rdscdb_b; Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: 2.00 KByte/s Real Time Query: OFF Instance(s): RDSCDB Database Status: SUCCESS DGMGRL> edit database rdscdb_b set state=apply-off; Succeeded. DGMGRL> show database rdscdb_b; Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-OFF	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> Transport Lag:
	0 seconds (computed 1
	second ago)
	  Apply Lag:
	0 seconds (computed 1
	second ago)
	  Average Apply Rate:
	(unknown)
	  Real Time Query:
	OFF
	  Instance(s):
	    RDSCDB
	Database Status:
	SUCCESS</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Öffnen Sie die Read Replica-Instanz im schreibgeschützten Modus.	Stellen Sie mithilfe des TNS-Eintrags eine Connect zur Standby-Datenbank her und öffnen Sie sie im schreibgeschützten Modus, indem Sie vom Primär- oder Standby-Knoten aus eine Verbindung herstellen.
	
	Nicht-CDB
	
	`$ sqlplus RDS_DATAGUARD@RDS_CUSTOM_ORCL_D as sysdg`
	`-bash-4.2$ sqlplus RDS_DATAGUARD@RDS_CUSTOM_ORCL_D as sysdg`
	`SQL*Plus: Release 19.0.0.0.0 - Production on Fri Sep 30 23:00:14 2022`
	`Version 19.10.0.0.0`
	`Copyright (c) 1982, 2020, Oracle. All rights reserved.`
	`Enter password:`
	`Last Successful login time: Fri Sep 30 2022 22:48:27 +00:00`
	`Connected to:`
	`Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production`
	`Version 19.10.0.0.0`
	`SQL> select open_mode from v$database;`
	`OPEN_MODE`
	`--------------------`
	`MOUNTED`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SQL> alter database open read only; Database altered. SQL> select open_mode from v$database; OPEN_MODE -------------------- READ ONLY SQL>	
	CDB -bash-4.2$ sqlplus C##RDS_DATAGUARD@R DS_CUSTOM_RDSCDB_B as sysdg SQL*Plus: Release 19.0.0.0.0 - Productio n on Wed Jan 11 21:14:07 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2022, Oracle. All rights reserved. Enter password: Last Successful login time: Wed Jan 11 2023 21:12:05 +00:00 Connected to: Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production Version 19.16.0.0.0 SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- --------- ---------- RDSCDB MOUNTED	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`SQL> alter database open read only;`
	`Database altered.`
	`SQL> select name,open_mode from v$database;`
	`NAME OPEN_MODE`
	`--------- ----------`
	`----------`
	`RDSCDB READ ONLY`
	`SQL>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie Redo Apply auf der Read Replica-Instanz.	Aktivieren Sie Redo Apply auf der Read Replica-Instanz, indem Sie DGMGR L vom Primär- oder Standby-Knoten aus verwenden. Nicht-CDB `$ dgmgrl RDS_DATAG UARD@RDS_CUSTOM_OR CL_D DGMGRL for Linux: Release 19.0.0.0.0 - Production on Fri Sep 30 23:02:16 2022 Version 19.10.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Welcome to DGMGRL, type "help" for informati on. Password: Connected to "ORCL_D" Connected as SYSDG. DGMGRL> edit database orcl_d set state=apply-on; DGMGRL> edit database orcl_d set state=app ly-on; Succeeded. DGMGRL> show database orcl_d Database - orcl_d Role: PHYSICAL STANDBY Intended State: APPLY-ON`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
Transport Lag: 0
 seconds (computed 0
 seconds ago)
Apply Lag: 0 seconds
 (computed 0 seconds
 ago)
Average Apply Rate:
 496.00 KByte/s
Real Time Query: ON
Instance(s):
ORCL
Database Status:
SUCCESS
DGMGRL>
```

CDB

```
-bash-4.2$ dgmgrl
 C##RDS_DATAGUARD@R
DS_CUSTOM_RDSCDB_B
-bash-4.2$ dgmgrl
 C##RDS_DATAGUARD@R
DS_CUSTOM_RDSCDB_B
DGMGRL for Linux:
 Release 19.0.0.0.0 -
 Production on Wed Jan
 11 21:21:11 2023
Version 19.16.0.0.0
Copyright (c) 1982,
 2019, Oracle and/or
 its affiliates.  All
 rights reserved.
Welcome to DGMGRL, type
 "help" for informati
on.
Password:
Connected to "RDSCDB_B
"
Connected as SYSDG.
```

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	DGMGRL> edit database rdscdb_b set state=app ly-on; Succeeded. DGMGRL> show database rdscdb_b Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Average Apply Rate: 35.00 KByte/s Real Time Query: ON Instance(s): RDSCDB Database Status: SUCCESS DGMGRL> show database rdscdb_b Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: 16.00 KByte/s Real Time Query: ON Instance(s): RDSCDB	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`Database Status: SUCCESS DGMGRL>`	

Zugehörige Ressourcen

- Konfiguration von Amazon RDS als PeopleSoft Oracle-Datenbank (AWS-Whitepaper)
- Handbuch zu Oracle Data Guard Broker (Oracle-Referenzdokumentation)
- Konzepte und Verwaltung von Data Guard (Oracle-Referenzdokumentation)

Zusätzliche Informationen

Wählen Sie Ihren Datenbank-Schutzmodus

Oracle Data Guard bietet drei Schutzmodi, mit denen Sie Ihre Data Guard-Umgebung auf der Grundlage Ihrer Verfügbarkeits-, Schutz- und Leistungsanforderungen konfigurieren können. In der folgenden Tabelle sind diese drei Modi zusammengefasst.

Schutzmodus	Transporteinstellung wiederholen	Beschreibung
MAXIMALE LEISTUNG	`ASYNC`	Bei Transaktionen, die in der Primärdatenbank stattfinden, werden Redo-Daten asynchron übertragen und in das Redo-Log der Standby-Datenbank geschrieben. Daher sind die Auswirkungen auf die Leistung minimal. `MaxPerformance` RPO=0 kann aufgrund des asynchronen Protokollversands nicht bereitgestellt werden.

MAXIMALER SCHUTZ	SYNC+AFFIRM	Bei Transaktionen in der Primärdatenbank werden Redo-Daten synchron übertragen und in das Redo-Log der Standby-Datenbank auf der Festplatte geschrieben, bevor die Transaktion bestätigt wird. Wenn die Standby-Datenbank nicht mehr verfügbar ist, fährt sich die Primärdatenbank selbst herunter, um sicherzustellen, dass die Transaktionen geschützt sind.
MAXIMALE VERFÜGBARKEIT	SYNC+AFFIRM	Dies ist dem `MaxProtection` Modus ähnlich, außer wenn keine Bestätigung von der Standby-Datenbank empfangen wird. In diesem Fall verhält es sich so, als ob es sich im `MaxPerformance` Modus zur Aufrechterhaltung der Verfügbarkeit der Primärdatenbank befinde, bis es seinen Redo-Stream wieder in eine synchronisierte Standby-Datenbank schreiben kann.

`SYNC+NOAFFIRM`	Bei Transaktionen in der Primärdatenbank wird Redo synchron an die Standby-Datenbank übertragen, und die Primärdatenbank wartet nur auf die Bestätigung, dass das Redo in der Standby-Datenbank empfangen wurde, nicht darauf, dass es auf das Standby-Laufwerk geschrieben wurde. Dieser Modus, auch bekannt als `FastSync`, kann in einem speziellen Fall mehrerer gleichzeitiger Ausfälle einen Leistungsvorteil bieten, allerdings auf Kosten potenzieller Datenverluste.

Read Replicas in RDS Custom for Oracle werden im Schutzmodus mit maximaler Leistung erstellt, der auch der Standardschutzmodus für Oracle Data Guard ist. Der Modus mit maximaler Leistung hat die geringste Auswirkung auf die Leistung der Primärdatenbank, sodass Sie die in Sekunden gemessene Recovery Point Objective (RPO) -Anforderung erfüllen können.

Um ein Ziel ohne Datenverlust (RPO=0) zu erreichen, können Sie den Oracle Data Guard-Schutzmodus so anpassen, dass er die `SYNC+NOAFFIRM` Einstellung für Redo-Transport `MaxAvailability` enthält, um eine bessere Leistung zu erzielen. Da Commits in der Primärdatenbank erst bestätigt werden, nachdem die entsprechenden Redo-Vektoren erfolgreich an die Standby-Datenbank übertragen wurden, kann die Netzwerklatenz zwischen der Primärinstanz und dem Replikat für Workloads, bei denen ein Commit berücksichtigt wird, entscheidend sein. Wir empfehlen, Belastungstests für Ihren Workload durchzuführen, um die Auswirkungen auf die Leistung zu beurteilen, wenn die Read Replica so angepasst ist, dass sie im Modus ausgeführt wird. `MaxAvailability`

Die Bereitstellung der Read Replica in derselben Availability Zone wie die Primärdatenbank bietet eine geringere Netzwerklatenz als die Bereitstellung der Read Replica in einer anderen Availability Zone. Die Bereitstellung der primären Replicas und der Read Replicas in derselben Availability Zone

entspricht jedoch möglicherweise nicht Ihren HA-Anforderungen, da in dem unwahrscheinlichen Fall, dass die Availability Zone nicht verfügbar ist, sowohl die primäre Instanz als auch die Read Replica-Instanz betroffen sind.

Beurteilen Sie die Abfrageleistung für die Migration von SQL Server-Datenbanken zu MongoDB Atlas auf AWS

Erstellt von Battulga Purevragchaa (AWS), Krishnakumar Sathyanarayana (US Inc) und Babu Srinivasan (MongoDB) PeerIslands

Übersicht

Dieses Muster bietet Anleitungen zum Laden von MongoDB mit nahezu realen Daten und zur Bewertung der MongoDB-Abfrageleistung, die dem Produktionsszenario so nahe wie möglich kommt. Die Bewertung liefert Informationen, die Ihnen bei der Planung Ihrer Migration von einer relationalen Datenbank zu MongoDB helfen. Das Muster verwendet PeerIslands Test Data Generator und Performance Analyzer, um die Abfrageleistung zu testen.

Dieses Muster ist besonders nützlich für die Migration von Microsoft SQL Server zu MongoDB, da das Durchführen von Schematransformationen und das Laden von Daten aus aktuellen SQL Server-Instanzen nach MongoDB sehr komplex sein kann. Stattdessen können Sie nahezu reale Daten in MongoDB laden, die Leistung von MongoDB verstehen und das Schemadesign verfeinern, bevor Sie mit der eigentlichen Migration beginnen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Vertrautheit mit MongoDB Atlas
- MongoDB-Zielschema
- Typische Abfragemuster

Einschränkungen

- Die Ladezeiten und die Leistung von Daten werden durch die Größe der MongoDB-Clusterinstanz begrenzt. Wir empfehlen Ihnen, Instances auszuwählen, die für den Produktionseinsatz empfohlen werden, um die Leistung in der Praxis zu verstehen.
- PeerIslands Test Data Generator und Performance Analyzer unterstützen derzeit nur Online-Datenladungen und -abfragen. Die Offline-Batchverarbeitung (z. B. das Laden von Daten in MongoDB mithilfe von Spark-Konnektoren) wird noch nicht unterstützt.

- PeerIslands Test Data Generator und Performance Analyzer unterstützen Feldbeziehungen innerhalb einer Sammlung. Es unterstützt keine Beziehungen zwischen Sammlungen.

Produkteditionen

- Dieses Muster unterstützt sowohl MongoDB Atlas als auch MongoDB Enterprise Advanced.

Architektur

Zieltechnologie-Stack

- MongoDB Atlas oder MongoDB Enterprise Advanced

Architektur

PeerIslands Test Data Generator and Performance Analyzer wurde mithilfe von Java und Angular erstellt und speichert die generierten Daten im Amazon Elastic Block Store (Amazon EBS). Das Tool besteht aus zwei Workflows: Generierung von Testdaten und Leistungstests.

- Bei der Testdatengenerierung erstellen Sie eine Vorlage, bei der es sich um die JSON-Darstellung des Datenmodells handelt, das generiert werden muss. Nachdem Sie die Vorlage erstellt haben, können Sie die Daten in einer Zielsammlung generieren, wie in der Konfiguration zur Ladegenerierung definiert.
- Bei Leistungstests erstellen Sie ein Profil. Ein Profil ist ein mehrstufiges Testszenario, in dem Sie CRUD-Operationen (Create, Lese, Update and Delete), Aggregationspipelines, die Gewichtung für jeden Vorgang und die Dauer jeder Phase konfigurieren können. Nachdem Sie das Profil erstellt haben, können Sie auf der Grundlage der Konfiguration Leistungstests für die Zieldatenbank ausführen.

PeerIslands Test Data Generator and Performance Analyzer speichert seine Daten auf Amazon EBS, sodass Sie Amazon EBS mit MongoDB verbinden können, indem Sie jeden von MongoDB unterstützten Verbindungsmechanismus verwenden, einschließlich Peering, Zulassungslisten und privaten Endpunkten. Standardmäßig enthält das Tool keine Betriebskomponenten. Es kann jedoch bei Bedarf mit Amazon Managed Service for Prometheus, Amazon Managed Grafana CloudWatch, Amazon und AWS Secrets Manager konfiguriert werden.

Tools

- PeerIslands Test Data Generator und Performance Analyzer bestehen aus zwei Komponenten. Die Komponente Test Data Generator hilft Ihnen dabei, hochgradig kundenspezifische, reale Daten auf der Grundlage Ihres MongoDB-Schemas zu generieren. Das Tool ist vollständig UI-gesteuert und verfügt über eine umfangreiche Datenbibliothek. Es kann verwendet werden, um schnell Milliarden von Datensätzen auf MongoDB zu generieren. Das Tool bietet auch Funktionen zum Implementieren von Beziehungen zwischen Feldern im MongoDB-Schema. Die Performance Analyzer-Komponente hilft Ihnen dabei, hochgradig kundenspezifische Abfragen und Aggregationen zu generieren und realistische Leistungstests auf MongoDB durchzuführen. Sie können den Performance Analyzer verwenden, um die MongoDB-Leistung mit umfangreichen Lastprofilen und parametrisierten Abfragen für Ihren speziellen Anwendungsfall zu testen.

Bewährte Methoden

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Bewährte Methoden für das MongoDB-Schemadesign (MongoDB-Entwickler-Website)
- Bewährte Methoden für die Bereitstellung von MongoDB Atlas auf AWS (MongoDB-Website)
- Sicheres Verbinden von Anwendungen mit einer MongoDB Atlas-Datenebene mit AWS PrivateLink (AWS-Blogbeitrag)
- Leitfaden mit bewährten Methoden für die Leistung von MongoDB (MongoDB-Website)

Epen

Verstehen Sie Ihre Quelldaten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Machen Sie sich mit dem Datenbank-Footprint der aktuellen SQL Server-Quelle vertraut.	Machen Sie sich mit Ihrem aktuellen SQL Server-Fo otprint vertraut. Dies kann erreicht werden, indem Abfragen anhand des `INFORMATION` Datenbank schemas ausgeführt werden.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ermitteln Sie die Anzahl der Tabellen und die Größe jeder Tabelle. Analysieren Sie den Index, der jeder Tabelle zugeordnet ist. Weitere Informationen zur SQL-Analyse finden Sie im Blogbeitrag SQL2Mongo: Data Migration Journey auf der PeerIslands Website.	
Verstehen Sie das Quellschema.	Ermitteln Sie das Tabellenschema und die geschäftliche Darstellung der Daten (z. B. Postleitzahlen, Namen und Währung). Verwenden Sie Ihr vorhandenes Entitätsbeziehungsdiagramm (ER) oder generieren Sie das ER-Diagramm aus der vorhandenen Datenbank. Weitere Informationen finden Sie im Blogbeitrag SQL2Mongo: Data Migration Journey auf der PeerIslands Website.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verstehen Sie Abfragemuster.	Dokumentieren Sie die 10 am häufigsten verwendeten SQL-Abfragen. Sie können die Tabellen performan ce_schema.events_statements _summary_by_digest verwenden, die in der Datenbank verfügbar sind, um die häufigsten Abfragen zu verstehen. Weitere Informati onen finden Sie im Blogbeitr ag Mongo: Data Migration Journey auf der Website. SQL2 PeerIslands	DBA
Verstehen Sie die SLA-Verpf lichtungen.	Dokumentieren Sie die angestrebten Service Level Agreements (SLAs) für Datenbankoperationen. Zu den typischen Messgröße n gehören Abfragelatenz und Abfragen pro Sekunde. Die Maßnahmen und ihre Ziele sind in der Regel in Dokumenten zu den nichtfunk tionalen Anforderungen (NFR) enthalten.	DBA

Definieren Sie das MongoDB-Schema

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie das Zielschem a.	Definieren Sie verschied ene Optionen für das	MongoDB-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	MongoDB-Zielschema . Weitere Informationen finden Sie unter Schemas in der MongoDB Atlas-Dok umentation. Beachten Sie die bewährten Methoden und Entwurfsmuster, die auf den Tabellenbeziehunge n basieren. Einzelheiten finden Sie in der MongoDB-D okumentation unter Beispiele und Muster für Datenmodelle.	
Definieren Sie Zielabfra gemuster.	Definieren Sie MongoDB-Abfragen und Aggregati onspipelines. Diese Abfragen entsprechen den häufigste n Abfragen, die Sie für Ihre SQL Server-Arbeitslast erfasst haben. Informationen zum Aufbau von MongoDB-A ggregationspipelines finden Sie in der MongoDB-D okumentation.	MongoDB-Ingenieur
Definieren Sie den MongoDB-I nstanztyp.	Ermitteln Sie die Größe der Instanz, die Sie zum Testen verwenden möchten. Anleitungen finden Sie in der MongoDB-Dokumentation.	MongoDB-Ingenieur

Bereiten Sie die Zieldatenbank vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie den MongoDB Atlas-Cluster ein.	Folgen Sie den Anweisungen in der MongoDB-Dokumentation, um einen MongoDB-Cluster auf AWS einzurichten.	MongoDB-Ingenieur
Erstellen Sie Benutzer in der Zieldatenbank.	Konfigurieren Sie den MongoDB Atlas-Cluster für Zugriffs- und Netzwerksicherheit, indem Sie den Anweisungen in der MongoDB-Dokumentation folgen.	MongoDB-Ingenieur
Erstellen Sie entsprechende Rollen in AWS und konfigurieren Sie die rollenbasierte Zugriffskontrolle für Atlas.	Richten Sie bei Bedarf weitere Benutzer ein, indem Sie den Anweisungen in der MongoDB-Dokumentation folgen. Konfigurieren Sie Authentifizierung und Autorisierung über AWS-Rollen.	MongoDB-Ingenieur
Richten Sie Compass für den MongoDB Atlas-Zugriff ein.	Richten Sie das MongoDB Compass GUI Utility ein, um die Navigation und den Zugriff zu vereinfachen.	MongoDB-Ingenieur

Richten Sie die Grundlast mithilfe von Test Data Generator ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den Testdatengenerator.	Installieren Sie PeerIsland Test Data Generator in Ihrer Umgebung.	MongoDB-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Testdatengenerator, um die entsprechenden Daten zu generieren.	Erstellen Sie eine Vorlage, indem Sie die Datenbibl iothek verwenden, um spezifische Daten für jedes Feld im MongoDB-Schema zu generieren. Weitere Informationen finden Sie unter MongoDB Data Generator & Perf. Videoanalysator.	MongoDB-Ingenieur
Skalieren Sie den Testdaten generator horizontal, um die erforderliche Last zu generiere n.	Verwenden Sie die von Ihnen erstellte Vorlage, um die Lastgenerierung für die Zielsammlung zu starten, indem Sie die erforderliche Parallelität konfigurieren. Legen Sie die Zeitrahmen und den Umfang für die Generieru ng der erforderlichen Daten fest.	MongoDB-Ingenieur
Überprüfen Sie die Ladung in MongoDB Atlas.	Überprüfen Sie die in MongoDB Atlas geladenen Daten.	MongoDB-Ingenieur
Generieren Sie die erforderl ichen Indizes auf MongoDB.	Definieren Sie Indizes nach Bedarf auf der Grundlage von Abfragemustern. Bewährte Methoden finden Sie in der MongoDB-Dokumentation.	MongoDB-Ingenieur

Führen Sie Leistungstests durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Lastprofile in Performance Analyzer ein.	Erstellen Sie ein Leistungstestprofil in Performance Analyzer, indem Sie spezifische Abfragen und deren entsprechende Gewichtung, Dauer des Testlaufs und Phasen konfigurieren. Weitere Informationen finden Sie unter MongoDB Data Generator & Perf. Videoanalysator.	MongoDB-Ingenieur
Führen Sie Leistungstests durch.	Verwenden Sie das von Ihnen erstellte Leistungstestprofil, um den Test anhand der Zielsammlung zu starten, indem Sie die erforderliche Parallelität konfigurieren. Skalieren Sie das Leistungstest-Tool horizontal, um Abfragen gegen MongoDB Atlas auszuführen.	MongoDB-Ingenieur
Testergebnisse aufzeichnen.	Zeichnen Sie die P95- und P99-Latenz für die Abfragen auf.	MongoDB-Ingenieur
Optimieren Sie Ihr Schema und Ihre Abfragemuster.	Ändern Sie Indizes und Abfragemuster, um Leistungsprobleme zu beheben.	MongoDB-Ingenieur

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre AWS-Ressourcen herunter.	Löschen Sie alle temporäre n Ressourcen, die Sie für Test Data Generator und Performance Analyzer verwendet haben.	AWS-Administrator
Aktualisieren Sie die Ergebnisse der Leistungstests.	Verstehen Sie die Leistung von MongoDB-Abfragen und vergleichen Sie sie mit Ihrer SLAs. Passen Sie bei Bedarf das MongoDB-Schema an und führen Sie den Vorgang erneut aus.	MongoDB-Ingenieur
Schließe das Projekt ab.	Schließen Sie das Projekt ab und geben Sie Feedback.	MongoDB-Ingenieur

Zugehörige Ressourcen

- GitHub Repositorium: S3ToAtlas
- Schema: MongoDB-Schemadesign
- Aggregationspipelines: MongoDB-Aggregationspipelines
- MongoDB Atlas Sizing: Auswahl der Größenstufen
- Video: MongoDB-Datengenerator und Perf. Analysator
- Referenzen: MongoDB-Dokumentation
- Tutorials: MongoDB-Entwicklerhandbuch, MongoDB Jumpstart
- AWS Marketplace: MongoDB Atlas auf AWS Marketplace
- AWS-Partnerlösungen: MongoDB Atlas auf AWS-Referenzbereitstellung

Zusätzliche Ressourcen:

- SQL-Analyse
- Foren der MongoDB-Entwickler-Community
- Fragen zur MongoDB-Leistungsoptimierung
- Operational Analytics mit Atlas und Redshift
- Anwendungsmodernisierung mit MongoDB Atlas und AWS Elastic Beanstalk

Automatisieren Sie blaue/grüne Bereitstellungen globaler Amazon Aurora Aurora-Datenbanken mithilfe von IaC-Prinzipien

Erstellt von Ishwar Chauthaiwale (AWS), ANKIT JAIN (AWS) und Ramu Jagini (AWS)

Übersicht

Die Verwaltung von Datenbank-Updates, Migrationen oder Skalierungsmaßnahmen kann für Unternehmen, die kritische Workloads auf globalen Amazon Aurora Aurora-Datenbanken ausführen, eine Herausforderung darstellen. Die Sicherstellung, dass diese Vorgänge reibungslos und ohne Ausfallzeiten ausgeführt werden, ist für die Aufrechterhaltung der Serviceverfügbarkeit und die Vermeidung von Unterbrechungen für Ihre Benutzer von entscheidender Bedeutung.

Eine blue/green deployment strategy offers a solution to this challenge by allowing you to run two identical environments concurrently: blue (the current environment) and green (the new environment). A blue/green Strategie ermöglicht es Ihnen, Änderungen zu implementieren, Tests durchzuführen und den Datenverkehr zwischen Umgebungen mit minimalem Risiko und minimalen Ausfallzeiten zu verlagern.

Dieses Muster hilft Ihnen dabei, den Blau/Grün-Bereitstellungsprozess für globale Aurora-Datenbanken zu automatisieren, indem Sie die Prinzipien von Infrastructure as Code (IaC) verwenden. Es verwendet AWS CloudFormation, AWS Lambda, und Amazon Route 53, um blaue/grüne Bereitstellungen zu vereinfachen. Um die Zuverlässigkeit zu verbessern, verwendet es globale Transaktions-Identifikatoren (GTIDs) für die Replikation. Die GTID-basierte Replikation bietet im Vergleich zur Replikation von Binärprotokollen (Binlog) eine bessere Datenkonsistenz und Failover-Funktionen zwischen Umgebungen.

> **Note**
>
> Bei diesem Muster wird davon ausgegangen, dass Sie einen globalen Datenbankcluster der Aurora MySQL-Compatible Edition verwenden. Wenn Sie stattdessen Aurora PostgreSQL-kompatibel verwenden, verwenden Sie bitte die PostgreSQL-Entsprechungen der MySQL-Befehle.

Wenn Sie den Schritten in diesem Muster folgen, können Sie:

- Stellen Sie eine grüne globale Aurora-Datenbank bereit: Mithilfe von CloudFormation Vorlagen erstellen Sie eine grüne Umgebung, die Ihre bestehende blaue Umgebung widerspiegelt.

- GTID-basierte Replikation einrichten: Sie konfigurieren die GTID-Replikation so, dass die blauen und grünen Umgebungen synchronisiert bleiben.
- Nahtloses Umschalten des Datenverkehrs: Sie verwenden Route 53 und Lambda, um den Verkehr nach der vollständigen Synchronisation automatisch von der blauen in die grüne Umgebung umzuschalten.
- Schließen Sie die Bereitstellung ab: Sie überprüfen, ob die grüne Umgebung als primäre Datenbank voll funktionsfähig ist, beenden dann die Replikation und bereinigen alle temporären Ressourcen.

Der Ansatz in diesem Muster bietet die folgenden Vorteile:

- Reduziert Ausfallzeiten bei wichtigen Datenbankaktualisierungen oder Migrationen: Die Automatisierung gewährleistet einen reibungslosen Übergang zwischen Umgebungen mit minimalen Serviceunterbrechungen.
- Ermöglicht schnelle Rollbacks: Wenn nach der Umstellung des Datenverkehrs auf die grüne Umgebung ein Problem auftritt, können Sie schnell zur blauen Umgebung zurückkehren und die Servicekontinuität aufrechterhalten.
- Verbessert das Testen und Überprüfen: Die grüne Umgebung kann vollständig getestet werden, ohne dass die Live-Blue-Umgebung beeinträchtigt wird, wodurch die Wahrscheinlichkeit von Produktionsfehlern verringert wird.
- Sorgt für Datenkonsistenz: Die GTID-basierte Replikation sorgt dafür, dass Ihre blauen und grünen Umgebungen synchron bleiben, wodurch Datenverlust oder Inkonsistenzen während der Migration vermieden werden.
- Sorgt für Geschäftskontinuität: Durch die Automatisierung Ihrer blauen/grünen Implementierungen können Sie lange Ausfälle und finanzielle Verluste vermeiden, da Ihre Dienste während Updates oder Migrationen verfügbar bleiben.

Voraussetzungen und Einschränkungen

Voraussetzungen

- AWS-Konto Ein aktiver.
- Ein mit Aurora MySQL kompatibler globaler Quelldatenbankcluster (blaue Umgebung). Globale Datenbanken bieten eine Konfiguration mit mehreren Regionen für Hochverfügbarkeit und

Notfallwiederherstellung. Anweisungen zum Einrichten eines globalen Datenbank-Clusters finden Sie in der Aurora-Dokumentation.

- Die GTID-basierte Replikation ist auf dem Quell-Cluster aktiviert.

Einschränkungen

- Einige AWS-Services sind nicht in allen verfügbar. AWS-Regionen Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie auf der Seite Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Produktversionen

- Aurora MySQL-kompatibel 8.0 oder höher

Architektur

Das Diagramm veranschaulicht folgende Vorgänge:

- Globales Datenbank-Setup: Ein globaler Aurora-Datenbankcluster wird strategisch in zwei Clustern eingesetzt AWS-Regionen. Diese Konfiguration ermöglicht eine geografische Verteilung und regionale Redundanz für verbesserte Disaster Recovery-Funktionen.
- Replikation von primärer zu sekundärer Region: Der logische Replikationsmechanismus gewährleistet eine nahtlose Datensynchronisierung von der primären Region zur sekundären Region. Diese Replikation gewährleistet die Datenkonsistenz mit minimaler Latenz über geografische Entfernungen hinweg.
- GTID-basierte Replikation zwischen Clustern: Die GTID-basierte Replikation gewährleistet die Transaktionskonsistenz und den geordneten Datenfluss zwischen dem blauen Primärcluster und dem grünen Primärcluster und gewährleistet eine zuverlässige Datensynchronisierung.
- Blaue Primär- zu Sekundärreplikation: Die logische Replikation stellt eine robuste Datenpipeline zwischen dem blauen Primärcluster und seinem sekundären Cluster her. Diese Replikation ermöglicht eine kontinuierliche Datensynchronisierung und hohe Verfügbarkeit.
- Route 53-DNS-Konfiguration: Route 53-Einträge für gehostete Zonen verwalten die DNS-Auflösung für alle blauen und grünen Cluster-Datenbank-Endpunkte. Diese Konfiguration ermöglicht

eine nahtlose Zuordnung von Endpunkten und ermöglicht eine effiziente Weiterleitung des Datenverkehrs in Failover-Szenarien.

Tools

AWS-Services

- Amazon Aurora ist eine vollständig verwaltete relationale Datenbank-Engine, die für die Cloud entwickelt wurde und mit MySQL und PostgreSQL kompatibel ist.
- AWS CloudFormationhilft Ihnen dabei, Ihre AWS Ressourcen zu modellieren und einzurichten, sodass Sie weniger Zeit mit der Verwaltung dieser Ressourcen verbringen und sich mehr auf Ihre Anwendungen konzentrieren können, auf denen sie ausgeführt werden. AWS Sie erstellen eine Vorlage, die alle AWS Ressourcen beschreibt, die Sie benötigen, und CloudFormation kümmert sich um die Bereitstellung und Konfiguration dieser Ressourcen für Sie.
- AWS Lambdaist ein Rechendienst, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.

Bewährte Methoden

Wir empfehlen Ihnen, die AWS Dokumentation gründlich zu lesen, um Ihr Verständnis der Blau/Grün-Implementierungsstrategie, der GTID-basierten Replikation und der gewichteten Routing-Richtlinien in Route 53 zu vertiefen. Dieses Wissen ist entscheidend für die effektive Implementierung und Verwaltung Ihrer Datenbankmigrationen, die Sicherstellung der Datenkonsistenz und die Optimierung des Datenverkehrs. Wenn Sie sich ein umfassendes Verständnis dieser AWS Funktionen und Best Practices aneignen, sind Sie besser gerüstet, um future Updates zu bewältigen, Ausfallzeiten zu minimieren und eine belastbare und sichere Datenbankumgebung aufrechtzuerhalten.

Richtlinien für die Verwendung von AWS-Services für dieses Muster finden Sie in der folgenden AWS Dokumentation:

- Bewährte Methoden mit Amazon Aurora MySQL
- AWS CloudFormation bewährte Verfahren
- Bewährte Methoden für die Arbeit mit AWS Lambda Funktionen
- Bewährte Methoden für Amazon Route 53

Epen

Schaffen Sie die grüne Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Snapshot-Backup aus dem blauen Cluster.	In einer blauen/grünen Bereitstellung steht die grüne Umgebung für eine neue, identische Version Ihrer aktuellen (blauen) Datenbank umgebung. Sie verwenden die grüne Umgebung, um Updates sicher zu testen, Änderungen zu validieren und die Stabilität sicherzus tellen, bevor Sie den Produktio nsdatenverkehr wechseln. Sie dient als Zwischenstation für die Implementierung von Datenbankänderungen bei minimaler Unterbrechung der Live-Umgebung. Um eine grüne Umgebung zu schaffen, erstellen Sie zunächst einen Snapshot des primären (blauen) Clusters in Ihrer Aurora MySQL-kom patiblen globalen Datenbank . Dieser Snapshot dient als Grundlage für die Schaffung einer grünen Umgebung. Um einen Snapshot zu erstellen:	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Melden Sie sich bei der Amazon Relational Database Service (Amazon RDS) -Konsole an AWS Management Console und öffnen Sie sie. 2. Wählen Sie Ihren primären (blauen) Cluster aus. 3. Wählen Sie „Aktionen“, „Snapshot erstellen“. 4. Geben Sie einen Namen für den Snapshot ein, z. B.`blue-green-demo`, und starten Sie den Backup-Vorgang. Alternativ können Sie das AWS Command Line Interface (AWS CLI) verwenden, um den Snapshot zu erstellen: `aws rds create-db-cluster-snapshot --db-cluster-snapshot-identifier blue-green-demo --db-cluster-identifier ex-global-cluster --region eu-west-1` Stellen Sie sicher, dass der Snapshot erfolgreich abgeschlossen wurde, bevor Sie mit dem nächsten Schritt fortfahren.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie die CloudFormation Vorlage für Ihre globale Datenbank und ihre Ressourcen.	Der CloudFormation IaC-Generator hilft Ihnen, CloudFormation Vorlagen aus vorhandenen AWS Ressourcen zu generieren. Verwenden Sie diese Funktion, um eine CloudFormation Vorlage für Ihre bestehende Aurora MySQL-kompatible globale Datenbank und die zugehörigen Ressourcen zu erstellen. Diese Vorlage konfiguriert Subnetzgruppen, Sicherheitsgruppen, Parametergruppen und andere Einstellungen. 1. Folgen Sie den Anweisungen in der CloudFormation Dokumentation, um zum Tool zu navigieren und es mit Ihrer AWS Umgebung zu verbinden. 2. Wählen Sie Ihre globale Aurora-Datenbank und die zugehörigen Ressourcen aus, um die Vorlage zu generieren.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die CloudFormation Vorlage für die grüne Umgebung.	Passen Sie die CloudFormation Vorlage an die Einstellungen für die grüne Umgebung an. Dazu gehört die Aktualisierung der Ressourcennamen und -kennungen, um sicherzustellen, dass die grüne Umgebung unabhängig vom blauen Cluster funktioniert. 1. Aktualisieren Sie die `DBInstanceIdentifier` Eigenschaften `DBClusterIdentifier` und, sodass sie die grüne Umgebung repräsentieren. 2. Ändern Sie andere Ressourcennamen (z. B. Subnetzgruppen und Sicherheitsgruppen), um Konflikte mit der vorhandenen blauen Umgebung zu vermeiden. 3. Aktivieren Sie die GTID-basierte Replikation in der Vorlage, indem Sie die richtigen Parameter konfigurieren, wie in der Aurora-Dokumentation beschrieben. 4. Ändern Sie die `SnapshotIdentifier` Eigenschaft, um die AWS-Region,	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ihre Konto-ID und den Namen des Snapshots aus dem vorherigen Schritt anzugeben: `SnapshotIdentifier: arn:aws:rds:<region>:<account-id>:snapshot:<snapshot-name>` **Note** Wenn Sie die `SnapshotIdentifier` Eigenschaft verwenden, um einen DB-Cluster wiederherzustellen, vermeiden Sie es, Eigenschaften wie `GlobalClusterIdentifier` `MasterUsername` , oder anzugeben `MasterUserPassword` .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den CloudFormation Stack bereit, um Ressourcen für eine grüne Umgebung zu schaffen.	In diesem Schritt stellen Sie die benutzerdefinierte CloudFormation Vorlage bereit, um die Ressourcen für die grüne Umgebung zu erstellen. So stellen Sie den CloudFormation Stack bereit: 1. Öffnen Sie die AWS CloudFormation -Konsole. 2. Wählen Sie oben rechts Stapel erstellen, Mit neuen Ressourcen (Standard) aus. 3. Laden Sie Ihre geänderte CloudFormation Vorlage hoch oder geben Sie die Vorlagen-URL an. Wählen Sie Weiter aus. 4. Geben Sie einen Stack-Namen wie `GreenClusterStack` ein und geben Sie alle erforderlichen Parameter an (z. B.`GreenClusterIdentifier`). Wählen Sie Weiter aus. 5. Konfigurieren Sie nach Bedarf zusätzliche Stack-Optionen und aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass dadurch CloudFormation möglicher	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	weise AWS Identity and Access Management (IAM-) Ressourcen erstellt werden. Wählen Sie Weiter aus. 6. Überprüfen Sie die Stack-Details. 7. Wählen Sie Absenden aus. CloudFormation leitet den Prozess der Schaffung der Ressourcen für eine grüne Umwelt ein. Dieser Vorgang kann mehrere Minuten in Anspruch nehmen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie den CloudFormation Stack und die Ressourcen.	Wenn die CloudFormation Stack-Bereitstellung abgeschlossen ist, müssen Sie überprüfen, ob die grüne Umgebung erfolgreich erstellt wurde: 1. Überprüfen Sie im Abschnitt Outputs des CloudFormation Stacks die Endpunkte des Datenbank-Clusters und der Datenbank-Instance, um die korrekte Einrichtung zu überprüfen. 2. Öffnen Sie die Amazon RDS-Konsole und vergewissern Sie sich, dass der neue Aurora-Datenbankcluster (grüne Umgebung) verfügbar ist. 3. Stellen Sie sicher, dass alle zugehörigen Ressourcen, wie Subnetze und Sicherheitsgruppen, erstellt und mit der grünen Umgebung verknüpft wurden. Nach der Überprüfung ist Ihre grüne Umgebung bereit für die weitere Einrichtung, einschließlich der Replikation aus der blauen Umgebung.	DBA

GTID-basierte Replikation konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die GTID-Einstellungen auf dem blauen Cluster.	GTIDs bieten eine äußerst zuverlässige Methode für die Replikation von Daten zwischen Ihren blauen und grünen Umgebungen. Die GTID-basierte Replikation bietet einen robusten, vereinfachten Ansatz, bei dem jeder Transaktion in der blauen Umgebung eine eindeutige Kennung zugewiesen wird. Diese Methode stellt sicher, dass die Datensynchronisierung zwischen Umgebungen nahtlos, konsistent und einfacher zu verwalten ist als die herkömmliche Binlog-Replikation. Bevor Sie die Replikation konfigurieren, müssen Sie sicherstellen, dass die GTID-basierte Replikation auf dem blauen Cluster ordnungsgemäß aktiviert ist. Dieser Schritt garantiert, dass jede Transaktion in der blauen Umgebung eindeutig nachverfolgt wird und in der grünen Umgebung repliziert werden kann.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Um zu überprüfen, ob GTID aktiviert ist: 1. Überprüfen Sie auf der Amazon RDS-Konsole die Parametergruppe, die dem blauen Cluster zugewiesen ist. 2. Stellen Sie sicher, dass die folgenden Parameter eingestellt sind: • `gtid-mode = ON` • `enforce_gtid_consistency = ON` Diese Einstellungen ermöglichen das GTID-Tracking für alle future Transaktionen in der blauen Umgebung. Nachdem Sie diese Einstellungen bestätigt haben, können Sie mit der Einrichtung der Replikation beginnen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Replikationsbenutzer.	Um Daten aus der blauen Umgebung in die grüne Umgebung zu replizieren, müssen Sie einen dedizierten Replikationsbenutzer auf dem blauen Cluster erstellen. Dieser Benutzer ist für die Verwaltung des Replikationsprozesses verantwortlich. So richten Sie den Replikationsbenutzer ein: 1. Stellen Sie mithilfe eines MySQL-Clients eine Connect zum blauen Cluster her. 2. Führen Sie die folgenden Befehle aus, um den Replikationsbenutzer zu erstellen: `CREATE USER 'repl_user'@'%' IDENTIFIED BY 'repl_password'; GRANT REPLICATION SLAVE ON . TO 'repl_user'@'%'; FLUSH PRIVILEGES;` Dieser Benutzer verfügt jetzt über die erforderlichen Berechtigungen, um Daten zwischen den beiden Umgebungen zu replizieren.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die GTID-basierte Replikation auf dem grünen Cluster.	Der nächste Schritt besteht darin, den grünen Cluster für die GTID-basierte Replikation zu konfigurieren. Dieses Setup stellt sicher, dass die grüne Umgebung kontinuierlich alle Transaktionen widerspiegelt, die in der blauen Umgebung stattfinden. Um den grünen Cluster zu konfigurieren: 1. Stellen Sie mithilfe eines MySQL-Clients eine Connect zum grünen Cluster her. 2. Führen Sie den folgenden Befehl aus, um die Replikation zu konfigurieren: `CHANGE MASTER TO MASTER_HOST='blue-cluster-endpoint', MASTER_USER='repl_user', MASTER_PASSWORD='repl_password', MASTER_AUTO_POSITION=1;` Wobei: • `blue-cluster-endpoint` Ersetzen Sie es durch den Endpunkt Ihres blauen Clusters.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Die `MASTER_AUTO_POSITION=1` Einstellung weist MySQL an, die GTID-basierte Replikation zu verwenden. Sie positioniert den grünen Cluster automatisch so, dass er die Transaktionen des blauen Clusters repliziert, ohne dass Logs und Positionen manuell nachverfolgt werden müssen.	
Starten Sie die Replikation auf dem grünen Cluster.	Sie können jetzt den Replikationsprozess starten. Führen Sie auf dem grünen Cluster den folgenden Befehl aus: `START SLAVE;` Dadurch kann die grüne Umgebung mit der Datensynchronisierung und dem Empfangen und Anwenden von Transaktionen aus der blauen Umgebung beginnen.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Replikationsprozess.	Gehen Sie wie folgt vor, um zu überprüfen, ob die grüne Umgebung die Daten aus dem blauen Cluster korrekt repliziert: 1. Führen Sie den folgenden Befehl auf dem grünen Cluster aus, um den Replikationsstatus zu überprüfen: `SHOW SLAVE STATUS\G;` 2. Überprüfen Sie die Ausgabe, um Folgendes zu überprüfen: • `Slave_IO_Running = Yes` • `Slave_SQL_Running = Yes` • Die `Executed_Gtid_Set` Werte `Retrieved_Gtid_Set` up-to-date und sind mit dem blauen Cluster synchronisiert. • In dem `Last_Error` Feld liegen keine Replikationsfehler vor. Wenn alle Indikatoren korrekt sind, funktioniert die GTID-basierte Replikation reibungsl	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	os und die grüne Umgebung ist vollständig mit der blauen Umgebung synchronisiert.	

Schalten Sie den Verkehr vom blauen auf den grünen Cluster um

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Richtlini en für gewichtetes Route-53-Routing.	Nachdem Sie die Datenkons istenz zwischen der blauen und der grünen Umgebung überprüft haben, können Sie den Datenverkehr vom blauen Cluster auf den grünen Cluster umstellen. Dieser Übergang sollte reibungslos ablaufen, Ausfallzeiten minimieren und die Integrität der Datenbank Ihrer Anwendung sicherste llen. Um diesen Anforderu ngen gerecht zu werden, können Sie Route 53 für DNS-Routing und Lambda zur Automatisierung des Verkehrswechsels verwenden . Darüber hinaus stellt ein klar definierter Rollback-Plan sicher, dass Sie bei Problemen zum blauen Cluster zurückkehren können. Der erste Schritt besteht darin, gewichtetes Routing in Route 53 zu konfigurieren. Mit gewichtetem Routing	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	können Sie die Verteilung des Datenverkehrs zwischen den blauen und grünen Clustern steuern und den Verkehr schrittweise von einer Umgebung in die andere verlagern. So konfigurieren Sie gewichtetes Routing: 1. Öffnen Sie die Route 53-Konsole und wählen Sie Ihre gehostete Zone aus. 2. Erstellen Sie zwei DNS-Einträge (CNAMEs) für die Datenbank: einen Datensatz für den blauen Cluster und einen Datensatz für den grünen Cluster. 3. Weisen Sie Anfangsgewichte zu: • Legen Sie eine niedrige Anfangsgewichtung (z. B. 5 Prozent) für den grünen Cluster fest, um einen kleinen Teil des Datenverkehrs zu Testzwecken weiterzuleiten. • Legen Sie eine höhere Gewichtung (z. B. 95 Prozent) für den blauen Cluster fest, damit der	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Großteil des Datenverkehrs darin gespeichert wird. Mit dieser Konfiguration können Sie einen schrittweisen Übergang durchführen, der das Risiko reduziert und Echtzeittests unterstützt, bevor Sie vollständig umsteigen. Weitere Informationen zu Richtlinien für gewichtetes Routing finden Sie in der Dokumentation zu Route 53.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie eine Lambda-Funktion bereit, um die Replikationsverzögerung zu überwachen.	Um sicherzustellen, dass die grüne Umgebung vollständig mit der blauen Umgebung synchronisiert ist, stellen Sie eine Lambda-Funktion bereit, die die Replikationsverzögerung zwischen den Clustern überwacht. Diese Funktion kann den Replikationsstatus, insbesondere die Seconds_Behind_Master-Metrik, überprüfen, um festzustellen, ob der grüne Cluster bereit ist, den gesamten Datenverkehr zu verarbeiten.
	
	Hier ist ein Beispiel für eine Lambda-Funktion, die Sie verwenden können:
	
	`import boto3`
	
	`def check_replication_lag(event, context):`
	`client = boto3.client('rds')`
	`response = client.describe_db_instances(DBInstanceIdentifier='green-cluster-instance')`
	`replication_status = response['DBInstances'][0]['ReadReplicaDBInstanceIdentifiers']`
	`if replication_status:`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>lag = replicati
	on_status[0]['Repl
	icationLag']
	return lag
	return -1</pre>
	Diese Funktion überprüft die Verzögerung bei der Replikation und gibt den Wert zurück. Wenn die Verzögerung Null ist, ist der grüne Cluster vollständig mit dem blauen Cluster synchronisiert.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Automatisieren Sie die DNS-Gewichtsanpassung mithilfe von Lambda.	Wenn die Verzögerung bei der Replikation Null erreicht, ist es an der Zeit, den gesamten Datenverkehr auf den grünen Cluster umzustellen. Sie können diesen Übergang automatisieren, indem Sie eine weitere Lambda-Funktion verwenden, die die DNS-Gewichtungen in Route 53 so anpasst, dass 100 Prozent des Datenverkehrs an den grünen Cluster weitergeleitet werden.
	
	Hier ist ein Beispiel für eine Lambda-Funktion, die den Traffic Switch automatisiert:
	
	`import boto3`
	
	`def switch_traffic(eve nt, context):`
	`route53 = boto3.cli ent('route53')`
	`lag = check_rep lication_lag(event, context)`
	`if lag == 0:`
	`response = route53.change_res ource_record_sets(`
	`HostedZon eId='YOUR_HOSTED_Z ONE_ID',`
	`ChangeBat ch={`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	'Changes': [
	{
	'Action': 'UPSERT',
	'ResourceRecordSet':
	{
	'Name': 'db.examp
	le.com',
	'Type': 'CNAME',
	'SetIdentifier':
	'GreenCluster',
	'Weight': 100,
	'TTL': 60,
	'ResourceRecords':
	[{'Value': 'green-cl
	uster-endpoint'}]
	}
	},
	{
	'Action': 'UPSERT',
	'ResourceRecordSet':
	{
	'Name': 'db.examp
	le.com',
	'Type': 'CNAME',
	'SetIdentifier':
	'BlueCluster',	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
    'Weight': 0,

    'TTL': 60,

    'ResourceRecords':
 [{'Value': 'blue-clu
ster-endpoint'}]

 }
                    }
                ]
            }
        )
        return response
```

Diese Funktion überprüft die Replikationsverzögerung und aktualisiert die Route 53-DNS-Gewichtungen, wenn die Verzögerung Null ist, um den Datenverkehr vollständig auf den grünen Cluster umzuleite n.

> **Note**
>
> Wenn während der Umstellung auf den blauen Cluster ein hoher Schreibverkehr auftritt, sollten Sie erwägen, die Schreibvo rgänge während der Umstellung vorüberge hend zu unterbrec hen. Dadurch wird

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	sichergestellt, dass die Replikation aufholt, und Dateninkonsistenzen zwischen den blauen und grünen Clustern werden vermieden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Traffic Switch.	Nachdem die Lambda-Fu nktion die DNS-Gewichtungen angepasst hat, sollten Sie überprüfen, ob der gesamte Datenverkehr an den grünen Cluster geleitet wird und ob der Switch erfolgreich war. Um zu überprüfen: 1. Überwachen Sie die Route 53-DNS-Einträge, um sicherzustellen, dass der Datenverkehr an den grünen Cluster weitergel eitet wird. Weitere Informati onen finden Sie in der Route 53-Dokumentation. 2. Überprüfen Sie die Anwendungsleistung, indem Sie sicherstellen, dass Benutzer von der grünen Umgebung aus bedient werden. 3. Überprüfen Sie die Datenbankverbindun gen, um sicherzustellen, dass der grüne Cluster alle Datenbankanfragen verarbeitet. 4. Überwachen Sie die CloudWatch Amazon-Me triken auf Anzeichen von Latenz, Replikationsverzög	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	erung oder Leistungs einbußen. Weitere Informati onen finden Sie in der Aurora-Dokumentation. Wenn alles wie erwartet funktioniert, ist der Traffic Switch abgeschlossen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wenn Sie auf Probleme stoßen, machen Sie die Änderungen rückgängig.	Ein Rollback-Plan ist entscheidend für den Fall, dass nach dem Verkehrsw echsel Probleme auftreten. So können Sie bei Bedarf schnell zum blauen Cluster zurückkeh ren: 1. DNS-Gewichtungen in Route 53 rückgängig machen: Verwenden Sie dieselbe Lambda-Funktion oder passen Sie die Route 53-DNS-Gewichtungen manuell an, um 100 Prozent des Datenverkehrs zurück zum blauen Cluster zu leiten. 2. Überwachen Sie die Anwendungsleistung: Überwachen Sie sofort die Anwendungsprotokol le, CloudWatch Metriken und die Datenbankleistung, um sicherzustellen, dass die Probleme durch den Wechsel zurück zur blauen Umgebung behoben wurden. 3. Identifizieren und lösen Sie Probleme: Untersuchen und beheben Sie alle Probleme mit dem grünen Cluster,	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bevor Sie erneut versuchen, den Traffic zu wechseln. Durch die Implementierung dieses Rollback-Plans können Sie sicherstellen, dass Ihre Benutzer bei unerwarteten Problemen so wenig wie möglich gestört werden.	

Validieren und beenden Sie die GTID-basierte Replikation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beenden Sie die GTID-basierte Replikation auf dem grünen Cluster.	Nachdem Sie den Datenverkehr von der blauen Umgebung auf die grüne Umgebung umgestellt haben, sollten Sie den Erfolg der Umstellung überprüfen und sicherstellen, dass der grüne Cluster wie erwartet funktioniert. Darüber hinaus muss die GTID-basierte Replikation zwischen den blauen und grünen Clustern gestoppt werden, da die grüne Umgebung jetzt als primäre Datenbank dient. Durch die Ausführung dieser Aufgaben wird sichergestellt, dass Ihre Umgebung sicher, optimiert und für den laufenden Betrieb optimiert ist.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	So beenden Sie die Replikation:
	1. Verwenden Sie einen MySQL-Client, um eine Verbindung zum grünen Cluster herzustellen.
	2. Führen Sie den folgenden SQL-Befehl aus, um den Replikationsprozess auf dem grünen Cluster zu beenden:
	`STOP SLAVE;`
	3. (Optional) Falls gewünscht, können Sie die Replikationskonfiguration zurücksetzen, um alle verbleibenden Replikationseinstellungen zu löschen:
	`RESET SLAVE ALL;`
	Wenn Sie die Replizierung beenden, wird der grüne Cluster vollständig unabhängig und fungiert als primäre Datenbankumgebung für Ihre Workloads.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen von Ressourcen.	Durch die Bereinigung aller temporären oder ungenutzten Ressourcen, die während der Migration vom blauen zum grünen Cluster entstanden sind, wird sichergestellt, dass Ihre Umgebung optimiert, sicher und kostengünstig bleibt. Die Säuberung umfasst die Anpassung der Sicherheitseinstellungen, die Erstellung letzter Backups und die Außerbetriebnahme unnötiger Ressourcen. So bereinigen Sie Ressourcen: 1. Sicherheitsgruppen aktualisieren: Konfigurieren Sie die Sicherheitsgruppen, die sowohl dem blauen als auch dem grünen Cluster zugeordnet sind, so, dass sie die neue primäre Umgebung (grün) widerspiegeln. Beschränken Sie den Zugriff auf die blaue Umgebung, wenn sie nicht mehr benötigt wird, und stellen Sie sicher, dass die Sicherheitseinstellungen des grünen Clusters den bewährten Methoden entsprechen.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Erstellen Sie ein letztes Backup des grünen Clusters: Erstellen Sie nach Abschluss der Migration einen letzten Snapshot des grünen Clusters, der als Backup dient. Sie können diesen Snapshot verwenden, um die Umgebung bei Bedarf in future wiederherzustellen. `aws rds create-db-snapshot --db-instance-identifier green-cluster-instance --db-snapshot-identifier green-cluster-final-snapshot` 3. Temporäre Ressourcen überprüfen und entfernen: Überprüfen Sie alle temporären Ressourcen, die während der Migration erstellt wurden, z. B. temporäre Sicherheitsgruppen, Snapshots oder andere Konfigurationen. Löschen Sie Ressourcen, die nicht mehr benötigt werden, um unnötige Kosten zu vermeiden. Löschen Sie beispielsweise den blauen Cluster, wenn er nicht mehr benötigt wird:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws rds delete-db-cluster --db-cluster-identifier blue-cluster-identifier --skip-final-snapshot` Die Bereinigung von Ressourcen trägt zur Aufrechterhaltung einer sicheren und optimierten Umgebung bei, senkt die Kosten und stellt sicher, dass nur die benötigte Infrastruktur erhalten bleibt.	

Zugehörige Ressourcen

AWS CloudFormation:

- AWS CloudFormation Benutzerhandbuch
- AWS CloudFormation bewährte Verfahren
- Generieren Sie mit IaC Generator Vorlagen aus vorhandenen Ressourcen
- Importieren Sie ganze Anwendungen in AWS CloudFormation (AWS Blogbeitrag)

Amazon Aurora:

- Amazon Aurora Benutzerhandbuch
- Verwaltung eines Amazon Aurora Aurora-DB-Clusters

Blaue/grüne Bereitstellungsstrategie:

- Überblick über Amazon Aurora Blue/Green-Bereitstellungen

GTID-basierte Replikation:

- Verwenden der GTID-basierten Replikation (Amazon RDS-Dokumentation)

AWS Lambda:

- AWS Lambda Entwicklerhandbuch
- Bewährte Methoden für die Arbeit mit Funktionen AWS Lambda

Amazonas-Route 53:

- Entwicklerhandbuch zu Amazon Route 53
- Gewichtetes Routing

MySQL-Client-Tools:

- PyMySQL

Automatisieren Sie Datenbankaufgaben in der SQL Server Express Edition, die auf Amazon ausgeführt wird, EC2 mithilfe eines AWS Lambda Taskplaners

Erstellt von Subhani Shaik (AWS)

Übersicht

Dieses Muster zeigt, wie Datenbankaufgaben in der SQL Server Express Edition, der kostenlosen Version von SQL Server, geplant und verwaltet werden. In der SQL Server Express Edition fehlt jedoch der SQL Server Agent-Dienst, der in der Regel automatisierte Datenbankvorgänge abwickelt. Dieses Muster erklärt, wie Sie Task Scheduler und Lambda als Alternative zur Automatisierung von Datenbankaufgaben in der SQL Server Express Edition verwenden können, die auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance ausgeführt wird.

Task Scheduler ist ein integriertes Windows-Systemdienstprogramm, das die automatische Ausführung von Routineaufgaben erleichtert. Es bietet einen Mechanismus zur Planung und Verwaltung automatisierter Vorgänge, sodass kein manuelles Eingreifen in wiederkehrende Prozesse erforderlich ist. AWS Lambdaist ein serverloser Computerdienst, der automatisch Code als Reaktion auf Ereignisse ausführt, ohne dass Sie die zugrunde liegende Infrastruktur verwalten müssen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Eine virtuelle private Cloud (VPC), die mit Amazon Virtual Private Cloud (Amazon VPC) erstellt wurde
- Eine EC2 Amazon-Instance mit Windows Server
- Amazon Elastic Block Store (Amazon EBS) -Volumes, die an eine EC2 Amazon-Instance mit Windows Server angehängt sind
- Binärdateien der SQL Server Express Edition

Einschränkungen

- Informationen zu den Funktionseinschränkungen der SQL Server Express Edition finden Sie auf der Microsoft-Website.

- Einige AWS-Services sind nicht in allen verfügbar AWS-Regionen. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie unter AWS Dienste nach Regionen. Informationen zu bestimmten Endpunkten finden Sie unter Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Produktversionen

- SQL Server 2016 oder höher mit SQL Server Express Edition

Architektur

Das folgende Diagramm zeigt eine EC2 Amazon-Instance, auf der die SQL Server Express Edition installiert ist. Auf die Instance kann über den Remote Desktop Protocol (RDP) -Client oder von aus AWS Systems Manager Session Manager zugegriffen werden. AWS Key Management Service (AWS KMS) übernimmt die Datenverschlüsselung für die Amazon EBS-Volumes, um die data-at-rest Sicherheit zu gewährleisten. Zur Infrastruktur gehört auch AWS Identity and Access Management (IAM), das die Zugriffskontrolle ermöglicht und die Berechtigungen für die Ausführung von Lambda-Funktionen verwaltet. Amazon Simple Storage Service (Amazon S3) speichert Lambda-Funktionen.

Tools

AWS-Services

- Amazon Elastic Block Store (Amazon EBS) bietet Speichervolumen auf Blockebene zur Verwendung mit Amazon-Instances. EC2
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Key Management Service (AWS KMS) hilft Ihnen dabei, kryptografische Schlüssel zu erstellen und zu kontrollieren, um Ihre Daten zu schützen.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Systems Manager Session Managerist ein vollständig verwaltetes AWS Systems Manager Tool. Mit Session Manager können Sie Ihre EC2 Amazon-Instances, Edge-Geräte, lokalen Server und virtuellen Maschinen (VMs) verwalten.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk bereitzustellen. Dieses virtuelle Netzwerk entspricht einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben würden, mit den Vorteilen der Verwendung der skalierbaren Infrastruktur von AWS.

Andere Tools

- Microsoft SQL Server Management Studio (SSMS) ist ein Tool für die Verwaltung von SQL Server, einschließlich des Zugriffs auf, der Konfiguration und der Verwaltung von SQL Server-Komponenten.
- Python ist eine Allzweck-Computerprogrammiersprache. Sie können es verwenden, um Anwendungen zu erstellen, Aufgaben zu automatisieren und Dienste auf der zu entwickeln. AWS Cloud
- Task Scheduler ist ein Microsoft-Tool, mit dem Sie Routineaufgaben auf Ihrem Computer automatisch planen können.

Bewährte Methoden

- Bewährte Methoden für Amazon EC2
- Bewährte Methoden für die Bereitstellung von Microsoft SQL Server auf Amazon EC2
- Bewährte Methoden für die Arbeit mit AWS Lambda Funktionen
- Bewährte Methoden für die Sicherheit in IAM

Epen

Erstellen Sie eine EC2 Amazon-Instance und installieren Sie die SQL Server Express Edition

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie eine EC2 Amazon-Instance bereit.	Um eine EC2 Amazon-Instance zu erstellen, öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/und wählen Sie ein Amazon Machine Image (AMI) aus der Liste der für Windows Server verfügbaren Instances aus. Weitere Informationen finden Sie in der AWS Dokumentation unter Starten einer EC2 Amazon-Instance.	DBA, AWS DevOps
Installieren Sie die SQL Server Express Edition.	Gehen Sie wie folgt vor, um die SQL Server Express Edition zu installieren: 1. Um eine Verbindung zu Ihrer EC2 Amazon-Instance herzustellen, wählen Sie eine Option: • Option A — Verwenden Sie das Remote Desktop Protocol (RDP). Anweisungen finden Sie in der AWS Dokumentation unter Herstellen einer Connect zu Ihrer Windows-Instanz mithilfe eines RDP-Clients.	DBA, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Option B — Verwenden Sie die EC2 Amazon-Konsole und AWS Systems Manager Session Manager. Anweisungen finden Sie in der AWS Dokumentation unter Connect zu Ihrer EC2 Amazon-Instance mithilfe von Session Manager. 2. Um die erforderliche SQL Server Express-Edition herunterzuladen, gehen Sie auf der Microsoft-Website zu SQL Server-Downloads. 3. Um die SQL Server Express Edition zu installieren, folgen Sie den Anweisungen unter Planen einer SQL Server-Installation auf der Microsoft-Website.	

Erstellen Sie automatisierte Datenbankwartungsaufgaben

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Routineaufgaben.	Identifizieren Sie die Routineaufgaben, die Sie automatisieren möchten. Beispielsweise kommen die folgenden Aufgaben für eine Automatisierung in Frage:	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Datenbanksicherungen (vollständige Backups, differenzielle Backups und Transaktionslog-Backups) • Wartung und Reorganisation des Indexes • Aktualisierungen der Statistiken • Anwendungsspezifische Operationen • Bereinigung oder Archivierung von Daten	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie SQL-Skripten vor.	Gehen Sie wie folgt vor, um SQL-Skripten vorzubereiten: 1. Erstellen Sie SQL-Abfragen für jede Wartungsaufgabe. Im Folgenden finden Sie ein Beispiel für eine T-SQL-Abfrage zur Durchführung einer bestimmten Datenbanksicherung: `Backup Database <Database_Name> To Disk='C:\Backups\Database_Name.bak'` 2. Speichern Sie die Skriptdatei unter. `<File Name>.sql` Speichern Sie die Skripts anschließend an einem zugänglichen Ort auf dem lokalen Laufwerk des Servers auf der EC2 Amazon-Instance oder auf einer Netzwerkdateifreigabe.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Zugriffsberechtigungen.	Gehen Sie wie folgt vor, um Zugriffsberechtigungen zu konfigurieren: 1. Legen Sie die entsprechenden Dateisystemberechtigungen fest. Anweisungen finden Sie auf der Microsoft-Website unter Konfigurieren von Dateisystemberechtigungen für den Zugriff auf das Datenbankmodul. 2. Stellen Sie sicher, dass das SQL Server-Dienstkonto über den erforderlichen Zugriff verfügt. Anweisungen finden Sie unter Konfigurieren von Windows-Dienstkonten und Berechtigungen auf der Microsoft-Website. 3. Überprüfen Sie die Netzwerkkonnektivität für Remote-Shares. Weitere Informationen finden Sie in der AWS Dokumentation unter Zugreifen auf Daten mithilfe von Dateifreigaben.	DBA

Automatisieren Sie Aufgaben mit dem Taskplaner

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie Batch-Dateien.	• Um eine Batch-Datei zu erstellen, verwenden Sie einen Texteditor, um den folgenden Befehl einzugeben. Ersetzen Sie die Parameter `username` und `password` durch Ihre eigenen Werte. Speichern Sie dann die Datei unter`<Name>.bat` .
	
	`sqlcmd -S servername -U username -P password -i <T-SQL query path.sql>`
	
	• Um eine Batchdatei für SQL-Aufgaben zu erstellen , verwenden Sie einen Texteditor und geben Sie die folgenden Befehle ein. Ersetzen Sie die Parameter `ServerName DatabaseName` ,`username`, und `password` durch Ihre eigenen Werte. Speichern Sie dann die Datei unter`<Name>.bat` .
	
	`@echo off`
	`sqlcmd -S [ServerName] -d [Database`
		AWS DevOps, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`Name] -U username -P password -i "PathToSQLScript\Script.sql" -o "PathToOutput\Output.txt"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Aufgaben im Taskplaner.	Gehen Sie wie folgt vor, um eine Aufgabe im Taskplaner zu erstellen: 1. Um den Taskplaner zu öffnen, geben Sie taskschd.msc in die Windows-Suche ein. 2. Wählen Sie das Aktionsmenü und wählen Sie dann Einfache Aufgabe erstellen aus. 3. Geben Sie unter Name einen Namen für die Aufgabe ein, und wählen Sie dann Weiter aus. 4. Wählen Sie unter Trigger die Option aus, wann die Aufgabe gestartet werden soll, und wählen Sie dann Weiter aus. 5. Geben Sie die Start - und Wiederholungsinformationen für die Aufgabe ein, und wählen Sie dann Weiter aus. 6. Wählen Sie im Abschnitt Aktion die Option Programm starten und dann Weiter aus. 7. Geben Sie für Programm/Script den Pfad für die Batch-Datei an, die Sie in der vorherigen Aufgabe	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	erstellt haben, und wählen Sie dann Weiter. 8. Wählen Sie Finish (Abschließen). Um die Aufgabe manuell auszuführen, klicken Sie mit der rechten Maustaste auf die neu erstellte Aufgabe und wählen Sie dann Ausführen.	
Aufgabenstatus anzeigen.	Gehen Sie wie folgt vor, um den Status einer Aufgabe im Taskplaner anzuzeigen: 1. Rufen Sie im Taskplaner die Taskplaner-Bibliothek auf, in der alle Aufgaben angezeigt werden. 2. Um den Status der Aufgabe zu sehen, die Sie zuvor erstellt haben, wählen Sie die Aufgabe aus und wechseln Sie dann zur Registerkarte Verlauf.	DBA, AWS DevOps

Automatisieren Sie Aufgaben mit AWS Lambda

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Implementieren Sie die Lösung.	Gehen Sie wie folgt vor, um die Lösung dieses Musters zu implementieren:	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Erstellen Sie eine Lambda-Funktion. Anweisungen finden Sie in der AWS Dokumentation unter Erstellen Sie Ihre erste Lambda-Funktion. 2. Planen Sie die Lambda-Funktion. Anweisungen finden Sie in der Dokumentation unter Eine Lambda-Funktion nach einem Zeitplan aufrufen. AWS 3. Führen Sie T-SQL-Abfragen aus. Weitere Informationen finden Sie in der AWS Dokumentation unter Tutorial: Verwenden einer Lambda-Funktion für den Zugriff auf eine Amazon RDS-Datenbank. Das Tutorial erklärt, wie Sie Amazon RDS-Datenbanken von Lambda-Funktionen aus verbinden, um SQL-Abfragen auszuführen	

Fehlerbehebung

Problem	Lösung
Lambda-Probleme	Hilfe zu Fehlern und Problemen, die bei der Verwendung auftreten können AWS Lambda,

Problem	Lösung
	finden Sie in der AWS Dokumentation unter Problembehandlung in Lambda.

Zugehörige Ressourcen

- EC2 Amazon-Instance-Typen
- AWS Lambda Dokumentation
- AWS Lambda Preisgestaltung
- Taskplaner für Entwickler (Microsoft-Website)

Automatisieren Sie regionsübergreifendes Failover und Failback mithilfe des DR Orchestrator Framework

Erstellt von Jitendra Kumar (AWS), Oliver Francis (AWS) und Pavithra Balasubramanian (AWS)

Übersicht

Dieses Muster beschreibt, wie DR Orchestrator Framework verwendet wird, um die manuellen, fehleranfälligen Schritte zur Durchführung der Notfallwiederherstellung in allen Amazon Web Services () -Regionen zu orchestrieren und zu automatisieren.AWS Das Muster deckt die folgenden Datenbanken ab:

- Amazon Relational Database Service (Amazon RDS) für MySQL, Amazon RDS for PostgreSQL oder Amazon RDS for MariaDB
- Amazon Aurora MySQL-Compatible Edition oder Amazon Aurora PostgreSQL-Compatible Edition (mit einer zentralisierten Datei)
- Amazon ElastiCache (Redis OSS)

Um die Funktionalität von DR Orchestrator Framework zu demonstrieren, erstellen Sie zwei DB-Instances oder Cluster. Die primäre befindet sich in der und AWS-Region `us-east-1` die sekundäre befindet sich in`us-west-2`. Um diese Ressourcen zu erstellen, verwenden Sie die AWS CloudFormation Vorlagen im `App-Stack` Ordner des GitHub Repositorys aws-cross-region-dr-databases.

Voraussetzungen und Einschränkungen

Allgemeine Voraussetzungen

- DR Orchestrator Framework wird sowohl primär als auch sekundär bereitgestellt AWS-Regionen
- Zwei Amazon Simple Storage Service-Buckets
- Eine virtuelle private Cloud (VPC) mit zwei Subnetzen und einer AWS Sicherheitsgruppe

Engine-spezifische Voraussetzungen

- Amazon Aurora — Mindestens eine globale Aurora-Datenbank muss in zwei verfügbar sein AWS-Regionen. Sie können `us-east-1` es als primäre Region und `us-west-2` als sekundäre Region verwenden.

- Amazon ElastiCache (Redis OSS) — Ein ElastiCache globaler Datenspeicher muss in zwei Einheiten verfügbar sein. AWS-Regionen Sie können `use us-east-1` es als primäre Region und `us-west-2` als sekundäre Region verwenden.

Einschränkungen von Amazon RDS

- DR Orchestrator Framework überprüft die Verzögerung bei der Replikation nicht, bevor ein Failover oder Failback durchgeführt wird. Die Replikationsverzögerung muss manuell überprüft werden.
- Diese Lösung wurde mit einer primären Datenbankinstanz mit einer Read Replica getestet. Wenn Sie mehr als eine Read Replica verwenden möchten, testen Sie die Lösung gründlich, bevor Sie sie in einer Produktionsumgebung implementieren.

Einschränkungen von Aurora

- Die Verfügbarkeit und der Support von Funktionen variieren je nach Version der einzelnen Datenbank-Engines und zwischen den einzelnen Versionen AWS-Regionen. Weitere Informationen zur Verfügbarkeit von Funktionen und Regionen für die regionsübergreifende Replikation finden Sie unter Regionsübergreifende Read Replicas.
- Für globale Aurora-Datenbanken gelten spezifische Konfigurationsanforderungen für unterstützte Aurora-DB-Instance-Klassen und die maximale Anzahl von AWS-Regionen. Weitere Informationen finden Sie unter Konfigurationsanforderungen für eine globale Amazon Aurora Aurora-Datenbank.
- Diese Lösung wurde mit einer primären Datenbank-Instance mit einer Read Replica getestet. Wenn Sie mehr als eine Read Replica verwenden möchten, testen Sie die Lösung gründlich, bevor Sie sie in einer Produktionsumgebung implementieren.

ElastiCache Einschränkungen

- Informationen zur regionalen Verfügbarkeit für Global Datastore und zu den ElastiCache Konfigurationsanforderungen finden Sie in der ElastiCache Dokumentation unter Voraussetzungen und Einschränkungen.

Amazon RDS-Produktversionen

Amazon RDS unterstützt die folgenden Engine-Versionen:

- MySQL — Amazon RDS unterstützt DB-Instances, auf denen die folgenden Versionen von MySQL ausgeführt werden: MySQL 8.0 und MySQL 5.7
- PostgreSQL — Informationen zu unterstützten Versionen von Amazon RDS for PostgreSQL finden Sie unter Verfügbare PostgreSQL-Datenbankversionen.
- MariaDB — Amazon RDS unterstützt DB-Instances, auf denen die folgenden Versionen von MariaDB ausgeführt werden:
  - MariaDB 10.11
  - MariaDB 10.6
  - MariaDB 10.5

Aurora-Produktversionen

- Für den globalen Datenbank-Switchover von Amazon Aurora ist Aurora MySQL-kompatibel mit MySQL 5.7-Kompatibilität, Version 2.09.1 und höher erforderlich

  Weitere Informationen finden Sie unter Einschränkungen der globalen Amazon Aurora Aurora-Datenbanken.

ElastiCache (Redis OSS) -Produktversionen

Amazon ElastiCache (Redis OSS) unterstützt die folgenden Redis-Versionen:

- Redis 7.1 (erweitert)
- Redis 7.0 (erweitert)
- Redis 6.2 (erweitert)
- Redis 6.0 (erweitert)
- Redis 5.0.6 (erweitert)

Weitere Informationen finden Sie unter Unterstützte Versionen ElastiCache (Redis OSS).

Architektur

Amazon RDS-Architektur

Die Amazon RDS-Architektur umfasst die folgenden Ressourcen:

- Die in der primären Region (`us-east-1`) erstellte primäre Amazon RDS-DB-Instance mit Lese-/Schreibzugriff für Kunden
- Eine Amazon RDS-Lesereplik, die in der sekundären Region (`us-west-2`) mit schreibgeschütztem Zugriff für Kunden erstellt wurde
- Das DR Orchestrator Framework wird sowohl in der primären als auch in der sekundären Region eingesetzt

Das Diagramm zeigt Folgendes:

1. Asynchrone Replikation zwischen der primären Instance und der sekundären Instance
2. Lese-/Schreibzugriff für Clients in der primären Region
3. Nur-Lese-Zugriff für Clients in der sekundären Region

Aurora-Architektur

Die Amazon Aurora Aurora-Architektur umfasst die folgenden Ressourcen:

- Der primäre Aurora-DB-Cluster, der in der primären Region (`us-east-1`) mit einem Active-Writer-Endpunkt erstellt wurde
- Ein Aurora-DB-Cluster, der in der sekundären Region (`us-west-2`) mit einem inaktiven Writer-Endpunkt erstellt wurde
- Das DR Orchestrator Framework wird sowohl in der primären als auch in der sekundären Region eingesetzt

Das Diagramm zeigt Folgendes:

1. Asynchrone Replikation zwischen dem primären Cluster und dem sekundären Cluster
2. Der primäre DB-Cluster mit einem Active-Writer-Endpunkt
3. Der sekundäre DB-Cluster mit einem inaktiven Writer-Endpunkt

ElastiCache (Redis OSS) -Architektur

Die Amazon-Architektur ElastiCache (Redis OSS) umfasst die folgenden Ressourcen:

- Ein globaler Datenspeicher ElastiCache (Redis OSS), der mit zwei Clustern erstellt wurde:
  1. Der primäre Cluster in der primären Region () `us-east-1`
  2. Der sekundäre Cluster in der sekundären Region (`us-west-2`)
- Ein regionsübergreifender Amazon-Link mit TLS 1.2-Verschlüsselung zwischen den beiden Clustern
- DR Orchestrator Framework wird sowohl in primären als auch in sekundären Regionen eingesetzt

Automatisierung und Skalierung

DR Orchestrator Framework ist skalierbar und unterstützt den Failover oder Failback von mehr als einer AWS Datenbank parallel.

Sie können den folgenden Payload-Code verwenden, um ein Failover für mehrere AWS Datenbanken in Ihrem Konto durchzuführen. In diesem Beispiel führen drei AWS Datenbanken (zwei globale Datenbanken wie Aurora MySQL-kompatibel oder Aurora PostgreSQL-kompatibel und eine Amazon RDS for MySQL MySQL-Instance) ein Failover zur DR-Region durch:

```
{
  "StatePayload": [
    {
      "layer": 1,
      "resources": [
        {
          "resourceType": "PlannedFailoverAurora",
          "resourceName": "Switchover (planned failover) of Amazon Aurora global
 databases (MySQL)",
          "parameters": {
            "GlobalClusterIdentifier": "!Import dr-globaldb-cluster-mysql-global-
identifier",
            "DBClusterIdentifier": "!Import dr-globaldb-cluster-mysql-cluster-
identifier"
          }
        },
        {
          "resourceType": "PlannedFailoverAurora",
```

```
          "resourceName": "Switchover (planned failover) of Amazon Aurora global
 databases (PostgreSQL)",
          "parameters": {
            "GlobalClusterIdentifier": "!Import dr-globaldb-cluster-postgres-global-
identifier",
            "DBClusterIdentifier": "!Import dr-globaldb-cluster-postgres-cluster-
identifier"
          }
        },
        {
          "resourceType": "PromoteRDSReadReplica",
          "resourceName": "Promote RDS for MySQL Read Replica",
          "parameters": {
            "RDSInstanceIdentifier": "!Import rds-mysql-instance-identifier",
            "TargetClusterIdentifier": "!Import rds-mysql-instance-global-arn"
          }
        }
      ]
    }
  ]
}
```

Tools

AWS Dienste

- Amazon Aurora ist eine vollständig verwaltete relationale Datenbank-Engine, die für die Cloud entwickelt wurde und mit MySQL und PostgreSQL kompatibel ist.
- Amazon ElastiCache unterstützt Sie bei der Einrichtung, Verwaltung und Skalierung verteilter In-Memory-Cache-Umgebungen in der AWS Cloud. Dieses Muster verwendet Amazon ElastiCache (Redis OSS).
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen. In diesem Muster werden Lambda-Funktionen verwendet AWS Step Functions , um die Schritte auszuführen.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der. AWS Cloud Dieses Muster unterstützt Amazon RDS for MySQL, Amazon RDS for PostgreSQL und Amazon RDS for MariaDB.

- AWS SDK für Python (Boto3)hilft Ihnen bei der Integration Ihrer Python-Anwendung, -Bibliothek oder Ihres Skripts mit AWS-Services. In diesem Muster APIs werden Boto3 verwendet, um mit den Datenbankinstanzen oder globalen Datenbanken zu kommunizieren.
- AWS Step Functionsist ein serverloser Orchestrierungsdienst, mit dem Sie AWS Lambda Funktionen und andere Funktionen kombinieren können, um geschäftskritische Anwendungen AWS-Services zu erstellen. In diesem Muster werden Step Functions Functions-Zustandsmaschinen verwendet, um den regionsübergreifenden Failover und das Failback der Datenbankinstanzen oder globalen Datenbanken zu orchestrieren und auszuführen.

Code-Repository

Der Code für dieses Muster ist im Repository aws-cross-region-dr-databases unter GitHub verfügbar.

Epen

Installieren Sie DR Orchestrator Framework

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	Führen Sie den folgenden Befehl aus, um das Repository zu klonen: `git clone https://github.com/aws-samples/aws-cross-region-dr-databases.git`	AWS DevOps, AWS-Administrator
Paketieren Sie den Code der Lambda-Funktionen in einem ZIP-Dateiarchiv.	Erstellen Sie die Archivdateien für Lambda-Funktionen, um die DR Orchestrator Framework-Abhängigkeiten einzubeziehen: `cd <YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`bash scripts/deploy-orchestrator-sh.sh`	
Erstellen Sie S3-Buckets.	S3-Buckets werden benötigt, um DR Orchestrator Framework zusammen mit Ihrer neuesten Konfiguration zu speichern. Erstellen Sie zwei S3-Buckets, einen in der primären Region (`us-east-1`) und einen in der sekundären Region (): `us-west-2` • `dr-orchestrator-xxxxxx-us-east-1` • `dr-orchestrator-xxxxxx-us-west-2` `xxxxxx`Ersetzen Sie ihn durch einen zufälligen Wert, um die Bucket-Namen eindeutig zu machen.	AWS-Administrator
Erstellen Sie Subnetze und Sicherheitsgruppen.	Erstellen Sie sowohl in der primären Region (`us-east-1`) als auch in der sekundären Region (`us-west-2`) zwei Subnetze und eine Sicherheitsgruppe für die Bereitstellung von Lambda-Funktionen in Ihrer VPC: • `subnet-XXXXXXX` • `subnet-YYYYYYY` • `sg-XXXXXXXXXXX`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die DR Orchestrator-Parameterdateien.	Aktualisieren Sie in dem `<YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts/cloudformation` Ordner die folgenden DR Orchestrator-Parameterdateien: • `Orchestrator-Deployer-parameters-us-east-1.json` • `Orchestrator-Deployer-parameters-us-west-2.json` Verwenden Sie die folgenden Parameterwerte x und y ersetzen Sie diese durch die Namen Ihrer Ressourcen: `[ { "ParameterKey": "TemplateStoreS3BucketName", "ParameterValue": "dr-orchestrator-xxxxxx-us-east-1" }, { "ParameterKey": "TemplateVPCId", "ParameterValue": "vpc-xxxxxx" }, {`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"ParameterKey": "TemplateLambdaSubnetID1", "ParameterValue": "subnet-xxxxx" }, { "ParameterKey": "TemplateLambdaSubnetID2", "ParameterValue": "subnet-yyyyy" }, { "ParameterKey": "TemplateLambdaSecurityGroupID", "ParameterValue": "sg-xxxxxxxxxx" }]	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den DR Orchestrator Framework-Code in den S3-Bucket hoch.	Der Code ist in einem S3-Bucket sicherer als im lokalen Verzeichnis. Laden Sie das `DR-Orchestration-artifacts` Verzeichnis, einschließlich aller Dateien und Unterordner, in die S3-Buckets hoch. Gehen Sie wie folgt vor, um den Code hochzuladen: 1. Melden Sie sich bei der an AWS Management Console. 2. Navigieren Sie zur Amazon S3 S3-Konsole. 3. Wählen Sie das `dr-orchestrator-xxxxxx-us-east-1` `bucket` aus. 4. Wählen Sie Upload und anschließend Ordner hinzufügen. 5. Wählen Sie den `DR-Orchestration-artifacts` -Ordner aus. 6. Klicken Sie auf Upload. 7. Wählen Sie den `dr-orchestrator-xxxxxx-us-west-2` Bucket aus.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Wiederholen Sie die Schritte 4—7.	

Stellen Sie das DR Orchestrator Framework in der primären Region bereit.	Führen Sie die folgenden Befehle aus, um DR Orchestrator Framework in der primären Region (`us-east-1`) bereitzustellen:
	`cd <YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts/cloudformation`
	
	`aws cloudformation deploy \`
	`--region us-east-1 \`
	`--stack-name dr-orchestrator \`
	`--template-file Orchestrator-Deployer.yaml \`
	`--parameter-overrides file://Orchestrator-Deployer-parameters-us-east-1.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
		AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie das DR Orchestrator Framework in der sekundären Region bereit.	Führen Sie in der sekundären Region (`us-west-2`) die folgenden Befehle aus:
	`cd <YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts/cloudformation`
	
	`aws cloudformation deploy \`
	`--region us-west-2 \`
	`--stack-name dr-orchestrator \`
	`--template-file Orchestrator-Deployer.yaml \`
	`--parameter-overrides file://Orchestrator-Deployer-parameters-us-west-2.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
		AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Bereitstellung.	Wenn der AWS CloudFormation Befehl erfolgreich ausgeführt wird, gibt er die folgende Ausgabe zurück: `Successfully created/updated stack - dr-orchestrator` Alternativ können Sie zur AWS CloudFormation Konsole navigieren und den Status des `dr-orchestrator` Stacks überprüfen.	AWS-Administrator

Erstellen Sie die Datenbank-Instances oder Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Datenbank-Subnetze und Sicherheitsgruppen.	Erstellen Sie in Ihrer VPC zwei Subnetze und eine Sicherheitsgruppe für die DB-Instance oder globale Datenbank sowohl in der primären (`us-east-1`) als auch in der sekundären (`us-west-2`) Region: • `subnet-XXXXXX` • `subnet-XXXXXX` • `sg-XXXXXXXXXX`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Parameterdatei für die primäre DB-Instance oder den Cluster.	Aktualisieren `<YOUR LOCAL GIT FOLDER>/App-Stack` Sie im Ordner die Parameter datei für die primäre Region. Amazon RDS Aktualisieren Sie in der `RDS-MySQL-parameter-us-east-1.json` Datei `SubnetIds` und geben `DBSecurityGroup` Sie die Namen der Ressourcen an, die Sie erstellt haben: `{ "Parameters": { "SubnetIds": "subnet-xxxxxx,subnet-xxxxxx", "DBSecurityGroup": "sg-xxxxxxxxxx", "MySqlGlobalIdentifier":"rds-mysql-instance", "InitialDatabaseName": "mysqldb", "DBPortNumber": "3789", "PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2", "KMSKeyAliasName": "rds/rds-mysql-instance-KmsKeyId" } }`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon Aurora Aktualisieren Sie in der `Aurora-MySQL-parameter-us-east-1.json` Datei `SubnetIds` und `DBSecurityGroup` mit den Namen der Ressourcen, die Sie erstellt haben: `{ "Parameters": { "SubnetIds": "subnet1-xxxxxx,subnet2-xxxxxx", "DBSecurityGroup": "sg-xxxxxxxxxx", "GlobalClusterIdentifier":"dr-globaldb-cluster-mysql", "DBClusterName":"dbcluster-01", "SourceDBClusterName":"dbcluster-02", "DBPortNumber": "3787", "DBInstanceClass": "db.r5.large", "InitialDatabaseName": "sampledb", "PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2", "KMSKeyAliasName": "rds/dr-globaldb-cluster-mysql-KmsKeyId" } }`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon ElastiCache (Redis OSS) Geben Sie in der `ElastiCache-parameter-us-east-1.json` Datei das Update ein `SubnetIds` und geben `DBSecurityGroup` Sie die Namen der Ressourcen an, die Sie erstellt haben. `{ "Parameters": { "CacheNodeType": "cache.m5.large", "DBSecurityGroup": "sg-xxxxxxxxxx", "SubnetIds": "subnet-xxxxxx,subnet-xxxxxx", "EngineVersion": "5.0.6", "GlobalReplicationGroupIdSuffix": "demo-redis-global-datastore", "NumReplicas": "1", "NumShards": "1", "ReplicationGroupId": "demo-redis-cluster", "DBPortNumber": "3788", "TransitEncryption": "true", "KMSKeyAliasName": "elasticache/demo-redis-global-datastore-KmsKeyId",`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2" } }</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie Ihre DB-Instanz oder Ihren Cluster in der primären Region bereit.	Um Ihre Instance oder Ihren Cluster in der primären Region (`us-east-1`) bereitzustellen, führen Sie die folgenden Befehle basierend auf Ihrer Datenbank-Engine aus.
	
	Amazon RDS
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-east-1 \`
	`--stack-name rds-mysql-app-stack \`
	`--template-file RDS-MySQL-Primary.yaml \`
	`--parameter-overrides file://RDS-MySQL-parameter-us-east-1.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
	
	Amazon Aurora
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-east-1 \`
		AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`--stack-name aurora-mysql-app-stack \`
	`--template-file Aurora-MySQL-Primary.yaml \`
	`--parameter-overrides file://Aurora-MySQL-parameter-us-east-1.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
	
	Amazon ElastiCache (Redis OSS)
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-east-1 --stack-name elasticache-ds-app-stack \`
	`--template-file ElastiCache-Primary.yaml \`
	`--parameter-overrides file://ElastiCache-parameter-us-east-1.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Stellen Sie sicher, dass die AWS CloudFormation Ressourcen erfolgreich bereitgestellt wurden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Parameterdatei für die sekundäre DB-Instance oder den Cluster.	Aktualisieren `<YOUR LOCAL GIT FOLDER>/App-Stack` Sie im Ordner die Parameter datei für die sekundäre Region. Amazon RDS Aktualisieren Sie die `RDS-MySQL-parameter-us-west-2.json` Datei `DBSecurityGroup` mit `SubnetIDs` den Namen der Ressourcen, die Sie erstellt haben. Aktualisieren Sie den `PrimaryRegionKMSKeyArn` mit dem Wert von `MySQLKmsKeyId` aus dem Abschnitt Outputs des AWS CloudFormation Stacks für die primäre DB-Instance: `{ "Parameters": { "SubnetIds": "subnet-aaaaaaaaa, subnet-bbbbbbbbb", "DBSecurityGroup": "sg-ccccccccc", "MySqlGlobalIdentifier":"rds-mysql-instance", "InitialDatabaseName": "mysqldb", "DBPortNumber": "3789", "PrimaryRegion": "us-east-1",`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"SecondaryRegion": "us-west-2", "KMSKeyAliasName": "rds/rds-mysql-instance-KmsKeyId", "PrimaryRegionKMSKeyArn":"arn:aws:kms:us-east-1:xxxxxxxxx:key/mrk-xxxxxxxxxxxxxxxxx" } }</pre> Amazon Aurora Aktualisieren Sie in der `Aurora-MySQL-parameter-us-west-2.json` Datei `SubnetIDs` und `DBSecurityGroup` mit den Namen der Ressourcen, die Sie erstellt haben. Aktualisieren Sie den `PrimaryRegionKMSKeyArn` mit dem Wert `AuroraKmsKeyId` aus dem Abschnitt Outputs des AWS CloudFormation Stacks für die primäre DB-Instance: <pre>{ "Parameters": { "SubnetIds": "subnet1-aaaaaaaaa,subnet2-bbbbbbbbb", "DBSecurityGroup": "sg-ccccccccc", "GlobalClusterIdentifier":"dr-globaldb-cluster-mysql",</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"DBClusterName":"dbcluster-01", "SourceDBClusterName":"dbcluster-02", "DBPortNumber": "3787", "DBInstanceClass": "db.r5.large", "InitialDatabaseName": "sampledb", "PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2", "KMSKeyAliasName": "rds/dr-globaldb-cluster-mysql-KmsKeyId" } } Amazon ElastiCache (Redis OSS) Geben Sie in der `ElastiCache-parameter-us-west-2.json` Datei das Update ein `SubnetIDs` und geben `DBSecurityGroup` Sie die Namen der Ressourcen an, die Sie erstellt haben. Aktualisieren Sie den `PrimaryRegionKMSKeyArn` mit dem Wert von `ElastiCacheKmsKeyId` aus dem Abschnitt Outputs des AWS CloudFormation	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Stacks für die primäre DB-Instance: `{ "Parameters": { "CacheNodeType": "cache.m5.large", "DBSecurityGroup": "sg-ccccccccc", "SubnetIds": "subnet-aaaaaaaaa, subnet-bbbbbbbbb", "EngineVersion": "5.0.6", "GlobalReplicationGroupIdSuffix": "demo-redis-global-datastore", "NumReplicas": "1", "NumShards": "1", "ReplicationGroupId": "demo-redis-cluster", "DBPortNumber": "3788", "TransitEncryption": "true", "KMSKeyAliasName": "elasticache/demo-redis-global-datastore-KmsKeyId", "PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2" } }`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie Ihre DB-Instanz oder Ihren Cluster in der sekundären Region bereit.	Führen Sie die folgenden Befehle basierend auf Ihrer Datenbank-Engine aus.
	
	Amazon RDS
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-west-2 \`
	`--stack-name rds-mysql-app-stack \`
	`--template-file RDS-MySQL-DR.yaml \`
	`--parameter-overrides file://RDS-MySQL-parameter-us-west-2.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
	
	Amazon Aurora
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-west-2 \`
	`--stack-name aurora-mysql-app-stack \`
	`--template-file Aurora-MySQL-DR.yaml \`
		AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`--parameter-overrides file://Aurora-MySQL-parameter-us-west-2.json \ --capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \ --disable-rollback`
	
	Amazon ElastiCache (Redis OSS)
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \ --region us-west-2 \ --stack-name elasticache-ds-app-stack \ --template-file ElastiCache-DR.yaml \ --parameter-overrides file://ElastiCache-parameter-us-west-2.json \ --capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \ --disable-rollback`
	
	Stellen Sie sicher, dass die AWS CloudFormation Ressourcen erfolgreich bereitgestellt wurden.	

Zugehörige Ressourcen

- Strategie zur Notfallwiederherstellung für Datenbanken auf AWS (AWS Prescriptive Guidance-Strategie)
- Automatisieren Sie Ihre DR-Lösung für relationale Datenbanken auf AWS (AWS Prescriptive Guidance Guide Guide)
- Verwenden von Amazon Aurora Global Databases
- Replikation über globale Datenspeicher hinweg AWS-Regionen
- Automatisieren Sie Ihre DR-Lösung für relationale Datenbanken auf AWS (AWS Prescriptive Guidance Guide)

Automatisieren Sie die Replikation von Amazon RDS-Instances auf AWS-Konten

Erstellt von Parag Nagwekar (AWS) und Arun Chandapillai (AWS)

Übersicht

Dieses Muster zeigt Ihnen, wie Sie den Prozess der Replikation, Nachverfolgung und Wiederherstellung Ihrer Amazon Relational Database Service (Amazon RDS) -DB-Instances auf verschiedenen Ebenen mithilfe AWS-Konten AWS Step Functions von und automatisieren können. AWS Lambda Sie können diese Automatisierung verwenden, um eine groß angelegte Replikation von RDS-DB-Instances ohne Leistungseinbußen oder betrieblichen Mehraufwand durchzuführen — unabhängig von der Größe Ihres Unternehmens. Sie können dieses Muster auch verwenden, um Ihr Unternehmen bei der Einhaltung verbindlicher Datenverwaltungsstrategien oder Compliance-Anforderungen zu unterstützen, die eine Replikation und Redundanz Ihrer Daten über verschiedene Länder hinweg erfordern. AWS-Konten AWS-Regionen Die kontenübergreifende Replikation von Amazon RDS-Daten in großem Umfang ist ein ineffizienter und fehleranfälliger manueller Prozess, der kostspielig und zeitaufwändig sein kann. Die Automatisierung in diesem Muster kann Ihnen jedoch dabei helfen, die kontenübergreifende Replikation sicher, effektiv und effizient durchzuführen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zwei AWS-Konten
- Eine RDS-DB-Instance, die in der Quelle läuft AWS-Konto
- Eine Subnetzgruppe für die RDS-DB-Instance im Ziel AWS-Konto
- Ein AWS Key Management Service (AWS KMS) -Schlüssel, der in der Quelle erstellt AWS-Konto und für das Zielkonto freigegeben wurde (Weitere Informationen zu Richtliniendetails finden Sie im Abschnitt Zusätzliche Informationen dieses Musters.)
- Ein AWS KMS key im Ziel AWS-Konto , um die Datenbank im Zielkonto zu verschlüsseln

Einschränkungen

- Einige AWS-Services sind nicht in allen AWS-Regionen verfügbar. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu

bestimmten Endpunkten finden Sie auf der Seite Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Produktversionen

- Python 3.9 (verwenden AWS Lambda)
- PostgreSQL 11.3, 13.x und 14.x

Architektur

Technologie-Stack

- Amazon Relational Database Service (Amazon RDS)
- Amazon-Simple-Notification-Service (Amazon-SNS)
- AWS Key Management Service (AWS KMS)
- AWS Lambda
- AWS Secrets Manager
- AWS Step Functions

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur für die Verwendung von Step Functions zur Orchestrierung der geplanten On-Demand-Replikation von RDS-DB-Instances von einem Quellkonto (Konto A) zu einem Zielkonto (Konto B).

Im Quellkonto (Konto A im Diagramm) führt die Step Functions-Zustandsmaschine Folgendes aus:

1. Erstellt einen Snapshot von der RDS-DB-Instance in Konto A.
2. Kopiert und verschlüsselt den Snapshot mit einem AWS KMS key From-Konto A. Um die Verschlüsselung während der Übertragung sicherzustellen, wird der Snapshot verschlüsselt, unabhängig davon, ob die DB-Instance verschlüsselt ist oder nicht.
3. Teilt den DB-Snapshot mit Konto B, indem Konto B Zugriff auf den Snapshot gewährt wird.
4. Sendet eine Benachrichtigung an das SNS-Thema, und dann ruft das SNS-Thema die Lambda-Funktion in Konto B auf.

Im Zielkonto (Konto B im Diagramm) führt die Lambda-Funktion die Step Functions Functions-Zustandsmaschine aus, um Folgendes zu orchestrieren:

1. Kopiert den gemeinsam genutzten Snapshot von Konto A auf Konto B, wobei zuerst das AWS KMS key Absenderkonto A verwendet wird, um die Daten zu entschlüsseln und dann die Daten mit dem Konto B zu verschlüsseln. AWS KMS key
2. Liest das Geheimnis aus Secrets Manager, um den Namen der aktuellen DB-Instance zu erfassen.
3. Stellt die DB-Instance aus dem Snapshot mit einem neuen Namen und Standard AWS KMS key für Amazon RDS wieder her.
4. Liest den Endpunkt der neuen Datenbank und aktualisiert das Geheimnis in Secrets Manager mit dem neuen Datenbank-Endpunkt und kennzeichnet dann die vorherige DB-Instance, sodass sie später gelöscht werden kann.
5. Behält die letzten N Instanzen der Datenbanken bei und löscht alle anderen Instanzen.

Tools

AWS-Services

- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der. AWS Cloud
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.
- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und AWS-Regionen zu verwalten.
- AWS Key Management Service (AWS KMS) hilft Ihnen dabei, kryptografische Schlüssel zu erstellen und zu kontrollieren, um Ihre Daten zu schützen.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS SDK für Python (Boto3)ist ein Softwareentwicklungskit, mit dem Sie Ihre Python-Anwendung, -Bibliothek oder Ihr Skript integrieren können AWS-Services.

- Mit AWS Secrets Manager können Sie fest codierte Anmeldeinformationen im Code (einschließlich Passwörter) durch einen API-Aufruf an Secrets Manager ersetzen und das Geheimnis programmgesteuert abrufen.
- AWS Step Functionsist ein serverloser Orchestrierungsservice, mit dem Sie Lambda-Funktionen und andere Funktionen kombinieren können, um geschäftskritische Anwendungen AWS-Services zu erstellen.

Code-Repository

Der Code für dieses Muster ist im GitHub Crossaccount RDS Replication Repository verfügbar.

Epen

Automatisieren Sie die Replikation von RDS-DB-Instances AWS-Konten mit einem einzigen Klick

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den CloudFormation Stack im Quellkonto bereit.	1. Melden Sie sich AWS Management Console beim Quellkonto (Konto A) an und öffnen Sie die CloudFormation Konsole. 2. Klicken Sie im Navigationsbereich auf Stacks. 3. Wählen Sie Stack erstellen und dann Mit vorhandenen Ressourcen (Ressourcen importieren). 4. Wählen Sie auf der Seite Ressourcen identifizieren die Option Weiter aus. 5. Wählen Sie auf der Seite „Vorlage angeben“ die Option Vorlage hochladen aus.	Cloud-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Wählen Sie Datei auswählen, wählen Sie die `Cloudformation-SourceAccountRDS.yaml` Datei aus dem GitHub Crossaccount RDS Replication Repository aus und klicken Sie dann auf Weiter. 7. Geben Sie unter Stackname einen Namen für Ihren Stack ein. 8. Geben Sie im Abschnitt Parameter die Parameter an, die in der Stack-Vorlage definiert sind: • Geben Sie für DestinationAccountNumberdie Kontonummer Ihrer Ziel-RDS-DB-Instance ein. • Für KeyName, geben Sie Ihre ein AWS KMS key. • Geben Sie für ScheduleExpressioneinen Cron-Ausdruck ein (die Standardeinstellung ist täglich 12:00 Uhr). • Geben Sie DBIdentifier unter Quelle den Namen der Quelldatenbank ein. • Geben Sie unter DBSnapshot Quellname den Namen des	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Snapshots ein, oder akzeptieren Sie die Standardeinstellung. 9. Wählen Sie Weiter aus. 10. Behalten Sie auf der Seite „Stack-Optionen konfigurieren“ die Standardwerte bei und wählen Sie dann Weiter. 11. Überprüfen Sie Ihre Stack-Konfiguration und wählen Sie dann Submit. 12. Wählen Sie die Registerkarte Ressourcen für Ihren Stack und notieren Sie sich dann den Amazon-Ressourcennamen (ARN) des SNS-Themas.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den CloudFormation Stack im Zielkonto bereit.	1. Melden Sie sich AWS Management Console beim Zielkonto (Konto B) an und öffnen Sie die CloudFormation Konsole. 2. Klicken Sie im Navigationsbereich auf Stacks. 3. Wählen Sie Stack erstellen und dann Mit vorhandenen Ressourcen (Ressourcen importieren). 4. Wählen Sie auf der Seite Ressourcen identifizieren die Option Weiter aus. 5. Wählen Sie auf der Seite „Vorlage angeben“ die Option Vorlage hochladen aus. 6. Wählen Sie Datei, wählen Sie die `Cloudformation-DestinationAccountRDS.yaml` Datei aus dem GitHub Crossaccount RDS Replication Repository aus und klicken Sie dann auf Weiter. 7. Geben Sie unter Stackname einen Namen für Ihren Stack ein. 8. Geben Sie im Abschnitt Parameter die Parameter an, die in der Stack-Vorlage definiert sind:	Cloud-Architekt, DevOps Ingenieur, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Geben Sie für DatabaseNameeinen Namen für Ihre Datenbank ein. • Geben Sie für Engine den Datenbank-Engine-Typ ein, der der Quelldatenbank entspricht. • Geben Sie für DBInstanceKlasse den bevorzugten Datenbankinstanztyp ein, oder akzeptieren Sie den Standardwert. • Geben Sie für Subnetzgruppen die bestehende VPC-Subnetzgruppe ein. Anweisungen zum Erstellen einer Subnetzgruppe finden Sie unter Schritt 2: Erstellen einer DB-Subnetzgruppe in der Amazon RDS-Dokumentation. • Geben Sie für SecretNameden Pfad und den geheimen Namen ein, oder akzeptieren Sie die Standardeinstellung. • Geben Sie für SGID die Sicherheitsgruppen-ID Ihres Zielclusters ein. • Geben Sie für KMSKeyden ARN des	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	KMS-Schlüssels in Ihrem Zielkonto ein. • Geben Sie für NoOfOlder Instancesdie Anzahl der alten Kopien der RDS-DB-Instances ein, die Sie für das Rollback behalten möchten. 9. Wählen Sie Weiter aus. 10. Behalten Sie auf der Seite „Stack-Optionen konfiguri eren“ die Standardwerte bei und wählen Sie dann Weiter. 11. Überprüfen Sie Ihre Stack-Konfiguration und wählen Sie dann Submit. 12. Wählen Sie den Tab Ressourcen für Ihren Stack und notieren Sie sich dann die physische ID und den ARN von`InvokeSte pFunction` .	
Überprüfen Sie die Erstellun g der RDS-DB-Instance im Zielkonto.	1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie. 2. Wählen Sie im Navigatio nsbereich Datenbanken aus und überprüfen Sie dann, ob die neue RDS-DB-In stance unter dem neuen Cluster angezeigt wird.	Cloud-Administrator, Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Abonnieren Sie die Lambda-Funktion für das SNS-Thema.	Sie müssen die folgenden Befehle AWS Command Line Interface (AWS CLI) ausführen , um die Lambda-Funktion im Zielkonto (Konto B) für das SNS-Thema im Quellkonto (Konto A) zu abonnieren.
	
	Führen Sie in Konto A den folgenden Befehl aus:
	
	`aws sns add-permission \ --label lambda-access --aws-account-id <DestinationAccount> \ --topic-arn <Arn of SNSTopic > \ --action-name Subscribe ListSubscriptionsB yTopic`
	
	Führen Sie in Konto B den folgenden Befehl aus:
	
	`aws lambda add-permi ssion \ --function-name <Name of InvokeStepFunction > \ --source-arn <Arn of SNSTopic > \ --statement-id function-with-sns \ --action lambda:In vokeFunction \`
		Cloud-Administrator, Cloud-Architekt, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`--principal sns.amazonaws.com`
	
	Führen Sie in Konto B den folgenden Befehl aus:
	
	`aws sns subscribe \ --protocol "lambda" \ --topic-arn <Arn of SNSTopic> \ --notification-endpoint <Arn of InvokeStepFunction>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Synchronisieren Sie die RDS-DB-Instance vom Quellkonto mit dem Zielkonto.	Initiieren Sie die On-Demand -Datenbankreplikation, indem Sie die Step Functions -Zustandsmaschine im Quellkonto starten. 1. Öffnen Sie die Step Functions Functions-Konsole. 2. Wählen Sie im Navigation sbereich State Machines aus. 3. Wählen Sie Ihren Zustandsmaschine aus. 4. Wählen Sie auf der Registerkarte Ausführungen Ihre Funktion aus und klicken Sie dann auf Ausführung starten, um den Workflow zu starten. **Note** Es gibt einen Scheduler, mit dem Sie die Replikation automatisch und planmäßig ausführen können. Der Scheduler ist jedoch standardmäßig ausgeschaltet. Den Namen der CloudWatch Amazon-Regel für	Cloud-Architekt, DevOps Ingenieur, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den Scheduler finden Sie auf der Registerkarte Ressourcen des CloudFormation Stacks im Zielkonto. Anweisungen zum Ändern der CloudWatch Ereignisregel finden Sie in der Dokumentation unter Löschen oder Deaktivieren einer CloudWatch Ereignisregel. CloudWatch	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie bei Bedarf ein Rollback Ihrer Datenbank auf eine der vorherigen Kopien durch.	1. Öffnen Sie die Secrets Manager-Konsole. 2. Wählen Sie aus der Liste der Geheimnis se das Geheimnis aus, das Sie zuvor mithilfe der CloudFormation Vorlage erstellt haben. Ihre Anwendung verwendet den geheimen Schlüssel, um auf die Datenbank im Zielcluster zuzugreifen. 3. Um den geheimen Wert auf der Detailseite zu aktualisieren, wählen Sie im Abschnitt Geheimer Wert die Option Geheimen Wert abrufen und dann Bearbeite n aus. 4. Geben Sie die Details des Datenbank-Endpunkts ein.	Cloud-Administrator, DBA, Ingenieur DevOps

Zugehörige Ressourcen

- Regionsübergreifende Read Replicas (Amazon RDS-Dokumentation)
- Blaue/grüne Bereitstellungen (Amazon RDS-Dokumentation)

Zusätzliche Informationen

Sie können die folgende Beispielrichtlinie verwenden, um Ihre AWS KMS key Across gemeinsam zu nutzen. AWS-Konten

```
{
    "Version": "2012-10-17",
```

```
    "Id": "cross-account-rds-kms-key",
    "Statement": [
        {
            "Sid": "Enable user permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<SourceAccount>:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow administration of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<DestinationAccount>:root"
            },
            "Action": [
                "kms:Create*",
                "kms:Describe*",
                "kms:Enable*",
                "kms:List*",
                "kms:Put*",
                "kms:Update*",
                "kms:Revoke*",
                "kms:Disable*",
                "kms:Get*",
                "kms:Delete*",
                "kms:ScheduleKeyDeletion",
                "kms:CancelKeyDeletion"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::<DestinationAccount>:root",
                    "arn:aws:iam::<SourceAccount>:root"
                ]
            },
            "Action": [
                "kms:Encrypt",
```

```
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey",
                "kms:CreateGrant"
            ],
            "Resource": "*"
        }
    ]
}
```

Automatisches Backup von SAP HANA-Datenbanken mit Systems Manager und EventBridge

Erstellt von Ambarish Satarkar (AWS) und Gaurav Rath (AWS)

Übersicht

Dieses Muster beschreibt, wie SAP HANA-Datenbanksicherungen mithilfe von AWS Systems Manager, Amazon EventBridge, Amazon Simple Storage Service (Amazon S3) und AWS Backint Agent for SAP HANA automatisiert werden.

Dieses Muster bietet einen Shell-Skriptbasierten Ansatz unter Verwendung des `BACKUP DATA` Befehls und macht es überflüssig, Skripts und Jobkonfigurationen für jede Betriebssysteminstanz (OS) auf zahlreichen Systemen zu verwalten.

> **Note**
>
> Im April 2023 kündigte AWS Backup die Unterstützung für SAP HANA-Datenbanken auf Amazon Elastic Compute Cloud (Amazon EC2) an. Weitere Informationen finden Sie unter Backup von SAP HANA-Datenbanken auf EC2 Amazon-Instances.

Je nach den Anforderungen Ihres Unternehmens können Sie den AWS Backup Backup-Service verwenden, um Ihre SAP HANA-Datenbanken automatisch zu sichern, oder Sie können dieses Muster verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine bestehende SAP HANA-Instance mit einer unterstützten Version im Running-Status auf einer verwalteten Amazon Elastic Compute Cloud (Amazon EC2) -Instance, die für Systems Manager konfiguriert ist
- Systems Manager Agent (SSM Agent) 2.3.274.0 oder höher installiert
- Ein S3-Bucket, für den der öffentliche Zugriff nicht aktiviert ist
- Ein `hdbuserstore` Schlüssel mit dem Namen `SYSTEM`

- Eine AWS Identity and Access Management (IAM) -Rolle für das Automation-Runbook zur planmäßigen Ausführung
- `AmazonSSMManagedInstanceCore`und `ssm:StartAutomationExecution` Richtlinien sind der Systems Manager Automation-Servicerolle zugeordnet.

Einschränkungen

- AWS Backint Agent for SAP HANA unterstützt keine Deduplizierung.
- AWS Backint Agent for SAP HANA unterstützt keine Datenkomprimierung.

Produktversionen

AWS Backint Agent wird auf den folgenden Betriebssystemen unterstützt:

- SUSE-Linux-Enterprise-Server
- SUSE Linux Enterprise Server für SAP
- RedHat Enterprise Linux für SAP

AWS Backint Agent unterstützt die folgenden Datenbanken:

- SAP HANA 1.0 SP12 (einzelner Knoten und mehrere Knoten)
- SAP HANA 2.0 und höher (einzelner Knoten und mehrere Knoten)

Architektur

Zieltechnologie-Stack

- AWS-Backing-Agent
- Amazon S3
- AWS Systems Manager
- Amazon EventBridge
- SAP HANA

Zielarchitektur

Das folgende Diagramm zeigt die Installationsskripte, die AWS Backint Agent, den S3-Bucket und Systems Manager installieren und die ein Command-Dokument verwenden EventBridge, um regelmäßige Backups zu planen.

Automatisierung und Skalierung

- Mithilfe eines Systems Manager Automation-Runbooks können mehrere AWS-Backint-Agents installiert werden.
- Jeder Lauf des Systems Manager Manager-Runbooks kann je nach Zielauswahl auf n SAP HANA-Instanzen skaliert werden.
- EventBridge kann SAP HANA-Backups automatisieren.

Tools

- AWS Backint Agent for SAP HANA ist eine eigenständige Anwendung, die sich in Ihre bestehenden Workflows integriert, um Ihre SAP HANA-Datenbank in einem S3-Bucket zu sichern, den Sie in der Konfigurationsdatei angeben. AWS Backint Agent unterstützt vollständige, inkrementelle und differenzielle Backups von SAP HANA-Datenbanken. Es läuft auf einem SAP HANA-Datenbankserver, auf dem Backups und Kataloge von der SAP HANA-Datenbank auf den AWS Backint Agent übertragen werden.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen verbinden können. EventBridge liefert einen Stream von Echtzeitdaten aus Ihren Anwendungen, SaaS-Anwendungen (Software as a Service) und AWS-Services an Ziele wie AWS Lambda-Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen Konten.
- Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen.
- AWS Systems Manager hilft Ihnen dabei, Ihre Infrastruktur auf AWS anzuzeigen und zu steuern. Mithilfe der Systems Manager Manager-Konsole können Sie Betriebsdaten von mehreren AWS-Services anzeigen und betriebliche Aufgaben in Ihren AWS-Ressourcen automatisieren.

Code

Der Code für dieses Muster ist im aws-backint-automated-backup GitHub Repository verfügbar.

Epen

Erstellen Sie ein hdbuserstore-SchlüsselSYSTEM

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie einen hdbuserstore-Schlüssel.	1. Navigieren Sie zu `/usr/sap/<SID>/HDB<InstNo>/exe`.
	2. Führen Sie den folgenden Befehl mit XX der Instanznummer der SAP HANA-Datenbank aus.
	`hdbuserstore -i set SYSTEM <hostname>:3XX13@SYSTEMDB SYSTEM`
	Führen Sie beispielsweise für einen SAP HANA-Host `saphanadb` mit Instanznummer `00` den folgenden Befehl aus.
	`hdbuserstore -i set SYSTEM saphanadb:30013@SYSTEMDB SYSTEM`
		AWS-Administrator, SAP HANA-Administrator

Installieren Sie den AWS Backint Agent

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den AWS Backint Agent.	Folgen Sie den Anweisungen unter Installieren und Konfigurieren von AWS	AWS-Administrator, SAP HANA-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Backint Agent für SAP HANA in der Dokumentation zu AWS Backint Agent.	

Erstellen Sie das Systems Manager Manager-Befehlsdokument

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Systems Manager Manager-Befehlsdokument.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS Systems Manager-Konsole. 2. Wählen Sie Dokumente und dann Mein Eigentum aus. 3. Vergewissern Sie sich, dass Sie sich in derselben AWS-Region wie Ihre SAP HANA-Datenbank befinden. 4. Wählen Sie Dokument erstellen, Befehl oder Sitzung, um Ihr Dokument zu erstellen. 5. Verwenden Sie einen eindeutigen und aussagekräftigen Namen ohne Leerzeichen (z. B. SAP HANA-Backup). 6. Stellen Sie sicher, dass der Dokumenttyp auf Befehlsdokument eingestellt ist. 7. Unter der Überschrift Inhalt befindet sich ein Beispielcode. Stellen Sie sicher,	AWS-Administrator, SAP HANA-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dass Sie den JSON-Code typ wählen und den Code durch den Code aus der `HDB_Backup_SSM_Document.json` Datei aus dem GitHub Repository ersetzen. 8. Wählen Sie Create document (Dokument erstellen) aus. 9. Überprüfe dein Dokument im Abschnitt „Mein Eigentum“.	

Planen Sie Backups in regelmäßigen Abständen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Planen Sie regelmäßige Backups mit Amazon EventBridge.	1. Öffnen Sie die EventBridge Amazon-Konsole, wählen Sie Regeln und dann Regel erstellen aus. 2. Geben Sie auf dem Bildschirm „Regeldetails definieren“ einen eindeutigen Namen und eine Beschreibung für Ihre Regel ein und verwenden Sie den Standard-Event-Bus. 3. Wählen Sie unter Regeltyp die Option Zeitplan und dann Weiter aus.	AWS-Administrator, SAP HANA-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie auf dem Bildschirm „Zeitplan definieren“ das entsprechende Zeitplanmuster und den Cron- oder Ratenausdruck auf der Grundlage der erforderlichen Häufigkeit aus. 5. Wählen Sie auf dem Bildschirm Ziele auswählen für Zieltyp die Option AWS-Service aus. Wählen Sie unter Ziel auswählen die Option Systems Manager Run Command aus. 6. Wählen Sie das Dokument aus, das Sie zuvor erstellt haben. 7. Geben Sie unter Zielschlüssel und Zielwert die Instanz-ID ein. Sie können Tagnamen und Tag-Werte verwenden, um mehrere Instanzen hinzuzufügen. 8. Wählen Sie unter Automatisierungsparameter konfigurieren die Option Konstant für inkrementelle oder differenzielle Backups aus. Wenn Sie ein vollständiges Backup wünschen, wählen Sie Keine Parameter aus. 9. Wählen Sie aus, ob Sie eine neue Rolle erstellen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	oder eine bestehende Rolle verwenden möchten. Wenn Sie eine vorhandene Rolle verwenden, stellen Sie sicher, dass sie über die Richtlinien verfügt, die zum Aufrufen des Ziels erforderl ich sind. 10. Behalten Sie die zusätzlic hen Standardeinstellungen bei und wählen Sie Weiter. 11. Der Bildschirm „Tags konfigurieren“ ist optional. Wählen Sie „Weiter“. 12. Überprüfen Sie auf dem Bildschirm Überprüfen und erstellen die Regeleins tellungen und wählen Sie Erstellen aus. Die Regel sollte erfolgreich erstellt werden. Sie können den Erfolg der Sicherung anhand des S3-Bucket-Pfads überprüfen. `s3:/<your_bucket_n ame>/<target folder>/ <SID>/usr/sap/<SID> /SYS/global/hdb/ba ckint/DB_<SID>/`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie können Backups auch aus dem SAP HANA-Backup-Katalog überprüfen.	

Zugehörige Ressourcen

- AWS-Backing-Agent für SAP HANA
- Installieren und konfigurieren Sie den AWS Backint Agent für SAP HANA

Automatisches Generieren eines PynamoDB-Modells und CRUD-Funktionen für Amazon DynamoDB mithilfe einer Python-Anwendung

Erstellt von Vijit Vashishtha (AWS), Dheeraj Alimchandani (AWS) und Dhananjay Karanjkar (AWS)

Übersicht

Es ist üblich, Entitäten und CRUD-Operationsfunktionen (Create, Read, Update and Delete) zu verlangen, um Amazon DynamoDB DynamoDB-Datenbankoperationen effizient durchzuführen. PynamoDB ist eine Python-basierte Schnittstelle, die Python 3 unterstützt. Es bietet auch Funktionen wie Unterstützung für Amazon DynamoDB-Transaktionen, automatische Serialisierung und Deserialisierung von Attributwerten sowie Kompatibilität mit gängigen Python-Frameworks wie Flask und Django. Dieses Muster hilft Entwicklern, die mit Python und DynamoDB arbeiten, indem es eine Bibliothek bereitstellt, die die automatische Erstellung von PynamoDB-Modellen und CRUD-Betriebsfunktionen optimiert. Es generiert zwar wichtige CRUD-Funktionen für Datenbanktabellen, kann aber auch PynamoDB-Modelle und CRUD-Funktionen aus Amazon DynamoDB-Tabellen zurückentwickeln. Dieses Muster wurde entwickelt, um Datenbankoperationen mithilfe einer Python-basierten Anwendung zu vereinfachen.

Im Folgenden sind die Hauptmerkmale dieser Lösung aufgeführt:

- JSON-Schema zu PynamoDB-Modell — Generieren Sie automatisch PynamoDB-Modelle in Python, indem Sie eine JSON-Schemadatei importieren.
- Generierung von CRUD-Funktionen — Generieren Sie automatisch Funktionen zur Ausführung von CRUD-Operationen in DynamoDB-Tabellen.
- Reverse Engineering von DynamoDB — Verwenden Sie PynamoDB Object-Relational Mapping (ORM), um PynamoDB-Modelle und CRUD-Funktionen für bestehende Amazon DynamoDB-Tabellen zurückzuentwickeln.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Python Version 3.8 oder höher, heruntergeladen und installiert
- Jinja2 Version 3.1.2 oder höher, heruntergeladen und installiert
- Amazon DynamoDB-Tabellen, für die Sie ORM generieren möchten

- AWS Command Line Interface (AWS CLI), installiert und konfiguriert
- PynamoDB Version 5.4.1 oder höher, installiert

Architektur

Zieltechnologie-Stack

- JSON-Skript
- Python-Anwendung
- PynamoDB-Modell
- Amazon DynamoDB DynamoDB-Datenbank-Instance

Zielarchitektur

1. Sie erstellen eine Eingabe-JSON-Schemadatei. Diese JSON-Schemadatei stellt die Attribute der jeweiligen DynamoDB-Tabellen dar, aus denen Sie PynamoDB-Modelle und CRUD-Funktionen erstellen möchten. Sie enthält die folgenden drei wichtigen Schlüssel:
   - `name`— Der Name der DynamoDB-Zieltabelle.
   - `region`— Der AWS-Region Ort, an dem die Tabelle gehostet wird
   - `attributes`— Die Attribute, die Teil der Zieltabelle sind, wie z. B. der Partitionsschlüssel (auch als Hash-Attribut bezeichnet), der Sortierschlüssel, lokale Sekundärindizes, globale Sekundärindizes und alle Nichtschlüsselattribute. Dieses Tool erwartet, dass das Eingabeschema nur die Nicht-Schlüsselattribute bereitstellt, da die Anwendung die Schlüsselattribute direkt aus der Zieltabelle abruft. Ein Beispiel für die Angabe von Attributen in der JSON-Schemadatei finden Sie im Abschnitt Zusätzliche Informationen dieses Musters.
2. Führen Sie die Python-Anwendung aus und geben Sie die JSON-Schemadatei als Eingabe an.
3. Die Python-Anwendung liest die JSON-Schemadatei.
4. Die Python-Anwendung stellt eine Verbindung zu den DynamoDB-Tabellen her, um das Schema und die Datentypen abzuleiten. Die Anwendung führt den Vorgang describe_table aus und ruft die Schlüssel- und Indexattribute für die Tabelle ab.
5. Die Python-Anwendung kombiniert die Attribute aus der JSON-Schemadatei und der DynamoDB-Tabelle. Es verwendet die Jinja-Template-Engine, um ein PynamoDB-Modell und entsprechende CRUD-Funktionen zu generieren.

6. Sie greifen auf das PynamoDB-Modell zu, um CRUD-Operationen in der DynamoDB-Tabelle durchzuführen.

Tools

AWS-Services

- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.

Andere Tools

- Jinja ist eine erweiterbare Templating-Engine, die Vorlagen zu optimiertem Python-Code kompiliert. Dieses Muster verwendet Jinja, um dynamische Inhalte zu generieren, indem Platzhalter und Logik in Vorlagen eingebettet werden.
- PynamoDB ist eine Python-basierte Schnittstelle für Amazon DynamoDB.
- Python ist eine Allzweck-Computerprogrammiersprache.

Code-Repository

Der Code für dieses Muster ist im Repository für GitHub automatisch generierte PynamoDB-Modelle und CRUD-Funktionen verfügbar. Das Repository ist in zwei Hauptteile unterteilt: das Controller-Paket und die Vorlagen.

Controller-Paket

Das Controller-Python-Paket enthält die Hauptanwendungslogik, die bei der Generierung des PynamoDB-Modells und der CRUD-Funktionen hilft. Sie enthält Folgendes:

- `input_json_validator.py`— Dieses Python-Skript validiert die Eingabe-JSON-Schemadatei und erstellt die Python-Objekte, die die Liste der DynamoDB-Zieltabellen und die jeweils erforderlichen Attribute enthalten.
- `dynamo_connection.py`— Dieses Skript stellt eine Verbindung zur DynamoDB-Tabelle her und verwendet die `describe_table` Operation, um die Attribute zu extrahieren, die für die Erstellung des PynamoDB-Modells erforderlich sind.

- `generate_model.py`— Dieses Skript enthält eine Python-Klasse`GenerateModel`, die das PynamoDB-Modell auf der Grundlage der Eingabe-JSON-Schemadatei und der Operation erstellt. `describe_table`
- `generate_crud.py`— Für die DynamoDB-Tabellen, die in der JSON-Schemadatei definiert sind, verwendet dieses Skript den `GenerateCrud` Vorgang, um die Python-Klassen zu erstellen.

Vorlagen

Dieses Python-Verzeichnis enthält die folgenden Jinja-Vorlagen:

- `model.jinja`— Diese Jinja-Vorlage enthält den Vorlagenausdruck für die Generierung des PynamoDB-Modellskripts.
- `crud.jinja`— Diese Jinja-Vorlage enthält den Vorlagenausdruck für die Generierung des CRUD-Funktionsskripts.

Epen

Richte die Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Geben Sie den folgenden Befehl ein, um das Repository für automatisch generierte PynamoDB-Modelle und CRUD-Funktionen zu klonen. `git clone https://github.com/aws-samples/amazon-reverse-engineer-dynamodb.git`	App-Developer
Richten Sie die Python-Umgebung ein.	1. Navigieren Sie in das Verzeichnis der obersten Ebene im geklonten Repository.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`cd amazon-reverse-eng ineer-dynamodb`
	2. Geben Sie den folgenden Befehl ein, um die erforderl ichen Bibliotheken und Pakete zu installieren.
	`pip install -r requirements.txt`	

Generieren Sie das PynamoDB-Modell und die CRUD-Funktionen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die JSON-Sche madatei.	1. Navigieren Sie in das Verzeichnis der obersten Ebene im geklonten Repository. `cd amazon-reverse-eng ineer-dynamodb` 2. Öffnen Sie die `test.json` Datei in Ihrem bevorzugt en Editor. Sie können diese Datei als Referenz verwenden, um Ihre eigene JSON-Schemadatei zu erstellen, oder Sie können die Werte in dieser Datei an Ihre Umgebung anpassen. 3. Ändern Sie den Namen und AWS-Region die Attributw	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	erte für Ihre DynamoDB-Zieltabellen. **Note** Wenn Sie eine Tabelle definiere n, die in der JSON-Schemadatei nicht vorhanden ist, generiert diese Lösung keine Modelle oder CRUD-Funktionen für diese Tabelle. 4. Speichern und schließen Sie die Datei `test.json` . Wir empfehlen, dass Sie diese Datei unter einem neuen Namen speichern.	
Führen Sie die Python-An wendung aus.	Geben Sie den folgenden Befehl ein, um die PynamoDB-Modelle und CRUD-Funk tionen zu generieren, wobei der Name Ihrer JSON-Schemadatei `<input_sc hema.json>` steht. `python main.py --file <input_schema.json>`	App-Developer

Überprüfen Sie das PynamoDB-Modell und die CRUD-Funktionen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie das generierte PynamoDB-Modell.	1. Geben Sie im obersten Verzeichnis des geklonten Repositorys den folgenden Befehl ein, um zum Repository zu navigieren. `models` `cd models` 2. Standardmäßig benennt diese Lösung die PynamoDB-Modelldatei. `demo_model.py` Stellen Sie sicher, dass diese Datei vorhanden ist.	App-Developer
Überprüfen Sie die generierten CRUD-Funktionen.	1. Geben Sie im obersten Verzeichnis des geklonten Repositorys den folgenden Befehl ein, um zum Repository zu navigieren. `crud` `cd crud` 2. Standardmäßig benennt diese Lösung das Skript. `demo_crud.py` Stellen Sie sicher, dass diese Datei vorhanden ist. 3. Verwenden Sie die Python-Klassen in der `demo_crud.py` Datei, um eine CRUD-Operation in der	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	DynamoDB-Zieltabelle durchzuführen. Vergewissern Sie sich, dass der Vorgang erfolgreich abgeschlossen wurde.	

Zugehörige Ressourcen

- Kernkomponenten von Amazon DynamoDB (DynamoDB-Dokumentation)
- Verbesserung des Datenzugriffs mit Sekundärindizes (DynamoDB-Dokumentation)

Zusätzliche Informationen

Beispielattribute für die JSON-Schemadatei

```
[
{
"name": "test_table",
"region": "ap-south-1",
"attributes": [
{
"name": "id",
"type": "UnicodeAttribute"
},
{
"name": "name",
"type": "UnicodeAttribute"
},
{
"name": "age",
"type": "NumberAttribute"
}
]
}
]
```

Blockieren Sie den öffentlichen Zugriff auf Amazon RDS mithilfe von Cloud Custodian

Erstellt von Abhay Kumar (AWS) und Dwarika Patra (AWS)

Übersicht

Viele Unternehmen führen ihre Workloads und Services auf mehreren Cloud-Anbietern aus. In diesen Hybrid-Cloud-Umgebungen erfordert die Cloud-Infrastruktur zusätzlich zur Sicherheit, die von den einzelnen Cloud-Anbietern bereitgestellt wird, eine strenge Cloud-Governance. Eine Cloud-Datenbank wie Amazon Relational Database Service (Amazon RDS) ist ein wichtiger Dienst, der auf Zugriffs- und Berechtigungsschwachstellen überwacht werden muss. Sie können zwar den Zugriff auf die Amazon RDS-Datenbank einschränken, indem Sie eine Sicherheitsgruppe konfigurieren, aber Sie können eine zweite Schutzebene hinzufügen, um Aktionen wie den öffentlichen Zugriff zu verbieten. Die Sperrung des öffentlichen Zugangs hilft Ihnen bei der Einhaltung der Allgemeinen Datenschutzverordnung (DSGVO), des Health Insurance Portability and Accountability Act (HIPAA), des National Institute of Standards and Technology (NIST) und des Payment Card Industry Data Security Standard (PCI DSS).

Cloud Custodian ist eine Open-Source-Regel-Engine, mit der Sie Zugriffsbeschränkungen für Amazon Web Services (AWS) -Ressourcen wie Amazon RDS durchsetzen können. Mit Cloud Custodian können Sie Regeln festlegen, die die Umgebung anhand definierter Sicherheits- und Compliance-Standards validieren. Sie können Cloud Custodian verwenden, um Ihre Cloud-Umgebungen zu verwalten, indem Sie dazu beitragen, die Einhaltung von Sicherheitsrichtlinien, Tag-Richtlinien und die Müllsammlung ungenutzter Ressourcen sowie das Kostenmanagement sicherzustellen. Mit Cloud Custodian können Sie eine einzige Oberfläche für die Implementierung von Governance in einer Hybrid-Cloud-Umgebung verwenden. Sie könnten beispielsweise die Cloud Custodian-Schnittstelle verwenden, um mit Microsoft Azure zu interagieren AWS und so den Aufwand für die Arbeit mit Mechanismen wie AWS Config AWS Sicherheitsgruppen und Azure-Richtlinien zu reduzieren.

Dieses Muster enthält Anweisungen zur Verwendung von Cloud Custodian AWS , um die Einschränkung des öffentlichen Zugriffs auf Amazon RDS-Instances durchzusetzen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto

- Ein key pair
- AWS Lambda installiert

Architektur

Das folgende Diagramm zeigt, wie Cloud Custodian die Richtlinie für Amazon AWS Lambda RDS bereitstellt, das `CreateDBInstance` Ereignis AWS CloudTrail auslöst und die Lambda-Funktion `PubliclyAccessible` auf False gesetzt hat.

Tools

AWS-Services

- AWS CloudTrailhilft Ihnen bei der Prüfung der Unternehmensführung, der Einhaltung von Vorschriften und des betrieblichen Risikos Ihrer AWS-Konto.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie AWS-Services über Befehle in Ihrer Befehlszeilen-Shell interagieren können.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem es kontrolliert, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der. AWS Cloud

Andere Tools

- Cloud Custodian vereint die Tools und Skripte, die viele Unternehmen zur Verwaltung ihrer Public-Cloud-Konten verwenden, in einem Open-Source-Tool. Es verwendet eine Engine für statuslose Regeln zur Definition und Durchsetzung von Richtlinien mit Metriken, strukturierten Ergebnissen und detaillierten Berichten für die Cloud-Infrastruktur. Sie lässt sich eng in eine serverlose Runtime integrieren, um Problembehebung und Reaktion in Echtzeit bei geringem Betriebsaufwand zu ermöglichen.

Epen

Richten Sie das ein AWS CLI

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie das AWS CLI.	Folgen Sie den Anweisungen in der AWS Dokumentation AWS CLI, um das zu installieren.	AWS-Administrator

Richten Sie AWS Anmeldeinformationen ein.	Konfigurieren Sie die Einstellungen, mit denen die AWS CLI Benutzer interagieren AWS, einschließlich des AWS-Region Ausgabeformats, das Sie verwenden möchten.
	`$>aws configure`
	`AWS Access Key ID [None]: <your_access_key_id>`
	`AWS Secret Access Key [None]: <your_secret_access_key>`
	`Default region name [None]:`
	`Default output format [None]:`
	Weitere Informationen finden Sie in der AWS -Dokumentation.
		AWS-Administrator

Erstellen Sie eine IAM-Rolle.	Führen Sie den folgenden Befehl aus, um eine IAM-Rolle mit der Lambda-Ausführungsrolle zu erstellen.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws iam create-role --role-name lambda-ex --assume-role-policy-document '{"Version": "2012-10-17","Statement": [{ "Effect": "Allow", "Principal": {"Service": "lambda.amazonaws.com"}, "Action": "sts:AssumeRole"}]}`	

Richten Sie Cloud Custodian ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Cloud Custodian.	Um Cloud Custodian für Ihr Betriebssystem und Ihre Umgebung zu installieren, folgen Sie den Anweisungen in der Cloud Custodian-Dokumentation.	DevOps Ingenieur
Überprüfen Sie das Cloud Custodian-Schema.	Verwenden Sie den folgenden Befehl, um die vollständige Liste der Amazon RDS-Ressourcen anzuzeigen, für die Sie Richtlinien ausführen können. `custodian schema aws.rds`	DevOps Ingenieur
Erstellen Sie die Cloud Custodian-Richtlinie.	Speichern Sie den Code, der sich unter der Cloud Custodian-Richtliniendatei im Abschnitt Zusätzliche	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Informationen befindet, mit einer YAML-Erweiterung.	
Definieren Sie Cloud Custodian-Aktionen, um die Kennzeichnung für öffentlich zugänglich zu ändern.	1. Suchen Sie den Depotbankcode (z. B. `/Users/abcd/custodian/lib/python3.9/site-packages/c7n/resources/rds.py`). 2. Suchen Sie die `RDSSetPublicAvailability` Klasse in und ändern Sie diese Klasse `rds.py`, indem Sie den Code verwenden, der sich in der Datei c7n resources rds.py im Abschnitt Zusätzliche Informationen befindet.	DevOps Ingenieur
Führen Sie einen Probelauf durch.	(Optional) Verwenden Sie den folgenden Befehl, um zu überprüfen, welche Ressourcen durch die Richtlinie identifiziert werden, ohne Aktionen für die Ressourcen auszuführen. `custodian run -dryrun <policy_name>.yaml -s <output_directory>`	DevOps Ingenieur

Stellen Sie die Richtlinie bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Richtlinie mithilfe von Lambda bereit.	Verwenden Sie den folgenden Befehl, um die Lambda-Funktion zu erstellen, mit der die Richtlinie ausgeführt wird. `custodian run -s policy.yaml` Diese Richtlinie wird dann durch das AWS CloudTrail `CreateDBInstance` Ereignis initiiert. Daher AWS Lambda wird die Kennzeichnung `false` für öffentlich zugängliche Instanzen, die den Kriterien entsprechen, auf „öffentlich zugänglich“ gesetzt.	DevOps Ingenieur

Zugehörige Ressourcen

- AWS Lambda website
- Amazon RDS-Webseite
- Dokumentation zu Cloud Custodian

Zusätzliche Informationen

YAML-Datei zur Cloud-Custodian-Richtlinie

```
policies:
  - name: "block-public-access"
    resource: rds
```

```
    description: |
      This Enforcement blocks public access for RDS instances.
    mode:
      type: cloudtrail
      events:
        - event: CreateDBInstance # Create RDS instance cloudtrail event
          source: rds.amazonaws.com
          ids: requestParameters.dBInstanceIdentifier
      role: arn:aws:iam::1234567890:role/Custodian-compliance-role
    filters:
      - type: event
        key: 'detail.requestParameters.publiclyAccessible'
        value: true
    actions:
      - type: set-public-access
        state: false
```

Datei rds.py für c7n-Ressourcen

```
@actions.register('set-public-access')
 class RDSSetPublicAvailability(BaseAction):

     schema = type_schema(
         "set-public-access",
         state={'type': 'boolean'})
     permissions = ('rds:ModifyDBInstance',)

     def set_accessibility(self, r):
         client = local_session(self.manager.session_factory).client('rds')
         waiter = client.get_waiter('db_instance_available')
         waiter.wait(DBInstanceIdentifier=r['DBInstanceIdentifier'])
         client.modify_db_instance(
             DBInstanceIdentifier=r['DBInstanceIdentifier'],
             PubliclyAccessible=self.data.get('state', False))


     def process(self, rds):
         with self.executor_factory(max_workers=2) as w:
             futures = {w.submit(self.set_accessibility, r): r for r in rds}
             for f in as_completed(futures):
                 if f.exception():
                     self.log.error(
                         "Exception setting public access on %s  \n %s",
```

```
                        futures[f]['DBInstanceIdentifier'], f.exception())
        return rds
```

Integration von Security Hub

Cloud Custodian kann integriert werden, um Sicherheitsfeststellungen AWS Security Hubzu senden und Abhilfemaßnahmen zu ergreifen. Weitere Informationen finden Sie unter Ankündigung der Cloud Custodian-Integration mit. AWS Security Hub

Kontenübergreifenden Zugriff auf Amazon DynamoDB konfigurieren

Erstellt von Shashi Dalmia (AWS), Esteban Serna Parra (AWS) und Imhoertha Ojior (AWS)

Übersicht

Dieses Muster erklärt die Schritte zur Konfiguration des kontoübergreifenden Zugriffs auf Amazon DynamoDB mithilfe ressourcenbasierter Richtlinien. Für Workloads, die DynamoDB verwenden, wird es immer üblicher, Strategien zur Workload-Isolierung zu verwenden, um Sicherheitsbedrohungen zu minimieren und Compliance-Anforderungen zu erfüllen. Die Implementierung von Strategien zur Workload-Isolierung erfordert häufig konto- und regionsübergreifenden Zugriff auf DynamoDB-Ressourcen mithilfe identitätsbasierter AWS Identity and Access Management (IAM-) Richtlinien. Dazu gehören das Festlegen von IAM-Berechtigungen und das Herstellen einer Vertrauensbeziehung zwischen den. AWS-Konten

Ressourcenbasierte Richtlinien für DynamoDB vereinfachen die Sicherheitslage für kontenübergreifende Workloads erheblich. Dieses Muster enthält Schritte und Beispielcode, um zu demonstrieren, wie Sie AWS Lambda Funktionen in einem konfigurieren können AWS-Konto , um Daten in eine DynamoDB-Datenbanktabelle in einem anderen Konto zu schreiben.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zwei aktiv. AWS-Konten Dieses Muster bezeichnet diese Konten als Konto A und Konto B.
- AWS Command Line Interface (AWS CLI) für den Zugriff auf Konto A installiert und konfiguriert, um die DynamoDB-Tabelle zu erstellen. Die anderen Schritte in diesem Muster enthalten Anweisungen zur Verwendung der IAM-, DynamoDB- und Lambda-Konsolen. Wenn Sie es AWS CLI stattdessen verwenden möchten, konfigurieren Sie es so, dass es auf beide Konten zugreift.

Einschränkungen

- Einige AWS-Services sind nicht in allen verfügbar AWS-Regionen. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie auf der Seite Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Architektur

Das folgende Diagramm zeigt eine Architektur mit einem einzigen Konto. AWS Lambda, Amazon Elastic Compute Cloud (Amazon EC2) und DynamoDB befinden sich alle in demselben Konto. In diesem Szenario können Lambda-Funktionen und EC2 Amazon-Instances auf DynamoDB zugreifen. Um Zugriff auf die DynamoDB-Tabelle zu gewähren, können Sie eine identitätsbasierte Richtlinie in IAM oder eine ressourcenbasierte Richtlinie in DynamoDB erstellen.

Das folgende Diagramm zeigt eine Architektur mit mehreren Konten. Wenn Ressourcen in einem AWS-Konto Konto Zugriff auf eine DynamoDB-Tabelle in einem anderen Konto benötigen, müssen Sie in DynamoDB eine ressourcenbasierte Richtlinie einrichten, um den erforderlichen Zugriff zu gewähren. Im folgenden Diagramm wird beispielsweise einer Lambda-Funktion in Konto B mithilfe einer ressourcenbasierten Richtlinie Zugriff auf die DynamoDB-Tabelle in Konto A gewährt.

Dieses Muster beschreibt den kontenübergreifenden Zugriff zwischen Lambda und DynamoDB. Sie können ähnliche Schritte für andere Konten verwenden, AWS-Services wenn die entsprechenden Berechtigungen für beide Konten konfiguriert sind. Wenn Sie beispielsweise einer Lambda-Funktion Zugriff auf einen Amazon Simple Storage Service (Amazon S3) -Bucket in Konto A gewähren möchten, können Sie eine ressourcenbasierte Richtlinie in Amazon S3 erstellen und die Berechtigungen zur Lambda-Ausführungsrolle in Konto B hinzufügen.

Tools

AWS-Services

- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, sie zu verwenden.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.

Code

Dieses Muster enthält Beispielcode im Abschnitt Zusätzliche Informationen, der zeigt, wie Sie eine Lambda-Funktion in Konto B so konfigurieren können, dass sie in die DynamoDB-Tabelle in Konto A schreibt. Der Code dient nur zur Veranschaulichung und zu Testzwecken. Wenn Sie dieses Muster in einer Produktionsumgebung implementieren, verwenden Sie den Code als Referenz und passen Sie ihn an Ihre eigene Umgebung an.

Bewährte Methoden

- Folgen Sie den Best Practices für ressourcenbasierte Richtlinien in der DynamoDB-Dokumentation.
- Folgen Sie dem Prinzip der geringsten Rechte und gewähren Sie die für die Ausführung einer Aufgabe erforderlichen Mindestberechtigungen. Weitere Informationen finden Sie in der IAM-Dokumentation unter Gewährung der geringsten Rechte und bewährte Methoden zur Sicherheit.

Epen

Erstellen Sie eine IAM-Richtlinie und -Rolle für die Lambda-Funktion in Konto B

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Richtlinie in Konto B.	Diese IAM-Richtlinie ermöglicht die PutItemAktion für eine DynamoDB-Tabelle in Konto A. 1. Melden Sie sich bei Konto B im an. AWS Management Console 2. Öffnen Sie die IAM-Konsole. 3. Wählen Sie im Navigationsbereich Richtlinien und dann Richtlinie erstellen. 4. Wählen Sie auf der Seite „Berechtigungen angeben“ für den Richtlinien-Editor die Option JSON aus.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Geben Sie die folgende Richtlinie ein: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "Statement1", "Effect": "Allow", "Action": "dynamodb:PutItem", "Resource": "arn:aws:dynamodb:<Region>:<Account-A-ID>:table/Table-Account-A" } ] }` 6. Ersetzen Sie `<Region>` und `<Account-A-ID>` durch Ihre Werte und wählen Sie dann Weiter aus. 7. Geben Sie unter Richtlinienname einen eindeutigen Namen für Ihre Richtlinie ein, z. `DynamoDB-PutItem-Policy` B. 8. (Optional) Fügen Sie eine Richtlinienbeschreibung hinzu.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	9. Wählen Sie Richtlinie erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Rolle in Konto B.	Die Lambda-Funktion in Konto B verwendet diese IAM-Rolle, um auf die DynamoDB-Tabelle in Konto A zuzugreifen. 1. Öffnen Sie die IAM-Konsole. 2. Wählen Sie im Navigationsbereich Roles (Rollen) und dann Create role (Rolle erstellen). 3. Wählen Sie für Select trusted entity (Vertrauenswürdige Entität auswählen) die Option AWS-Service aus. 4. Wählen Sie im Abschnitt Anwendungsfall die Option Lambda aus. 5. Wählen Sie Weiter: Berechtigungen aus. 6. Geben Sie im Feld Filterrichtlinien DynamoDB ein. 7. Wählen Sie in der Liste der DynamoDB-Richtlinien die Option. `DynamoDB-PutItem-Policy` 8. Löschen Sie das Feld Filterrichtlinien, und geben Sie dann Lambda ein. 9. Wählen Sie in der Liste der Lambda-Richtlinien	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Option AWSLambda Ausführen aus. 10. Wählen Sie Weiter: Benennen, überprüfen und erstellen. 11. Geben Sie unter Role name (Rollenname) einen eindeutigen Namen für die Rolle ein, z. B. `DynamoDB-PutItemAccess` . 12. (Optional) Fügen Sie eine Rollenbeschreibung hinzu. 13. (Optional) Fügen Sie der Rolle Metadaten hinzu, indem Sie Tags als Schlüssel-Wert-Paare anfügen. 14. Wählen Sie Rolle erstellen aus. Weitere Informationen zum Erstellen von Rollen finden Sie in der IAM-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beachten Sie die Rollen-ARN.	1. Öffnen Sie die IAM-Konsole. 2. Wählen Sie im Navigationsbereich Roles aus. 3. Geben Sie `DynamoDB-PutItemAccess` im Suchfeld die Rolle ein und wählen Sie sie aus. 4. Kopieren Sie auf der Übersichtsseite für die Rolle den Amazon-Ressourcennamen (ARN). Sie verwenden den ARN, wenn Sie die Lambda-Funktion einrichten.	Allgemeines AWS

Erstellen Sie eine DynamoDB-Tabelle in Konto A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine DynamoDB-Tabelle.	Verwenden Sie den folgenden AWS CLI Befehl, um eine DynamoDB-Tabelle zu erstellen. `aws dynamodb create-table \ --table-name Table-Account-A \ --attribute-definitions \ Attribute Name=category,Attr ibuteType=S \`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`Attribute Name=item,AttributeType=S \ --key-schema \ Attribute Name=category,KeyType=HASH \ Attribute Name=item,KeyType=RANGE \ --provisioned-throughput \ ReadCapacityUnits=5,WriteCapacityUnits=5 \ --resource-policy \ '{ "Version": "2012-10-17", "Statement": [{ "Sid": "Statement1", "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::<Account-B-ID>:role/<Role-Name>" }, "Action": "dynamodb:PutItem", "Resource": "arn:aws:dynamodb:<Region>:<Account-A-ID>:table/Table-Account-A"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> }
	
	         ]
	    }'</pre>
	Ersetzen Sie in diesem Codebeispiel Folgendes:
	• `<Account-B-ID>` ist die ID von Konto B.
	• `<Role-Name>` ist der Name der IAM-Rolle, die Sie erstellt haben, z. B. `DynamoDB-PutItemAccess`
	• `<Region>`ist der AWS-Region Ort, an dem Sie die DynamoDB-Tabelle erstellen.
	• `<Account-A-ID>` ist die ID von Konto A.
	
	Note
	Sie geben die ressourcenbasierte Richtlinienkonfiguration in der `create-table` Anweisung mithilfe des `--resource-policy` Flags an. Diese Richtlinie bezieht sich auf den ARN für die	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	DynamoDB-Tabelle in Konto A. Weitere Informationen zum Erstellen von Tabellen finden Sie in der DynamoDB-Dokumentation.	

Erstellen Sie eine Lambda-Funktion in Konto B

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Lambda-Funktion, um Daten in DynamoDB zu schreiben.	1. Melden Sie sich bei Konto B in der an. AWS Management Console 2. Öffnen Sie die Lambda-Konsole. 3. Wählen Sie im Navigationsbereich Funktionen und dann Funktion erstellen aus. 4. Geben Sie unter Name `lambda_write_function` ein. 5. Wählen Sie für Runtime Python 3.8 oder höher. 6. Wählen Sie unter Standardausführungsrolle ändern die Option Bestehende Rolle verwenden aus.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Wählen Sie für Existierende Rolle die IAM-Rolle aus, die Sie erstellt haben, z. B. `DynamoDB-PutItemAccess` 8. Wählen Sie Funktion erstellen. 9. Fügen Sie auf der Registerkarte Code den Beispielcode ein, der im Abschnitt Zusätzliche Informationen dieses Musters bereitgestellt wird. Ersetzen Sie in diesem Codebeispiel Folgendes: • `<Account-A-ID>` ist die ID von Konto A. • `<Region>`ist der AWS-Region Ort, an dem Sie die DynamoDB-Tabelle erstellt haben. 10. Wählen Sie Bereitstellen. 11. Wählen Sie Test aus. Sie werden aufgefordert, ein Testereignis zu konfigurieren. Erstellen Sie ein neues Ereignis mit Ihrem bevorzugten Namen, z. B. `MyTestEventForWrite` , und speichern Sie dann die Konfiguration. 12. Wählen Sie erneut Test (Testen) aus. Dadurch	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wird die Lambda-Fu nktion mit dem von Ihnen angegebenen Ereignisn amen ausgeführt. 13. Überprüfen Sie die Ausgabe der Funktion. Es sollte angeben, dass die Funktion auf die DynamoDB-Tabelle in Konto A zugegriffen hat und Daten in diese Tabelle schreiben konnte. Weitere Informationen zum Erstellen von Lambda-Fu nktionen finden Sie in der Lambda-Dokumentation.	

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ressourcen löschen.	Um zu vermeiden, dass Kosten im Zusammenh ang mit den nach diesem Muster erstellten Ressourcen anfallen, gehen Sie wie folgt vor, um diese Ressourcen zu löschen: 1. Löschen Sie in Konto B die Lambda-Funktion, die Sie für die Verbindung mit DynamoDB erstellt haben.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anweisungen finden Sie in der Lambda-Dokumentation. 2. Löschen Sie in Konto A die DynamoDB-Tabelle, die Sie erstellt haben. Anweisungen finden Sie in der DynamoDB-Dokumentation. 3. Bewährte Sicherheitsmethoden finden Sie, wenn Sie die IAM-Richtlinie (`DynamoDB-PutItem-Policy`) löschen, wenn sie nicht mehr benötigt wird. Weitere Informationen finden Sie in der IAM-Dokumentation. 4. Aus Sicherheitsgründen empfiehlt es sich, die IAM-Rolle (`DynamoDB-PutItemAccess`) zu löschen, wenn sie nicht mehr benötigt wird. Weitere Informationen finden Sie in der IAM-Dokumentation.	

Fehlerbehebung

Problem	Lösung
Beim Erstellen der Lambda-Funktion erhalten Sie eine `ResourceNotFoundException` Fehlermeldung.	Vergewissern Sie sich, dass Sie die ID AWS-Region und die ID von Konto A korrekt eingegeben haben. Diese sind Teil des ARN für die DynamoDB-Tabelle.

Zugehörige Ressourcen

- Erste Schritte mit DynamoDB (DynamoDB-Dokumentation)
- Erste Schritte mit Lambda (Lambda-Dokumentation)
- Verwenden ressourcenbasierter Richtlinien für DynamoDB (DynamoDB-Dokumentation)
- IAM-Richtlinien erstellen (IAM-Dokumentation)
- Logik zur kontenübergreifenden Bewertung von Richtlinien (IAM-Dokumentation)
- Referenz zu den IAM-JSON-Richtlinienelementen (IAM-Dokumentation)

Zusätzliche Informationen

Beispielcode

```
import boto3
from datetime import datetime

dynamodb_client = boto3.client('dynamodb')

def lambda_handler(event, context):
     now = datetime.now().isoformat()
     data = dynamodb_client.put_item(TableName='arn:aws:dynamodb:<Region>:<Account-
A-ID>:table/Table-Account-A', Item={"category": {"S": "Fruit"},"item": {"S":
 "Apple"},"time": {"S": now}})
     return data
```

> **Note**
>
> Wenn der DynamoDB-Client instanziiert wird, wird der ARN der DynamoDB-Tabelle anstelle des Tabellennamens bereitgestellt. Dies ist erforderlich, damit die Lambda-Funktion bei ihrer Ausführung eine Verbindung zur richtigen DynamoDB-Tabelle herstellt.

Konfigurieren Sie das schreibgeschützte Routing in einer Always-On-Verfügbarkeitsgruppe in SQL Server auf AWS

Erstellt von Subhani Shaik (AWS)

Übersicht

Dieses Muster beschreibt, wie das sekundäre Standby-Replikat in SQL Server Always On verwendet wird, indem die schreibgeschützten Workloads vom primären Replikat auf das sekundäre Replikat verlagert werden.

Die Datenbankspiegelung verfügt über eine Zuordnung. one-to-one Sie können die sekundäre Datenbank nicht direkt lesen, daher müssen Sie Snapshots erstellen. Die Always-On-Verfügbarkeitsgruppenfunktion wurde in Microsoft SQL Server 2012 eingeführt. In späteren Versionen wurden wichtige Funktionen eingeführt, darunter schreibgeschütztes Routing. In Always-On-Verfügbarkeitsgruppen können Sie die Daten direkt aus dem sekundären Replikat lesen, indem Sie den Replikatmodus auf Schreibgeschützt ändern.

Die Always-On-Lösung für Verfügbarkeitsgruppen unterstützt Hochverfügbarkeit (HA), Notfallwiederherstellung (DR) und ist eine Alternative zur Datenbankspiegelung. Always-On-Verfügbarkeitsgruppen arbeiten auf Datenbankebene und maximieren die Verfügbarkeit einer Reihe von Benutzerdatenbanken.

SQL Server verwendet den Nur-Lese-Routing-Mechanismus, um die eingehenden schreibgeschützten Verbindungen an das sekundäre Lesereplikat umzuleiten. Um dies zu erreichen, sollten Sie der Verbindungszeichenfolge die folgenden Parameter und Werte hinzufügen:

- `ApplicationIntent=ReadOnly`
- `Initial Catalog=<database name>`

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit einer Virtual Private Cloud (VPC), zwei Availability Zones, privaten Subnetzen und einer Sicherheitsgruppe
- Zwei Amazon Elastic Compute Cloud (Amazon EC2) -Maschinen mit SQL Server 2019 Enterprise Edition Amazon Machine Image with Windows Server Failover Clustering (WSFC), konfiguriert auf Instanzebene und einer Always-On-Verfügbarkeitsgruppe, die auf SQL Server-Ebene zwischen

dem primären Knoten (`WSFCNODE1`) und dem sekundären Knoten (`WSFCNODE2`) konfiguriert ist, die Teil des AWS Directory Service for Microsoft Active Directory-Verzeichnisses mit dem Namen `tagechtalk.com`
- Ein oder mehrere Knoten, die für die Annahme `read-only` im sekundären Replikat konfiguriert sind
- Ein Listener, der nach der `SQLAG1` Always-On-Verfügbarkeitsgruppe benannt ist
- SQL Server Database Engine wird mit demselben Dienstkonto auf zwei Knoten ausgeführt
- SQL Server Management Studio (SSMS)
- Eine Testdatenbank mit dem Namen `test`

Produktversionen

- SQL Server 2014 und höher

Architektur

Zieltechnologie-Stack

- Amazon EC2
- AWS Managed Microsoft AD
- Amazon FSx

Zielarchitektur

Das folgende Diagramm zeigt, wie der Always On Availability Group (AG) -Listener Abfragen, die den `ApplicationIntent` Parameter in der Verbindung enthalten, an den entsprechenden sekundären Knoten umleitet.

1. Eine Anfrage wird an den Always-On-Verfügbarkeitsgruppen-Listener gesendet.
2. Wenn die Verbindungszeichenfolge den `ApplicationIntent` Parameter nicht enthält, wird die Anfrage an die primäre Instanz gesendet.
3. Wenn die Verbindungszeichenfolge Folgendes enthält`ApplicationIntent=ReadOnly`, wird die Anforderung an die sekundäre Instanz mit schreibgeschützter Routing-Konfiguration gesendet, bei der es sich um WSFC mit einer Always-On-Verfügbarkeitsgruppe handelt.

Tools

AWS-Services

- AWS Directory Service für Microsoft Active Directory ermöglicht Ihren verzeichnissensitiven Workloads und AWS-Ressourcen die Nutzung von Microsoft Active Directory in der AWS-Cloud.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon FSx bietet Dateisysteme, die branchenübliche Konnektivitätsprotokolle unterstützen und Hochverfügbarkeit und Replikation in allen AWS-Regionen bieten.

Andere Dienste

- SQL Server Management Studio (SSMS) ist ein Tool zum Verbinden, Verwalten und Verwalten der SQL Server-Instanzen.
- sqlcmd ist ein Befehlszeilenprogramm.

Bewährte Methoden

Weitere Informationen zu AlwaysOn-Verfügbarkeitsgruppen finden Sie in der SQL Server-Dokumentation.

Epen

Richten Sie schreibgeschütztes Routing ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Replikate so, dass sie schreibgeschützt sind.	Um sowohl das primäre als auch das sekundäre Replikat auf schreibgeschützt zu aktualisieren, stellen Sie von SSMS aus eine Verbindung zum primären Replikat her und führen Sie den Schritt 1-Code	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	aus dem Abschnitt Zusätzliche Informationen aus.	
Erstellen Sie die Routing-URL.	Um die Routing-URL für beide Replikate zu erstellen, führen Sie den Schritt 2-Code aus dem Abschnitt Zusätzliche Informationen aus. In diesem Code `tagechtalk.com` steht der Name des AWS Managed Microsoft AD-Verzeichnisses.	DBA
Erstellen Sie die Routing-Liste.	Um die Routingliste für beide Replikate zu erstellen, führen Sie den Schritt 3-Code aus dem Abschnitt Zusätzliche Informationen aus.	DBA
Überprüfen Sie die Routingliste.	Stellen Sie von SQL Server Management Studio aus eine Connect der primären Instanz her, und führen Sie den Schritt 4-Code aus dem Abschnitt Zusätzliche Informationen aus, um die Routingliste zu überprüfen.	DBA

Testen Sie das schreibgeschützte Routing

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie mithilfe des ApplicationIntent Parameters eine Verbindung her.	1. Stellen Sie von SSMS aus eine Verbindung zum Listener-Namen	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Always-On-Verfügba rkeitsgruppe mit her. `ApplicationIntent= ReadOnly;Initial Catalog=test` 2. Die Verbindung wird mit dem sekundären Replikat hergestellt. Um dies zu testen, führen Sie den folgenden Befehl aus, um den Namen des verbunden en Servers anzuzeigen. `SELECT SERVERPRO PERTY('Computernam ePhysicalNetBios')` In der Ausgabe wird der aktuelle Name des sekundären Replikats (`WSFCNODE2`) angezeigt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie einen Failover durch.	1. Stellen Sie von SSMS aus eine Verbindung zum Listener-Namen der Always-On-Verfügba rkeitsgruppe her. 2. Stellen Sie sicher, dass die primäre und die sekundäre Datenbank synchron und ohne Datenverlust synchronisiert sind. 3. Führen Sie einen Failover durch, sodass das aktuelle primäre Replikat zum sekundären Replikat und das sekundäre Replikat zum primären Replikat wird. 4. Stellen Sie von SSMS aus eine Verbindung mit dem Listener-Namen der Always-On-Verfügba rkeitsgruppe mit her. `ApplicationIntent=ReadOnly;Initial Catalog=test` 5. Die Verbindung wird mit dem sekundären Replikat hergestellt. Um dies zu testen, zeigen Sie den Namen des verbundenen Servers an, indem Sie den folgenden Befehl ausführen.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`SELECT SERVERPRO PERTY('Computernam ePhysicalNetBios')` Es wird der aktuelle Name des sekundären Replikats angezeigt (`WSFCNODE1`).	

Stellen Sie mithilfe des Befehlszeilenprogramms sqlcmd eine Verbindung her

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie mithilfe von sqlcmd eine Connect.	Um von sqlcmd aus eine Verbindung herzustellen, führen Sie in der Befehlszeile den Schritt 5-Code aus dem Abschnitt Zusätzliche Informati onen aus. Nachdem Sie die Verbindung hergestellt haben, führen Sie den folgenden Befehl aus, um den Namen des verbundenen Servers anzuzeigen. `SELECT SERVERPRO PERTY('Computernam ePhysicalNetBios') .` In der Ausgabe wird der aktuelle Name des sekundäre n Replikats (`WSFCNODE1`) angezeigt.	DBA

Fehlerbehebung

Problem	Lösung
Das Erstellen des Listeners schlägt fehl und es wird die Meldung „Der WSFC-Cluster konnte die Netzwerknamenressource nicht online bringen“ angezeigt.	Weitere Informationen finden Sie im Microsoft-Blogbeitrag Create Listener Fails with Message 'The WSFC-Cluster could not bring the Network Name resource online'.
Mögliche Probleme, einschließlich anderer Listener-Probleme oder Netzwerkzugriffspr obleme.	Weitere Informationen finden Sie unter Problembehandlung bei der Konfiguration von Always-On-Verfügbarkeitsgruppen (SQL Server) in der Microsoft-Dokumentation.

Zugehörige Ressourcen

- Konfigurieren Sie schreibgeschütztes Routing für eine Always-On-Verfügbarkeitsgruppe
- Problembehandlung bei der Konfiguration von AlwaysOn-Verfügbarkeitsgruppen (SQL Server)

Zusätzliche Informationen

Schritt 1. Aktualisieren Sie die Replikate so, dass sie schreibgeschützt sind

```
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE1' WITH (SECONDARY_ROLE
 (ALLOW_CONNECTIONS = READ_ONLY))
GO
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE2' WITH (SECONDARY_ROLE
 (ALLOW_CONNECTIONS = READ_ONLY))
GO
```

Schritt 2. Erstellen Sie die Routing-URL

```
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE1' WITH (SECONDARY_ROLE
 (READ_ONLY_ROUTING_URL = N'TCP://WSFCNode1.tagechtalk.com:1433'))
GO
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE2' WITH (SECONDARY_ROLE
 (READ_ONLY_ROUTING_URL = N'TCP://WSFCNode2.tagechtalk.com:1433'))
GO
```

Schritt 3. Erstellen Sie die Routing-Liste

```
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE1' WITH
 (PRIMARY_ROLE(READ_ONLY_ROUTING_LIST=('WSFCNODE2','WSFCNODE1')));
GO
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE2' WITH (PRIMARY_ROLE
 (READ_ONLY_ROUTING_LIST=('WSFCNODE1','WSFCNODE2')));
GO
```

Schritt 4. Validieren Sie die Routing-Liste

```
SELECT AGSrc.replica_server_name AS PrimaryReplica, AGRepl.replica_server_name AS
 ReadOnlyReplica, AGRepl.read_only_routing_url AS RoutingURL , AGRL.routing_priority
 AS RoutingPriority FROM sys.availability_read_only_routing_lists AGRL INNER JOIN
 sys.availability_replicas AGSrc ON AGRL.replica_id = AGSrc.replica_id INNER JOIN
 sys.availability_replicas AGRepl ON AGRL.read_only_replica_id = AGRepl.replica_id
 INNER JOIN sys.availability_groups AV ON AV.group_id = AGSrc.group_id ORDER BY
 PrimaryReplica
```

Schritt 5. SQL-Befehlsdienstprogramm

```
sqlcmd -S SQLAG1,1433 -E -d test -K ReadOnly
```

Stellen Sie eine Connect über einen SSH-Tunnel in pgAdmin her

Erstellt von Jeevan Shetty (AWS) und Bhanu Ganesh Gudivada (AWS)

Übersicht

Aus Sicherheitsgründen ist es immer gut, Datenbanken in einem privaten Subnetz zu platzieren. Abfragen an der Datenbank können ausgeführt werden, indem eine Verbindung über einen Amazon Elastic Compute Cloud (Amazon EC2) -Bastion-Host in einem öffentlichen Subnetz in der Amazon Web Services (AWS) Cloud hergestellt wird. Dies erfordert die Installation von Software wie pgAdmin oder DBeaver, die häufig von Entwicklern oder Datenbankadministratoren verwendet werden, auf dem EC2 Amazon-Host.

Um pgAdmin auf einem Linux-Server auszuführen und über einen Webbrowser darauf zuzugreifen, müssen zusätzliche Abhängigkeiten installiert, Berechtigungen eingerichtet und konfiguriert werden.

Als alternative Lösung können Entwickler oder Datenbankadministratoren eine Verbindung zu einer PostgreSQL-Datenbank herstellen, indem sie pgAdmin verwenden, um einen SSH-Tunnel von ihrem lokalen System aus zu aktivieren. Bei diesem Ansatz verwendet pgAdmin den EC2 Amazon-Host im öffentlichen Subnetz als Zwischenhost, bevor eine Verbindung zur Datenbank hergestellt wird. Das Diagramm im Abschnitt Architektur zeigt das Setup.

> **Note**
>
> Stellen Sie sicher, dass die an die PostgreSQL-Datenbank angehängte Sicherheitsgruppe eine Verbindung über Port 5432 vom Amazon-Host aus zulässt. EC2

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein bestehendes AWS-Konto
- Eine virtuelle private Cloud (VPC) mit einem öffentlichen Subnetz und einem privaten Subnetz
- Eine EC2 Instanz mit einer angehängten Sicherheitsgruppe
- Eine Amazon Aurora PostgreSQL-kompatible Edition-Datenbank mit einer angehängten Sicherheitsgruppe
- Ein Secure Shell (SSH) -Schlüsselpaar für die Einrichtung des Tunnels

Produktversionen

- pgAdmin versie 6.2+
- Amazon Aurora PostgreSQL-kompatible Edition Version 12.7+

Architektur

Zieltechnologie-Stack

- Amazon EC2
- Amazon Aurora PostgreSQL-kompatibel

Zielarchitektur

Das folgende Diagramm zeigt die Verwendung von pgAdmin mit einem SSH-Tunnel, um über ein Internet-Gateway eine Verbindung zu der EC2 Instanz herzustellen, die eine Verbindung zur Datenbank herstellt.

Tools

AWS-Services

- Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.

Andere Dienste

- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL. Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, verwalten und verwenden können.

Epen

Stellen Sie die Verbindung her

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Server.	Wählen Sie in pgAdmin Create und dann Server aus. Zusätzliche Hilfe zur Einrichtung von pgAdmin für die Registrierung eines Servers, die Konfiguration einer Verbindung und die Verbindung über SSH-Tunne ling mithilfe des Server-Di alogs finden Sie unter den Links im Abschnitt Verwandte Ressourcen.	DBA
Geben Sie einen Namen für den Server ein.	Geben Sie auf der Registerk arte Allgemein einen Namen ein.	DBA
Geben Sie die Datenbank details ein.	Geben Sie auf der Registerk arte Verbindung Werte für Folgendes ein: • Hostname/Adresse • Port • Wartungsdatenbank • Username • Passwort	DBA
Geben Sie die EC2 Amazon-Serverdetails ein.	Geben Sie auf der Registerk arte SSH-Tunnel die Details der EC2 Amazon-Instance	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ein, die sich im öffentlichen Subnetz befindet. • Setzen Sie SSH-Tunneling verwenden auf Ja, um anzugeben, dass pgAdmin bei der Verbindung mit dem angegebenen Server einen SSH-Tunnel verwenden soll. • Geben Sie im Feld Tunnelhost den Namen oder die IP-Adresse des SSH-Hosts an (z. B. 10.x.x.x). • Geben Sie im Feld Tunnel-Port den Port des SSH-Hosts an (z. B. 22). • Geben Sie im Feld Benutzername den Namen eines Benutzers mit Anmeldeberechtigungen für den SSH-Host an (z. B. ec2-user). • Geben Sie den Authentifizierungstyp als Identitätsdatei an, damit pgAdmin bei der Verbindung eine private Schlüsseldatei verwendet. • Geben Sie den Speicherort der Privacy Enhanced Mail (PEM) -Datei in das Feld Identitätsdatei ein. Die.pem-Datei ist das	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	EC2 Amazon-Schlüsselpaar.	
Speichern und verbinden.	Wählen Sie Speichern, um die Einrichtung abzuschließen und mithilfe des SSH-Tunnels eine Verbindung zur Aurora PostgreSQL-kompatiblen Datenbank herzustellen.	DBA

Zugehörige Ressourcen

- Dialogfeld „Server“
- Connect zum Server herstellen

JSON-Oracle-Abfragen in PostgreSQL-Datenbank-SQL konvertieren

Erstellt von Pinesh Singal (AWS) und Lokesh Gurram (AWS)

Übersicht

Dieser Migrationsprozess für den Umstieg von der lokalen Infrastruktur zur Amazon Web Services (AWS) -Cloud verwendet das AWS Schema Conversion Tool (AWS SCT), um den Code aus einer Oracle-Datenbank in eine PostgreSQL-Datenbank zu konvertieren. Der größte Teil des Codes wird automatisch von AWS SCT konvertiert. JSON-bezogene Oracle-Abfragen werden jedoch nicht automatisch konvertiert.

Ab der Version Oracle 12.2 unterstützt Oracle Database verschiedene JSON-Funktionen, die bei der Konvertierung von JSON-basierten Daten in zeilenbasierte Daten helfen. AWS SCT konvertiert JSON-basierte Daten jedoch nicht automatisch in eine Sprache, die von PostgreSQL unterstützt wird.

Dieses Migrationsmuster konzentriert sich hauptsächlich auf die manuelle Konvertierung der JSON-bezogenen Oracle-Abfragen mit Funktionen wie `JSON_OBJECT`, `JSON_ARRAYAGG`, und `JSON_TABLE` von einer Oracle-Datenbank in eine PostgreSQL-Datenbank.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine lokale Oracle-Datenbankinstanz (läuft)
- Eine Amazon Relational Database Service (Amazon RDS) für PostgreSQL oder Amazon Aurora PostgreSQL-kompatible Edition-Datenbank-Instance (betriebsbereit)

Einschränkungen

- JSON-bezogene Abfragen erfordern ein festes UND-Format. `KEY VALUE` Wenn dieses Format nicht verwendet wird, wird das falsche Ergebnis zurückgegeben.
- Wenn durch eine Änderung der JSON-Struktur neue `KEY` und `VALUE` Paare im Ergebnisabschnitt hinzugefügt werden, muss die entsprechende Prozedur oder Funktion in der SQL-Abfrage geändert werden.
- Einige JSON-bezogene Funktionen werden in früheren Versionen von Oracle und PostgreSQL unterstützt, verfügen jedoch über weniger Funktionen.

Produktversionen

- Oracle Database Version 12.2 und höher
- Amazon RDS for PostgreSQL oder Aurora PostgreSQL-kompatible Version 9.5 und höher
- Aktuelle Version von AWS SCT (getestet mit Version 1.0.664)

Architektur

Quelltechnologie-Stack

- Eine Oracle-Datenbankinstanz mit Version 19c

Zieltechnologie-Stack

- Eine Amazon RDS for PostgreSQL- oder Aurora PostgreSQL-kompatible Datenbank-Instance mit Version 13

Zielarchitektur

1. Verwenden Sie AWS SCT mit dem JSON-Funktionscode, um den Quellcode von Oracle nach PostgreSQL zu konvertieren.
2. Die Konvertierung erzeugt PostgreSQL-unterstützte migrierte .sql-Dateien.
3. Konvertieren Sie die nicht konvertierten Oracle-JSON-Funktionscodes manuell in PostgreSQL-JSON-Funktionscodes.
4. Führen Sie die .sql-Dateien auf der Aurora PostgreSQL-kompatiblen Ziel-DB-Instance aus.

Tools

AWS-Services

- Amazon Aurora ist eine vollständig verwaltete relationale Datenbank-Engine, die für die Cloud entwickelt wurde und mit MySQL und PostgreSQL kompatibel ist.
- Amazon Relational Database Service (Amazon RDS) für PostgreSQL unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen PostgreSQL-Datenbank in der AWS-Cloud.

- Das AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist.

Andere Dienste

- Oracle SQL Developer ist eine integrierte Entwicklungsumgebung, die die Entwicklung und Verwaltung von Oracle-Datenbanken sowohl in herkömmlichen als auch in Cloud-basierten Bereitstellungen vereinfacht.
- pgAdmin oder DBeaver. pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL. Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, verwalten und verwenden können. DBeaverist ein universelles Datenbanktool.

Bewährte Methoden

Die Oracle-Abfrage verwendet `CAST` standardmäßig den Typ, wenn die `JSON_TABLE` Funktion verwendet wird. Eine bewährte Methode ist die Verwendung auch `CAST` in PostgreSQL, wobei das Doppelte größer als Zeichen () verwendet wird. >>

Weitere Informationen finden Sie unter Postgres_SQL_Read_JSON im Abschnitt Zusätzliche Informationen.

Epen

Generieren Sie die JSON-Daten in den Oracle- und PostgreSQL-Datenbanken

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Speichern Sie die JSON-Daten in der Oracle-Datenbank.	Erstellen Sie eine Tabelle in der Oracle-Datenbank und speichern Sie die JSON-Daten in der `CLOB` Spalte. Verwenden Sie das Oracle_Table_Creation_Insert_Script, das sich im Abschnitt Zusätzliche Informationen befindet.	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Speichern Sie die JSON-Daten in der PostgreSQL-Datenbank.	Erstellen Sie eine Tabelle in der PostgreSQL-Datenbank und speichern Sie die JSON-Daten in der `TEXT` Spalte. Verwenden Sie das Postgres_Table_Creation_Insert_Script, das sich im Abschnitt Zusätzliche Informationen befindet.	Migrationsingenieur

Konvertiert das JSON in das ROW-Format

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konvertieren Sie die JSON-Daten in der Oracle-Datenbank.	Schreiben Sie eine Oracle SQL-Abfrage, um die JSON-Daten in das ROW-Format zu lesen. Weitere Informationen und eine Beispielsyntax finden Sie unter Oracle_SQL_Read_JSON im Abschnitt Zusätzliche Informationen.	Migrationsingenieur
Konvertiert die JSON-Daten in der PostgreSQL-Datenbank.	Schreiben Sie eine PostgreSQL-Abfrage, um die JSON-Daten in das ROW-Format zu lesen. Weitere Informationen und eine Beispielsyntax finden Sie unter Postgres_SQL_Read_JSON im Abschnitt Zusätzliche Informationen.	Migrationsingenieur

Konvertieren Sie die JSON-Daten manuell mithilfe der SQL-Abfrage und melden Sie die Ausgabe im JSON-Format

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie Aggregationen und Validierungen für die Oracle SQL-Abfrage durch.	Um die JSON-Daten manuell zu konvertieren, führen Sie eine Verknüpfung, Aggregation und Validierung der Oracle SQL-Abfrage durch und melden Sie die Ausgabe im JSON-Format. Verwenden Sie den Code unter Oracle_SQL_JSON_Aggregation_Join im Abschnitt Zusätzliche Informationen. 1. JOIN — Die Daten im JSON-Format werden als Eingabeparameter an die Abfrage übergeben. Zwischen diesen statischen Daten und den JSON-Daten in der Oracle-DB-Tabelle wird ein innerer JOIN erstellt. `aws_test_table` 2. Aggregation mit Validierung — Die JSON-Daten haben `VALUE` Parameter mit Werten wie`accountNumber` , `businessUnitId` und `parentAccountNumber` `positionId` , die für `SUM` `COUNT` Aggregationen verwendet werden. `KEY`	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. JSON-Format — Nach dem Join und der Aggregation werden die Daten mithilfe von und im JSON-Format gemeldet. `JSON_OBJECT` `JSON_ARRAYAGG`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie Aggregationen und Validierungen für die Postgres-SQL-Abfrage durch.	Um die JSON-Daten manuell zu konvertieren, führen Sie eine Verknüpfung, Aggregation und Validierung der PostgreSQL-Abfrage durch und melden Sie die Ausgabe im JSON-Format. Verwenden Sie den Code unter Postgres_SQL_JSON_Aggregation_Join im Abschnitt Zusätzliche Informationen. 1. JOIN — Die Daten im JSON-Format () werden als Eingabeparameter an die Klauselabfrage übergeben . `tab1` `WITH` Zwischen diesen statischen Daten und den JSON-Daten, die sich in der Tabelle befinden, wird ein JOIN erstellt. `tab` Ein JOIN wird auch mit der `WITH` Klausel erstellt, die JSON-Daten in der `aws_test_pg_table` Tabelle enthält. 2. Aggregation — Die JSON-Daten haben `VALUE` Parameter mit Werten wie`accountNumber` ,`parentAccountNumber` , und `businessUnitId` `positionId` , die	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	für die `COUNT` Aggregati onen `SUM` und verwendet werden. `KEY` 3. JSON-Format — Nach dem Zusammenführen und der Aggregation werden die Daten mithilfe von und im JSON-Format gemeldet. `JSON_BUILD_OBJECT` `JSON_AGG`	

Konvertieren Sie die Oracle-Prozedur in eine PostgreSQL-Funktion, die JSON-Abfragen enthält

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konvertieren Sie die JSON-Abfragen in der Oracle-Pr ozedur in Zeilen.	Verwenden Sie für die Oracle-Beispielprozedur die vorherige Oracle-Abfrage und den Code unter Oracle_Procedure_w ith_JSON_Query im Abschnitt Zusätzliche Informationen.	Ingenieur für Migration
Konvertieren Sie die PostgreSQL-Funktionen mit JSON-Abfragen in zeilenbas ierte Daten.	Verwenden Sie für die PostgreSQL-Beispielfunktion en die vorherige PostgreSQ L-Abfrage und den Code, der sich unter Postgres_ Function_with_JSON_Query im Abschnitt Zusätzliche Informationen befindet.	Migrationsingenieur

Zugehörige Ressourcen

- Oracle JSON-Funktionen

- PostgreSQL JSON-Funktionen
- Beispiele für Oracle JSON-Funktionen
- Beispiele für PostgreSQL JSON-Funktionen
- AWS-Schemakonvertierungstool

Zusätzliche Informationen

Verwenden Sie die folgenden Skripten der Reihe nach, um JSON-Code von der Oracle-Datenbank in die PostgreSQL-Datenbank zu konvertieren.

1. Oracle_Table_Creation_Insert_Script

```
create table aws_test_table(id number,created_on date default sysdate,modified_on
 date,json_doc clob);

REM INSERTING into EXPORT_TABLE
SET DEFINE OFF;
Insert into aws_test_table (ID,CREATED_ON,MODIFIED_ON,json_doc)
values (1,to_date('02-AUG-2022 12:30:14','DD-MON-YYYY HH24:MI:SS'),to_date('02-AUG-2022
 12:30:14','DD-MON-YYYY HH24:MI:SS'),TO_CLOB(q'[{
  "metadata" : {
    "upperLastNameFirstName" : "ABC XYZ",
    "upperEmailAddress" : "abc@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "032323323",
    "displayName" : "Abc, Xyz",
    "firstName" : "Xyz",
    "lastName" : "Abc",
    "emailAddress" : "abc@gmail.com",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0100",
    "arrayPattern" : " -'",
    "a]')
|| TO_CLOB(q'[ccount" : {
      "companyId" : "SMGE",
      "businessUnitId" : 7,
      "accountNumber" : 42000,
      "parentAccountNumber" : 32000,
      "firstName" : "john",
```

```
      "lastName" : "doe",
      "street1" : "retOdertcaShr ",
      "city" : "new york",
      "postalcode" : "XY ABC",
      "country" : "United States"
    },
    "products" : [
      {
        "appUserGuid" : "i0acc4450000001823fbad478e2eab8a0",
        "id" : "0000000046",
]')
|| TO_CLOB(q'[        "name" : "ProView",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}]'));
Insert into aws_test_table (ID,CREATED_ON,MODIFIED_ON,json_doc) values (2,to_date('02-
AUG-2022 12:30:14','DD-MON-YYYY HH24:MI:SS'),to_date('02-AUG-2022 12:30:14','DD-MON-
YYYY HH24:MI:SS'),TO_CLOB(q'[{
  "metadata" : {
    "upperLastNameFirstName" : "PQR XYZ",
    "upperEmailAddress" : "pqr@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "54534343",
    "displayName" : "Xyz, pqr",
    "firstName" : "pqr",
    "lastName" : "Xyz",
    "emailAddress" : "pqr@gmail.com",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0090",
    "arrayPattern" : " -'",
    "account" : {
      "companyId" : "CARS",
      "busin]')
|| TO_CLOB(q'[essUnitId" : 6,
      "accountNumber" : 42001,
      "parentAccountNumber" : 32001,
      "firstName" : "terry",
      "lastName" : "whitlock",
```

```
      "street1" : "UO  123",
      "city" : "TOTORON",
      "region" : "NO",
      "postalcode" : "LKM 111",
      "country" : "Canada"
    },
    "products" : [
      {
        "appUserGuid" : "ia744d7790000016899f8cf3f417d6df6",
        "id" : "0000000014",
        "name" : "ProView eLooseleaf",
      ]')
|| TO_CLOB(q'[  "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}]'));

commit;
```

2. Postgres_Table_Creation_Insert_Script

```
create table aws_test_pg_table(id int,created_on date ,modified_on date,json_doc text);
insert into aws_test_pg_table(id,created_on,modified_on,json_doc)
values(1,now(),now(),'{
  "metadata" : {
    "upperLastNameFirstName" : "ABC XYZ",
    "upperEmailAddress" : "abc@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "032323323",
    "displayName" : "Abc, Xyz",
    "firstName" : "Xyz",
    "lastName" : "Abc",
    "emailAddress" : "abc@gmail.com",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0100",
    "arrayPattern" : " -",
    "account" : {
      "companyId" : "SMGE",
```

```
      "businessUnitId" : 7,
      "accountNumber" : 42000,
      "parentAccountNumber" : 32000,
      "firstName" : "john",
      "lastName" : "doe",
      "street1" : "retOdertcaShr ",
      "city" : "new york",
      "postalcode" : "XY ABC",
      "country" : "United States"
    },
    "products" : [
      {
        "appUserGuid" : "i0acc4450000001823fbad478e2eab8a0",
        "id" : "0000000046",
        "name" : "ProView",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}');


insert into aws_test_pg_table(id,created_on,modified_on,json_doc)
values(2,now(),now(),'{
  "metadata" : {
    "upperLastNameFirstName" : "PQR XYZ",
    "upperEmailAddress" : "pqr@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "54534343",
    "displayName" : "Xyz, pqr",
    "firstName" : "pqr",
    "lastName" : "Xyz",
    "emailAddress" : "a*b**@h**.k**",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0090",
    "arrayPattern" : " -",
    "account" : {
      "companyId" : "CARS",
      "businessUnitId" : 6,
      "accountNumber" : 42001,
```

```
      "parentAccountNumber" : 32001,
      "firstName" : "terry",
      "lastName" : "whitlock",
      "street1" : "UO  123",
      "city" : "TOTORON",
      "region" : "NO",
      "postalcode" : "LKM 111",
      "country" : "Canada"
    },
    "products" : [
      {
        "appUserGuid" : "ia744d7790000016899f8cf3f417d6df6",
        "id" : "0000000014",
        "name" : "ProView eLooseleaf",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}');
```

3. Oracle_SQL_Read_JSON

Die folgenden Codeblöcke zeigen, wie Oracle JSON-Daten in das Zeilenformat konvertiert werden.

Beispielabfrage und Syntax

```
SELECT   JSON_OBJECT(
 'accountCounts' VALUE JSON_ARRAYAGG(
           JSON_OBJECT(
               'businessUnitId' VALUE business_unit_id,
                       'parentAccountNumber' VALUE parent_account_number,
                       'accountNumber' VALUE account_number,
                       'totalOnlineContactsCount' VALUE online_contacts_count,
                       'countByPosition' VALUE
                   JSON_OBJECT(
                       'taxProfessionalCount' VALUE tax_count,
                       'attorneyCount' VALUE attorney_count,
                       'nonAttorneyCount' VALUE non_attorney_count,
                       'clerkCount' VALUE clerk_count
                              ) ) ) ) FROM
    (SELECT   tab_data.business_unit_id,
           tab_data.parent_account_number,
```

```
           tab_data.account_number,
           SUM(1) online_contacts_count,
           SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE 0 END) tax_count,
           SUM(CASE    WHEN tab_data.position_id = '0100' THEN 1 ELSE 0 END)
attorney_count,
           SUM(CASE    WHEN tab_data.position_id = '0090' THEN 1 ELSE 0 END)
non_attorney_count,
           SUM(CASE    WHEN tab_data.position_id = '0050' THEN 1 ELSE 0 END)
clerk_count
       FROM aws_test_table scco,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
 COLUMNS (
         parent_account_number NUMBER PATH
          '$.data.account.parentAccountNumber',
           account_number NUMBER PATH '$.data.account.accountNumber',
           business_unit_id NUMBER PATH '$.data.account.businessUnitId',
           position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
           ) AS tab_data
           INNER JOIN JSON_TABLE ( '{
       "accounts": [{
         "accountNumber": 42000,
         "parentAccountNumber": 32000,
         "businessUnitId": 7
       }, {
         "accountNumber": 42001,
         "parentAccountNumber": 32001,
         "businessUnitId": 6
       }]
     }', '$.accounts[*]' ERROR ON ERROR
     COLUMNS (
     parent_account_number PATH '$.parentAccountNumber',
     account_number PATH '$.accountNumber',
     business_unit_id PATH '$.businessUnitId')
     ) static_data
     ON ( static_data.parent_account_number = tab_data.parent_account_number
          AND static_data.account_number = tab_data.account_number
          AND static_data.business_unit_id = tab_data.business_unit_id )
       GROUP BY
           tab_data.business_unit_id,
           tab_data.parent_account_number,
           tab_data.account_number );
```

Das JSON-Dokument speichert die Daten als Sammlungen. Jede Sammlung kann aus KEY und aus VALUE Paaren bestehen. Jeder VALUE kann Verschachtelungen KEY und VALUE Paare haben. Die

folgende Tabelle enthält Informationen zum Lesen der spezifischen Daten VALUE aus dem JSON-Dokument.

SCHLÜSSEL	HIERARCHIE oder PFAD, der verwendet werden soll, um den WERT zu ermitteln	WERT
profileType	metadata -> profileType	„P“
positionId	data -> positionId	„0100"
accountNumber	data-> Konto -> accountNumber	42000

In der vorherigen Tabelle KEY profileType ist der ein VALUE von. metadata KEY Das KEY positionId ist ein VALUE von dataKEY. Das KEY accountNumber ist ein VALUE von der accountKEY, und das account KEY ist ein VALUE von der dataKEY.

Beispiel für ein JSON-Dokument

```
{
  "metadata" : {
    "upperLastNameFirstName" : "ABC XYZ",
    "upperEmailAddress" : "abc@gmail.com",
"profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "032323323",
    "displayName" : "Abc, Xyz",
    "firstName" : "Xyz",
    "lastName" : "Abc",
    "emailAddress" : "abc@gmail.com",
    "productRegistrationStatus" : "Not registered",
"positionId" : "0100",
    "arrayPattern" : " -",
    "account" : {
      "companyId" : "SMGE",
      "businessUnitId" : 7,
"accountNumber" : 42000,
      "parentAccountNumber" : 32000,
      "firstName" : "john",
```

```
      "lastName" : "doe",
      "street1" : "retOdertcaShr ",
      "city" : "new york",
      "postalcode" : "XY ABC",
      "country" : "United States"
    },
    "products" : [
      {
        "appUserGuid" : "i0acc4450000001823fbad478e2eab8a0",
        "id" : "0000000046",
        "name" : "ProView",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}
```

SQL-Abfrage, die verwendet wird, um die ausgewählten Felder aus dem JSON-Dokument abzurufen

```
select parent_account_number,account_number,business_unit_id,position_id from
 aws_test_table aws,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
COLUMNS (
parent_account_number NUMBER PATH '$.data.account.parentAccountNumber',
account_number NUMBER PATH '$.data.account.accountNumber',
business_unit_id NUMBER PATH '$.data.account.businessUnitId',
position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'
)) as sc
```

In der vorherigen Abfrage `JSON_TABLE` ist eine in Oracle integrierte Funktion enthalten, die die JSON-Daten in das Zeilenformat konvertiert. Die Funktion JSON_TABLE erwartet Parameter im JSON-Format.

Jedes Element in `COLUMNS` hat ein vordefiniertes`PATH`, und dort wird ein `VALUE` für ein bestimmtes Element geeignetes Objekt im `KEY` Zeilenformat zurückgegeben.

Ergebnis der vorherigen Abfrage

PARENT_ACCOUNT_NUMBER	KONTONUMMER	ID DER GESCHÄFTSEINHEIT	POSITIONS-ID

32000	42000	7	0 100
32001	42001	6	0090

4 Postgres_SQL_Read_JSON

Beispielabfrage und Syntax

```
select *
from (
select (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER as
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER as accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER as businessUnitId,
(json_doc::json->'data'->>'positionId')::VARCHAR as positionId
from aws_test_pg_table) d ;
```

PATHWird in Oracle verwendet, um das spezifische KEY und zu identifizierenVALUE. PostgreSQL verwendet jedoch ein HIERARCHY Modell zum Lesen KEY und VALUE aus JSON. In den folgenden Beispielen werden dieselben JSON-Daten Oracle_SQL_Read_JSON verwendet, die unten erwähnt werden.

SQL-Abfrage mit dem Typ CAST ist nicht zulässig

(Wenn Sie die Eingabe erzwingenCAST, schlägt die Abfrage mit einem Syntaxfehler fehl.)

```
select *
from (
select (json_doc::json->'data'->'account'->'parentAccountNumber') as
 parentAccountNumber,
(json_doc::json->'data'->'account'->'accountNumber')as accountNumber,
(json_doc::json->'data'->'account'->'businessUnitId') as businessUnitId,
(json_doc::json->'data'->'positionId')as positionId
from aws_test_pg_table) d ;
```

Wenn Sie einen einzigen Operator für größer als (>) verwenden, wird der dafür VALUE definierte Wert zurückgegeben. KEY Zum BeispielKEY:positionId, undVALUE:. "0100"

Typ CAST ist nicht zulässig, wenn Sie den einzelnen Operator „Größer als“ () > verwenden.

SQL-Abfrage mit dem Typ CAST ist zulässig

```
select *
from (
select (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER as
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER as accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER as businessUnitId,
(json_doc::json->'data'->>'positionId')::varchar as positionId
from aws_test_pg_table) d ;
```

Um den Typ zu verwendenCAST, müssen Sie den Operator Double Greater-than verwenden. Wenn Sie den Operator „Größer als“ verwenden, gibt die Abfrage den VALUE definierten Operator zurück (z. B.KEY:positionId, und:). VALUE "0100" Wenn Sie den Operator für ein doppeltes Größer-als-Zeichen (>>) verwenden, wird der tatsächlich dafür definierte Wert zurückgegeben KEY (z. B.KEY:, undVALUE: positionId0100, ohne doppelte Anführungszeichen).

Im vorherigen Fall ist Typ zu, parentAccountNumber ist Typ CAST zuINT, accountNumber ist Typ CAST zuINT, businessUnitId ist Typ CAST zu INT und positionId ist Typ CAST zu. VARCHAR

Die folgenden Tabellen zeigen Abfrageergebnisse, in denen die Rolle des Operators für einen einzelnen Größer-als-Operator (>) und des doppelten Größer-als-Operators () erklärt wird. >>

In der ersten Tabelle verwendet die Abfrage den einzigen Operator „Größer als“ (). > Jede Spalte ist vom Typ JSON und kann nicht in einen anderen Datentyp konvertiert werden.

parentAccountNumber	Kontonummer	businessUnitId	Positions-ID
2003565430	2003564830	7	„0100“
2005284042	2005284042	6	„0090“
2000272719	2000272719	1	„0100“

In der zweiten Tabelle verwendet die Abfrage den doppelten Größer-als-Operator (). >> Jede Spalte unterstützt den Typ, der auf dem Spaltenwert CAST basiert. Zum Beispiel INTEGER in diesem Kontext.

parentAccountNumber	Kontonummer	businessUnitId	Positions-ID
2003565430	2003564830	7	0 100
2005284042	2005284042	6	0090
2000272719	2000272719	1	0 100

5. Oracle_SQL_JSON_Aggregation_Join

Beispiel für eine Abfrage

```
SELECT
    JSON_OBJECT(
        'accountCounts' VALUE JSON_ARRAYAGG(
            JSON_OBJECT(
                'businessUnitId' VALUE business_unit_id,
                        'parentAccountNumber' VALUE parent_account_number,
                        'accountNumber' VALUE account_number,
                        'totalOnlineContactsCount' VALUE online_contacts_count,
                        'countByPosition' VALUE
                    JSON_OBJECT(
                        'taxProfessionalCount' VALUE tax_count,
                        'attorneyCount' VALUE attorney_count,
                        'nonAttorneyCount' VALUE non_attorney_count,
                        'clerkCount' VALUE clerk_count
                               ) ) ) )
FROM
    (SELECT
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number,
            SUM(1) online_contacts_count,
            SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE 0 END) tax_count,
            SUM(CASE    WHEN tab_data.position_id = '0100' THEN 1 ELSE 0 END)
 attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0090' THEN 1 ELSE 0 END)
 non_attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0050' THEN 1 ELSE 0 END)
 clerk_count
```

```
       FROM aws_test_table scco,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
  COLUMNS (
          parent_account_number NUMBER PATH
           '$.data.account.parentAccountNumber',
            account_number NUMBER PATH '$.data.account.accountNumber',
            business_unit_id NUMBER PATH '$.data.account.businessUnitId',
            position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
            ) AS tab_data
            INNER JOIN JSON_TABLE ( '{
        "accounts": [{
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }, {
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }]
      }', '$.accounts[*]' ERROR ON ERROR
      COLUMNS (
      parent_account_number PATH '$.parentAccountNumber',
      account_number PATH '$.accountNumber',
      business_unit_id PATH '$.businessUnitId')
      ) static_data
      ON ( static_data.parent_account_number = tab_data.parent_account_number
           AND static_data.account_number = tab_data.account_number
           AND static_data.business_unit_id = tab_data.business_unit_id )
        GROUP BY
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number
    );
```

Um die Daten auf Zeilenebene in das JSON-Format zu konvertieren, verfügt Oracle über integrierte Funktionen wie`JSON_OBJECT`, `JSON_ARRAY``JSON_OBJECTAGG`, und. `JSON_ARRAYAGG`

- `JSON_OBJECT`akzeptiert zwei Parameter: `KEY` und. `VALUE` Der `KEY` Parameter sollte fest codiert oder statisch sein. Der `VALUE` Parameter wird aus der Tabellenausgabe abgeleitet.
- `JSON_ARRAYAGG`akzeptiert `JSON_OBJECT` als Parameter. Dies hilft bei der Gruppierung des Satzes von `JSON_OBJECT` Elementen als Liste. Wenn Sie beispielsweise ein `JSON_OBJECT` Element haben, das mehrere Datensätze hat (mehrere `KEY` und `VALUE` Paare im Datensatz), `JSON_ARRAYAGG` fügen Sie den Datensatz an und erstellen eine Liste. Gemäß der

Datenstruktursprache `LIST` handelt es sich um eine Gruppe von Elementen. In diesem Zusammenhang `LIST` handelt es sich um eine Gruppe von `JSON_OBJECT` Elementen.

Das folgende Beispiel zeigt ein `JSON_OBJECT` Element.

```
{
   "taxProfessionalCount": 0,
   "attorneyCount": 0,
   "nonAttorneyCount": 1,
   "clerkCount": 0
}
```

Das nächste Beispiel zeigt zwei `JSON_OBJECT` Elemente, die durch eckige Klammern (`[ ]`) `LIST` gekennzeichnet sind.

```
[
    {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
,
    {
        "taxProfessionalCount": 2,
        "attorneyCount": 1,
        "nonAttorneyCount": 3,
        "clerkCount":4
      }
]
```

Beispiel für eine SQL-Abfrage

```
SELECT
    JSON_OBJECT(
        'accountCounts' VALUE JSON_ARRAYAGG(
            JSON_OBJECT(
                'businessUnitId' VALUE business_unit_id,
                        'parentAccountNumber' VALUE parent_account_number,
                        'accountNumber' VALUE account_number,
                        'totalOnlineContactsCount' VALUE online_contacts_count,
```

```
                        'countByPosition' VALUE
                    JSON_OBJECT(
                        'taxProfessionalCount' VALUE tax_count,
                        'attorneyCount' VALUE attorney_count,
                        'nonAttorneyCount' VALUE non_attorney_count,
                        'clerkCount' VALUE clerk_count
                               )
                        )
                                        )
              )
FROM
    (SELECT
             tab_data.business_unit_id,
             tab_data.parent_account_number,
             tab_data.account_number,
             SUM(1) online_contacts_count,
             SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE   0 END
             )      tax_count,
             SUM(CASE    WHEN tab_data.position_id = '0100' THEN        1    ELSE
  0 END
             )      attorney_count,

             SUM(CASE    WHEN tab_data.position_id = '0090' THEN        1    ELSE
  0 END
             )      non_attorney_count,

             SUM(CASE    WHEN tab_data.position_id = '0050' THEN        1    ELSE
  0 END
             )      clerk_count

         FROM
             aws_test_table scco,  JSON_TABLE ( json_doc, '$' ERROR ON ERROR
             COLUMNS (
             parent_account_number NUMBER PATH '$.data.account.parentAccountNumber',
             account_number NUMBER PATH '$.data.account.accountNumber',
             business_unit_id NUMBER PATH '$.data.account.businessUnitId',
             position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
             ) AS tab_data
             INNER JOIN JSON_TABLE ( '{
         "accounts": [{
           "accountNumber": 42000,
           "parentAccountNumber": 32000,
           "businessUnitId": 7
         }, {
```

```
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }]
      }', '$.accounts[*]' ERROR ON ERROR
      COLUMNS (
      parent_account_number PATH '$.parentAccountNumber',
      account_number PATH '$.accountNumber',
      business_unit_id PATH '$.businessUnitId')
      ) static_data ON ( static_data.parent_account_number =
 tab_data.parent_account_number
                         AND static_data.account_number = tab_data.account_number

                         AND static_data.business_unit_id =
 tab_data.business_unit_id )
        GROUP BY
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number
    );
```

Beispielausgabe der vorherigen SQL-Abfrage

```
{
  "accountCounts": [
    {
      "businessUnitId": 6,
      "parentAccountNumber": 32001,
      "accountNumber": 42001,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
    },
    {
      "businessUnitId": 7,
      "parentAccountNumber": 32000,
      "accountNumber": 42000,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
```

```
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

6. Postgres_SQL_JSON_Aggregation_Join

Die integrierten Funktionen JSON_BUILD_OBJECT von PostgreSQL JSON_AGG konvertieren die Daten auf Zeilenebene in das JSON-Format. PostgreSQL JSON_BUILD_OBJECT und JSON_AGG entsprechen Oracle JSON_OBJECT und. JSON_ARRAYAGG

Beispielabfrage

```
select
JSON_BUILD_OBJECT ('accountCounts',
    JSON_AGG(
        JSON_BUILD_OBJECT ('businessUnitId',businessUnitId
        ,'parentAccountNumber',parentAccountNumber
        ,'accountNumber',accountNumber
        ,'totalOnlineContactsCount',online_contacts_count,
        'countByPosition',
            JSON_BUILD_OBJECT (
            'taxProfessionalCount',tax_professional_count
            ,'attorneyCount',attorney_count
            ,'nonAttorneyCount',non_attorney_count
            ,'clerkCount',clerk_count
            )
        )
    )
)
from (
with tab as (select * from (
select (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER as
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER as accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER as businessUnitId,
(json_doc::json->'data'->>'positionId')::varchar as positionId
from aws_test_pg_table) a ) ,
tab1 as ( select
```

```
(json_array_elements(b.jc -> 'accounts') ->> 'accountNumber')::integer accountNumber,
(json_array_elements(b.jc -> 'accounts') ->> 'businessUnitId')::integer
 businessUnitId,
(json_array_elements(b.jc -> 'accounts') ->> 'parentAccountNumber')::integer
 parentAccountNumber
from (
select '{
        "accounts": [{
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }, {
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }]
      }'::json as jc) b)
select
tab.businessUnitId::text,
tab.parentAccountNumber::text,
tab.accountNumber::text,
SUM(1) online_contacts_count,
SUM(CASE WHEN tab.positionId::text = '0095' THEN 1 ELSE 0  END)
  tax_professional_count,
SUM(CASE WHEN tab.positionId::text = '0100' THEN 1 ELSE 0  END)      attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0090' THEN      1  ELSE      0 END)
  non_attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0050' THEN      1  ELSE      0 END)
  clerk_count
from tab1,tab
where tab.parentAccountNumber::INTEGER=tab1.parentAccountNumber::INTEGER
and tab.accountNumber::INTEGER=tab1.accountNumber::INTEGER
and tab.businessUnitId::INTEGER=tab1.businessUnitId::INTEGER
GROUP BY      tab.businessUnitId::text,
            tab.parentAccountNumber::text,
            tab.accountNumber::text) a;
```

Beispielausgabe aus der vorherigen Abfrage

Die Ausgabe von Oracle und PostgreSQL ist exakt identisch.

```
{
  "accountCounts": [
    {
```

```
      "businessUnitId": 6,
      "parentAccountNumber": 32001,
      "accountNumber": 42001,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
    },
    {
      "businessUnitId": 7,
      "parentAccountNumber": 32000,
      "accountNumber": 42000,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

7. Oracle_Procedure_with_JSON_Query

Dieser Code konvertiert die Oracle-Prozedur in eine PostgreSQL-Funktion mit JSON-SQL-Abfragen. Es zeigt, wie die Abfrage JSON in Zeilen und umgekehrt transponiert.

```
CREATE OR REPLACE PROCEDURE p_json_test(p_in_accounts_json IN varchar2,
 p_out_accunts_json  OUT varchar2)
IS
BEGIN
/*
p_in_accounts_json paramter should have following format:
       {
        "accounts": [{
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }, {
```

```
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }]
      }
*/
SELECT
    JSON_OBJECT(
        'accountCounts' VALUE JSON_ARRAYAGG(
            JSON_OBJECT(
                'businessUnitId' VALUE business_unit_id,
                        'parentAccountNumber' VALUE parent_account_number,
                        'accountNumber' VALUE account_number,
                        'totalOnlineContactsCount' VALUE online_contacts_count,
                        'countByPosition' VALUE
                    JSON_OBJECT(
                        'taxProfessionalCount' VALUE tax_count,
                        'attorneyCount' VALUE attorney_count,
                        'nonAttorneyCount' VALUE non_attorney_count,
                        'clerkCount' VALUE clerk_count
                               ) ) ) )
into p_out_accunts_json
FROM
    (SELECT
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number,
            SUM(1) online_contacts_count,
            SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE 0 END) tax_count,
            SUM(CASE    WHEN tab_data.position_id = '0100' THEN 1 ELSE 0 END)
 attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0090' THEN 1 ELSE 0 END)
 non_attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0050' THEN 1 ELSE 0 END)
 clerk_count
       FROM aws_test_table scco,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
            COLUMNS (
            parent_account_number NUMBER PATH '$.data.account.parentAccountNumber',
            account_number NUMBER PATH '$.data.account.accountNumber',
            business_unit_id NUMBER PATH '$.data.account.businessUnitId',
            position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
            ) AS tab_data
            INNER JOIN JSON_TABLE ( p_in_accounts_json, '$.accounts[*]' ERROR ON ERROR
```

```
      COLUMNS (
      parent_account_number PATH '$.parentAccountNumber',
      account_number PATH '$.accountNumber',
      business_unit_id PATH '$.businessUnitId')
      ) static_data
      ON ( static_data.parent_account_number = tab_data.parent_account_number
           AND static_data.account_number = tab_data.account_number
           AND static_data.business_unit_id = tab_data.business_unit_id )
        GROUP BY
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number
    );
EXCEPTION
WHEN OTHERS THEN
   raise_application_error(-20001,'Error while running the JSON query');
END;
/
```

Das Verfahren wird ausgeführt

Der folgende Codeblock erklärt, wie Sie die zuvor erstellte Oracle-Prozedur mit einer Beispiel-JSON-Eingabe für die Prozedur ausführen können. Außerdem erhalten Sie das Ergebnis oder die Ausgabe dieser Prozedur.

```
set serveroutput on;
declare
v_out varchar2(30000);
v_in varchar2(30000):= '{
        "accounts": [{
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }, {
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }]
      }';
begin
  p_json_test(v_in,v_out);
  dbms_output.put_line(v_out);
end;
```

```
/
```

Ausgabe der Prozedur

```
{
  "accountCounts": [
    {
      "businessUnitId": 6,
      "parentAccountNumber": 32001,
      "accountNumber": 42001,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
    },
    {
      "businessUnitId": 7,
      "parentAccountNumber": 32000,
      "accountNumber": 42000,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

8. Postgres_Function_with_JSON_Query

Beispielfunktion

```
CREATE OR REPLACE  FUNCTION f_pg_json_test(p_in_accounts_json  text)
RETURNS text
LANGUAGE plpgsql
AS
$$
DECLARE
```

```
 v_out_accunts_json   text;
BEGIN
SELECT
JSON_BUILD_OBJECT ('accountCounts',
    JSON_AGG(
        JSON_BUILD_OBJECT ('businessUnitId',businessUnitId
        ,'parentAccountNumber',parentAccountNumber
        ,'accountNumber',accountNumber
        ,'totalOnlineContactsCount',online_contacts_count,
        'countByPosition',
            JSON_BUILD_OBJECT (
            'taxProfessionalCount',tax_professional_count
            ,'attorneyCount',attorney_count
            ,'nonAttorneyCount',non_attorney_count
            ,'clerkCount',clerk_count
            ))))
INTO v_out_accunts_json
FROM (
WITH tab AS (SELECT * FROM (
SELECT (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER AS
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER AS accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER AS businessUnitId,
(json_doc::json->'data'->>'positionId')::varchar AS positionId
FROM aws_test_pg_table) a ) ,
tab1 AS ( SELECT
(json_array_elements(b.jc -> 'accounts') ->> 'accountNumber')::integer accountNumber,
(json_array_elements(b.jc -> 'accounts') ->> 'businessUnitId')::integer businessUnitId,
(json_array_elements(b.jc -> 'accounts') ->> 'parentAccountNumber')::integer
 parentAccountNumber
FROM (
SELECT p_in_accounts_json::json AS jc) b)
SELECT
tab.businessUnitId::text,
tab.parentAccountNumber::text,
tab.accountNumber::text,
SUM(1) online_contacts_count,
SUM(CASE WHEN tab.positionId::text = '0095' THEN 1 ELSE 0  END)
  tax_professional_count,
SUM(CASE WHEN tab.positionId::text = '0100' THEN 1 ELSE 0  END)      attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0090' THEN      1  ELSE      0 END)
  non_attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0050' THEN      1  ELSE      0 END)
  clerk_count
```

```
FROM tab1,tab
WHERE tab.parentAccountNumber::INTEGER=tab1.parentAccountNumber::INTEGER
AND tab.accountNumber::INTEGER=tab1.accountNumber::INTEGER
AND tab.businessUnitId::INTEGER=tab1.businessUnitId::INTEGER
GROUP BY      tab.businessUnitId::text,
            tab.parentAccountNumber::text,
            tab.accountNumber::text) a;
RETURN v_out_accunts_json;
END;
$$;
```

Die Funktion wird ausgeführt

```
select    f_pg_json_test('{
        "accounts": [{
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }, {
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }]
      }')   ;
```

Ausgabe der Funktion

Die folgende Ausgabe ähnelt der Ausgabe der Oracle-Prozedur. Der Unterschied besteht darin, dass diese Ausgabe im Textformat vorliegt.

```
{
  "accountCounts": [
    {
      "businessUnitId": "6",
      "parentAccountNumber": "32001",
      "accountNumber": "42001",
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
```

```
    },
    {
      "businessUnitId": "7",
      "parentAccountNumber": "32000",
      "accountNumber": "42000",
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

Kopieren Sie Amazon DynamoDB-Tabellen zwischen Konten mit AWS Backup

Erstellt von Ramkumar Ramanujam (AWS)

Übersicht

Wenn Sie mit Amazon DynamoDB arbeiten AWS, besteht ein häufiger Anwendungsfall darin, DynamoDB-Tabellen in Entwicklungs-, Test- oder Staging-Umgebungen mit den Tabellendaten in der Produktionsumgebung zu kopieren oder zu synchronisieren. Standardmäßig verwendet jede Umgebung eine andere. AWS-Konto

AWS Backup unterstützt regionsübergreifende und kontoübergreifende Sicherung und Wiederherstellung von Daten für DynamoDB, Amazon Simple Storage Service (Amazon S3) und andere. AWS-Services Dieses Muster enthält die Schritte für die Verwendung von AWS Backup kontenübergreifendem Sichern und Wiederherstellen, um DynamoDB-Tabellen zwischen diesen zu kopieren. AWS-Konten

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zwei aktive AWS-Konten , die derselben Organisation angehören in AWS Organizations
- Berechtigungen zum Erstellen von DynamoDB-Tabellen in beiden Konten
- AWS Identity and Access Management (IAM) -Berechtigungen zum Erstellen und Verwenden von Tresoren AWS Backup

Einschränkungen

- Quelle und Ziel AWS-Konten sollten Teil derselben Organisation in sein. AWS Organizations

Architektur

Zieltechnologie-Stack

- AWS Backup
- Amazon-DynamoDB

Zielarchitektur

1. Erstellen Sie die DynamoDB-Tabellensicherung im AWS Backup Backup-Tresor des Quellkontos.
2. Kopieren Sie das Backup in den Backup-Tresor im Zielkonto.
3. Stellen Sie die DynamoDB-Tabelle im Zielkonto wieder her, indem Sie die Sicherung aus dem Backup-Tresor im Zielkonto verwenden.

Automatisierung und Skalierung

Sie können Backups so AWS Backup planen, dass sie in bestimmten Intervallen ausgeführt werden.

Tools

- AWS Backupist ein vollständig verwalteter Service zur Zentralisierung und Automatisierung des Datenschutzes in der Cloud und vor Ort. AWS-Services Mit diesem Service können Sie Backup-Richtlinien konfigurieren und die Aktivitäten für Ihre AWS Ressourcen von einem zentralen Ort aus überwachen. Er ermöglicht Ihnen die Automatisierung und Konsolidierung von Backup-Aufgaben, die zuvor Service für Service ausgeführt wurden, und macht die Erstellung benutzerdefinierter Skripts und manueller Prozesse überflüssig.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der schnelle und vorhersehbare Leistung mit nahtloser Skalierbarkeit bietet.

Epen

Aktiviere AWS Backup Funktionen in den Quell- und Zielkonten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie erweiterte Funktionen für DynamoDB und kontoübergreifendes Backup.	Gehen Sie sowohl in der Quelle als auch im Ziel wie AWS-Konten folgt vor: 1. Öffnen Sie auf dem AWS Management Console die AWS Backup Konsole.	AWS DevOps, Migration singenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie Einstellungen aus. 3. Vergewissern Sie sich unter Erweiterte Funktionen für Amazon DynamoDB-Backups, dass Erweiterte Funktionen aktiviert sind, oder wählen Sie Aktivieren. 4. Wählen Sie unter Kontoübergreifende Verwaltung für kontoübergreifende Sicherung die Option Aktivieren aus.	

Erstellen Sie Backup-Tresore in den Quell- und Zielkonten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Backup-Tresore.	Gehen Sie sowohl in der Quelle als auch im Ziel AWS-Konten wie folgt vor: 1. Wählen Sie auf der AWS Backup Konsole Backup-Tresore aus. 2. Wählen Sie Create backup vault (Sicherungstresor erstellen) aus. 3. Kopieren Sie den Amazon-Ressourcennamen (ARN) des Backup-Tresors und speichern Sie ihn.	AWS DevOps, Migration singenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Der ARNs des Quell- und des Ziel-Backup-Tresors ist erforderlich, wenn Sie das DynamoDB-Tabellen-Backup zwischen dem Quell- und dem Zielkonto kopieren.	

Führen Sie Backups und Wiederherstellungen mithilfe von Backup-Tresoren durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie im Quellkonto eine DynamoDB-Tabellens icherung.	Gehen Sie wie folgt vor, um ein Backup für die DynamoDB-Tabelle im Quellkonto zu erstellen: 1. Wählen Sie auf der AWS Backup Dashboard-Seite die Option On-Demand-Backup erstellen aus. 2. Wählen Sie im Abschnitt Einstellungen für Ressourcentyp die Option DynamoDB und dann den Tabellennamen aus. 3. Wählen Sie in der Dropdownliste Backup-Tresor den Backup-Tresor aus, den Sie im Quellkonto erstellt haben. 4. Wählen Sie den gewünschten Aufbewahrungszeitraum aus.	AWS DevOps, DBA, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Wählen Sie On-Demand-Backup erstellen. Ein neuer Backup-Job wird erstellt. Um den Status des Backup-Jobs zu überwachen, wählen Sie auf der Seite AWS Backup Jobs die Registerkarte Backup-Jobs. Alle aktiven, laufenden und abgeschlossenen Backup-Jobs werden auf dieser Registerkarte aufgelistet.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopieren Sie das Backup vom Quellkonto auf das Zielkonto.	Nachdem der Backup-Job abgeschlossen ist, kopieren Sie die DynamoDB-Tabellensicherung aus dem Backup-Tresor im Quellkonto in den Backup-Tresor im Zielkonto. Gehen Sie wie folgt vor, um den Backup-Tresor im Quellkonto zu kopieren: 1. Wählen Sie auf der AWS Backup Konsole Backup-Tresore aus. 2. Wählen Sie unter Backups das DynamoDB-Tabellen-Backup aus. 3. Wählen Sie Aktionen, Kopieren. 4. Geben Sie das AWS-Region des Zielkontos ein. 5. Geben Sie unter External Vault ARN den ARN des Backup-Tresors ein, den Sie im Zielkonto erstellt haben. 6. Um Backups vom Quellkonto auf das Zielkonto zu kopieren, aktivieren Sie im Backup-Tresor des Zielkontos den Zugriff von einem anderen Konto aus.	AWS DevOps, Migrationsingenieur, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie das Backup im Zielkonto wieder her.	Gehen Sie im Ziel AWS-Konto wie folgt vor: 1. Wählen Sie auf der AWS Backup Konsole Backup-Tresore aus. 2. Wählen Sie unter Backups das Backup aus, das Sie aus dem Quellkonto kopiert haben. 3. Wählen Sie Aktionen, Wiederherstellen aus. 4. Geben Sie den Namen der DynamoDB-Zieltabelle ein, die Sie wiederherstellen möchten.	AWS DevOps, DBA, Migrationsingenieur

Zugehörige Ressourcen

- Verwendung AWS Backup mit DynamoDB
- Erstellen von Sicherungskopien auf AWS-Konten
- AWS Backup Preisgestaltung

Amazon DynamoDB-Tabellen mithilfe einer benutzerdefinierten Implementierung kontenübergreifend kopieren

Erstellt von Ramkumar Ramanujam (AWS)

Übersicht

Bei der Arbeit mit Amazon DynamoDB auf Amazon Web Services (AWS) besteht ein häufiger Anwendungsfall darin, DynamoDB-Tabellen in Entwicklungs-, Test- oder Staging-Umgebungen mit den Tabellendaten in der Produktionsumgebung zu kopieren oder zu synchronisieren. Standardmäßig verwendet jede Umgebung ein anderes AWS-Konto.

DynamoDB unterstützt jetzt kontoübergreifende Backups mit AWS Backup. Informationen zu den damit verbundenen Speicherkosten bei der Nutzung von AWS Backup finden Sie unter AWS Backup Backup-Preise. Wenn Sie AWS Backup zum Kopieren zwischen Konten verwenden, müssen die Quell- und Zielkonten Teil einer Organisation von AWS Organizations sein. Es gibt andere Lösungen für kontoübergreifende Sicherung und Wiederherstellung mithilfe von AWS-Services wie AWS Glue. Die Verwendung dieser Lösungen erhöht jedoch den Anwendungsbedarf, da mehr AWS-Services bereitgestellt und verwaltet werden müssen.

Sie können Amazon DynamoDB Streams auch verwenden, um Tabellenänderungen im Quellkonto zu erfassen. Anschließend können Sie eine AWS Lambda Lambda-Funktion initiieren und die entsprechenden Änderungen in der Zieltabelle im Zielkonto vornehmen. Diese Lösung gilt jedoch für Anwendungsfälle, in denen Quell- und Zieltabellen immer synchron gehalten werden müssen. Sie gilt möglicherweise nicht für Entwicklungs-, Test- und Staging-Umgebungen, in denen Daten häufig aktualisiert werden.

Dieses Muster enthält Schritte zur Implementierung einer benutzerdefinierten Lösung zum Kopieren einer Amazon DynamoDB-Tabelle von einem Konto in ein anderes. Dieses Muster kann mit gängigen Programmiersprachen wie C#, Java und Python implementiert werden. Wir empfehlen die Verwendung einer Sprache, die von einem AWS-SDK unterstützt wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zwei aktive AWS-Konten
- DynamoDB-Tabellen in beiden Konten
- Kenntnis der Rollen und Richtlinien von AWS Identity and Access Management (IAM)

- Kenntnis des Zugriffs auf Amazon DynamoDB-Tabellen mit einer gängigen Programmiersprache wie C#, Java oder Python

Einschränkungen

Dieses Muster gilt für DynamoDB-Tabellen mit einer Größe von etwa 2 GB oder weniger. Es verfügt über zusätzliche Logik zur Behandlung von Verbindungs- oder Sitzungsunterbrechungen, Drosselungen sowie Ausfällen und Wiederholungsversuchen und kann daher für größere Tabellen verwendet werden.

Der DynamoDB-Scanvorgang, der Elemente aus der Quelltabelle liest, kann in einem einzigen Aufruf nur bis zu 1 MB an Daten abrufen. Bei größeren Tabellen, die größer als 2 GB sind, kann diese Beschränkung die Gesamtzeit bis zum vollständigen Kopieren der Tabelle verlängern.

Architektur

Das folgende Diagramm zeigt die benutzerdefinierte Implementierung zwischen den AWS-Quell- und Zielkonten. Bei der benutzerdefinierten Implementierung werden IAM-Richtlinien und Sicherheitstoken verwendet. Daten werden aus Amazon DynamoDB im Quellkonto gelesen und im Zielkonto in DynamoDB geschrieben.

Automatisierung und Skalierung

Dieses Muster gilt für DynamoDB-Tabellen, die kleiner sind, etwa 2 GB.

Um dieses Muster auf größere Tabellen anzuwenden, beheben Sie die folgenden Probleme:

- Während des Tabellenkopiervorgangs werden zwei aktive Sitzungen aufrechterhalten, wobei unterschiedliche Sicherheitstoken verwendet werden. Wenn der Vorgang zum Kopieren der Tabelle länger dauert als die Ablaufzeiten der Token, müssen Sie eine Logik zur Aktualisierung der Sicherheitstoken einrichten.
- Wenn nicht genügend Lesekapazitätseinheiten (RCUs) und Schreibkapazitätseinheiten (WCUs) bereitgestellt werden, werden Lese- oder Schreibvorgänge in der Quell- oder Zieltabelle möglicherweise gedrosselt. Achten Sie darauf, diese Ausnahmen zu erkennen und zu behandeln.
- Behandeln Sie alle anderen Fehler oder Ausnahmen und richten Sie einen Wiederholungsmechanismus ein, um es erneut zu versuchen oder an der Stelle fortzusetzen, an der der Kopiervorgang fehlgeschlagen ist.

Tools

Tools

- Amazon DynamoDB — Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der schnelle und vorhersehbare Leistung mit nahtloser Skalierbarkeit bietet.
- Welche zusätzlichen Tools erforderlich sind, hängt von der Programmiersprache ab, die Sie für die Implementierung auswählen. Wenn Sie beispielsweise C# verwenden, benötigen Sie Microsoft Visual Studio und die folgenden NuGet Pakete:
  - `AWSSDK`
  - `AWSSDK.DynamoDBv2`

Code

Der folgende Python-Codeausschnitt löscht eine DynamoDB-Tabelle mithilfe der Boto3-Bibliothek und erstellt sie neu.

Verwenden Sie nicht das `AWS_ACCESS_KEY_ID` und `AWS_SECRET_ACCESS_KEY` eines IAM-Benutzers, da es sich dabei um langfristige Anmeldeinformationen handelt, die für den programmatischen Zugriff auf AWS-Services vermieden werden sollten. Weitere Informationen zu temporären Anmeldeinformationen finden Sie im Abschnitt Bewährte Methoden.

Die im folgenden Codeausschnitt `TEMPORARY_SESSION_TOKEN` verwendeten `AWS_ACCESS_KEY_IDAWS_SECRET_ACCESS_KEY`, und sind temporäre Anmeldeinformationen, die vom AWS Security Token Service (AWS STS) abgerufen wurden.

```
import boto3
import sys
import json

#args = input-parameters = GLOBAL_SEC_INDEXES_JSON_COLLECTION,
 ATTRIBUTES_JSON_COLLECTION, TARGET_DYNAMODB_NAME, TARGET_REGION, ...

#Input param: GLOBAL_SEC_INDEXES_JSON_COLLECTION
#[{"IndexName":"Test-index","KeySchema":[{"AttributeName":"AppId","KeyType":"HASH"},
{"AttributeName":"AppType","KeyType":"RANGE"}],"Projection":
{"ProjectionType":"INCLUDE","NonKeyAttributes":["PK","SK","OwnerName","AppVersion"]}}]

#Input param: ATTRIBUTES_JSON_COLLECTION
```

```
#[{"AttributeName":"PK","AttributeType":"S"},
{"AttributeName":"SK","AttributeType":"S"},
{"AttributeName":"AppId","AttributeType":"S"},
{"AttributeName":"AppType","AttributeType":"N"}]

region = args['TARGET_REGION']
target_ddb_name = args['TARGET_DYNAMODB_NAME']

global_secondary_indexes = json.loads(args['GLOBAL_SEC_INDEXES_JSON_COLLECTION'])
attribute_definitions = json.loads(args['ATTRIBUTES_JSON_COLLECTION'])

# Drop and create target DynamoDB table
dynamodb_client = boto3.Session(
        aws_access_key_id=args['AWS_ACCESS_KEY_ID'],
        aws_secret_access_key=args['AWS_SECRET_ACCESS_KEY'],
        aws_session_token=args['TEMPORARY_SESSION_TOKEN'],
    ).client('dynamodb')

# Delete table
print('Deleting table: ' + target_ddb_name + ' ...')

try:
    dynamodb_client.delete_table(TableName=target_ddb_name)

    #Wait for table deletion to complete
    waiter = dynamodb_client.get_waiter('table_not_exists')
    waiter.wait(TableName=target_ddb_name)
    print('Table deleted.')
except dynamodb_client.exceptions.ResourceNotFoundException:
    print('Table already deleted / does not exist.')
    pass

print('Creating table: ' + target_ddb_name + ' ...')

table = dynamodb_client.create_table(
    TableName=target_ddb_name,
    KeySchema=[
        {
            'AttributeName': 'PK',
            'KeyType': 'HASH'  # Partition key
        },
        {
            'AttributeName': 'SK',
            'KeyType': 'RANGE'  # Sort key
```

```
        }
    ],
    AttributeDefinitions=attribute_definitions,
    GlobalSecondaryIndexes=global_secondary_indexes,
    BillingMode='PAY_PER_REQUEST'
)

waiter = dynamodb_client.get_waiter('table_exists')
waiter.wait(TableName=target_ddb_name)

print('Table created.')
```

Bewährte Methoden

Temporäre Anmeldeinformationen

Aus Sicherheitsgründen sollten Sie beim programmgesteuerten Zugriff auf AWS-Services die Verwendung `AWS_SECRET_ACCESS_KEY` des `AWS_ACCESS_KEY_ID` und eines IAM-Benutzers vermeiden, da es sich dabei um langfristige Anmeldeinformationen handelt. Versuchen Sie immer, temporäre Anmeldeinformationen zu verwenden, um programmgesteuert auf AWS-Services zuzugreifen.

Beispielsweise kodiert ein Entwickler während der Entwicklung das `AWS_ACCESS_KEY_ID` Ende eines IAM-Benutzers in `AWS_SECRET_ACCESS_KEY` der Anwendung fest, kann die hartcodierten Werte jedoch nicht entfernen, bevor die Änderungen in das Code-Repository übertragen werden. Diese offengelegten Anmeldeinformationen können von unbeabsichtigten oder böswilligen Benutzern verwendet werden, was schwerwiegende Folgen haben kann (insbesondere, wenn die offengelegten Anmeldeinformationen Administratorrechte haben). Diese offengelegten Anmeldeinformationen sollten sofort mithilfe der IAM-Konsole oder der AWS-Befehlszeilenschnittstelle (AWS CLI) deaktiviert oder gelöscht werden.

Verwenden Sie AWS STS, um temporäre Anmeldeinformationen für den programmatischen Zugriff auf AWS-Services zu erhalten. Temporäre Anmeldeinformationen sind nur für die angegebene Zeit gültig (von 15 Minuten bis zu 36 Stunden). Die maximal zulässige Dauer temporärer Anmeldeinformationen hängt von Faktoren wie Rolleneinstellungen und Rollenverkettung ab. Weitere Informationen zu AWS STS finden Sie in der Dokumentation.

Epen

DynamoDB-Tabellen einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie DynamoDB-Tabellen.	Erstellen Sie DynamoDB-Tabellen mit Indizes in AWS-Quell- und Zielkonten. Stellen Sie die Kapazität sbereitstellung auf den On-Demand-Modus ein, sodass DynamoDB die Lese-/Sch reibkapazitäten dynamisch auf der Grundlage der Arbeitslast skalieren kann. Alternativ können Sie die bereitgestellte Kapazität mit 4000 und 4000 verwenden. RCUs WCUs	App-Entwickler, DBA, Migrationsingenieur
Füllen Sie die Quelltabelle aus.	Füllen Sie die DynamoDB-Tabelle im Quellkonto mit Testdaten auf. Wenn Sie mindestens 50 MB an Testdaten haben, können Sie den Spitzenwert und den RCUs Durchschnittsverbr auch beim Kopieren der Tabelle ermitteln. Anschließ end können Sie die Kapazität sbereitstellung nach Bedarf ändern.	App-Entwickler, DBA, Migrationsingenieur

Anmeldeinformationen für den Zugriff auf die DynamoDB-Tabellen einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie IAM-Rollen für den Zugriff auf die DynamoDB-Quell- und Zieltabellen.	Erstellen Sie eine IAM-Rolle im Quellkonto mit Berechtigungen für den Zugriff (das Lesen) der DynamoDB-Tabelle im Quellkonto. Fügen Sie das Quellkonto als vertrauenswürdige Entität für diese Rolle hinzu. Erstellen Sie eine IAM-Rolle im Zielkonto mit Zugriffsberechtigungen (Erstellen, Lesen, Aktualisieren, Löschen) auf die DynamoDB-Tabelle im Zielkonto. Fügen Sie das Zielkonto als vertrauenswürdige Entität für diese Rolle hinzu.	App-Entwickler, AWS DevOps

Kopieren Sie Tabellendaten von einem Konto in ein anderes

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Besorgen Sie sich temporäre Anmeldeinformationen für die IAM-Rollen.	Rufen Sie temporäre Anmeldeinformationen für die IAM-Rolle ab, die im Quellkonto erstellt wurde. Rufen Sie temporäre Anmeldeinformationen für die	App-Entwickler, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	im Zielkonto erstellte IAM-Rolle ab. Eine Möglichkeit, die temporären Anmeldeinformationen für die IAM-Rolle abzurufen, besteht darin, AWS STS über die AWS-CLI zu verwenden. `aws sts assume-role --role-arn arn:aws:iam::<account-id>:role/<role-name> --role-session-name <session-name> --profile <profile-name>` Verwenden Sie das entsprechende AWS-Profil (entspricht dem Quell- oder Zielkonto). Weitere Informationen zu den verschiedenen Möglichkeiten, temporäre Anmeldeinformationen zu erhalten, finden Sie im Folgenden: • API-Referenz für den AWS Security Token Service • Abrufen von IAM-Rolle nanmeldedaten für den CLI-Zugriff	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initialisieren Sie die DynamoDB-Clients für den Quell- und Ziel-DynamoDB-Zugriff.	Initialisieren Sie die DynamoDB-Clients, die vom AWS-SDK bereitgestellt werden, für die DynamoDB-Quell- und Zieltabellen. • Verwenden Sie für den DynamoDB-Quellclient die temporären Anmeldein formationen, die vom Quellkonto abgerufen wurden. • Verwenden Sie für den DynamoDB-Zielclient die temporären Anmeldein formationen, die vom Zielkonto abgerufen wurden. Weitere Informationen zum Stellen von Anfragen mithilfe temporärer IAM-Anmel deinformationen finden Sie in der AWS-Dokumentation.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die Zieltabelle und erstellen Sie sie neu.	Löschen Sie die DynamoDB-Zieltabelle (zusammen mit den Indizes) im Zielkonto und erstellen Sie sie neu, indem Sie den DynamoDB-Client für das Zielkonto verwenden. Das Löschen aller Datensätze aus einer DynamoDB-Tabelle ist ein kostspieliger Vorgang, da dafür bereitgestellte Daten verbraucht werden. WCUs Durch das Löschen und Neuerstellen der Tabelle werden diese zusätzlichen Kosten vermieden. Sie können einer Tabelle Indizes hinzufügen, nachdem Sie sie erstellt haben, aber das dauert 2—5 Minuten länger. Das Erstellen von Indizes während der Tabellenerstellung, indem die Indexsammlung an den `createTable` Aufruf übergeben wird, ist effizienter.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Tabellenkopie durch.	Wiederholen Sie die folgenden Schritte, bis alle Daten kopiert sind: • Führen Sie mithilfe des DynamoDB-Quellclients einen Scan der Tabelle im Quellkonto durch. Jeder DynamoDB-Scan ruft nur 1 MB an Daten aus der Tabelle ab. Daher müssen Sie diesen Vorgang wiederholen, bis alle Elemente oder Datensätze gelesen sind. • Schreiben Sie für jeden Satz gescannter Elemente die Elemente mithilfe des `BatchWriteItem` Aufrufs im AWS SDK for DynamoDB mit dem DynamoDB-Zielclient in die Tabelle im Zielkonto. Dadurch wird die Anzahl der `PutItem` Anfragen an DynamoDB reduziert. • `BatchWriteItem` hat eine Beschränkung auf 25 Schreibvorgänge oder Eingaben oder bis zu 16 MB. Sie müssen eine Logik hinzufügen, um gescannte Objekte in einer Anzahl von 25 zu sammeln, bevor	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie anrufen`BatchWrit eItem` . `BatchWrit eItem` gibt eine Liste von Elementen zurück, die nicht erfolgreich kopiert werden konnten. Fügen Sie anhand dieser Liste eine Wiederhol ungslogik hinzu, um einen weiteren `BatchWrit eItem` Aufruf nur mit den Elementen durchzuführen, die nicht erfolgreich waren. Weitere Informationen finden Sie in der Referenzimplementi erung in C# (zum Löschen, Erstellen und Auffüllen von Tabellen) im Abschnitt Anlagen. Ein Beispiel für eine JavaScript Objektnotationsdat ei (JSON) für die Tabellenk onfiguration ist ebenfalls angehängt.	

Zugehörige Ressourcen

- Dokumentation zu Amazon DynamoDB
- Einen IAM-Benutzer in Ihrem AWS-Konto erstellen
- AWS SDKs
- Temporäre Anmeldeinformationen mit AWS-Ressourcen verwenden

Zusätzliche Informationen

Dieses Muster wurde mithilfe von C# implementiert, um eine DynamoDB-Tabelle mit 200.000 Elementen (durchschnittliche Elementgröße von 5 KB und Tabellengröße von 250 MB) zu kopieren. Die DynamoDB-Zieltabelle wurde mit einer bereitgestellten Kapazität von 4000 und 4000 RCUs eingerichtet. WCUs

Das vollständige Kopieren der Tabelle (vom Quellkonto zum Zielkonto), einschließlich Löschen und Neuerstellen der Tabelle, dauerte 5 Minuten. Insgesamt verbrauchte Kapazitätseinheiten: 30.000 RCUs und etwa 400.000 WCUs.

Weitere Informationen zu DynamoDB-Kapazitätsmodi finden Sie unter Kapazitätsmodus Lesen/Schreiben in der AWS-Dokumentation.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Erstellen Sie detaillierte Kosten- und Nutzungsberichte für Amazon RDS und Amazon Aurora

Erstellt von Lakshmanan Lakshmanan (AWS) und Sudarshan Narasimhan

Übersicht

Dieses Muster zeigt, wie die Nutzungskosten für Amazon Relational Database Service (Amazon RDS) - oder Amazon Aurora Aurora-Cluster verfolgt werden, indem benutzerdefinierte Kostenzuweisungs-Tags konfiguriert werden. Sie können diese Tags verwenden, um detaillierte Kosten- und Nutzungsberichte in AWS Cost Explorer für Cluster in mehreren Dimensionen zu erstellen. Sie können beispielsweise die Nutzungskosten auf Team-, Projekt- oder Kostenstellenebene verfolgen und die Daten anschließend in Amazon Athena analysieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine oder mehrere Amazon RDS- oder Amazon Aurora Aurora-Instances

Einschränkungen

Informationen zu Tagging-Einschränkungen finden Sie im AWS Billing User Guide.

Architektur

Zieltechnologie-Stack

- Amazon RDS oder Amazon Aurora
- AWSKosten- und Nutzungsbericht
- AWS Cost Explorer
- Amazon Athena

Arbeitsablauf und Architektur

Der Tagging- und Analyse-Workflow besteht aus den folgenden Schritten:

1. Ein Dateningenieur, Datenbankadministrator oder AWS-Administrator erstellt benutzerdefinierte Kostenzuweisungs-Tags für die Amazon RDS- oder Aurora-Cluster.
2. Ein AWS-Administrator aktiviert die Tags.
3. Die Tags melden Metadaten an AWS Cost Explorer.
4. Ein Dateningenieur, Datenbankadministrator oder AWS-Administrator erstellt einen monatlichen Kostenverteilungsbericht.
5. Ein Dateningenieur, Datenbankadministrator oder AWS-Administrator analysiert den monatlichen Kostenzuordnungsbericht mithilfe von Amazon Athena.

Das folgende Diagramm zeigt, wie Sie Tags anwenden, um die Nutzungskosten für Amazon RDS- oder Aurora-Instances nachzuverfolgen.

Das folgende Architekturdiagramm zeigt, wie der Kostenzuordnungsbericht zu Analysezwecken in Amazon Athena integriert ist.

Der monatliche Kostenzuordnungsbericht wird in einem von Ihnen angegebenen Amazon S3 S3-Bucket gespeichert. Wenn Sie Athena mit der CloudFormation AWS-Vorlage einrichten, wie im Abschnitt Epics beschrieben, stellt die Vorlage mehrere zusätzliche Ressourcen bereit, darunter einen AWS Glue-Crawler, eine AWS Glue Glue-Datenbank, ein Amazon Simple Notification System (Amazon SNS) -Ereignis, AWS Lambda Lambda-Funktionen und AWS Identity and Access Management (IAM) -Rollen für die Lambda-Funktionen. Wenn neue Kostendatendateien im S3-Bucket ankommen, werden diese Dateien mithilfe von Ereignisbenachrichtigungen zur Verarbeitung an eine Lambda-Funktion weitergeleitet. Die Lambda-Funktion initiiert einen AWS Glue Glue-Crawler-Job, um die Tabelle im AWS Glue Glue-Datenkatalog zu erstellen oder zu aktualisieren. Diese Tabelle wird dann verwendet, um Daten in Athena abzufragen.

Tools

- Amazon Athena ist ein interaktiver Abfrageservice, der es einfach macht, Daten in Amazon S3 mithilfe von Standard-SQL zu analysieren.
- Amazon Aurora ist eine vollständig verwaltete relationale Datenbank-Engine, die für die Cloud entwickelt wurde und mit MySQL und PostgreSQL kompatibel ist.

- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der AWS-Cloud.
- AWS CloudFormation ist ein Infrastructure-as-Code-Service (IaC), mit dem Sie Ressourcen von AWS und Drittanbietern einfach modellieren, bereitstellen und verwalten können.
- Mit AWS Cost Explorer können Sie Ihre AWS-Kosten und -Nutzung anzeigen und analysieren.

Epen

Erstellen und aktivieren Sie Tags für Ihren Amazon RDS- oder Aurora-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie benutzerdefinierte Kostenzuweisungs-Tags für Ihren Amazon RDS- oder Aurora-Cluster.	Um Tags zu einem neuen oder vorhandenen Amazon RDS- oder Aurora-Cluster hinzuzufügen, folgen Sie den Anweisungen unter Hinzufügen, Auflisten und Entfernen von Tags im Amazon Aurora Aurora-Benutzerhandbuch. **Note** Informationen zur Einrichtung eines Amazon Aurora Aurora-Clusters finden Sie in den Anweisungen für MySQL und PostgreSQL im Amazon Aurora Aurora-Benutzerhandbuch.	AWS-Administrator, Dateningenieur, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie die benutzerdefinierten Tags für die Kostenzuweisung.	Folgen Sie den Anweisungen unter Aktivierung von benutzerdefinierten Kostenzuweisungs-Tags im AWS-Abrechnungsbenutzerhandbuch.	AWS-Administrator

Kosten- und Nutzungsberichte erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und konfigurieren Sie Kosten- und Nutzungsberichte für Ihre Cluster.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS-Abrechnungskonsole. 2. Wählen Sie im linken Navigationsbereich die Option Kosten- und Nutzungsberichte aus. 3. Wählen Sie Create report (Bericht erstellen) aus. 4. Geben Sie einen Berichtsnamen ein, behalten Sie die Standardeinstellungen für andere Optionen bei und wählen Sie dann Weiter aus. 5. Wählen Sie Konfigurieren und geben Sie die Details eines vorhandenen S3-Buckets an. Auf diesem Bildschirm können Sie auch wählen, ob Sie einen	App-Besitzer, AWS-Administrator, DBA, General AWS, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	neuen S3-Bucket erstellen möchten. Wählen Sie Weiter aus. 6. Überprüfen Sie die Standardrichtlinie, die auf Ihren Bucket angewende t wird, aktivieren Sie das Bestätigungs-Kontrollkästch en und wählen Sie dann Speichern aus. 7. Geben Sie unter Präfix für den Berichtspfad das Präfix an, das Sie dem Berichtsnamen voranstellen möchten. 8. Wählen Sie unter Zeitgranu larität die Option Stündlich, Täglich oder Monatlich aus, je nachdem, wie oft Daten für den Bericht erfasst werden sollen. 9. Wählen Sie für die Berichtsversionierung aus, ob neue Versionen des Berichts separat erstellt werden sollen oder ob der vorhandene Bericht mit jeder Version überschrieben werden soll. 10. Wählen Sie unter Berichtsd atenintegration aktiviere n für die Option Amazon Athena aus. Stellen Sie sicher, dass der Komprimie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	rungstyp auf Parquet eingestellt ist. 11. Wählen Sie Weiter aus. 12. Überprüfen Sie die Berichtseinstellungen und wählen Sie dann Überprüfe n und Abschließen aus. Die Daten werden in 24 Stunden verfügbar sein.	

Analysieren Sie die Kosten- und Nutzungsberichtsdaten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie die Daten des Kosten- und Nutzungsberichts.	1. Richten Sie Athena ein und verwenden Sie es, um die Berichtsdaten zu analysier en. Anweisungen finden Sie unter Abfragen von Kosten- und Nutzungsberichten mit Amazon Athena im AWS-Benutzerhandbuch für Kosten- und Nutzungsb erichte. Wir empfehlen Ihnen, die von Athena bereitgestellte CloudForm ation AWS-Vorlage zu verwenden. 2. Führen Sie Athena-Ab fragen aus. Sie können beispielsweise die folgende SQL-Abfrage verwenden	App-Besitzer, AWS-Admin istrator, DBA, General AWS, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	, um den Status der Datenaktualisierung zu überprüfen. `select status from cost_and_usage_data_status` Weitere Informationen finden Sie unter Ausführen von Amazon Athena Athena-Abfragen im AWS-Benutzerhandbuch für Kosten- und Nutzungsberichte. **Note** Wenn Sie Ihre SQL-Abfrage ausführen , stellen Sie sicher, dass die richtige Datenbank aus der Dropdownliste ausgewählt ist.	

Zugehörige Ressourcen

Referenzen

- Einrichtung von Athena mithilfe von CloudFormation AWS-Vorlagen (empfohlen)
- Manuelles Einrichten von Athena
- Amazon Athena Athena-Abfragen ausführen
- Berichtsdaten werden in andere Ressourcen geladen

Tutorials und Videos

- Analysieren Sie Kosten- und Nutzungsberichte mit Amazon Athena (YouTube Video)

Stellen Sie mithilfe von Terraform SQL Server-Failover-Cluster-Instances auf Amazon EC2 und Amazon FSx bereit

Erstellt von Mark Hudson (AWS) und Matt Burgess (AWS)

Übersicht

Dieses Muster verwendet Terraform, um SQL Server-Failover-Cluster-Instances (FCIs) auf Windows Server Failover Cluster (WSFC) -Knoten auf Amazon Elastic Compute Cloud (Amazon) bereitzustellen. EC2 Darüber hinaus verwendet das Muster FSx gemeinsam genutzten Speicher von Amazon für Daten und Protokolldateien.

Wenn SQL Server-Datenbanken migriert werden AWS, ist Amazon RDS for SQL Server die erste Wahl. Manchmal ist Amazon RDS for SQL Server jedoch nicht geeignet und SQL Server muss auf Amazon EC2 in einer hochverfügbaren Architektur bereitgestellt werden. In dieser Lösung FCIs werden SQL Server auf allen WSFC-Knoten installiert.

Das in diesem Muster enthaltene Terraform-Modul stellt bis zu zwei Amazon EC2 SQL Server-Instances bereit. Ein Dateisystem von Amazon FSx für Windows File Server fungiert als Quorum-Zeuge und speichert gemeinsam genutzte Daten und Protokolldateien. Unabhängig von der Anzahl der konfigurierten Instances erstellen die SQL Server-Instanzknoten immer einen FCI-Cluster und schließen sich diesem an, um die Umgebungsparität sicherzustellen. (In der Regel wird eine Instanz für die Entwicklung und zwei Instanzen für Produktionsumgebungen konfiguriert.) Für Konfigurationen, die zwei Knoten für hohe Verfügbarkeit verwenden, wird ein interner Network Load Balancer bereitgestellt. Der Network Load Balancer verwendet eine auf dem FCI-Cluster konfigurierte Integritätsprüfung, um zu ermitteln, welcher Knoten der primäre ist.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver. AWS-Konto
- Amazon Virtual Private Cloud (Amazon VPC) mit zwei Subnetzen in separaten Availability Zones.
- Amazon VPC DHCP-Optionssatz. Konfigurieren Sie den Domänennamen so, dass er in Ihren Active Directory-Domänennamen aufgelöst wird, und konfigurieren Sie die Domänen- und NetBIOS-Nameserver so, dass sie auf Ihre Active Directory-Domänencontroller verweisen. Weitere Informationen finden Sie unter VPC-Konfiguration unter Zusätzliche Informationen.
- AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD).

- Benutzerdefiniertes Amazon Machine Image (AMI). Weitere Informationen finden Sie unter AMI-Konfiguration unter Zusätzliche Informationen.
- Amazon Simple Storage Service (Amazon S3) -Bucket, der das SQL Server-ISO-Image enthält. Diese Voraussetzung ist nur erforderlich, wenn Sie EC2 Image Builder mit der bereitgestellten `component.yaml` Datei verwenden, um das benutzerdefinierte AMI zu erstellen.
- AWS Key Management Service (AWS KMS) Verschlüsselungsschlüssel.
- Standardmäßig wird SQL Server mit einem Product Key für die Developer Edition installiert. Von Produktionssystemen wird erwartet, dass sie einen gültigen Produktschlüssel verwenden, der von der entsprechenden Variablen an das Modul übergeben wird.

Einschränkungen

- Diese Lösung erfordert AWS Managed Microsoft AD. Wenn Sie möchten, können Sie jedoch stattdessen eine selbstverwaltete Active Directory-Implementierung verwenden. Ändern Sie dazu das enthaltene Amazon FSx Terraform-Modul, um das Attribut zu entfernen. `active_directory_id` Fügen Sie dann die vier Attribute hinzu, die für selbstverwaltetes Active Directory erforderlich sind, wie in der Terraform-Dokumentation gezeigt.
- SQL Server ist für die Verwendung der Authentifizierung im gemischten Modus eingerichtet. Wenn Sie möchten, können Sie die reine Windows-Authentifizierung verwenden. Entfernen Sie dazu im bereitgestellten Benutzerdatenskript die `/SAPWD` Parameter `/SECURITYMODE` und, die für den `setup.exe` Befehl angegeben wurden. Sie können die `sql_accounts.tf` Datei entfernen, und Sie können die `instances.tf` Datei ändern, um den `sql_sa_password` Eintrag zu entfernen.
- Wenn Sie einen bereitgestellten Cluster löschen, müssen Sie die entsprechenden virtuellen Computerobjekte und einzelne Computerobjekte in Active Directory entfernen. Verwenden Sie die Active Directory-Verwaltungstools, um die Objekte zu entfernen.
- Einige AWS-Services sind nicht in allen verfügbar AWS-Regionen. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie unter AWS Dienste nach Regionen. Informationen zu bestimmten Endpunkten finden Sie unter Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Produktversionen

Diese Lösung wurde mit den folgenden Versionen getestet:

- Windows Server 2019

- SQL Server 2019
- Terraform v0.13.0

Architektur

Quelltechnologie-Stack

- SQL Server

Zieltechnologie-Stack

- SQL Server FCI auf WSFC-Knoten mit Amazon EC2
- Amazon FSx für Windows-Dateiserver
- Amazon-S3-Bucket
- AWS Secrets Manager
- AWS Managed Microsoft AD
- AWS KMS
- AWS Identity and Access Management (IAM)

Zielarchitektur

Das folgende Diagramm zeigt die Architektur für diese Lösung.

Das Diagramm zeigt Folgendes:

- Eine IAM-Rolle, die den EC2 Instances Zugriff auf AWS KMS und Secrets Manager bietet
- Zwei SQL Server-Knoten, die auf EC2 Amazon-Instances in privaten Subnetzen in zwei Availability Zones bereitgestellt werden
- Ein Network Load Balancer zur Erleichterung von Verbindungen zur aktiven SQL Server-Instanz (wird nicht bei der Einrichtung eines Clusters mit einem einzelnen Knoten bereitgestellt)
- Das Dateisystem Amazon FSx for Windows File Server wird in beiden privaten Subnetzen für gemeinsamen Speicher durch die SQL Server-Knoten bereitgestellt
- Secrets Manager zum Speichern von Anmeldeinformationen und Konfigurationen für Active Directory und SQL Server

- Amazon S3 S3-Bucket zum Speichern des SQL Server-Installationsabbilds
- AWS Managed Microsoft AD für die Windows-Authentifizierung
- AWS KMS zur Erstellung des Verschlüsselungsschlüssels

Automatisierung und Skalierung

Sie können die Bereitstellung der Zielarchitektur automatisieren, indem Sie die Terraform-Module verwenden, die sich im GitHub Repository befinden. Sie müssen die `terraform.tfvars` Datei so ändern, dass sie Variablenwerte enthält, die für Ihre Umgebung spezifisch sind. Der Amazon S3 S3-Bucket, die AWS Managed Microsoft AD Komponenten, der AWS KMS Verschlüsselungsschlüssel und einige Geheimnisse sind Voraussetzungen für diese Bereitstellung und nicht im Terraform-Code enthalten.

Tools

AWS-Services

- AWS Directory Service for Microsoft Active Directoryermöglicht Ihren verzeichnissensitiven Workloads und AWS Ressourcen die Verwendung von Microsoft Active Directory in der. AWS Cloud In diesem Muster AWS Managed Microsoft AD wird es für die Windows Server- und SQL Server-Authentifizierung sowie für DNS verwendet.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren. In diesem Muster werden SQL Server-Failover-Cluster-Instances auf EC2 Amazon-Instances installiert.
- EC2 Mit Image Builder können Sie die Erstellung, Verwaltung und Bereitstellung von benutzerdefinierten Server-Images automatisieren.
- Amazon FSx für Windows File Server bietet vollständig verwalteten gemeinsamen Speicher auf Windows Server. In diesem Muster stellt der Dateiserver FSx für Windows gemeinsam genutzten Speicher für SQL Server-Daten und Protokolldateien sowie den Quorum-Zeugen bereit.
- AWS Identity and Access Management (IAM) unterstützt Sie bei der sicheren Verwaltung des Zugriffs auf Ihre AWS Ressourcen, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Key Management Service (AWS KMS) hilft Ihnen dabei, kryptografische Schlüssel zu erstellen und zu kontrollieren, um Ihre Daten zu schützen. In diesem Muster wird es verwendet, um Secrets Manager Manager-Geheimnisse, den SQL Server-Speicher auf Amazon Elastic

Block Store (Amazon EBS) -Volumes und das Dateisystem FSx für Windows File Server zu verschlüsseln.

- Mit AWS Secrets Manager können Sie fest codierte Anmeldeinformationen im Code (einschließlich Passwörter) durch einen API-Aufruf an Secrets Manager ersetzen und das Geheimnis programmgesteuert abrufen. In diesem Muster werden die Active Directory-Anmeldeinformationen für die Installation und Ausführung von SQL Server, die `sa` Benutzeranmeldeinformationen und die Datenbankverbindungsinformationen in Secrets Manager gespeichert.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt. Dieses Muster verwendet einen Amazon S3 S3-Bucket zum Speichern des SQL Server-Installationsabbilds.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk bereitzustellen. Dieses virtuelle Netzwerk entspricht einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben würden, mit den Vorteilen der Verwendung der skalierbaren Infrastruktur von AWS.

Andere Tools

- Microsoft SQL Server FCIs werden auf allen Windows Server-Clusterknoten installiert. Darüber hinaus können sie in mehreren Subnetzen installiert werden. In diesem Muster werden SQL Server-FCI-Instanzen auf allen WSFC-Knoten installiert.
- Terraform ist ein IaC-Tool (Infrastructure as Code), mit dem Sie mithilfe von Code Cloud-Infrastruktur und -Ressourcen bereitstellen und verwalten können. In diesem Muster wird Terraform verwendet, um die Ressourcen zu erstellen und die SQL Server-FCI-Instanzen zu konfigurieren.
- Windows Server Failover Clustering bietet Infrastrukturfunktionen, die die Hochverfügbarkeit von gehosteten Serveranwendungen wie SQL Server unterstützen. In diesem Muster nutzen die FCI-Knoten die WSFC-Funktionalität, um lokale Hochverfügbarkeit durch Redundanz auf Instanzebene zu gewährleisten.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub cluster-amazon-elastic-compute- cloud-amazon-fsx-microsoft -sql-server verfügbar. Die folgenden Ressourcen sind im Repository verfügbar:

- Eine `README.md` Datei, die einen Überblick über die Lösung und zusätzliche Installations- und Nutzungsinformationen bietet

- Ein Basissatz von Terraform-Konfigurationsdateien und ein FSx Amazon-spezifisches Modul zur Bereitstellung der Komponenten für dieses Muster
- Ein Instance-Setup-Skript, das als EC2 Amazon-Benutzerdatenskript ausgeführt wird
- Eine `component.yaml`-Datei, mit der Image Builder ein benutzerdefiniertes AMI erstellen kann

Bewährte Methoden

Sicherheit und Patching

- Die erforderlichen AMI-Installationen und -Konfigurationen sind die Mindestanforderungen für die Bereitstellung von SQL Server-FCI-Clustern. Zusätzliche Software und Konfigurationen sind möglicherweise erforderlich, um die Standards und Sicherheitsanforderungen Ihres Unternehmens zu erfüllen.
- Patchen Sie Windows nach der Bereitstellung regelmäßig. Patchen Sie entweder direkt die laufenden Instances oder erstellen Sie ein neues AMI mit den neuesten Windows-Patches und ersetzen Sie die Instances (nacheinander) mithilfe des neuen AMI. AWS veröffentlicht AMIs monatlich neue Windows-Versionen, die die neuesten Betriebssystem-Patches, Treiber und Start-Agents enthalten. Wir empfehlen Ihnen, beim Starten neuer Instances oder beim Erstellen eigener benutzerdefinierter Images nach dem neuesten AMI zu suchen.
- Die EC2 Amazon-Instances sind so konfiguriert, dass sie den gesamten ausgehenden Datenverkehr zulassen. Bei der Bereitstellung in einer Produktionsumgebung sollten Regeln für ausgehenden Datenverkehr in der Sicherheitsgruppe eingerichtet werden, um diesen Datenverkehr auf die erforderlichen Ziele zu beschränken.
- Das Dateisystem FSx für Windows File Server kann automatisch Auditprotokolle für Dateifreigaben sowie Datei- und Ordnerzugriffe aufzeichnen und sie an das gewünschte Ziel senden, falls dies in Ihrer Umgebung erforderlich ist.
- Rotieren Sie Secrets Manager-Geheimnisse automatisch und regelmäßig. Ziehen Sie für das EC2 Amazon-Instance-Schlüsselpaar eine automatisierte Rotationslösung in Betracht, wie unter So verwenden Sie AWS Secrets Manager zum sicheren Speichern und Rotieren von SSH-Schlüsselpaaren beschrieben. Richten Sie für die Active Directory-Anmeldeinformationen und die SQL `sa` Server-Anmeldeinformationen eine automatische Rotation gemäß Ihren Richtlinien für die Passwortverwaltung ein.

Active Directory-Verwaltung

- Als Teil des FCI-Clusters generiert Windows ein Computer Name Object (CNO) in Active Directory. Das CNO reagiert auf DNS-Anfragen und leitet den Datenverkehr an den aktiven SQL-Knoten weiter. Wir empfehlen nicht, dieses von Active Directory bereitgestellte DNS zu verwenden. Die TTL ist zu hoch, um eine angemessene Failover-Zeit zu gewährleisten, und es dauert oft mehr als 5 Minuten, bis die neue primäre IP-Adresse wiedergegeben wird. Im Gegensatz dazu ist der interne Network Load Balancer für Installationen mit hoher Verfügbarkeit so konfiguriert, dass er innerhalb von 30 Sekunden ein Failover durchführt.
- Für die Erstellung des Clusters ist ein Active Directory-Domänenadministrator erforderlich. Diese Anforderung ist auf die erhöhten Berechtigungen zurückzuführen, die zum Erstellen der Clusterobjekte und zum Ändern von Berechtigungen in Active Directory erforderlich sind. Die SQL Server-Dienste müssen jedoch nicht als Domänenadministrator ausgeführt werden. Daher empfehlen wir, dass Sie zu diesem Zweck einen zweiten Active Directory-Benutzer erstellen. Sie können diesen Benutzer jedoch entfernen, wenn die Dienste als Domänenadministratorbenutzer ausgeführt werden. In diesem Fall muss der Domänenadministratorbenutzer der Active Directory-Administratorgruppe hinzugefügt werden, die als Teil dieses Musters erstellt wurde.

Epen

Richten Sie Cluster-Anmeldeinformationen ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Active Directory-Gruppen.	Erstellen AWS Managed Microsoft AD Sie in die folgenden Gruppen: • Cluster-Administratorgruppe — Diese Gruppe wird der lokalen Administratorgrupp e auf jedem Clusterknoten hinzugefügt. • Cluster-Remote-Desktop-Gruppe — Diese Gruppe wird der lokalen Gruppe der Remote-Desktop-Benutzer auf jedem Clusterknoten hinzugefügt.	AD-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie in der AWS Dokumentation unter AWS Managed Microsoft AD Gruppe erstellen.	
Erstellen Sie Active Directory-Benutzer.	Erstellen AWS Managed Microsoft AD Sie in die folgenden Benutzer • Domänenadministrator-Benutzer — Verwenden Sie dieses Konto, um den Cluster zu erstellen. • Domänenbenutzer — Die SQL Server-Dienste verwenden dieses Konto zur Ausführung. Fügen Sie diesen Benutzer der Cluster-Administratorgruppe hinzu, die Sie in der vorherigen Aufgabe erstellt haben. Weitere Informationen finden Sie in der AWS Dokumentation unter AWS Managed Microsoft AD Benutzer erstellen.	AD-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Active Directory -Anmeldeinformationen zu Geheimnissen hinzu.	Verwenden Sie Secrets Manager, um vier Secrets zum Speichern der folgenden Informationen zu erstellen: • Benutzername des Domain-Administrator-Benutzers • Passwort des Domain-Administrator-Benutzers • Der Benutzername des Domänenbenutzers • Passwort des Domänenbenutzers Weitere Informationen finden Sie in der AWS Dokumentation unter Create an AWS Secrets Manager Secret.	AWS-Administrator

Bereiten Sie die Umgebung vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Windows-AMI.	Erstellen Sie ein benutzerdefiniertes Windows-AMI, das die erforderliche Software und die erforderlichen Konfigurationen enthält. Weitere Informationen finden Sie unter Zusätzliche Informationen.	AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Terraform.	Folgen Sie den Anweisungen auf der Terraform-Website, um Terraform zu installieren.	AWS DevOps
Klonen Sie das Repository	Klonen Sie das Repository dieses Musters. Weitere Informationen finden Sie unter Klonen eines Repositorys auf der GitHub Website.	AWS DevOps

Installieren Sie den Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Terraform-Variablen.	Aktualisieren Sie die bereitgestellte `terraform.tfvars` Datei, um alle Variablen auf Werte zu setzen, die für Ihre Umgebung geeignet sind. Aktualisieren Sie beispielsweise die `domain_group_rdp_users` Variablen `domain_group_administrators` und, sodass sie Ihren Active Directory-Domänennamen und den Namen der zuvor erstellten Active Directory-Gruppen verwenden.	AWS DevOps
Initialisieren Sie Terraform.	Um die vorgeschlagene Bereitstellung zu sehen, navigieren Sie zum Stammverzeichnis des	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Repositorys. Verwenden Sie die Terraform-Befehlsz eilenschnittstelle (CLI) zum Ausführen `terraform init` und dann zum Ausführen. `terraform plan`	
Ressourcen bereitstellen.	Um den SQL-Cluster und die zugehörigen Ressourcen bereitzustellen, verwenden Sie zum Ausführen die Terraform-CLI. `terraform apply`	AWS DevOps, AWS-Admin istrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Bereitstellung.	Gehen Sie wie folgt vor, um die Bereitstellung zu validieren: 1. Stellen Sie mithilfe von Remote Desktop eine Connect zu einer der bereitgestellten Windows EC2 Amazon-Instances her. 2. Weitere Informationen finden Sie in der AWS Dokumentation unter Herstellen einer Connect zu Ihrer Windows-Instanz mithilfe von RDP. 3. Öffnen Sie den Windows Failover Cluster Manager. Überprüfen Sie, ob der Cluster erstellt wurde und ob die SQL Server-Rolle erstellt wurde und ausgeführt wird. 4. Um die Konnektivität und Authentifizierung mit SQL Server zu testen, verwenden Sie ein Datenbanktool wie SQL Server Management Studio, um eine Verbindung zum SQL Server-Endpunkt herzustellen. (Der Endpunktwert wird in Secrets Manager gespeichert.) Weitere Informationen	DBA, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	finden Sie EC2 in der AWS Dokumentation unter Connect to Microsoft SQL Server on Amazon.	

Fehlerbehebung

Problem	Lösung
Die Terraform-Bereitstellung wurde abgeschlossen, aber Windows Failover Cluster Manager zeigt nicht an, dass ein Cluster erstellt wurde oder der Cluster nicht betriebsbereit ist.	Die gesamte Installation der Ressourcen und die Konfiguration der Cluster können 45 bis 60 Minuten dauern. Nach Abschluss von Terraform muss das Benutzerdatenskript vollständig ausgeführt werden, was mehrere Neustarts erfordert. Um den Fortschritt zu überwachen, können Sie das `Checkpoints` Verzeichnis im `C:\` Laufwerk verwenden und die SQL Server-Installation meldet sich an. `C:\Program Data\Microsoft SQL Server\150\Log` Wenn der Vorgang abgeschlossen ist, ist die Meldung Installation abgeschlossen in der `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\UserdataExecution.log` Datei verfügbar.
Nach der Bereitstellung eines funktionierenden Clusters ist die Verwendung von Terraform zum Löschen und Neuerstellen des Clusters nicht erfolgreich. Terraform wird abgeschlossen, aber der Cluster ist nicht richtig eingerichtet.	Ein Teil des Bereitstellungsprozesses umfasst die Registrierung von Maschinen und virtuellen Objekten in Active Directory und Active Directory-DNS. Wenn Computernamen für die EC2 Amazon-Cluster-Knoten und den Cluster-Knoten existieren, kann FCI nicht korrekt initialisiert werden und die Bereitstellung schlägt fehl.

Problem	Lösung
	Gehen Sie wie folgt vor, um dieses Problem zu beheben: 1. Löschen Sie die EC2 Amazon-Knoten, den virtuellen Cluster-Computer und die Cluster-ID in Active Directory-Benutzern und -Computern. 2. Löschen Sie den DNS-Eintrag für den virtuellen Cluster-Computer in Active Directory-DNS. 3. Führen Sie den folgenden Befehl aus, um die Terraform-Ressource mit zufälliger Zeichenfolge für die Cluster-ID zu löschen. `terragrunt destroy -target=random_string.cluster_id` Diese Aktion löscht die vorhandenen EC2 Amazon-Instances. 4. Führen Sie `terraform apply` das Programm aus und erwarten Sie die folgenden drei neuen Ressourcen: Zwei EC2 FCI-Amazon-Instances und eine Cluster-ID mit zufälliger Zeichenfolge.

Zugehörige Ressourcen

AWS Dokumentation

- Erstellen Sie benutzerdefinierte Bilder mit Image Builder
- Erstellen Sie einen KMS-Schlüssel
- Einen Allzweck-Bucket erstellen
- Eine wichtige Richtlinie erstellen
- Erstellen Sie Ihre AWS Managed Microsoft AD

Zusätzliche Informationen

Informationen zum Terraform-Modul

Dieses Modul verwendet eine Mischung aus AMI-Konfiguration und Benutzerdatenkonfiguration, um eine gute Mischung aus Bereitstellungszeit und Stabilität zu erzielen. Während der Bereitstellung erfordert Windows mehrere Neustarts und Wartezeiten. Zum Schutz vor Endlosschleifen bei Neustarts der persistenten Benutzerdaten wurde eine Checkpoint-Methode implementiert. Benutzerdaten sind so konfiguriert, dass sie persistent sind. Daher müssen die Skripts zur Konfiguration von Benutzerdaten so weiterentwickelt werden, dass sie idempotent sind, und müssen dies auch weiterhin tun. Idempotenz optimiert den Aktualisierungsprozess, sodass Instanzen während eines Aktualisierungszyklus ausgetauscht werden können, ohne dass eine manuelle Konfiguration erforderlich ist, um FCI-Clustern erneut beizutreten oder sie neu zu erstellen.

SQL Server-Verbindungszeichenfolgen und Failover-Clustering

Das Modul veröffentlicht einen geheimen Schlüssel, der die Endpunktadresse enthält, die in Verbindungszeichenfolgen für diese Datenbank verwendet werden soll. Der geheime Name folgt dem Format`{environment_name}/sqlserver/{cluster_name}/endpoint`. Bei Installationen, in denen nur ein Knoten verwendet wird, können Sie davon ausgehen, dass dies die IP-Adresse der SQL Server-Schnittstelle der EC2 Amazon-Instance ist. Bei Installationen mit hoher Verfügbarkeit (zwei Instanzen) können Sie davon ausgehen, dass dies der DNS-Name des internen Network Load Balancer ist.

Virtuelles Failover-Clustering wird in diesem Modul IPs nicht unterstützt. Eine virtuelle IP muss im selben Subnetz verbleiben, um zu funktionieren. In kann AWS sich ein einzelnes Subnetz nicht über mehrere Availability Zones erstrecken. Daher IPs würde die Verwendung von Virtual dazu führen, dass dieses Modul nicht mehr als hochverfügbar angesehen werden kann.

Jede EC2 Amazon-Instance erhält drei private IP-Adressen. Ihre Verwendung ist wie folgt:

- Primäre IP für Netzwerkverkehr — Die Quell-IP für ausgehenden Verkehr.
- FCI-Kommunikation — Wird verwendet, um den Status und die Synchronisierung des Failover-Clusters aufrechtzuerhalten.
- SQL Server (TCP-Port 1433) — Listener und überwacht auch den Heartbeat-Verkehr, um festzustellen, welche Instanz primär ist.

VPC-Konfiguration

In den Voraussetzungen ist ein DHCP-Optionssatz aufgeführt, der für die Verwendung von Active Directory für die DNS-Auflösung konfiguriert ist. Diese Voraussetzung ist jedoch keine zwingende Anforderung. Die grundlegende Anforderung besteht darin, dass die EC2 Instanzen in der Lage sein müssen, Ihren Active Directory-Domänennamen aufzulösen. Die Erfüllung dieser Anforderung kann auch auf andere Weise erreicht werden, z. B. durch die Verwendung von Amazon Route 53 Resolver Endpunkten. Weitere Informationen finden Sie unter Integrieren der DNS-Auflösung Ihres Verzeichnisdienstes mit Amazon Route 53-Resolvern (AWS Blogbeitrag).

AMI-Konfiguration

Das in diesem Muster verwendete AMI muss die folgenden Softwarevoraussetzungen und Konfigurationen enthalten:

1. Laden Sie die SQL Server 2019-Installationsdateien herunter und erweitern Sie sie in`C:\SQL_Install_media`.
2. Installieren Sie die folgenden Windows-Funktionen:
   - `Install-WindowsFeature Failover-Clustering`
   - `Install-WindowsFeature RSAT-AD-PowerShell`
   - `Install-WindowsFeature RSAT-AD-Tools`
   - `Install-WindowsFeature RSAT-Clustering-Mgmt`
   - `Install-WindowsFeature RSAT-Clustering-PowerShell`
   - `Install-WindowsFeature RSAT-Clustering-CmdInterface`
3. Deaktivieren Sie die Windows-Firewall wie folgt:
   - `Get-NetFirewallProfile | Set-NetFirewallProfile -Enabled False`
4. Aktivieren Sie die CredSSP-Authentifizierungsmethode (`<domain>`ersetzen Sie sie durch den Windows-Domänennamen Ihrer Organisation) wie folgt:
   - `Enable-WSManCredSSP -Role "Server" -Force`
   - `Enable-WSManCredSSP -Role "Client" -DelegateComputer *.<domain>.com -Force`
5. Legen Sie die folgenden Registrierungsschlüssel fest:
   - NTLM-Authentifizierungsdaten zulassen:
     - `HKLM:\Software\Policies\Microsoft\Windows\CredentialsDelegation`
       - Name: `AllowFreshCredentialsWhenNTLMOnly`
       - Wert: 1

    - Typ: `REG_DWORD`
- Erlauben Sie lokalen Domänencomputern, NTLM zu verwenden von: PowerShell
    - Pfad: `HKLM:\Software\Policies\Microsoft\Windows\CredentialsDelegation\AllowFreshCredentialsWhenNTLMOnly`
        - Name: 1
        - Wert: `wsman/*.<domain>.com`
        - Typ: `REG_SZ`

6. Richten Sie die PowerShell Galerie wie folgt ein:
    - `[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12`
    - `Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force`
    - `Set-PSRepository -Name PSGallery -InstallationPolicy Trusted`
7. Installieren Sie die folgenden PowerShell Windows-Module*:
    - `Install-Module -Name ComputerManagementDsc`
    - `Install-Module -Name FailOverClusterDsc`
    - `Install-Module -Name PSDscResources`
    - `Install-Module -Name xSmbShare`
    - `Install-Module -Name xActiveDirectory`
    - `Install-Module -Name SqlServer`

Um Image Builder zum Erstellen des AMI zu verwenden, folgen Sie den Anweisungen unter Erstellen einer Image-Pipeline mithilfe des EC2 Image Builder-Konsolenassistenten in der Image Builder Builder-Dokumentation. Gehen Sie wie folgt vor, um die Rezeptkomponente mit den vorherigen Voraussetzungen zu erstellen:

1. Laden Sie die Datei component.yaml aus dem `ami` Ordner des Repositorys herunter. GitHub
2. Kopieren Sie den Inhalt in eine neue Image Builder Builder-Komponente.
3. Aktualisieren Sie die folgenden Platzhalter mit Ihren Informationen:
    - `<domain>`— Ihr Active Directory-Domainname
    - `<bucket_name>`— Name des Amazon S3 S3-Buckets, der das SQL Server-Image enthält

Emulieren Sie Oracle RAC-Workloads mithilfe benutzerdefinierter Endpunkte in Aurora PostgreSQL

Erstellt von HariKrishna Boorgadda (AWS)

Übersicht

Dieses Muster beschreibt, wie Services in einem Oracle Real Application Clusters (Oracle RAC) -Workload emuliert werden, indem Amazon Aurora PostgreSQL-Compatible Edition mit benutzerdefinierten Endpunkten verwendet wird, die Workloads auf Instances innerhalb eines einzelnen Clusters verteilen. Das Muster zeigt Ihnen, wie Sie benutzerdefinierte Endpunkte für Amazon Aurora Aurora-Datenbanken erstellen. Mit benutzerdefinierten Endpunkten können Sie Workloads auf verschiedene Gruppen von DB-Instances in Ihrem Aurora-Cluster verteilen und den Lastausgleich durchführen.

In einer Oracle RAC-Umgebung können sich Services auf eine oder mehrere Instances erstrecken und den Workload-Balancing auf der Grundlage der Transaktionsleistung erleichtern. Zu den Servicefunktionen gehören die end-to-end unbeaufsichtigte Wiederherstellung, fortlaufende Änderungen je nach Arbeitslast und vollständige Standorttransparenz. Sie können dieses Muster verwenden, um einige dieser Funktionen zu emulieren. Sie können beispielsweise die Fähigkeit emulieren, Verbindungen für Berichtsanwendungen weiterzuleiten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein PostgreSQL JDBC-Treiber
- Eine Aurora PostgreSQL-kompatible Datenbank
- Eine Oracle RAC-Datenbank wurde auf eine Aurora PostgreSQL-kompatible Datenbank migriert

Einschränkungen

- Informationen zu Einschränkungen, die für benutzerdefinierte Endpunkte gelten, finden Sie unter Eigenschaften für benutzerdefinierte Endpunkte angeben in der Amazon RDS-Dokumentation.

Architektur

Quelltechnologie-Stack

- Eine Oracle RAC-Datenbank mit drei Knoten

Zieltechnologie-Stack

- Eine Aurora PostgreSQL-kompatible Datenbank mit zwei Read Replicas

Quellarchitektur

Das folgende Diagramm zeigt die Architektur einer Oracle RAC-Datenbank mit drei Knoten.

Zielarchitektur

Das folgende Diagramm zeigt die Architektur einer Aurora PostgreSQL-kompatiblen Datenbank mit zwei Read Replicas. Drei verschiedene Anwendungen/Dienste verwenden benutzerdefinierte Endpunkte, die unterschiedliche Anwendungsbenutzer bedienen und den Datenverkehr und die Last zwischen Primär- und Lesereplikaten umleiten.

Tools

- Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt.
- Amazon CloudWatch hilft Ihnen dabei, die Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie auf AWS ausführen, in Echtzeit zu überwachen.
- Amazon Relational Database Service (Amazon RDS) für PostgreSQL unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen PostgreSQL-Datenbank in der AWS-Cloud.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

Epen

Erstellen Sie den Aurora PostgreSQL-kompatiblen Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Cluster.	Informationen zum Erstellen des Clusters finden Sie unter Erstellen eines DB-Clusters und Herstellen einer Verbindung zu einer Datenbank auf einem Aurora PostgreSQL-DB-Cluster in der Amazon RDS-Dokumentation.	AWS-Administrator
Erstellen Sie eine benutzerd efinierte Parametergruppe für den Workload.	Informationen zum Erstellen einer Parametergruppe finden Sie unter Erstellen einer DB-Cluster-Parametergruppe in der Amazon RDS-Dokum entation.	AWS-Administrator
Erstellen Sie Ereignisb enachrichtigungen und Alarme.	Sie können Ereignisb enachrichtigungen und CloudWatch Amazon-Al arme verwenden, um Sie zu benachrichtigen, wenn sich der Status des Clusters ändert, und um Metriken zu erfassen, wenn ein vordefini erter Schwellenwert erreicht wird. Informationen zum Erstellen eines CloudWatch Alarms finden Sie in der CloudWatch Dokumentation unter Erstellen eines CloudWatch Alarms auf	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Grundlage eines statische n Schwellenwerts. Informationen zum Erstellen einer Ereignisbenachrich tigung finden Sie in der CloudWatch Dokumenta tion unter Erstellen einer CloudWatch Ereignisregel, die bei einem Ereignis ausgelöst wird.	

Hinzufügen von Replikaten zum Aurora PostgreSQL-kompatiblen DB-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die Read Replicas dem Cluster hinzu.	1. Erstellen Sie eine Read Replica. 2. **Note** Fügen Sie die Read Replica derselben Availability Zone hinzu, in der sich Ihr DB-Cluste r befindet. : Sie können eine andere Availability Zone verwenden, wenn Sie Anforderungen haben, die für Ihren Failover-Knoten erfüllt sein müssen.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Notieren Sie sich den Read Replica-Endpunkt.	Dokumentieren Sie Ihren Read Replica-Endpunkt zur späteren Verwendung bei der Erstellung der benutzerdefinierten Endpunkte.	AWS-Administrator

Erstellen benutzerdefinierter Endpunkte

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie einen Namen für den benutzerdefinierten Endpunkt ein.	Erstellen Sie für jeden benötigten Endpunkt einen eindeutigen Endpunktnamen, der sich auf Ihren Workload oder Ihre Anwendung bezieht.	AWS-Administrator
Fügen Sie die Endpunktmitglieder hinzu.	Fügen Sie Ihre Read Replica-Endpunkte zu einer benutzerdefinierten Gruppe hinzu. Weitere Informationen finden Sie unter Bearbeiten eines benutzerdefinierten Endpunkts in der Amazon RDS-Dokumentation.	AWS-Administrator
(Optional) Fügen Sie dem Cluster future Instances hinzu.	Wenn Sie der benutzerdefinierten Gruppe weitere Replikate oder Endpoints hinzufügen möchten, finden Sie weitere Informationen unter Hinzufügen von Aurora-Repliken zu einem DB-Cluster in der Amazon RDS-Dokumentation.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Endpunkt.	Informationen zum Erstellen des Endpunkts finden Sie unter Erstellen eines benutzerdefinierten Endpunkts in der Amazon RDS-Dokumentation.	AWS-Administrator

Testen Sie Anwendungsverbindungen mithilfe benutzerdefinierter Endpunkte

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Teilen Sie die benutzerdefinierten Endpunktdetails mit der Anwendung, die auf Ihren Workload verweist.	Fügen Sie Ihre benutzerdefinierten Endpunktdetails zu den Datenbankverbindungsdetails in der Berichtsanwendung hinzu, die Sie testen möchten.	AWS-Administrator
Connect den Workload mithilfe des benutzerdefinierten Endpunkts.	Überprüfen Sie die benutzerdefinierten Endpunktdetails in der Berichtsanwendung.	AWS-Administrator
Überprüfen Sie die Verbindungsdetails in der Datenbank.	1. Testen Sie den Benutzernamen und die Anzahl der Verbindungen für Ihre Anwendung. 2. Überprüfen Sie den Lastenausgleich zwischen Ihren Workloads, um sicherzustellen, dass die Verbindungen auf verschiedene benutzerdefinierte Endpunkte (Primär- und Read Replicas) verteilt sind.	AWS-Administrator

Zugehörige Ressourcen

- Arten von Aurora-Endpunkten
- Mitgliedschaftsregeln für benutzerdefinierte Endpunkte
- End-to-end AWS-CLI-Beispiel für benutzerdefinierte Endpunkte
- Amazon Aurora als Alternative zu Oracle RAC
- Herausforderungen bei der Migration von Oracle zu PostgreSQL — und wie man sie bewältigt

Verschlüsselte Verbindungen für PostgreSQL-DB-Instances in Amazon RDS aktivieren

Erstellt von Rohit Kapoor (AWS)

Übersicht

Amazon Relational Database Service (Amazon RDS) unterstützt SSL-Verschlüsselung für PostgreSQL-DB-Instances. Mit SSL können Sie eine PostgreSQL-Verbindung zwischen Ihren Anwendungen und Ihren Amazon RDS for PostgreSQL PostgreSQL-DB-Instances verschlüsseln. Standardmäßig verwendet Amazon RDS for PostgreSQL VerschlüsselungSSL/TLS and expects all clients to connect by using SSL/TLS. Amazon RDS for PostgreSQL unterstützt die TLS-Versionen 1.1 und 1.2.

Dieses Muster beschreibt, wie Sie verschlüsselte Verbindungen für eine Amazon RDS for PostgreSQL PostgreSQL-DB-Instance aktivieren können. Sie können dasselbe Verfahren verwenden, um verschlüsselte Verbindungen für Amazon Aurora PostgreSQL-Compatible Edition zu aktivieren.

Voraussetzungen und Einschränkungen

- Ein aktives AWS-Konto
- Eine Amazon RDS for PostgreSQL PostgreSQL-DB-Instance
- Ein SSL-Paket

Architektur

Tools

- pgAdmin ist eine Open-Source-Verwaltungs- und Entwicklungsplattform für PostgreSQL. Sie können pgAdmin unter Linux, Unix, macOS und Windows verwenden, um Ihre Datenbankobjekte in PostgreSQL 10 und höher zu verwalten.
- PostgreSQL-Editoren bieten eine benutzerfreundlichere Oberfläche, mit der Sie Abfragen erstellen, entwickeln und ausführen und Code gemäß Ihren Anforderungen bearbeiten können.

Bewährte Methoden

- Überwachen Sie unsichere Datenbankverbindungen.
- Überprüfen Sie die Datenbankzugriffsrechte.
- Stellen Sie sicher, dass Backups und Snapshots im Ruhezustand verschlüsselt sind.
- Überwachen Sie den Datenbankzugriff.
- Vermeiden Sie Gruppen mit uneingeschränktem Zugriff.
- Verbessern Sie Ihre Benachrichtigungen mit Amazon GuardDuty.
- Überwachen Sie regelmäßig die Einhaltung der Richtlinien.

Epen

Laden Sie ein vertrauenswürdiges Zertifikat herunter und importieren Sie es in Ihren Trust Store

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie ein vertrauen swürdiges Zertifikat auf Ihren Computer.	Gehen Sie wie folgt vor, um Zertifikate zum Speicher vertrauenswürdiger Stammzert ifizierungsstellen für Ihren Computer hinzuzufügen. (In diesen Anweisungen wird Windows Server als Beispiel verwendet.) 1. Wählen Sie in Windows Server Start und Ausführen aus, und geben Sie dann mmc ein. 2. Wählen Sie in der Konsole „Datei“, „Snap-In hinzufüge n/entfernen“. 3. Wählen Sie unter Verfügbar e Snap-Ins die Option	DevOps Ingenieur, Migration singenieur, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Zertifikate und dann Hinzufügen aus. 4. Wählen Sie unter Dieses Snap-In verwaltet immer Zertifikate für die Option Computerkonto und Weiter aus. 5. Wählen Sie Lokaler Computer, Fertig stellen aus. 6. Wenn Sie der Konsole keine weiteren Snap-Ins hinzufügen möchten, wählen Sie OK. 7. Doppelklicken Sie in der Konsolenstruktur auf Zertifikate. 8. Klicken Sie mit der rechten Maustaste auf vertrauen swürdige Stammzert ifizierungsstellen 9. Wählen Sie Alle Aufgaben, Import, um die heruntergeladenen Zertifikate zu importieren. 10. Folgen Sie den Schritten im Assistenten zum Import von Zertifikaten.	

SSL-Verbindungen erzwingen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Parameter gruppe und legen Sie den rds.force_ssl-Parameter fest.	Wenn die PostgreSQL-DB-Instance über eine benutzerd efinierte Parametergruppe verfügt, bearbeiten Sie die Parametergruppe und ändern Sie `rds.force_ssl` sie auf 1. Wenn die DB-Instance die Standardparametergruppe verwendet, für die keine `rds.force_ssl` Option aktiviert wurde, erstellen Sie eine neue Parameter gruppe. Sie können die neue Parametergruppe mithilfe der Amazon RDS-API oder manuell wie in der folgenden Anleitung beschrieben ändern. Um eine neue Parameter gruppe zu erstellen: 1. Melden Sie sich bei der AWS-Managementkons ole an und öffnen Sie die Amazon RDS-Konsole für die AWS-Region, in der die DB-Instance gehostet wird. 2. Wählen Sie im Navigatio nsbereich Parameter groups (Parametergruppen) aus.	DevOps Ingenieur, Migration singenieur, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie Parameter gruppe erstellen und legen Sie die folgenden Werte fest: • Wählen Sie für Parameter gruppenfamilie die Option postgres14 aus. • <database_instance >Geben Sie als Gruppenname pgsql - -ssl ein. • Geben Sie unter Beschreibung eine formlose Beschreibung für die Parametergruppe ein, die Sie hinzufügen. • Wählen Sie Erstellen aus. 4. Wählen Sie die Parameter gruppe aus, die Sie erstellt haben. 5. Wählen Sie für Parameter group actions (Paramete rgruppenaktionen) die Option Bearbeiten. 6. Suchen Sie rds.force_ssl und ändern Sie die Einstellu ng auf 1. **Note** Führen Sie clientsei tige Tests durch,	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bevor Sie diesen Parameter ändern. 7. Wählen Sie Änderungen speichern aus. So verknüpfen Sie die Parametergruppe mit Ihrer PostgreSQL-DB-Instance: 1. Wählen Sie in der Amazon RDS-Konsole im Navigationsbereich Datenbanken und dann die PostgreSQL-DB-Instance aus. 2. Wählen Sie Ändern aus. 3. Wählen Sie unter Zusätzliche Konfiguration die neue Parametergruppe aus und klicken Sie dann auf Weiter. 4. Wählen Sie unter Änderungen planen die Option Sofort anwenden aus. 5. Wählen Sie Modify DB Instance (DB-Instance ändern) aus. Weitere Informationen finden Sie in der Dokumentation zu Amazon RDS.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
SSL-Verbindungen erzwingen.	Connect zur Amazon RDS for PostgreSQL PostgreSQL-DB-Instance her. Verbindungsversuche, die kein SSL verwenden, werden mit einer Fehlermeldung zurückgewiesen. Weitere Informationen finden Sie in der Dokumentation zu Amazon RDS.	DevOps Ingenieur, Migrationsingenieur, DBA

Installieren Sie die SSL-Erweiterung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie die SSL-Erweiterung.	1. Starten Sie eine psql- oder pgAdmin-Verbindung als DBA.
	2. Rufen Sie die Funktion ssl_is_used () auf, um festzustellen, ob SSL verwendet wird.
	`select ssl_is_used();`
	Die Funktion gibt zurück, `t` ob die Verbindung SSL verwendet; andernfalls kehrt sie zurück. `f`
	3. Installieren Sie die SSL-Erweiterung.
	`create extension sslinfo;`
	`show ssl;`
		DevOps Ingenieur, Migrationsingenieur, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`select ssl_cipher();` Weitere Informationen finden Sie in der Dokumentation zu Amazon RDS.	

Konfigurieren Sie Ihren PostgreSQL-Client für SSL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie einen Client für SSL.	Mithilfe von SSL können Sie den PostgreSQL-Server mit Unterstützung für verschlüsselte Verbindungen starten, die TLS-Protokolle verwenden. Der Server überwacht sowohl Standard- als auch SSL-Verbindungen auf demselben TCP-Port und verhandelt mit jedem Client, der eine Verbindung herstellt, darüber, ob SSL verwendet werden soll. Standardmäßig ist dies eine Client-Option. Wenn Sie den PSQL-Client verwenden: 1. Stellen Sie sicher, dass das Amazon RDS-Zertifikat auf Ihren lokalen Computer geladen wurde.	DevOps Ingenieur, Migrationsingenieur, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	2. Starten Sie eine SSL-Client-Verbindung, indem Sie Folgendes hinzufügen:
	
	`psql postgres -h SOMEHOST.amazonaws.com -p 8192 -U someuser sslmode=verify-full sslrootcert=rds-ssl-ca-cert.pem`
	`select ssl_cipher();`
	
	Für andere PostgreSQL-Clients:
	
	• Ändern Sie den jeweiligen öffentlichen Schlüsselparameter der Anwendung. Dies ist möglicherweise als Option, als Teil Ihrer Verbindungszeichenfolge oder als Eigenschaft auf der Verbindungsseite in GUI-Tools verfügbar.
	
	Sehen Sie sich die folgenden Seiten für diese Clients an:
	
	• pgAdmin-Dokumentation
	• JDBC-Dokumentation	

Fehlerbehebung

Problem	Lösung
Das SSL-Zertifikat kann nicht heruntergeladen werden.	Überprüfen Sie Ihre Verbindung zur Website und versuchen Sie erneut, das Zertifikat auf Ihren lokalen Computer herunterzuladen.

Zugehörige Ressourcen

- Dokumentation zu Amazon RDS for PostgreSQL
- Verwenden von SSL mit einer PostgreSQL-DB-Instance (Amazon RDS-Dokumentation)
- Sichere TCP/IP-Verbindungen mit SSL (PostgreSQL-Dokumentation)
- Verwendung von SSL (JDBC-Dokumentation)

Verschlüsseln Sie eine bestehende Amazon RDS for PostgreSQL PostgreSQL-DB-Instance

Erstellt von Piyush Goyal (AWS), Shobana Raghu (AWS) und Yaser Raja (AWS)

Übersicht

Dieses Muster erklärt, wie eine bestehende Amazon Relational Database Service (Amazon RDS) für PostgreSQL-DB-Instance in der AWS-Cloud mit minimalen Ausfallzeiten verschlüsselt wird. Dieser Prozess funktioniert auch für Amazon RDS for MySQL MySQL-DB-Instances.

Sie können die Verschlüsselung für eine Amazon RDS-DB-Instance aktivieren, wenn Sie sie erstellen, aber nicht, nachdem sie erstellt wurde. Sie können jedoch einer unverschlüsselten DB-Instance Verschlüsselung hinzufügen, indem Sie einen Snapshot Ihrer DB-Instance und anschließend eine verschlüsselte Kopie dieses Snapshots erstellen. Anschließend können Sie eine DB-Instance aus dem verschlüsselten Snapshot wiederherstellen, um eine verschlüsselte Kopie Ihrer ursprünglichen DB-Instance zu erhalten. Wenn Ihr Projekt während dieser Aktivität Ausfallzeiten (zumindest für Schreibtransaktionen) zulässt, ist dies alles, was Sie tun müssen. Wenn die neue, verschlüsselte Kopie der DB-Instance verfügbar ist, können Sie Ihre Anwendungen auf die neue Datenbank verweisen. Wenn Ihr Projekt jedoch keine nennenswerten Ausfallzeiten für diese Aktivität vorsieht, benötigen Sie einen alternativen Ansatz, der dazu beiträgt, die Ausfallzeiten zu minimieren. Dieses Muster verwendet den AWS Database Migration Service (AWS DMS), um die Daten zu migrieren und kontinuierlich zu replizieren, sodass die Umstellung auf die neue, verschlüsselte Datenbank mit minimalen Ausfallzeiten erfolgen kann.

Amazon RDS-verschlüsselte DB-Instances verwenden den Industriestandard-Verschlüsselungsalgorithmus AES-256, um Ihre Daten auf dem Server zu verschlüsseln, der Ihre Amazon RDS-DB-Instances hostet. Nachdem Ihre Daten verschlüsselt wurden, verarbeitet Amazon RDS die Authentifizierung des Zugriffs und die Entschlüsselung Ihrer Daten transparent und mit minimalen Auswirkungen auf die Leistung. Sie müssen Ihre Datenbank-Client-Anwendungen nicht ändern, um Verschlüsselung anzuwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine unverschlüsselte Amazon RDS for PostgreSQL PostgreSQL-DB-Instance

- Erfahrung in der Arbeit mit (Erstellen, Ändern oder Stoppen) von AWS DMS-Aufgaben (siehe Arbeiten mit AWS DMS-Aufgaben in der AWS DMS-Dokumentation)
- Vertrautheit mit dem AWS Key Management Service (AWS KMS) zur Verschlüsselung von Datenbanken (siehe die AWS KMS KMS-Dokumentation)

Einschränkungen

- Sie können die Verschlüsselung für eine Amazon RDS-DB-Instance nur aktivieren, wenn Sie sie erstellen, nicht nachdem die DB-Instance erstellt wurde.
- Daten in Tabellen, die nicht protokolliert wurden, werden nicht mithilfe von Snapshots wiederhergestellt. Weitere Informationen finden Sie unter Bewährte Methoden für die Arbeit mit PostgreSQL.
- Es ist nicht möglich, ein verschlüsseltes Lesereplikat einer unverschlüsselten DB-Instance oder ein unverschlüsseltes Lesereplikat einer verschlüsselten DB-Instance zu erstellen.
- Sie können ein unverschlüsseltes Backup oder einen solchen Snapshot nicht als verschlüsselte DB-Instance wiederherstellen.
- AWS DMS überträgt die Sequenzen nicht automatisch, daher sind zusätzliche Schritte erforderlich, um dies zu handhaben.

Weitere Informationen finden Sie unter Einschränkungen von Amazon RDS-verschlüsselten DB-Instances in der Amazon RDS-Dokumentation.

Architektur

Quellarchitektur

- Unverschlüsselte RDS-DB-Instance

Zielarchitektur

- Verschlüsselte RDS-DB-Instance
  - Die Ziel-RDS-DB-Instance wird erstellt, indem die DB-Snapshot-Kopie der Quell-RDS-DB-Instance wiederhergestellt wird.
  - Ein AWS-KMS-Schlüssel wird für die Verschlüsselung bei der Wiederherstellung des Snapshots verwendet.
  - Eine AWS DMS-Replikationsaufgabe wird verwendet, um die Daten zu migrieren.

Tools

Tools, die zur Aktivierung der Verschlüsselung verwendet werden:

- AWS-KMS-Schlüssel für die Verschlüsselung — Wenn Sie eine verschlüsselte DB-Instance erstellen, können Sie einen vom Kunden verwalteten Schlüssel oder den von AWS verwalteten Schlüssel für Amazon RDS wählen, um Ihre DB-Instance zu verschlüsseln. Wenn Sie die Schlüssel-ID für einen vom Kunden verwalteten Schlüssel nicht angeben, verwendet Amazon RDS den von AWS verwalteten Schlüssel für Ihre neue DB-Instance. Amazon RDS erstellt einen AWS-verwalteten Schlüssel für Amazon RDS für Ihr AWS-Konto. Ihr AWS-Konto hat für jede AWS-Region einen anderen AWS-verwalteten Schlüssel für Amazon RDS. Weitere Informationen zur Verwendung von KMS-Schlüsseln für die Amazon RDS-Verschlüsselung finden Sie unter Amazon RDS-Ressourcen verschlüsseln.

Tools, die für die laufende Replikation verwendet werden:

- AWS DMS — Sie können den AWS Database Migration Service (AWS DMS) verwenden, um Änderungen von der Quell-DB in die Ziel-DB zu replizieren. Es ist wichtig, die Quell- und Ziel-DB synchron zu halten, um Ausfallzeiten auf ein Minimum zu reduzieren. Informationen zur Einrichtung von AWS DMS und zur Erstellung von Aufgaben finden Sie in der AWS DMS-Dokumentation.

Epen

Erstellen Sie einen Snapshot der Quell-DB-Instance und verschlüsseln Sie ihn

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Details für die Quell-PostgreSQL-DB-Instance.	Wählen Sie in der Amazon RDS-Konsole die Quell-PostgreSQL-DB-Instance aus. Stellen Sie auf der Registerkarte Konfiguration sicher, dass die Verschlüsselung für die Instance nicht aktiviert ist. Eine Bildschirmdarstell	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ung finden Sie im Abschnitt Zusätzliche Informationen.	
Erstellen Sie den DB-Snapsh ot.	Erstellen Sie einen DB-Snapshot der Instance, die Sie verschlüsseln möchten. Wie lange es dauert, einen Snapshot zu erstellen, hängt von der Größe Ihrer Datenbank ab. Anweisung en finden Sie unter Erstellen eines DB-Snapshots in der Amazon RDS-Dokumentation.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verschlüsseln Sie den Snapshot.	Wählen Sie im Navigatio nsbereich der Amazon RDS-Konsole Snapshots und wählen Sie den DB-Snapsh ot aus, den Sie erstellt haben. Wählen Sie für Actions (Aktionen) die Option Copy Snapshot (Snapshot kopieren) . Geben Sie die AWS-Zielr egion und den Namen der DB-Snapshot-Kopie in die entsprechenden Felder ein. Wählen Sie das Kontrollk ästchen Verschlüsselung aktivieren aus. Geben Sie für Master Key (Mastersc hlüssel) den Bezeichner des zum Verschlüsseln der DB-Snapshot-Kopie zu verwenden den KMS-Schlüssel an. Wählen Sie Copy Snapshot (Snapshot kopieren) aus. Weitere Informationen finden Sie unter Kopieren eines Snapshots in der Amazon RDS-Dokumentation.	DBA

Bereiten Sie die Ziel-DB-Instance vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den DB-Snapshot wieder her.	Wählen Sie auf der Amazon RDS-Konsole Snapshots aus. Wählen Sie den verschlüs	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	selten Snapshot aus, den Sie erstellt haben. Wählen Sie unter Actions (Aktionen) die Option Restore Snapshot (Snapshot wiederherstellen). Geben Sie für DB Instance Identifier einen eindeutigen Namen für die neue DB-Instance ein. Überprüfen Sie die Instance-Details und wählen Sie dann Restore DB Instance aus. Aus Ihrem Snapshot wird eine neue, verschlüsselte DB-Instance erstellt. Weitere Informationen finden Sie unter Wiederherstellen aus einem DB-Snapshot in der Amazon RDS-Dokumentation.	
Migrieren Sie Daten mithilfe von AWS DMS.	Erstellen Sie auf der AWS DMS-Konsole eine AWS DMS-Aufgabe. Wählen Sie als Migrationstyp die Option Bestehende Daten migrieren und laufende Änderungen replizieren aus. Wählen Sie in den Aufgabeneinstellungen für Target-Tabellenvorbereitungsmodus die Option Truncate aus. Weitere Informationen finden Sie in der AWS DMS-Dokumentation unter Aufgabe erstellen.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie die Datenvalidierung.	Wählen Sie in den Aufgabeneinstellungen die Option Validierung aktivieren aus. Auf diese Weise können Sie die Quelldaten mit den Zieldaten vergleichen, um sicherzustellen, dass die Daten korrekt migriert wurden.	DBA
Deaktivieren Sie Einschränkungen für die Ziel-DB-Instance.	Deaktivieren Sie alle Trigger und Fremdschlüsseleinschränkungen auf der Ziel-DB-Instance und starten Sie dann die AWS DMS-Aufgabe. Weitere Informationen zur Deaktivierung von Triggern und Fremdschlüsseleinschränkungen finden Sie in der AWS DMS-Dokumentation.	DBA
Daten verifizieren.	Nachdem der vollständige Ladevorgang abgeschlossen ist, überprüfen Sie die Daten auf der Ziel-DB-Instance, um festzustellen, ob sie mit den Quelldaten übereinstimmen. Weitere Informationen finden Sie unter AWS DMS-Datenvalidierung in der AWS DMS-Dokumentation.	DBA

Wechseln Sie zur Ziel-DB-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beenden Sie Schreibvorgänge auf der Quell-DB-Instance.	Stoppen Sie die Schreibvorgänge auf der Quell-DB-Instance, sodass die Ausfallzeit der Anwendung beginnen kann. Stellen Sie sicher, dass AWS DMS die Replikation für die Daten in der Pipeline abgeschlossen hat. Aktivieren Sie Trigger und Fremdschlüssel auf der Ziel-DB-Instance.	DBA
Datenbanksequenzen aktualisieren	Wenn die Quelldatenbank Sequenznummern enthält, überprüfen und aktualisieren Sie die Sequenzen in der Zieldatenbank.	DBA
Konfigurieren Sie den Anwendungsendpunkt.	Konfigurieren Sie Ihre Anwendungsverbindungen für die Verwendung der neuen Amazon RDS-DB-Instance-Endpunkte. Die DB-Instance ist jetzt verschlüsselt.	DBA, Besitzer der Anwendung

Zugehörige Ressourcen

- Eine AWS-DMS-Aufgabe erstellen
- Überwachung von Replikationsaufgaben mit Amazon CloudWatch
- Überwachung von AWS DMS-Aufgaben
- Aktualisierung des Amazon RDS-Verschlüsselungsschlüssels

Zusätzliche Informationen

Überprüfung der Verschlüsselung für die Quell-PostgreSQL-DB-Instance:

Zusätzliche Hinweise zu diesem Muster:

- Aktivieren Sie die Replikation auf PostgreSQL, indem Sie den `rds.logical_replication` Parameter auf 1 setzen.

Wichtiger Hinweis: In Replikationsslots werden die Write-Ahead-Log-Dateien (WAL) aufbewahrt, bis die Dateien extern verwendet werden, z. B. durch `pg_recvlogical` ETL-Jobs (Extrahieren, Transformieren und Laden) oder durch AWS DMS. Wenn Sie den `rds.logical_replication` Parameterwert auf 1 setzen, legt AWS DMS die `max_connections` Parameter`wal_level`, `max_wal_sendersmax_replication_slots`, und fest. Wenn logische Replikationssteckplätze vorhanden sind, es aber keinen Verbraucher für die im Replikationssteckplatz gespeicherten WAL-Dateien gibt, kann es zu einem Anstieg der Festplattennutzung im Transaktionsprotokoll und zu einer ständigen Verringerung des freien Speicherplatzes kommen. Weitere Informationen und Schritte zur Behebung dieses Problems finden Sie im Artikel Wie kann ich feststellen, was die Ursache für den Fehler „Kein Speicherplatz auf dem Gerät übrig“ oder "DiskFull" in Amazon RDS for PostgreSQL ist? im AWS Support Knowledge Center.

- Alle Schemaänderungen, die Sie nach der Erstellung des DB-Snapshots an der Quell-DB-Instance vornehmen, sind in der Ziel-DB-Instance nicht vorhanden.
- Nachdem Sie eine verschlüsselte DB-Instance erstellt haben, können Sie den von dieser DB-Instance verwendeten KMS-Schlüssel nicht ändern. Stellen Sie sicher, dass Sie Ihre KMS-Schlüsselanforderungen ermitteln, bevor Sie Ihre verschlüsselte DB-Instance erstellen.
- Sie müssen Trigger und Fremdschlüssel auf der Ziel-DB-Instance deaktivieren, bevor Sie die AWS DMS-Aufgabe ausführen. Sie können diese wieder aktivieren, wenn die Aufgabe abgeschlossen ist.

Automatisches Tagging von Amazon RDS-Datenbanken beim Start erzwingen

Erstellt von Susanne Kangnoh (AWS) und Archit Mathur (AWS)

Übersicht

Amazon Relational Database Service (Amazon RDS) ist ein Webservice, der die Einrichtung, den Betrieb und die Skalierung einer relationalen Datenbank in der Amazon Web Services (AWS) Cloud erleichtert. Dieser Service bietet kostengünstige und anpassbare Kapazität für eine Branchenstandards entsprechende relationale Datenbank sowie die Verwaltung gängiger Datenbankaufgaben.

Sie können Tagging verwenden, um Ihre AWS-Ressourcen auf unterschiedliche Weise zu kategorisieren. Relationales Datenbank-Tagging ist nützlich, wenn Sie viele Ressourcen in Ihrem Konto haben und Sie anhand der Tags schnell eine bestimmte Ressource identifizieren möchten. Sie können Amazon RDS-Tags verwenden, um Ihren RDS-DB-Instances benutzerdefinierte Metadaten hinzuzufügen. Ein Tag besteht aus einem benutzerdefinierten Schlüssel und Wert. Wir empfehlen Ihnen, einen konsistenten Satz von Stichwörtern zu erstellen, um die Anforderungen Ihrer Organisation zu erfüllen.

Dieses Muster bietet eine CloudFormation AWS-Vorlage, mit der Sie RDS-DB-Instances überwachen und kennzeichnen können. Die Vorlage erstellt ein Amazon CloudWatch Events-Ereignis, das nach dem AWS CloudTrail DBInstanceCreate-Ereignis Ausschau hält. (CloudTrail erfasst API-Aufrufe für Amazon RDS als Ereignisse.) Wenn es dieses Ereignis erkennt, ruft es eine AWS-Lambda-Funktion auf, die automatisch von Ihnen definierte Tag-Schlüssel und -Werte anwendet. Die Vorlage sendet auch eine Benachrichtigung, dass die Instance mithilfe von Amazon Simple Notification Service (Amazon SNS) markiert wurde.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket zum Hochladen des Lambda-Codes.
- Eine E-Mail-Adresse, an die Sie Tagging-Benachrichtigungen erhalten möchten.

Einschränkungen

- Die Lösung unterstützt CloudTrail Create DBInstance Events. Es werden keine Benachrichtigungen für andere Ereignisse erstellt.

Architektur

Workflow-Architektur

Automatisierung und Skalierung

- Sie können die CloudFormation AWS-Vorlage mehrfach für verschiedene AWS-Regionen und Konten verwenden. Sie müssen die Vorlage in jeder Region oder jedem Konto nur einmal ausführen.

Tools

AWS-Services

- AWS CloudTrail — AWS CloudTrail ist ein AWS-Service, der Sie bei der Steuerung, Einhaltung von Vorschriften sowie der Betriebs- und Risikoprüfung Ihres AWS-Kontos unterstützt. Aktionen, die von einem Benutzer, einer Rolle oder einem AWS-Service ausgeführt werden, werden als Ereignisse in aufgezeichnet CloudTrail.
- Amazon CloudWatch Events — Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit. CloudWatch Events wird sofort auf betriebliche Änderungen aufmerksam und ergreift bei Bedarf Korrekturmaßnahmen, indem es Nachrichten sendet, um auf die Umgebung zu reagieren, Funktionen aktiviert, Änderungen vornimmt und Statusinformationen erfasst.
- AWS Lambda — AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne dass Server bereitgestellt oder verwaltet werden müssen. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice, der für eine Vielzahl von Speicherlösungen verwendet werden kann, darunter Websites, mobile Anwendungen, Backups und Data Lakes.

- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) ist ein Webservice, der es Anwendungen, Endbenutzern und Geräten ermöglicht, sofort Benachrichtigungen aus der Cloud zu senden und zu empfangen.

Code

Dieses Muster beinhaltet einen Anhang mit zwei Dateien:

- `index.zip`ist eine komprimierte Datei, die den Lambda-Code für dieses Muster enthält.
- `rds.yaml`ist eine CloudFormation Vorlage, die den Lambda-Code bereitstellt.

Informationen zur Verwendung dieser Dateien finden Sie im Abschnitt Epics.

Epen

Stellen Sie den Lambda-Code bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Code in einen S3-Bucket hoch.	Erstellen Sie einen neuen S3-Bucket oder verwenden Sie einen vorhandenen S3-Bucket, um die angehängte `index.zip` Datei hochzuladen (Lambda-Code). Dieser Bucket muss sich in derselben AWS-Region befinden wie die Ressourcen (RDS-DB-Instances), die Sie überwachen möchten.	Cloud-Architekt
Stellen Sie die CloudFormation Vorlage bereit.	Öffnen Sie die Cloudformation-Konsole in derselben AWS-Region wie der S3-Bucket und stellen Sie die `rds.yaml` Datei bereit, die im Anhang bereitgestellt wird. Geben Sie im nächsten	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Epic Werte für die Vorlagenp arameter an.	

Vervollständigen Sie die Parameter in der CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den S3-Bucket-Namen an.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epic erstellt oder ausgewählt haben. Dieser S3-Bucket enthält die ZIP-Datei für den Lambda-Code und muss sich in derselben AWS-Region befinden wie die CloudFormation Vorlage und die RDS-DB-Instances, die Sie überwachen möchten.	Cloud-Architekt
Geben Sie den S3-Schlüssel an.	Geben Sie den Speicherort der Lambda-Code-ZIP-Datei in Ihrem S3-Bucket an, ohne vorangestellte Schrägstriche (z. B. `index.zip` oder). `controls/index.zip`	Cloud-Architekt
Geben Sie eine E-Mail-Ad resse an.	Geben Sie eine aktive E-Mail-Adresse an, unter der Sie Benachrichtigungen über Verstöße erhalten möchten.	Cloud-Architekt
Geben Sie eine Protokoll ierungsebene an.	Geben Sie die Protokoll ierungsebene und die Ausführlichkeit an. `Info`bezeichnet detaillie	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	rte Informationsmeldungen über den Fortschritt der Anwendung und sollte nur zum Debuggen verwendet werden. `Error`bezeichne t Fehlerereignisse, die es der Anwendung dennoch ermöglichen könnten, weiter zu laufen. `Warning`bezeichnet potenziell schädliche Situation en.	
Geben Sie die Tag-Schlüssel und Werte für Ihre RDS-DB-In stances ein.	Geben Sie die erforderlichen Tag-Schlüssel und -Werte ein, die Sie automatisch auf die RDS-Instance anwenden möchten. Weitere Informati onen finden Sie unter Tagging Amazon RDS-Ressourcen in der AWS-Dokumentation.	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das E-Mail-Ab onnement.	Wenn die CloudFormation Vorlage erfolgreich bereitges tellt wurde, sendet sie eine Abonnement-E-Mail-Nachricht an die von Ihnen angegebene E-Mail-Adresse. Um Benachric htigungen zu erhalten, wenn Ihre Instances markiert	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wurden, müssen Sie dieses E-Mail-Abonnement bestätigen.	

Zugehörige Ressourcen

- Einen Bucket erstellen (Amazon S3 S3-Dokumentation)
- Markieren von Amazon RDS-Ressourcen (Amazon Aurora Aurora-Dokumentation)
- Objekte hochladen (Amazon S3 S3-Dokumentation)
- Erstellen einer CloudWatch Ereignisregel, die bei einem AWS-API-Aufruf mithilfe von AWS ausgelöst wird CloudTrail (CloudWatch Amazon-Dokumentation)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Schätzen Sie die Kosten einer DynamoDB-Tabelle für On-Demand-Kapazität

Erstellt von Moinul Al-Mamun (AWS)

Übersicht

Amazon DynamoDB ist eine NoSQL-Transaktionsdatenbank, die selbst im Petabyte-Bereich Latenz im einstelligen Millisekundenbereich bietet. Dieses serverlose Angebot von Amazon Web Services (AWS) erfreut sich aufgrund seiner gleichbleibenden Leistung und Skalierbarkeit immer größerer Beliebtheit. Sie müssen die zugrunde liegende Infrastruktur nicht bereitstellen. Ihre einzelne Tabelle kann bis zu Petabyte groß werden.

Im On-Demand-Kapazitätsmodus zahlen Sie pro Anfrage für die Lese- und Schreibvorgänge, die Ihre Anwendung an den Tabellen durchführt. Die AWS-Gebühren basieren auf den kumulierten Leseanforderungseinheiten (RRUs) und Schreibanforderungseinheiten (WRUs) in einem Monat. DynamoDB überwacht den ganzen Monat über kontinuierlich die Größe Ihrer Tabelle, um Ihre Speichergebühren zu ermitteln. Es unterstützt kontinuierliches Backup mit point-in-time-recovery (PITR). DynamoDB überwacht den ganzen Monat über kontinuierlich die Größe Ihrer PITR-fähigen Tabellen, um Ihre Backup-Gebühren zu ermitteln.

Um die DynamoDB-Kosten für ein Projekt abzuschätzen, ist es wichtig zu berechnen, wie viel RRU, WRU und Speicherplatz in den verschiedenen Phasen Ihres Produktlebenszyklus verbraucht werden. Für eine grobe Kostenschätzung können Sie den AWS-Preisrechner verwenden. Sie müssen jedoch eine ungefähre Anzahl von RRUs WRUs, und Speicheranforderungen für Ihre Tabelle angeben. Zu Beginn des Projekts kann es schwierig sein, diese abzuschätzen. Der AWS-Preisrechner berücksichtigt weder die Datenwachstumsrate noch die Artikelgröße und berücksichtigt auch nicht die Anzahl der Lese- und Schreibvorgänge für die Basistabelle und die globalen Sekundärindizes (GSIs) getrennt. Um den AWS-Preisrechner verwenden zu können, müssen Sie all diese Aspekte abschätzen, um von ungefähren Zahlen für WRU, RRU und Speichergröße auszugehen, um Ihre Kostenschätzung zu erhalten.

Dieses Muster bietet einen Mechanismus und eine wiederverwendbare Microsoft Excel-Vorlage zur Schätzung grundlegender DynamoDB-Kostenfaktoren wie Schreib-, Lese-, Speicher-, Sicherungs- und Wiederherstellungskosten für den On-Demand-Kapazitätsmodus. Er ist detaillierter als der AWS-Preisrechner und berücksichtigt die Basistabelle und die GSIs Anforderungen unabhängig voneinander. Es berücksichtigt auch die monatliche Wachstumsrate der Artikeldaten und prognostiziert die Kosten für drei Jahre.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Grundkenntnisse in DynamoDB und DynamoDB-Datenmodelldesign
- Grundkenntnisse zu DynamoDB-Preisen, WRU, RRU, Speicher sowie Backup und Recovery (weitere Informationen finden Sie unter Preise für On-Demand-Kapazität)
- Kenntnis Ihrer Daten, Ihres Datenmodells und Ihrer Elementgröße in DynamoDB
- Kenntnisse von DynamoDB GSIs

Einschränkungen

- Die Vorlage bietet Ihnen eine ungefähre Berechnung, ist jedoch nicht für alle Konfigurationen geeignet. Um eine genauere Schätzung zu erhalten, müssen Sie die individuelle Artikelgröße für jeden Artikel in der Basistabelle und messen GSIs.
- Für eine genauere Schätzung müssen Sie die erwartete Anzahl von Schreibvorgängen (Einfügen, Aktualisieren und Löschen) und Lesevorgängen für jedes Element in einem durchschnittlichen Monat berücksichtigen.
- Dieses Muster ermöglicht es, nur die Schreib-, Lese-, Speicher-, Sicherungs- und Wiederherstellungskosten für die nächsten Jahre auf der Grundlage fester Annahmen zum Datenwachstum zu schätzen.

Tools

AWS-Services

- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.

Andere Tools

- Der AWS-Preisrechner ist ein webbasiertes Planungstool, mit dem Sie Schätzungen für Ihre AWS-Anwendungsfälle erstellen können.

Bewährte Methoden

Um die Kosten niedrig zu halten, sollten Sie die folgenden Best Practices für den DynamoDB-Entwurf berücksichtigen.

- Entwerfen von Partitionsschlüsseln – Verwenden Sie einen Partitionsschlüssel mit hoher Kardinalität, um die Last gleichmäßig zu verteilen.
- Entwurfsmuster für Adjazenzlisten — Verwenden Sie dieses Entwurfsmuster für Verwaltung one-to-many und Beziehungen. many-to-many
- Sparse-Index — Verwenden Sie den Sparse-Index für Ihren. GSIs Wenn Sie einen GSI erstellen, geben Sie einen Partitionsschlüssel und optional einen Sortierschlüssel an. Nur Elemente in der Basistabelle, die einen entsprechenden GSI-Partitionsschlüssel enthalten, werden im Sparse-Index angezeigt. Dies hilft, kleiner zu bleiben GSIs .
- Überladen von Indizes – Verwenden Sie dieselbe GSI für die Indizierung verschiedener Arten von Elementen.
- GSI Write-Sharding— Sharden Sie mit Bedacht, um Daten auf die Partitionen zu verteilen und so effiziente und schnellere Abfragen zu ermöglichen.
- Große Gegenstände – Speichern Sie nur Metadaten in der Tabelle, speichern Sie den Blob in Amazon S3 und behalten Sie die Referenz in DynamoDB bei. Teilen Sie große Elemente in mehrere Elemente auf und indizieren Sie sie effizient mithilfe von Sortierschlüsseln.

Weitere bewährte Methoden finden Sie im Leitfaden für Entwickler von Amazon DynamoDB.

Epen

Extrahieren Sie Artikelinformationen aus Ihrem DynamoDB-Datenmodell

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Artikelgröße ermitteln.	1. Prüfen Sie, wie viele verschiedene Artikelty pen Sie in Ihrer Tabelle speichern werden. 2. Um die Größe jedes Elements in Kilobyte zu berechnen, fügen Sie die	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Schlüssel- und Wertgröße jedes Attributs hinzu. 3. Berechnet die Elementgröße für eine Basistabelle und für jeden globalen Index.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Schätzen Sie die Schreibkosten ab.	Um die Schreibkosten im On-Demand-Kapazitätsmodus zu schätzen, müssen Sie zunächst messen, wie viele Kapazitäten in einem Monat verbraucht WRUs werden. Dazu müssen Sie die folgenden Faktoren berücksichtigen:
	• Anzahl der Erstellungs-, Aktualisierungs- und Löschvorgänge für jedes Element in einem Monat.
	• Anzahl der verfügbaren GSIs. Betrachten Sie jeden Index unabhängig voneinander.
	  • Durchschnittliche Größe eines Indexelements
	  • Anzahl der Synchronisationszeiten für einen Index
	• Wie viele neue Dinge (z. B. Komponenten oder Produkte) werden der Tabelle jeden Monat hinzugefügt? Die Anzahl der hinzugefügten Dinge kann von Monat zu Monat unterschiedlich sein, aber Sie können auf der Grundlage Ihrer Geschäftsszenarien von
		Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	einer durchschnittlichen Wachstumsrate ausgehen. Weitere Informationen finden Sie im Abschnitt Zusätzliche Informationen.	
Schätzen Sie die Lesekosten ab.	Um die Lesekosten im On-Demand-Modus zu schätzen, müssen Sie zunächst messen, wie viele Lesekosten in einem Monat verbraucht RRUs werden. Dazu müssen Sie die folgenden Faktoren berücksichtigen: • Anzahl der verfügbaren GSIs. Betrachten Sie jeden Index unabhängig voneinander. • Durchschnittliche Größe eines Indexelements • Durchschnittliche Anzahl von Lesevorgängen pro Produkt und Monat. • Anzahl der insgesamt verfügbaren Dinge (Komponenten oder Produkte) in der DynamoDB-Tabelle.	Dateningenieur, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schätzen Sie die Speicherg röße und die Kosten ab.	Schätzen Sie zunächst den durchschnittlichen monatlich en Lagerbedarf auf der Grundlage Ihrer Artikelgröße in der Tabelle. Berechnen Sie dann die Speicherkosten, indem Sie die Speichergröße mit dem Speicherpreis pro GB für Ihre AWS-Region multipliz ieren. Wenn Sie bereits Daten zur Schätzung der Schreibkosten eingegeben haben, müssen Sie diese zur Berechnung der Speichergröße nicht erneut eingeben. Andernfalls müssen Sie bei der Schätzung der Speichergröße die folgenden Faktoren berücksichtigen: • Anzahl der Datenelemente in einem Modul (Produkt) , basierend auf Ihrem Tabellenentwurf. • Durchschnittliche Elementgr öße in Kilobyte. • Anzahl der verfügbar en. GSIs Betrachten Sie jeden Index unabhängig voneinander. • Durchschnittliche Größe eines Indexelements	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wie viele neue Produkte werden jeden Monat in die Tabelle aufgenomm en? Die Anzahl der neuen Produkte kann von Monat zu Monat unterschiedlich sein, aber Sie können auf der Grundlage Ihrer Geschäftsszenarien von einer durchschnittlichen Wachstumsrate ausgehen. In diesem Beispiel werden durchschnittlich 10 Millionen neue Produkte pro Monat verwendet.	

Geben Sie die Artikel- und Objektinformationen in die Excel-Vorlage ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Excel-Vorlage aus dem Bereich Anlagen herunter und passen Sie sie an Ihre Anwendungsfalltabelle an.	1. Laden Sie die Excel-Vor lage herunter. 2. Passen Sie das Geschäfts modul und GSIs, basierend auf Ihrem Tabellendesign, an.	Dateningenieur
Geben Sie Informationen in die Excel-Vorlage ein.	1. Aktualisieren Sie die Artikelinformationen im Blatt. Daten nur in orangefarbenen Zellen aktualisieren. 2. Passen Sie die Objektnum mern an: Wie viel könnte	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Tabelle jeden Monat hinzugefügt werden? 3. Aktualisieren Sie die WRU- und RRU-Preise pro Million für Ihre AWS-Region. 4. Aktualisieren Sie die Speicher- und Backup-Preise pro GB-Monat für Ihre AWS-Region. 5. Aktualisieren Sie den Wiederherstellungspreis pro GB für Ihre AWS-Region. In der Vorlage gibt es drei Elemente oder Entitäten: Informationen, Metadaten und Beziehung. Es gibt zwei GSIs. Wenn Sie für Ihren Anwendungsfall mehr Elemente benötigen, erstellen Sie neue Zeilen. Wenn Sie mehr benötigen GSIs, kopieren Sie einen vorhandenen GSI-Block und fügen Sie ihn ein, um so viele GSI-Blöcke zu erstellen, wie Sie benötigen. Passen Sie dann die Berechnungen der Spalten SUM und TOTAL an.	

Zugehörige Ressourcen

Referenzen

- Amazon DynamoDB DynamoDB-Preise für On-Demand-Kapazität
- AWS-Preisrechner für DynamoDB
- Bewährte Methoden für Design und Architektur mit DynamoDB
- Erste Schritte mit DynamoDB

Anleitungen und Muster

- Modellieren von Daten mit Amazon DynamoDB
- Schätzung der Speicherkosten für eine Amazon DynamoDB-Tabelle

Zusätzliche Informationen

Schreiben Sie ein Beispiel für eine Kostenberechnung

Das DynamoDB-Datenmodelldesign zeigt drei Elemente für ein Produkt und eine durchschnittliche Artikelgröße von 4 KB. Wenn Sie der DynamoDB-Basistabelle ein neues Produkt hinzufügen, verbraucht es die Anzahl der Elemente * (Artikelgröße/1 KB Schreibeinheit) = 3 * (4/1) = 12 WRU. In diesem Beispiel verbraucht das Produkt beim Schreiben von 1 KB 1 WRU.

Lesen Sie das Beispiel für die Kostenberechnung

Um die RRU-Schätzung zu erhalten, berücksichtigen Sie den Durchschnitt, wie oft jeder Artikel in einem Monat gelesen wird. Beispielsweise wird das Informationselement im Durchschnitt zehnmal pro Monat gelesen, und das Metadatenelement wird zweimal gelesen und das Beziehungselement wird fünfmal gelesen. In der Beispielvorlage gilt: Gesamt-RRU für alle Komponenten = Anzahl der jeden Monat neu erstellten Komponenten * RRU pro Komponente pro Monat = 10 Millionen * 17 RRU = 170 Millionen RRU pro Monat.

Jeden Monat werden neue Dinge (Komponenten oder Produkte) hinzugefügt, und die Gesamtzahl der Produkte wird im Laufe der Zeit zunehmen. Daher werden auch die RRU-Anforderungen im Laufe der Zeit steigen.

- Im ersten Monat RRU wird der Verbrauch 170 Millionen betragen.
- Im zweiten Monat wird der RRU-Verbrauch 2 * 170 Millionen = 340 Millionen betragen.
- Im dritten Monat wird der RRU-Verbrauch 3 × 170 Millionen = 510 Millionen betragen.

Die folgende Grafik zeigt die monatlichen RRU-Verbrauchs- und Kostenprognosen.

Beachten Sie, dass die Preise in der Grafik nur zur Veranschaulichung dienen. Um genaue Prognosen für Ihren Anwendungsfall zu erstellen, besuchen Sie die AWS-Preisseite und verwenden Sie diese Preise in der Excel-Tabelle.

Beispiele für die Berechnung der Kosten für Speicherung, Sicherung und Wiederherstellung

DynamoDB-Speicher, Backup und Wiederherstellung sind alle miteinander verbunden. Das Backup ist direkt mit dem Speicher verbunden, und die Wiederherstellung ist direkt mit der Größe des Backups verbunden. Mit zunehmender Tabellengröße steigen die entsprechenden Speicher-, Sicherungs- und Wiederherstellungskosten proportional.

Speichergröße und Kosten

Die Speicherkosten werden im Laufe der Zeit entsprechend Ihrer Datenwachstumsrate steigen. Nehmen wir beispielsweise an, dass die durchschnittliche Größe einer Komponente oder eines Produkts in der Basistabelle 11 KB GSIs beträgt und dass Ihrer Datenbanktabelle jeden Monat 10 Millionen neue Produkte hinzugefügt werden. In diesem Fall wächst die Größe Ihrer DynamoDB-Tabelle (11 KB x 10 Millionen) /1024/1024 = 105 GB pro Monat. Im ersten Monat beträgt Ihre Tabellenspeichergröße 105 GB, im zweiten Monat 105 + 105 = 210 usw. GBs

- Im ersten Monat betragen die Speicherkosten 105 GB* Speicherpreis pro GB für Ihre AWS-Region.
- Für den zweiten Monat belaufen sich die Speicherkosten auf 210 GB* Speicherpreis pro GB für Ihre Region.
- Für den dritten Monat belaufen sich die Speicherkosten auf 315 GB* Speicherpreis pro GB für Ihre Region.

Informationen zur Speichergröße und zu den Kosten für die nächsten drei Jahre finden Sie im Abschnitt Speichergröße und Prognose.

Kosten für Backup

Die Backup-Kosten werden im Laufe der Zeit entsprechend Ihrer Datenwachstumsrate steigen. Wenn Sie Continuous Backup mit point-in-time-recovery (PITR) aktivieren, basieren die Gebühren für kontinuierliches Backup auf dem durchschnittlichen Speichervolumen pro Monat. In einem Kalendermonat würde die durchschnittliche Backup-Größe der Größe Ihres Tabellenspeichers entsprechen, obwohl die tatsächliche Größe etwas anders sein könnte. Da jeden Monat neue

Produkte hinzugefügt werden, werden die Gesamtspeichergröße und die Backup-Größe im Laufe der Zeit zunehmen. Beispielsweise könnte die durchschnittliche Backup-Größe von 105 GB für den ersten Monat auf 210 GB für den zweiten Monat ansteigen.

- Im ersten Monat belaufen sich die Backup-Kosten auf 105 GB-Monat* Preis für kontinuierliches Backup pro GB für Ihre AWS-Region.
- Im zweiten Monat belaufen sich die Backup-Kosten auf 210 GB-Monat* Preis für kontinuierliches Backup pro GB für Ihre Region.
- Im dritten Monat belaufen sich die Backup-Kosten auf 315 GB pro Monat * Preis für kontinuierliches Backup pro GB für Ihre Region.
- und so weiter

Die Backup-Kosten sind in der Grafik im Abschnitt Speichergröße und Kostenprognose enthalten.

Kosten für die Wiederherstellung

Wenn Sie ein kontinuierliches Backup mit aktiviertem PITR erstellen, richten sich die Gebühren für den Wiederherstellungsvorgang nach dem Umfang der Wiederherstellung. Bei jeder Wiederherstellung zahlen Sie auf der Grundlage von Gigabyte wiederhergestellter Daten. Wenn Ihre Tabelle groß ist und Sie die Wiederherstellung mehrmals im Monat durchführen, ist dies kostspielig.

Um die Wiederherstellungskosten abzuschätzen, wird in diesem Beispiel davon ausgegangen, dass Sie einmal pro Monat am Monatsende eine PITR-Wiederherstellung durchführen. In dem Beispiel wird die durchschnittliche monatliche Backup-Größe als Größe der Wiederherstellungsdaten für diesen Monat verwendet. Für den ersten Monat beträgt die durchschnittliche Backup-Größe 105 GB, und für die Wiederherstellung am Monatsende würde die Größe der Wiederherstellungsdaten 105 GB betragen. Für den zweiten Monat wären es 210 GBs und so weiter.

Die Wiederherstellungskosten werden im Laufe der Zeit entsprechend Ihrer Datenwachstumsrate steigen.

- Im ersten Monat betragen die Wiederherstellungskosten 105 GB* Wiederherstellungspreis pro GB für Ihre AWS-Region.
- Im zweiten Monat belaufen sich die Wiederherstellungskosten auf 210 GB* Wiederherstellungspreis pro GB für Ihre Region.
- Im dritten Monat belaufen sich die Wiederherstellungskosten auf 315 GB* Wiederherstellungspreis pro GB für Ihre Region.

Weitere Informationen finden Sie auf der Registerkarte Speicher, Sicherung und Wiederherstellung in der Excel-Vorlage und in der Grafik im folgenden Abschnitt.

Prognose der Speichergröße und der Kosten

In der Vorlage wird die tatsächliche fakturierbare Speichergröße berechnet, indem das kostenlose Kontingent 25 GB pro Monat für die Standard-Tabellenklasse subtrahiert wird. In dem Blatt erhalten Sie ein Prognosediagramm, das in monatliche Werte unterteilt ist.

Das folgende Beispieldiagramm prognostiziert die monatliche Speichergröße in GB, die fakturierbaren Speicherkosten, die Kosten für On-Demand-Backups und die Wiederherstellungskosten für die nächsten 36 Kalendermonate. Alle Kosten sind in USD angegeben. Aus der Grafik wird deutlich, dass die Speicher-, Backup- und Wiederherstellungskosten proportional zur Speichergröße steigen.

Beachten Sie, dass die in der Grafik verwendeten Preise nur zur Veranschaulichung dienen. Um genaue Preise für Ihren Anwendungsfall zu erstellen, besuchen Sie die AWS-Preisseite und verwenden Sie diese Preise in der Excel-Vorlage.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Schätzung der Speicherkosten für eine Amazon DynamoDB-Tabelle

Erstellt von Moinul Al-Mamun (AWS)

Übersicht

Amazon DynamoDB ist eine NoSQL-Transaktionsdatenbank, die selbst im Petabyte-Bereich Latenz im einstelligen Millisekundenbereich bietet. Dieses beliebte serverlose Angebot von bietet konsistente Leistung und Skalierbarkeit. AWS Sie müssen keinen Speicher bereitstellen, und Ihre einzelne Tabelle kann bis zu Petabyte anwachsen.

DynamoDB überwacht den ganzen Monat über kontinuierlich die Größe Ihrer Tabelle, um Ihre Speichergebühren zu ermitteln. AWS berechnet Ihnen dann die durchschnittliche Speichergröße in Gigabyte. Je mehr Ihre Tabelle im Laufe der Zeit wächst, desto stärker steigen Ihre Speicherkosten. Um die Speicherkosten zu berechnen, können Sie den AWS Preisrechner verwenden. Sie müssen jedoch die ungefähre Größe Ihrer Tabelle einschließlich globaler Sekundärindizes (GSIs) angeben, was zu Beginn des Projekts nur schwer abzuschätzen ist. Außerdem berücksichtigt der AWS Preisrechner nicht die Datenwachstumsrate.

Dieses Muster bietet einen Mechanismus und eine wiederverwendbare Microsoft Excel-Vorlage zur Berechnung von DynamoDB-Speichergröße und -kosten. Es berücksichtigt die Speicheranforderungen für die Basistabelle und die GSIs unabhängige Tabelle. Es berechnet die Speichergröße unter Berücksichtigung der Größe Ihrer einzelnen Elemente und der Datenwachstumsrate im Laufe der Zeit.

Um eine Schätzung zu erhalten, fügen Sie zwei Informationen in die Vorlage ein:

- Die Größe der einzelnen Elemente in Kilobyte für die Basistabelle und GSIs
- Wie viele neue Objekte oder Produkte könnten der Tabelle im Durchschnitt in einem Monat hinzugefügt werden (z. B. 10 Millionen)

Die Vorlage generiert ein Diagramm zur Speicher- und Kostenprognose für die nächsten drei Jahre, das im folgenden Beispiel dargestellt wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Grundkenntnisse in DynamoDB, einschließlich DynamoDB-Speicher und Preisgestaltung
- Kenntnis Ihrer Daten, Ihres Datenmodells und Ihrer Elementgröße in DynamoDB
- Kenntnis der globalen Sekundärindizes von DynamoDB () GSIs

Einschränkungen

- Die Vorlage bietet Ihnen eine ungefähre Berechnung, ist jedoch nicht für alle Konfigurationen geeignet. Um eine genauere Schätzung zu erhalten, müssen Sie die individuelle Artikelgröße für jeden Artikel in der Basistabelle und messen GSIs.
- Dieses Muster unterstützt lediglich die Schätzung der Speichergröße und der Kosten für die nächsten Jahre auf der Grundlage fester Annahmen zum Datenwachstum.

Tools

AWS-Services

- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.

Andere Tools

- AWS Pricing Calculator ist ein webbasiertes Planungstool, mit dem Sie Schätzungen für Ihre AWS Anwendungsfälle erstellen können.

Epen

Extrahieren Sie Artikelinformationen aus Ihrem DynamoDB-Datenmodell

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Artikelgröße ermitteln.	1. Bestimmen Sie, wie viele verschiedene Artikelty pen Sie in Ihrer Tabelle speichern möchten. 2. Um die Größe jedes Elements in Kilobyte zu	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	berechnen, addieren Sie die `Value` Größe `Key` und die Größe jedes Attributs. 3. Berechnet die Elementgr öße für eine Basistabelle und für jeden GSI.	
Ermittelt die Anzahl der Objekte, die in einem Monat hinzugefügt wurden.	Schätzen Sie, wie viele Komponenten oder Objekte durchschnittlich in einem Monat zur DynamoDB-Tabelle hinzugefügt werden.	Dateningenieur

Geben Sie die Artikel- und Objektinformationen in die Excel-Vorlage ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Excel-Tabelle herunter und passen Sie sie an.	1. Laden Sie die Excel-Vor lage aus dem angehängten Dokument herunter. 2. Passen Sie das Geschäfts modul und GSIs, basierend auf Ihrem Tabellendesign, an.	Dateningenieur
Geben Sie Informationen in die Excel-Vorlage ein.	1. Aktualisieren Sie die Artikelinformationen im Blatt. 2. Passen Sie die Objektnum mern an: Wie viel könnte der Tabelle jeden Monat hinzugefügt werden? 3. Aktualisieren Sie den Speicherpreis pro GB-	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Monat für Ihren. AWS-Region	

Zugehörige Ressourcen

- Preise für On-Demand-Kapazität für Amazon DynamoDB
- AWS Preisrechner für DynamoDB

Zusätzliche Informationen

Beachten Sie, dass die beigefügte Vorlage nur die Speichergröße und die Kosten für die Standard-Speichertabellenklasse prognostiziert. Auf der Grundlage der Prognose für die Lagerkosten und unter Berücksichtigung der Größe einzelner Artikel und der Wachstumsrate von Produkten oder Objekten können Sie Folgendes abschätzen:

- Kosten für den Datenexport
- Kosten für Backup und Wiederherstellung
- Anforderungen an die Datenspeicherung.

Amazon DynamoDB DynamoDB-Datenspeicherkosten

DynamoDB überwacht kontinuierlich die Größe Ihrer Tabellen, um Ihre Speichergebühren zu ermitteln. DynamoDB misst die Größe Ihrer fakturierbaren Daten, indem es die Rohbytegröße Ihrer Daten zuzüglich eines Speicheraufwands pro Element addiert, der von den von Ihnen aktivierten Funktionen abhängt. Weitere Informationen finden Sie im DynamoDB Developer Guide.

Der Preis für die Datenspeicherung hängt von Ihrer Tabellenklasse ab. Die ersten 25 GB, die jeden Monat gespeichert werden, sind kostenlos, wenn Sie die DynamoDB-Standard-Tabellenklasse verwenden. Weitere Informationen zu den Speicherkosten für die unterschiedlichen AWS-Regionen Tabellenklassen Standard und Standard Infrequent Access finden Sie unter Preise für On-Demand-Kapazität.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Schätzen Sie die Größe der Amazon RDS-Engine für eine Oracle-Datenbank mithilfe von AWR-Berichten

Erstellt von Abhishek Verma (AWS) und Eduardo Valentim (AWS)

Übersicht

Wenn Sie eine Oracle-Datenbank zu Amazon Relational Database Service (Amazon RDS) oder Amazon Aurora migrieren, ist die Berechnung der CPU, des Arbeitsspeichers und der Festplatten-I/O für die Zieldatenbank eine wichtige Anforderung. Sie können die erforderliche Kapazität der Zieldatenbank abschätzen, indem Sie die AWR-Berichte (Oracle Automatic Workload Repository) analysieren. Dieses Muster erklärt, wie AWR-Berichte verwendet werden, um diese Werte zu schätzen.

Die Oracle-Quelldatenbank kann vor Ort sein oder auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance gehostet werden, oder es könnte sich um eine Amazon RDS for Oracle DB-Instance handeln. Die Zieldatenbank kann eine beliebige Amazon RDS- oder Aurora-Datenbank sein.

> **Note**
>
> Kapazitätsschätzungen sind genauer, wenn es sich bei Ihrer Zieldatenbank-Engine um Oracle handelt. Bei anderen Amazon RDS-Datenbanken kann die Engine-Größe aufgrund von Unterschieden in der Datenbankarchitektur variieren.

Wir empfehlen, dass Sie den Leistungstest ausführen, bevor Sie Ihre Oracle-Datenbank migrieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Oracle Database Enterprise Edition-Lizenz und eine Oracle Diagnostics Pack-Lizenz, um AWR-Berichte herunterzuladen.

Produktversionen

- Alle Oracle Database-Editionen für die Versionen 11g (Versionen 11.2.0.3.v1 und höher) und bis zu 12.2 und 18c,19c.
- Dieses Muster gilt nicht für Oracle Engineered Systems oder Oracle Cloud Infrastructure (OCI).

Architektur

Quelltechnologie-Stack

Eine der beiden folgenden Komponenten:

- Eine lokale Oracle-Datenbank
- Eine Oracle-Datenbank auf einer Instanz EC2
- Eine Amazon RDS for Oracle Oracle-DB-Instance

Zieltechnologie-Stack

- Beliebige Amazon RDS- oder Amazon Aurora Aurora-Datenbank

Zielarchitektur

Informationen zum vollständigen Migrationsprozess finden Sie im Muster Migrieren Sie eine Oracle-Datenbank mithilfe von AWS DMS und AWS SCT zu Aurora PostgreSQL.

Automatisierung und Skalierung

Wenn Sie mehrere Oracle-Datenbanken migrieren müssen und zusätzliche Leistungskennzahlen verwenden möchten, können Sie den Prozess automatisieren, indem Sie die im Blogbeitrag Skalierbare Größe von Amazon RDS-Instances auf der Grundlage von Oracle-Leistungskennzahlen anpassen beschriebenen Schritte ausführen.

Tools

- Das Oracle Automatic Workload Repository (AWR) ist ein Repository, das in Oracle-Datenbanken integriert ist. Es sammelt und speichert regelmäßig Systemaktivitäts- und Workload-Daten, die dann vom Automatic Database Diagnostic Monitor (ADDM) analysiert werden. AWR erstellt regelmäßig (standardmäßig alle 60 Minuten) Snapshots der Systemleistungsdaten und speichert die Informationen (standardmäßig bis zu 8 Tage). Sie können AWR-Ansichten und -Berichte verwenden, um diese Daten zu analysieren.

Bewährte Methoden

- Um den Ressourcenbedarf für Ihre Zieldatenbank zu berechnen, können Sie einen einzelnen AWR-Bericht, mehrere AWR-Berichte oder dynamische AWR-Ansichten verwenden. Wir

empfehlen, dass Sie während der Spitzenlastperiode mehrere AWR-Berichte verwenden, um abzuschätzen, welche Ressourcen zur Bewältigung dieser Spitzenlasten erforderlich sind. Darüber hinaus bieten dynamische Ansichten mehr Datenpunkte, mit denen Sie den Ressourcenbedarf genauer berechnen können.

- Sie sollten die IOPS nur für die Datenbank schätzen, die Sie migrieren möchten, nicht für andere Datenbanken und Prozesse, die die Festplatte verwenden.
- Verwenden Sie nicht die Informationen im Abschnitt Load Profile des AWR-Berichts, um zu berechnen, wie viel I/O von der Datenbank verwendet wird. Verwenden Sie stattdessen den Abschnitt I/O-Profil, falls dieser verfügbar ist, oder springen Sie zum Abschnitt Instanzaktivitätsstatistiken und sehen Sie sich die Gesamtwerte für physische Lese- und Schreibvorgänge an.
- Wenn Sie die CPU-Auslastung schätzen, empfehlen wir, die Methode der Datenbankmetriken anstelle von Betriebssystemstatistiken (OS) zu verwenden, da sie auf der CPU basiert, die nur von Datenbanken verwendet wird. (Betriebssystemstatistiken beinhalten auch die CPU-Auslastung durch andere Prozesse.) Sie sollten auch die CPU-bezogenen Empfehlungen im ADDM-Bericht überprüfen, um die Leistung nach der Migration zu verbessern.
- Berücksichtigen Sie bei der Bestimmung des richtigen Instance-Typs die I/O-Durchsatzgrenzen — den Durchsatz von Amazon Elastic Block Store (Amazon EBS) und den Netzwerkdurchsatz — für die jeweilige Instance-Größe.
- Führen Sie vor der Migration den Leistungstest durch, um die Engine-Größe zu überprüfen.

Epen

Erstellen Sie einen AWR-Bericht

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie den AWR-Bericht.	Folgen Sie den Anweisungen in der Oracle-Dokumentation, um den Bericht zu aktivieren.	DBA
Überprüfen Sie die Aufbewahrungsfrist.	Verwenden Sie die folgende Abfrage, um den Aufbewahrungszeitraum des AWR-Berichts zu überprüfen.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`SQL> SELECT snap_interval,retention FROM dba_hist_wr_control;`	
Generieren Sie den Snapshot.	Wenn das AWR-Snapshot-Intervall nicht detailliert genug ist, um die Spitze der Arbeitslast zu erfassen, können Sie den AWR-Bericht manuell generieren. Verwenden Sie die folgende Abfrage, um den manuellen AWR-Snapshot zu generieren. `SQL> EXEC dbms_workload_repository.create_snapshot;`	DBA
Sehen Sie sich die letzten Schnappschüsse an.	Verwenden Sie die folgende Abfrage, um die letzten AWR-Snapshots zu überprüfen. `SQL> SELECT snap_id, to_char(begin_interval_time,'dd/MON/yy hh24:mi') Begin_Interval, to_char(end_interval_time,'dd/MON/yy hh24:mi') End_Interval FROM dba_hist_snapshot ORDER BY 1;`	DBA

Schätzen Sie die Festplatten-I/O-Anforderungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie eine Methode.	IOPS ist das Standardmaß für Eingabe- und Ausgabevorgänge pro Sekunde auf einem Speichergerät und umfasst sowohl Lese- als auch Schreibvorgänge. Wenn Sie eine lokale Datenbank zu AWS migrieren, müssen Sie die maximale Festplatten-I/O ermitteln, die von der Datenbank verwendet wird. Sie können die folgenden Methoden verwenden, um die Festplatten-I/O für Ihre Zieldatenbank abzuschätzen: • Abschnitt „Profil laden“ des AWR-Berichts • Abschnitt „Instanzaktivitätsstatistiken“ des AWR-Berichts (verwenden Sie diesen Abschnitt für Oracle Database 12c oder höher) • Abschnitt „I/O-Profil“ des AWR-Berichts (verwenden Sie diesen Abschnitt für Oracle-Datenbankversionen vor 12c) • AWR-Ansichten	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	In den folgenden Schritten werden diese vier Methoden beschrieben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 1: Verwenden Sie das Lastprofil.	Die folgende Tabelle zeigt ein Beispiel für den Abschnitt „Lastprofil“ des AWR-Berichts. **Important** Für genauere Informationen empfehlen wir, Option 2 (I/O-Profile) oder Option 3 (Instanzaktivitätsstatistiken) anstelle des Lastprofils zu verwenden. Pro Seku / Pro Transon / Pro Führraft / Pro Anruf DB-Zeit (en): 26,6 / 0.2 / 0,00 / 0,02 DB-CPU (n): 18,0 / 0.1 / 0,00 / 0.01 CPU (s) im Hinternd: 0.2 / 0.0 / 0,00 / 0,00	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Redo 2.458 17.09 Größ ,9 e (Byte Logis 3.37 23.4 Lese ,5 (Blöc Ände 21.64 150,5 n block n: Phys 13.57 94,4 sche Lese (Blöc Phys 3.467 24,1 s Schr (Blöc IO- 3.586 24,9 Anfra en leser Schr 574.7 4,0 Sie IO- Anfra en:	

Aufgabe	Beschreibung		Erforderliche Fähigkeiten
	I/O leser (MB)	106,'	0.7
	Schr Sie IO (MB)	27,1	0.2
	IM-Scar Z eilen	0.0	0.0
	Sitzu logis Lese IM:		
	Benu ruft an:	1.24	8,7
	Anal t (SQL	4.62	32,2
	Harte Anal (SQL	8.9	0.1
	SQL- Arbe tsber (MB)	824,9	5,7

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anm 1,7 0.0 en: Führ 136.(950,4 aus (SQL Rollb 22,9 0.2 : Tran 143.8 onen Auf der Grundlage dieser Informationen können Sie den Durchsatz wie folgt berechnen IOPs : IOPS = I/O-Anfragen lesen: + I/O-Anfragen schreiben = 3.586,8 + 574,7 = 4134,5 Durchsatz = Physisches Lesen (Blöcke) + Physisches Schreiben (Blöcke) = 13.575,1 + 3.467,3 = 17.042,4 Da die Blockgröße in Oracle 8 KB beträgt, können Sie den Gesamtdurchsatz wie folgt berechnen: Der Gesamtdurchsatz in MB beträgt 17042,4 * 8 * 1024/ 1024/ 1024 = 133,2 MB	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Warning Verwenden Sie nicht das Lastprofil, um die Instance-Größe zu schätzen. Es ist nicht so präzise wie Statistiken zur Instanzaktivität oder I/O-Profile.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 2: Verwenden Sie Statistiken zur Instanzaktivität.	Wenn Sie eine Oracle-Datenbankversion vor 12c verwenden, können Sie den Abschnitt Instance Activity Stats des AWR-Berichts verwenden, um IOPS und Durchsatz zu schätzen. Die folgende Tabelle zeigt ein Beispiel für diesen Abschnitt. Statist / Gesan / pro Sekun / pro Trans Gesan l der physis n Lesev nge der I/O-Anfra gen / 2.547. .217 / 3.610, / 25,11 Gesan l der physis gelese Bytes / 80.776 6.124. / 114.48 26,26 / 796.149 8 Gesan l der I/O-Anfra gen / 534.19 08 / 757,11 / 5,27	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	beim physischen Schrei Gesamtl der physischen Schreirgänge: 25.517.849. 36.165 1,84 251.508 8 Basierend auf diesen Informationen können Sie die Gesamt-IOPS und den Durchsatz wie folgt berechnen: Gesamt-IOPS = 3.610,28 + 757,11 = 4367 Mbit/s insgesamt = 114.482.426,26 + 36.165.631,84 = 150648058,1/1024/ 1024 = 143 Mbit/s	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 3: Verwenden Sie I/O-Profile.	In Oracle Database 12c enthält der AWR-Bericht einen Abschnitt mit I/O-Profilen, der alle Informationen in einer einzigen Tabelle darstellt und genauere Daten zur Datenbankleistung liefert. Die folgende Tabelle zeigt ein Beispiel für diesen Abschnitt. |	Lesen +Schreiben pro Sekun	Lesen pro Sekun	Schreib Sie pro Sekund | | --- | --- | --- | --- | | Anfrag insges : | 4.367, | 3.610, | 757,1 | | Datenl anfrag | 4.161, | 3.586, | 574,7 | | Optimi e Anfrag | 0.0 | 0.0 | 0.0 | | Anfrag wiede en: | 179,3 | 2,8 | 176,6 | | Insges (MB): | 143,7 | 109,2 | 34,5 | | Datenl (MB): | 133,1 | 106,1 | 27,1 |	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Optimi 0.0 0.0 0.0 e Summ (MB): Wiede 7.6 2.7 4,9 en bis (MB): 4,9 Datenl 17.042 13.575 3.467,3 (Blöck Über 5.898, 5.360, 537,6 Buffer Cache (Blöck Direkt 11.143 8.214, 2.929,7 (Blöck Diese Tabelle enthält die folgenden Werte für den Durchsatz und die Gesamt-IOPS: Durchsatz = 143 MBPS (aus der fünften Zeile mit der Bezeichnung Gesamt, zweite Spalte) IOPS = 4.367,4 (aus der ersten Zeile mit der Bezeichnung Gesamtzahl der Anfragen, zweite Spalte)	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 4: Verwenden Sie AWR-Ansichten.	Mithilfe von AWR-Ansichten können Sie dieselben IOPS- und Durchsatzinformationen anzeigen. Verwenden Sie die folgende Abfrage, um diese Informationen abzurufen: `break on report compute sum of Value on report select METRIC_NAME,avg(AVERAGE) as "Value" from dba_hist_sysmetric_summary where METRIC_NAME in ('Physical Read Total IO Requests Per Sec','Physical Write Total IO Requests Per Sec') group by metric_name;`	DBA

Schätzen Sie die CPU-Anforderungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie eine Methode.	Sie können den CPU-Bedarf für die Zieldatenbank auf drei Arten schätzen: • Indem Sie die tatsächlich verfügbaren Kerne des Prozessors verwenden • Durch die Verwendung der verwendeten Kerne auf der	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Grundlage von Betriebss ystemstatistiken • Durch die Verwendung der verwendeten Kerne auf der Grundlage von Datenbank statistiken Wenn Sie sich die verwendet en Kerne ansehen, empfehlen wir Ihnen, die Methode der Datenbankmetriken anstelle von Betriebssystemstat istiken zu verwenden, da sie auf der CPU basiert, die nur von den Datenbank en verwendet wird, die Sie migrieren möchten. (Betriebs systemstatistiken beinhalte n auch die CPU-Auslastung durch andere Prozesse.) Sie sollten auch die CPU-bezogenen Empfehlungen im ADDM-Bericht überprüfe n, um die Leistung nach der Migration zu verbessern. Sie können die Anforderungen auch auf der Grundlage der CPU-Generierung abschätze n. Wenn Sie verschiedene CPU-Generationen verwenden , können Sie den CPU-Bedar f der Zieldatenbank schätzen, indem Sie den Anweisung en im Whitepaper Demystify	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ing the Number of v CPUs for Optimal Workload Performan ce folgen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 1: Schätzung der Anforderungen auf der Grundlage der verfügbaren Kerne.	In AWR-Berichten: • CPUs beziehen sich auf logisch und virtuell CPUs. • Kerne sind die Anzahl der Prozessoren in einem physischen CPU-Chipsatz. • Ein Sockel ist ein physische s Gerät, das einen Chip mit einer Platine verbindet . Mehrkernprozessoren haben Sockel mit mehreren CPU-Kernen. Sie können die verfügbar en Kerne auf zwei Arten schätzen: • Mithilfe von Betriebss ystembefehlen • Mithilfe des AWR-Berichts Um die verfügbaren Kerne mithilfe von Betriebss ystembefehlen zu schätzen Verwenden Sie den folgenden Befehl, um die Kerne im Prozessor zu zählen. `$ cat /proc/cpuinfo | grep "cpu cores"|uniq cpu cores : 4 cat /proc/cpuinfo | egrep "core id|physic`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`al id" | tr -d "\n" | sed s/physical/\\nphysical/g | grep -v ^$ | sort | uniq | wc -l`
	
	Verwenden Sie den folgenden Befehl, um die Sockets im Prozessor zu zählen.
	
	`grep "physical id" /proc/cpuinfo | sort -u`
	`physical id : 0`
	`physical id : 1`
	
	Note
	Es wird nicht empfohlen, Betriebssystembefehle wie nmon und sar zu verwenden, um die CPU-Auslastung zu ermitteln. Das liegt daran, dass diese Berechnungen die CPU-Auslastung durch andere Prozesse beinhalten und möglicherweise nicht die tatsächliche CPU-Auslastung der Datenbank widerspiegeln.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Um die verfügbaren Kerne mithilfe des AWR-Berichts zu schätzen Sie können die CPU-Auslastung auch aus dem ersten Abschnitt des AWR-Berichts ableiten. Hier ist ein Auszug aus dem Bericht. D N / X DB-ID / <DB Inst / XX> Inst mm / 1 Star / 05. Sep 20 23:(Ver lichu / 12.1 0 RA g / NO Hos Nar (Ho) Plat / Linu x86 64- Bit CPU / 80 Ker / 80 Ste n / 2 Arbe eiche (GB) / 441,7 In diesem Beispiel ist die CPUs Anzahl 80, was darauf hinweist, dass diese logisch (virtuell) sind. CPUs Sie können auch sehen, dass diese Konfiguration zwei Sockets, einen physische	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	n Prozessor auf jedem Socket (also insgesamt zwei physische Prozessoren) und 40 Kerne für jeden physischen Prozessor oder Socket hat.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 2: Schätzen Sie die CPU-Auslastung mithilfe von Betriebssystemstatistiken.	Sie können die Statistiken zur CPU-Auslastung des Betriebssystems entweder direkt im Betriebssystem überprüfen (mit sar oder einem anderen Host-Betr iebssystemprogramm) oder indem Sie die IDLE/ (IDLE +BUSY) -Werte aus dem Abschnitt Betriebssystemstat istiken des AWR-Berichts überprüfen. Sie können die CPU-Auslastung in Sekunden direkt in v$osstat sehen. In den AWR- und Statspack-Berichten werden diese Daten auch im Abschnitt Betriebss ystemstatistiken angezeigt. Wenn sich mehrere Datenbanken auf derselben Box befinden, haben sie alle dieselben v$osstat-Werte für BUSY_TIME. Statistik Wert Endwert FREE_M RY_BYT 6.810.67 .248 12.280.79 9.232 INAKTIV SPEICHI YTES 175.627. 33.632 160.380.6 53.568	DBA

Aufgabe	Beschreibung		Erforderliche Fähigkeiten
	SWAP_F _BYTES	17.145.6 4.336	17.145.87 2.384
	GESCHÄ GE ZEIT	1.305.56 .937	
	LEERLA EIT	4.312.71 .839	
	ICH WARTE	53.417.1 4	
	NETTE ZEIT	29.815	
	SYS_TIM	148.567. 70	
	BENUTZ EIT	1.146.91 .783	
	LADEN	25	29
	VM_IN_E ES	593.920	
	AUSGEC NE VM- BYTES	327.680	
	PHYSIS(S_SPEIC RBYTES	474.362. 17.152	
	ANZAHL US	80	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ANZAHL U-KERNE 80 NUM_CPU_SOCKETS 2 GLOBAL_RECEIVE_SIZE_MAX 4.194.304 GLOBAL_SEND_SIZE_MAX 2.097.152 TCP_RECV_SIZE_DEFAULT 87.380 TCP_RECV_SIZE_MAX 6.291.456 GRÖSSE VON TCP_RECV_MIN 4.096 TCP_SEND_SIZE_STANDARD 16.384 TCP_SEND_SIZE_MAX 4.194.304 TCP_SEND_SIZE_MIN 4.096	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wenn es im System keine anderen großen CPU-Verbr aucher gibt, verwenden Sie die folgende Formel, um den Prozentsatz der CPU-Ausla stung zu berechnen: Auslastung = Betriebszeit/ Gesamtzeit Betriebszeit = Anforderungen = v$osstat.BUSY_TIME C = Gesamtzeit (Beschäftigt + Inaktiv) C = Kapazität = v$ostat.B USY_TIME + V$OSTAT.I DLE_TIME Auslastung = BUSY_TIME/ (BUSY_TIME + IDLE_TIME) = -1.305.569.937/(1.305.569.9 37 + 4.312.718,839) = 23% genutzt	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 3: Schätzen Sie die CPU-Auslastung mithilfe von Datenbankmetriken.	Wenn mehrere Datenbanken im System laufen, können Sie die Datenbankmetriken verwenden, die zu Beginn des Berichts angezeigt werden. Snap ID / Schnit / Sitzu / Cursor Sitzung Snap start 1846 28.09 09:00 1226 35,8 Snap been 1854 06-Okt-2 13:00 1876 41,1 Vers en: 11.75 (Minu DB-Zeit: 312.6 0 (Minu Verwenden Sie diese Formel, um Metriken zur CPU-Auslastung zu erhalten: CPU-Auslastung der Datenbank (% der verfügbaren CPU-Leistung) = CPU-Zeit/NUM_CPUS/verstrichene Zeit wobei die CPU-Auslastung durch die CPU-Zeit beschrieb	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en wird und die für die CPU aufgewendete Zeit darstellt , nicht die Wartezeit auf die CPU. Diese Berechnung ergibt: = 312.625,40/11.759,64/80 = 33% der CPU werden genutzt Anzahl der Kerne (33%) * 80 = 26,4 Kerne Gesamtzahl der Kerne = 26,4 * (120%) = 31,68 Kerne Sie können den größeren dieser beiden Werte verwenden, um die CPU-Auslastung der Amazon RDS- oder Aurora-DB-Instance zu berechnen. **Note** Auf IBM AIX stimmt die berechnete Auslastung nicht mit den Werten aus dem Betriebssystem oder der Datenbank überein. Diese Werte stimmen auf anderen Betriebssystemen überein.	

Schätzen Sie den Speicherbedarf

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schätzen Sie den Speicherbedarf anhand von Speicherstatistiken ab.	Sie können den AWR-Bericht verwenden, um den Speicher der Quelldatenbank zu berechnen und ihn in der Zieldatenbank abzugleichen. Sie sollten auch die Leistung der vorhandenen Datenbank überprüfen und Ihren Speicherbedarf reduzieren, um Kosten zu sparen, oder Ihre Anforderungen erhöhen, um die Leistung zu verbessern. Dazu ist eine detaillierte Analyse der AWR-Reaktionszeit und des Service Level Agreements (SLA) der Anwendung erforderlich. Verwenden Sie die Summe der Nutzung von Oracle System Global Area (SGA) und Program Global Area (PGA) als geschätzte Speicherauslastung für Oracle. Fügen Sie weitere 20 Prozent für das Betriebssystem hinzu, um die gewünschte Speichergröße zu ermitteln. Verwenden Sie für Oracle RAC die Summe der geschätzten Speicherauslastung auf allen RAC-Knoten und reduzieren Sie den Gesamtspeicher, da er	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	auf gemeinsamen Blöcken gespeichert wird. 1. Suchen Sie in der Tabelle zur Instanzeffizienz in Prozent nach den Metriken. In der Tabelle werden die folgenden Begriffe verwendet: • Buffer Hit% gibt an, wie oft ein bestimmte r Block im Puffer-Ca che gefunden wurde, anstatt eine physische I/O durchzuführen. Für eine bessere Leistung sollten Sie 100% als Ziel angeben. • Buffer Nowait% sollte fast 100 Prozent betragen. • Latch Hit% sollte nahe bei 100 Prozent liegen. • % Non-Parse-CPU ist der Prozentsatz der CPU-Zeit, die für Aktivitäten aufgewendet wird, die nichts mit Parsing zu tun haben. Dieser Wert sollte nahe bei 100 Prozent liegen.. Prozentsätze der Instanzef fizienz (Ziel: 100%)	

Aufgabe	Beschreibung				Erforderliche Fähigkeiten
	Puffer jetzt, warte %:	99,99	% wieder en: NoWa	100,00	
	Puffer Tr effer %:	99,84	In-Memo - Sortie ng %:	100,00	
	Treffe ote in der Biblio k%:	748.7	Sanfte Analy %:	99,81	
	Zum Analy en von % ausfü :	96,61	Treffe ote %:	100,00	
	CPU parse um verstr en %	72,73	% CPU, die nicht analys t wurde	99,21	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zu parse Flash Cache-Treffer%: 0,00 In diesem Beispiel sehen alle Metriken einwandfrei aus, sodass Sie SGA und PGA für die bestehende Datenbank als Kapazitätsplanungsanforderung verwenden können. 2. Überprüfen Sie den Abschnitt mit den Speicherstatistiken und berechnen Sie den SGA/PGA. Beginnt Ende Host-Mem (MB): 452.387 452.387,3 SGA-Nutzung (MB): 220.544 220.544,0 PGA-Nutzu 36.874,9 45.270,0	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ng (MB): Insgesamt verwendeter Instance-Speicher = SGA + PGA = 220 GB + 45 GB = 265 GB Fügen Sie 20 Prozent des Puffers hinzu: Gesamter Instanzspeicher = 1,2 * 265 GB = 318 GB Da SGA und PGA 70 Prozent des Hostspeichers ausmachen, beträgt der Gesamtspeicherbedarf: Gesamter Hostspeicher = 318/0,7 = 464 GB **Note** Wenn Sie zu Amazon RDS for Oracle migrieren, werden PGA und SGA auf der Grundlage einer vordefinierten Formel vorab berechnet. Stellen Sie sicher, dass die vorberechneten Werte Ihren	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Schätzungen nahe kommen.	

Ermitteln Sie den DB-Instance-Typ der Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie den DB-Instance-Typ auf der Grundlage von Schätzungen für Festplatten-I/O, CPU und Arbeitsspeicher.	Basierend auf den Schätzungen in den vorherigen Schritten sollte die Kapazität der Amazon RDS- oder Aurora-Zieldatenbank wie folgt sein: • 68 CPU-Kerne • 143 MBIT/S Durchsatz • 4367 IOPS für Festplatten-I/O • 464 GB Arbeitsspeicher In der Amazon RDS- oder Aurora-Zieldatenbank können Sie diese Werte dem Instance-Typ db.r5.16xlarge zuordnen, der eine Kapazität von 32 Kernen, 512 GB RAM und 13.600 Mbit/s Durchsatz hat. Weitere Informationen finden Sie im AWS-Blogbeitrag Richtiges Skalieren von Amazon RDS-Instances auf der Grundlage von Oracle-Leistungskennzahlen.	DBA

Zugehörige Ressourcen

- Aurora-DB-Instance-Klasse (Amazon Aurora Aurora-Dokumentation)
- Amazon RDS-DB-Instance-Speicher (Amazon RDS-Dokumentation)
- AWS-Miner-Tool (GitHub Repository)

Exportieren Sie Amazon RDS for SQL Server-Tabellen mithilfe von AWS DMS in einen S3-Bucket

Erstellt von Subhani Shaik (AWS)

Übersicht

Amazon Relational Database Service (Amazon RDS) für SQL Server unterstützt das Laden von Daten auf andere mit der DB-Engine verknüpfte Server in der Amazon Web Services (AWS) -Cloud nicht. Stattdessen können Sie AWS Database Migration Service (AWS DMS) verwenden, um Amazon RDS for SQL Server-Tabellen in einen Amazon Simple Storage Service (Amazon S3) -Bucket zu exportieren, wo die Daten für andere DB-Engines verfügbar sind.

Mit AWS DMS können Sie Datenbanken schnell und sicher zu AWS migrieren. Die Quelldatenbank bleibt während der Migration voll funktionsfähig, wodurch Ausfallzeiten für Anwendungen, die auf die Datenbank angewiesen sind, minimiert werden. AWS DMS kann Ihre Daten zu und von den am häufigsten verwendeten kommerziellen und Open-Source-Datenbanken migrieren.

Dieses Muster verwendet AWS Secrets Manager bei der Konfiguration der AWS DMS-Endpunkte. Secrets Manager hilft Ihnen beim Schutz von Geheimnissen, die Sie für den Zugriff auf Ihre Anwendungen, Dienste und IT-Ressourcen benötigen. Sie können den Service verwenden, um Datenbankanmeldedaten, API-Schlüssel und andere Geheimnisse während ihres gesamten Lebenszyklus zu rotieren, zu verwalten und abzurufen. Benutzer und Anwendungen rufen Geheimnisse mit einem Aufruf von Secrets Manager ab, wodurch die Notwendigkeit reduziert wird, vertrauliche Informationen fest zu codieren. Secrets Manager bietet geheime Rotation mit integrierter Integration für Amazon RDS, Amazon Redshift und Amazon DocumentDB. Der Service ist auch auf andere Arten von Geheimnissen erweiterbar, einschließlich API-Schlüsseln und Tokens. OAuth Mit Secrets Manager können Sie den Zugriff auf geheime Daten kontrollieren, indem Sie detaillierte Berechtigungen verwenden und die Rotation von Geheimnissen zentral für Ressourcen in der AWS-Cloud, in Diensten von Drittanbietern und vor Ort überprüfen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein S3-Bucket
- Eine virtuelle private Cloud (VPC)

- Ein DB-Subnetz
- Amazon RDS für SQL Server
- Eine AWS Identity and Access Management (IAM) -Rolle mit Zugriff (Objekte auflisten, abrufen und ablegen) auf den S3-Bucket im Namen der Amazon RDS-Instance.
- Secrets Manager zum Speichern der Anmeldeinformationen für die RDS-Instanz.

Architektur

Technologie-Stack

- Amazon RDS für SQL Server
- AWS DMS
- Amazon S3
- AWS Secrets Manager

Zielarchitektur

Das folgende Diagramm zeigt die Architektur für den Import von Daten aus der Amazon RDS-Instance in den S3-Bucket mit Hilfe von AWS DMS.

1. Die AWS DMS-Migrationsaufgabe, die über den Quellendpunkt eine Verbindung zur Amazon RDS-Quellinstanz herstellt
2. Daten aus der Amazon RDS-Quellinstanz kopieren
3. Die AWS DMS-Migrationsaufgabe, die über den Zielendpunkt eine Verbindung zum Ziel-S3-Bucket herstellt
4. Exportieren kopierter Daten in den S3-Bucket im CSV-Format (Comma-Separated Values)

Tools

AWS-Services

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS-Cloud oder zwischen Kombinationen von Cloud- und lokalen Setups.

- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der AWS-Cloud.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Secrets Manager hilft Ihnen dabei, hartcodierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Geheimnis programmgesteuert abzurufen.

Andere Dienste

- Microsoft SQL Server Management Studio (SSMS) ist ein Tool für die Verwaltung von SQL Server, einschließlich des Zugriffs auf, der Konfiguration und der Verwaltung von SQL Server-Komponenten.

Epen

Konfiguration der Amazon RDS for SQL Server Server-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Amazon RDS for SQL Server-Instance.	1. Öffnen Sie die AWS-Management konsole, wählen Sie RDS und verwenden Sie die Option Standard create, um eine Amazon RDS-Instance mit der erforderlichen Edition wie SQL Server Express Edition, SQL Server Standard Edition oder SQL Server Enterprise Edition zu erstellen. Wählen Sie für die Version 2016 oder später.	DBA, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie unter Vorlagen die Option Dev/Test aus.	
Richten Sie Anmeldein formationen für die Instanz ein.	1. Geben Sie einen Namen für die Instanz ein. 2. Geben Sie einen Benutzern amen und ein Passwort für die Amazon RDS-Instance ein.	DBA, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Instanzklasse, den Speicher, die auto Skalierung und die Verfügbarkeit.	1. Wählen Sie die DB-Instance-Klasse aus der Liste aus: Standard -, Memory Optimized - und Burstable -Klassen. Wählen Sie den DB-Instance-Typ, der die Rechen-, Netzwerk- und Speicherkapazität zuweist, die für die für diese DB-Instance geplanten Workloads erforderlich sind. Weitere Informationen finden Sie in der AWS-Dokumentation. 2. Wählen Sie den Speichertyp aus der Liste aus: Allzweck-SSD, Provisioned IOPS SSD oder Magnetic. Weisen Sie die Standards peichergröße nach Bedarf zu. 3. Wählen Sie Automatische Speicherskalierung aktivieren, um den Amazon RDS-Speicher auf der Grundlage Ihrer Kapazitätsplanung zu erhöhen. 4. Eine Multi-AZ-Bereitstellung mit einer Replikationsinstanz wird von AWS DMS unterstützt. Im Falle eines Ausfalls in der Availability Zone, der internen Hardware oder im Netzwerk	DBA, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	erstellt AWS DMS eine Standby-Instance und bietet Hochverfügbarkeit (HA) durch automatisches Failover auf die Standby-Replikate. Wählen Sie je nach Größe Ihres Imports die entsprechende Option aus.	
Geben Sie die VPC, die Subnetzgruppe, den öffentlichen Zugriff und die Sicherheitsgruppe an.	Wählen Sie die VPC, die DB-Subnetzgruppen und die VPC-Sicherheitsgruppe nach Bedarf aus, um die Amazon RDS-Instance zu erstellen . Folgen Sie den bewährten Methoden, zum Beispiel: • Aktivieren Sie nicht den öffentlichen Zugriff auf die RDS-DB-Instance. • Verwenden Sie CIDR 0.0.0.0/0 nicht in den Sicherheitsgruppen. • Verwenden Sie nur die erforderlichen IP-Adressen und Portdetails, um auf die RDS-Instance zuzugreifen.	DBA, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Überwachung, Sicherung und Wartung.	1. Geben Sie die gewünschten Backup-Optionen an. Standardmäßig sind automatische Backups mit einer Aufbewahrungsfrist von 7 Tagen aktiviert. 2. Wählen Sie die entsprechenden Einstellungen für das auto Upgrade der Nebenversion und das Wartungsfenster, um die ausstehenden Änderungen oder Wartungsarbeiten durch Amazon RDS auf die Datenbank anzuwenden. 3. Wählen Sie Datenbank erstellen aus.	DBA, Ingenieur DevOps

Richten Sie die Datenbank und die Beispieldaten ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Tabelle und laden Sie die Beispieldaten.	Erstellen Sie in der neuen Datenbank eine Tabelle. Verwenden Sie den Beispielcode im Abschnitt Zusätzliche Informationen, um Daten in die Tabelle zu laden.	DBA, Ingenieur DevOps

Richten Sie Anmeldeinformationen ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Geheimnis.	1. Wählen Sie auf der Konsole Secrets Manager und anschließend Store a new secret aus. 2. Geben Sie einen Benutzern amen und ein Passwort für die Amazon RDS for SQL Server Server-Datenbank ein. Dieses Geheimnis wird für den AWS DMS-Quellendpunkt verwendet.	DBA, Ingenieur DevOps

Richten Sie den Zugriff zwischen der Datenbank und dem S3-Bucket ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle für den Zugriff auf Amazon RDS.	1. Wählen Sie auf der Konsole IAM und erstellen Sie eine IAM-Rolle, die einem S3-Bucket Lese-/Schreibzugriff auf Amazon RDS gewährt. 2. Wählen Sie unter Funktion die Option S3-Integration aus.	DBA, Ingenieur DevOps

Erstellen Sie den S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den S3-Bucket.	Um die Daten von Amazon RDS for SQL Server zu speichern, wählen Sie in der Konsole S3 und dann Create Bucket aus. Stellen Sie sicher, dass der S3-Bucket nicht öffentlich verfügbar ist.	DBA, Ingenieur DevOps

Richten Sie den Zugriff zwischen AWS DMS und dem S3-Bucket ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle für AWS DMS, um auf Amazon S3 zuzugreifen.	Erstellen Sie eine IAM-Rolle , die es AWS DMS ermöglich t, Objekte aus dem S3-Bucket aufzulisten, abzurufen und zu platzieren.	DBA, Ingenieur DevOps

AWS DMS konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den AWS DMS-Quellendpunkt.	1. Wählen Sie in der Konsole Database Migration Service und dann Endpoints aus. Erstellen Sie den Quellendp unkt und aktivieren Sie das Kontrollkästchen RDS-DB-Instance auswählen.	DBA, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie für die Quell-Engine Microsoft SQL Server aus. 3. Wählen Sie unter Zugriff auf die Endpunktdatenbank die Option AWS Secrets Manager aus und geben Sie die geheime und die IAM-Rolle ein, die Sie zuvor erstellt haben, sowie den Datenbanknamen. 4. Testen Sie den Quellendpunkt.	
Erstellen Sie den AWS DMS-Zielendpunkt.	Erstellen Sie den Target-Endpunkt und wählen Sie Amazon S3 als Target-Engine aus. Geben Sie den S3-Bucket-Namen und den Ordnernamen für die IAM-Rolle an, die Sie zuvor erstellt haben.	DBA, Ingenieur DevOps
Erstellen Sie die AWS DMS-Replikationsinstanz.	Erstellen Sie in derselben VPC, demselben Subnetz und derselben Sicherheitsgruppe die AWS DMS-Replikationsinstanz. Weitere Informationen zur Auswahl einer Instance-Klasse finden Sie in der AWS-Dokumentation.	DBA, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die AWS DMS-Migrationsaufgabe.	Um die Daten von Amazon RDS for SQL Server in den S3-Bucket zu exportieren, erstellen Sie eine Datenbank migrationsaufgabe. Wählen Sie für den Migrationstyp die Option Bestehende Daten migrieren aus. Wählen Sie die AWS DMS-Endpoints und die Replikationsinstanz aus, die Sie erstellt haben.	DBA, Ingenieur DevOps

Exportieren Sie die Daten in den S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Aufgabe zur Datenbankmigration aus.	Um die SQL Server-Ta bellendaten zu exportieren, starten Sie die Datenbank migrationsaufgabe. Die Aufgabe exportiert die Daten von Amazon RDS for SQL Server in den S3-Bucket im CSV-Format.	DBA, Ingenieur DevOps

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die Ressourcen.	Um zusätzliche Kosten zu vermeiden, verwenden Sie die Konsole, um die Ressourcen	DBA, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in der folgenden Reihenfolge zu löschen: 1. Migrationsaufgabe 2. Replikations-Instance 3. Endpunkte 4. S3-Bucket 5. Datenbank-Instance	

Zugehörige Ressourcen

- AWS DMS
- Amazon S3
- Amazon RDS für SQL Server
- Amazon S3 S3-Integration

Zusätzliche Informationen

Verwenden Sie den folgenden Code, um die Datenbank und die Tabelle zu erstellen und die Beispieldaten zu laden.

```
--Step1: Database creation in RDS SQL Server
CREATE DATABASE [Test_DB]
 ON  PRIMARY
( NAME = N'Test_DB', FILENAME = N'D:\rdsdbdata\DATA\Test_DB.mdf' , SIZE = 5120KB ,
 FILEGROWTH = 10%)
 LOG ON
( NAME = N'Test_DB_log', FILENAME = N'D:\rdsdbdata\DATA\Test_DB_log.ldf' , SIZE =
 1024KB , FILEGROWTH = 10%)
GO

--Step2: Create Table
USE Test_DB
GO
Create Table Test_Table(ID int, Company Varchar(30), Location Varchar(20))
```

```
--Step3: Load sample data.
USE Test_DB
GO
Insert into Test_Table values(1,'AnyCompany','India')
Insert into Test_Table values(2,'AnyCompany','USA')
Insert into Test_Table values(3,'AnyCompany','UK')
Insert into Test_Table values(4,'AnyCompany','Hyderabad')
Insert into Test_Table values(5,'AnyCompany','Banglore')
```

Behandeln Sie anonyme Blöcke in dynamischen SQL-Anweisungen in Aurora PostgreSQL

Erstellt von anuradha chintha (AWS)

Übersicht

Dieses Muster zeigt Ihnen, wie Sie den Fehler vermeiden können, der beim Umgang mit anonymen Blöcken in dynamischen SQL-Anweisungen auftritt. Sie erhalten eine Fehlermeldung, wenn Sie das AWS Schema Conversion Tool verwenden, um eine Oracle-Datenbank in eine Aurora PostgreSQL-Compatible Edition-Datenbank zu konvertieren. Um den Fehler zu vermeiden, müssen Sie den Wert einer `OUT` Bind-Variablen kennen, aber Sie können den Wert einer `OUT` Bind-Variablen erst kennen, nachdem Sie die SQL-Anweisung ausgeführt haben. Der Fehler ist darauf zurückzuführen, dass das AWS Schema Conversion Tool (AWS SCT) die Logik in der Dynamic SQL-Anweisung nicht versteht. AWS SCT kann die dynamische SQL-Anweisung nicht in PL/SQL-Code (d. h. Funktionen, Prozeduren und Pakete) konvertieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Aktives AWS-Konto
- Aurora PostgreSQL-Datenbank-Instance (DB)
- Amazon Relational Database Service (Amazon RDS) für Oracle-DB-Instance
- Interaktives PostgreSQL-Terminal (psql)
- SQL*Plus
- `AWS_ORACLE_EXT`Schema (Teil des AWS SCT-Erweiterungspakets) in Ihrer Zieldatenbank
- Aktuelle Version des AWS Schema Conversion Tool (AWS SCT) und der erforderlichen Treiber

Architektur

Quelltechnologie-Stack

- Lokale Oracle-Datenbank 10g und neuere Version

Zieltechnologie-Stack

- Amazon Aurora PostgreSQL
- Amazon RDS für PostgreSQL
- AWS-Schemakonvertierungstool (AWS SCT)

Architektur der Migration

Das folgende Diagramm zeigt, wie Sie AWS SCT- und `OUT` Oracle-Bind-Variablen verwenden, um Ihren Anwendungscode nach Embedded SQL-Anweisungen zu scannen und den Code in ein kompatibles Format zu konvertieren, das eine Aurora-Datenbank verwenden kann.

Das Diagramm zeigt den folgenden Workflow:

1. Generieren Sie einen AWS SCT-Bericht für die Quelldatenbank, indem Sie Aurora PostgreSQL als Zieldatenbank verwenden.
2. Identifizieren Sie den anonymen Block im Dynamic SQL-Codeblock (für den AWS SCT den Fehler ausgelöst hat).
3. Konvertieren Sie den Codeblock manuell und stellen Sie den Code in einer Zieldatenbank bereit.

Tools

AWS-Services

- Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt.
- Amazon Relational Database Service (Amazon RDS) für Oracle unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Oracle-Datenbank in der AWS-Cloud.
- Das AWS Schema Conversion Tool (AWS SCT) hilft Ihnen dabei, heterogene Datenbankmigrationen vorhersehbar zu machen, indem das Quelldatenbankschema und ein Großteil der Datenbankcode-Objekte automatisch in ein mit der Zieldatenbank kompatibles Format konvertiert werden.

Andere Tools

- pgAdmin ermöglicht es Ihnen, eine Verbindung zu Ihrem Datenbankserver herzustellen und mit ihm zu interagieren.
- Oracle SQL Developer ist eine integrierte Entwicklungsumgebung, mit der Sie Datenbanken in Oracle Database entwickeln und verwalten können. Sie können entweder SQL *Plus oder Oracle SQL Developer für dieses Muster verwenden.

Epen

Konfigurieren Sie die Oracle-Quelldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Oracle-Instanz auf Amazon RDS oder Amazon EC2.	Informationen zum Erstellen einer Oracle-DB-Instance auf Amazon RDS finden Sie unter Eine Oracle-DB-Instance erstellen und eine Verbindung zu einer Datenbank auf einer Oracle-DB-Instance herstellen in der Amazon RDS-Dokumentation. Informationen zum Erstellen einer Oracle-DB-Instance auf Amazon Elastic Compute Cloud (Amazon EC2) finden Sie unter Amazon EC2 for Oracle in der AWS Prescriptive Guidance Guidance-Dokumentation.	DBA
Erstellen Sie ein Datenbankschema und Objekte für die Migration.	Sie können Amazon Cloud Directory verwenden, um ein Datenbankschema zu erstellen. Weitere Informationen finden Sie in der Cloud	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Directory Directory-Dokumentation unter Schema erstellen.	
Konfigurieren Sie Sicherheitsgruppen für eingehenden und ausgehenden Datenverkehr.	Informationen zum Erstellen und Konfigurieren von Sicherheitsgruppen finden Sie unter Steuern des Zugriffs mit Sicherheitsgruppen in der Amazon RDS-Dokumentation.	DBA
Vergewissern Sie sich, dass die Datenbank läuft.	Informationen zum Überprüfen des Status Ihrer Datenbank finden Sie unter Amazon RDS-Ereignisse anzeigen in der Amazon RDS-Dokumentation.	DBA

Konfigurieren Sie die Aurora PostgreSQL-Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Aurora PostgreSQL-Instance in Amazon RDS.	Informationen zum Erstellen einer Aurora PostgreSQL-Instance finden Sie unter Erstellen eines DB-Clusters und Herstellen einer Verbindung zu einer Datenbank auf einem Aurora PostgreSQL-DB-Cluster in der Amazon RDS-Dokumentation.	DBA
Konfigurieren Sie eine Sicherheitsgruppe für eingehenden und ausgehenden Datenverkehr.	Informationen zum Erstellen und Konfigurieren von Sicherheitsgruppen finden Sie in der Aurora-Dokumentation unter Gewähren des Zugriffs	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	auf den DB-Cluster in der VPC durch Erstellen einer Sicherheitsgruppe.	
Vergewissern Sie sich, dass die Aurora PostgreSQL-Datenbank läuft.	Informationen zum Überprüfen des Status Ihrer Datenbank finden Sie unter Amazon RDS-Ereignisse anzeigen in der Aurora-Dokumentation.	DBA

AWS SCT einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Connect AWS SCT mit der Quelldatenbank.	Informationen zur Verbindung von AWS SCT mit Ihrer Quelldatenbank finden Sie unter Connecting to PostgreSQL as a source in der AWS SCT-Dokumentation.	DBA
Connect AWS SCT mit der Zieldatenbank.	Informationen zur Verbindung von AWS SCT mit Ihrer Zieldatenbank finden Sie unter Was ist das AWS Schema Conversion Tool? im AWS Schema Conversion Tool-Benutzerhandbuch.	DBA
Konvertieren Sie das Datenbankschema in AWS SCT und speichern Sie den automatisch konvertierten Code als SQL-Datei.	Informationen zum Speichern von mit AWS SCT konvertierten Dateien finden Sie unter Speichern und Anwenden Ihres konvertierten Schemas	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in AWS SCT im AWS Schema Conversion Tool User Guide.	

Migrieren Sie den Code

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Holen Sie sich die SQL-Datei für die manuelle Konvertie rung.	Rufen Sie in der von AWS SCT konvertierten Datei die SQL-Datei ab, für die eine manuelle Konvertierung erforderlich ist.	DBA
Aktualisiere das Skript.	Aktualisieren Sie die SQL-Datei manuell.	DBA

Zugehörige Ressourcen

- Amazon RDS
- Amazon Aurora Aurora-Funktionen

Zusätzliche Informationen

Der folgende Beispielcode zeigt, wie die Oracle-Quelldatenbank konfiguriert wird:

```
CREATE or replace PROCEDURE calc_stats_new1 (
  a NUMBER,
  b NUMBER,
  result out NUMBER)
IS
BEGIN
result:=a+b;
END;
/
```

```
set serveroutput on ;

DECLARE
  a NUMBER := 4;
  b NUMBER := 7;
  plsql_block VARCHAR2(100);
  output number;
BEGIN
  plsql_block := 'BEGIN calc_stats_new1(:a, :b,:output); END;';
  EXECUTE IMMEDIATE plsql_block USING a, b,out output;
  DBMS_OUTPUT.PUT_LINE('output:'||output);

END;
```

Der folgende Beispielcode zeigt, wie die Aurora PostgreSQL-Zieldatenbank konfiguriert wird:

```
 w integer,
 x integer)
RETURNS integer
AS
$BODY$
DECLARE
begin
return w + x ;
end;
$BODY$
LANGUAGE  plpgsql;


CREATE OR REPLACE FUNCTION test_pg.init()
RETURNS void
AS
$BODY$
BEGIN
if aws_oracle_ext.is_package_initialized
      ('test_pg' ) then
      return;
    end if;
    perform aws_oracle_ext.set_package_initialized
      ('test_pg' );

PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_output', NULL::INTEGER);
PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_status', NULL::text);
```

```
END;
$BODY$
LANGUAGE  plpgsql;


DO $$
declare
v_sql text;
v_output_loc int;
a integer :=1;
b integer :=2;
BEGIN
perform  test_pg.init();
--raise notice 'v_sql %',v_sql;
execute 'do $a$ declare v_output_l int; begin select * from test_pg.calc_stats_new1('||
a||','||b||') into v_output_l;
PERFORM aws_oracle_ext.set_package_variable(''test_pg'', ''v_output'', v_output_l) ;
 end; $a$'  ;
v_output_loc := aws_oracle_ext.get_package_variable('test_pg', 'v_output');
raise notice 'v_output_loc %',v_output_loc;
END ;
$$
```

Behandeln Sie überladene Oracle-Funktionen in Aurora PostgreSQL-kompatibel

Erstellt von Sumana Yanamandra (AWS)

Übersicht

Der Code, den Sie von einer lokalen Oracle-Datenbank zur Amazon Aurora PostgreSQL-Compatible Edition migrieren, kann überladene Funktionen enthalten. Diese Funktionen haben dieselbe Definition, d. h. denselben Funktionsnamen und dieselbe Anzahl und denselben Datentyp der Eingabe- () -Parameter. Der Datentyp oder die Anzahl der Output (`IN`) -Parameter können sich jedoch unterscheiden. `OUT`

Diese Parameterabweichungen können in PostgreSQL zu Problemen führen, da es schwierig ist, zu bestimmen, welche Funktion ausgeführt werden soll. Dieses Muster veranschaulicht, wie Sie mit überladenen Funktionen umgehen, wenn Sie Ihren Datenbankcode zu Aurora PostgreSQL-kompatibel migrieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Oracle-Datenbankinstanz als Quelldatenbank
- Eine Aurora PostgreSQL-kompatible DB-Instance als Ihre Zieldatenbank (siehe Anweisungen in der Aurora-Dokumentation)

Produktversionen

- Oracle Database 9i oder höher
- Oracle SQL Developer Version 18.4.0.376
- pgAdmin 4-Klient
- Aurora PostgreSQL-kompatible Version 11 oder höher (siehe Identifizieren von Versionen von Amazon Aurora PostgreSQL in der Aurora-Dokumentation)

Tools

AWS-Services

- Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt.

Andere Tools

- Oracle SQL Developer ist eine kostenlose, integrierte Entwicklungsumgebung für die Arbeit mit SQL in Oracle-Datenbanken sowohl in herkömmlichen als auch in Cloud-Umgebungen.
- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL. Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, verwalten und verwenden können.

Epen

Erstelle eine einfache Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Funktion in PostgreSQL, die einen Eingabeparameter und einen Ausgabeparameter hat.	Das folgende Beispiel veranschaulicht eine Funktion mit dem Namen `test_overloading` Aurora PostgreSQL-compatible. Diese Funktion hat zwei Parameter: einen Eingabe-Textparameter und einen Ausgabetextparameter. `CREATE OR REPLACE FUNCTION public.test_overloading( str1 text, OUT str2 text) LANGUAGE 'plpgsql' COST 100 VOLATILE AS $BODY$ DECLARE BEGIN str2 := 'Success';`	Dateningenieur, Aurora PostgreSQL-kompatibel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`RETURN ;`
	`EXCEPTION`
	`WHEN others THEN`
	`RETURN ;`
	`END;`
	`$BODY$;`	

Führen Sie die Funktion in PostgreSQL aus.	Führen Sie die Funktion aus, die Sie im vorherigen Schritt erstellt haben.
	`select public.test_overloading('Test');`
	Es sollte die folgende Ausgabe anzeigen.
	`Success`
		Dateningenieur, Aurora PostgreSQL-kompatibel

Überladen Sie die Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie denselben Funktionsnamen, um eine überladene Funktion in PostgreSQL zu erstellen.	Erstellen Sie eine überladene Funktion in Aurora PostgreSQL-kompatibel, die denselben Funktionsnamen wie Ihre vorherige Funktion verwendet. Das folgende Beispiel ist ebenfalls benannt`test_overloading` , hat aber drei Parameter: einen Eingabe-Textparameter, einen Ausgabetextparameter und	Dateningenieur, Aurora PostgreSQL-kompatibel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	einen Integer-Ausgabepar ameter. `CREATE OR REPLACE FUNCTION public.test_overloading( str1 text, OUT str2 text, OUT num1 integer) LANGUAGE 'plpgsql' COST 100 VOLATILE AS $BODY$ DECLARE str3 text; BEGIN str2 := 'Success'; num1 := 100; RETURN ; EXCEPTION WHEN others THEN RETURN ; END; $BODY$;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Führen Sie die Funktion in PostgreSQL aus.	Wenn Sie diese Funktion ausführen, schlägt sie mit der folgenden Fehlermeldung fehl.
	`ERROR: cannot change return type of existing function`
	`HINT: Use DROP FUNCTION test_over loading(text) first.`
	Dies liegt daran, dass Aurora PostgreSQL-kompatibel das direkte Überladen von Funktionen nicht unterstützt. Es kann nicht identifiziert werden, welche Funktion ausgeführt werden soll, da die Anzahl der Ausgabeparameter in der zweiten Version der Funktion unterschiedlich ist, obwohl die Eingabeparameter identisch sind.
		Dateningenieur, Aurora PostgreSQL-kompatibel

Wenden Sie die Problemumgehung an

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie INOUT zum ersten Ausgabeparameter hinzu.	Um das Problem zu umgehen, ändern Sie den Funktionscode, indem Sie den ersten Ausgabeparameter als `INOUT` darstellen.	Dateningenieur, Aurora PostgreSQL-kompatibel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>CREATE OR REPLACE
	 FUNCTION public.te
	st_overloading(
	         str1 text,
	         INOUT str2
	 text,
	         OUT num1
	 integer)
	    LANGUAGE 'plpgsql'
	
	    COST 100
	    VOLATILE
	AS $BODY$
	DECLARE
	str3 text;
	BEGIN
	
	         str2 :=
	 'Success';
	         num1 := 100;
	
	    RETURN ;
	    EXCEPTION
	        WHEN others THEN
	             RETURN ;
	END;
	$BODY$;</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Führen Sie die überarbeitete Funktion aus.	Führen Sie die Funktion aus, die Sie aktualisiert haben, mithilfe der folgenden Abfrage. Sie übergeben einen Nullwert als zweites Argument dieser Funktion, weil Sie diesen Parameter so deklariert haben, `INOUT` dass der Fehler vermieden wird.
	`select public.test_overloading('Test', null);`
	Die Funktion wurde jetzt erfolgreich erstellt.
	`Success, 100`
		Dateningenieur, Aurora PostgreSQL-kompatibel

Validieren Sie die Abfrageergebnisse.	Stellen Sie sicher, dass der Code mit der überladenen Funktion erfolgreich konvertiert wurde.	Dateningenieur, Aurora PostgreSQL-kompatibel

Zugehörige Ressourcen

- Arbeiten mit Amazon Aurora PostgreSQL (Aurora-Dokumentation)
- Überladen von Funktionen in Oracle (Oracle-Dokumentation)
- Überladen von Funktionen in PostgreSQL (PostgreSQL-Dokumentation)

Helfen Sie mit, DynamoDB-Tagging durchzusetzen

Erstellt von Mansi Suratwala (AWS)

Übersicht

Dieses Muster richtet automatische Benachrichtigungen ein, wenn ein vordefiniertes Amazon DynamoDB-Tag fehlt oder aus einer DynamoDB-Ressource in der Amazon Web Services (AWS) -Cloud entfernt wird.

DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankdienst, der schnelle und vorhersehbare Leistung mit Skalierbarkeit bietet. Mit DynamoDB können Sie den Verwaltungsaufwand für den Betrieb und die Skalierung einer verteilten Datenbank verringern. Wenn Sie DynamoDB verwenden, müssen Sie sich keine Gedanken über Hardwarebereitstellung, Einrichtung und Konfiguration, Replikation, Software-Patches oder Clusterskalierung machen.

Das Muster verwendet eine CloudFormation AWS-Vorlage, die ein Amazon CloudWatch Events-Ereignis und eine AWS-Lambda-Funktion erstellt. Das Ereignis sucht mithilfe von AWS nach neuen oder vorhandenen DynamoDB-Tagging-Informationen. CloudTrail Wenn ein vordefiniertes Tag fehlt oder entfernt wird, wird eine Lambda-Funktion CloudWatch ausgelöst, die Ihnen eine Amazon Simple Notification Service (Amazon SNS) -Benachrichtigung sendet, die Sie über den Verstoß informiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket für die Lambda-.zip-Datei, die das Python-Skript für die Ausführung der Lambda-Funktion enthält

Einschränkungen

- Die Lösung funktioniert nur, wenn die Ereignisse `TagResource` oder `UntagResource` CloudTrail eintreten. Es werden keine Benachrichtigungen für andere Ereignisse erstellt.

Architektur

Zieltechnologie-Stack

- Amazon-DynamoDB
- AWS CloudTrail
- Amazon CloudWatch
- AWS Lambda
- Amazon S3
- Amazon SNS

Zielarchitektur

Automatisierung und Skalierung

Sie können die CloudFormation AWS-Vorlage mehrfach für verschiedene AWS-Regionen und Konten verwenden. Sie müssen die Vorlage in jeder Region oder jedem Konto nur einmal ausführen.

Tools

Tools

- Amazon DynamoDB — DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der schnelle und vorhersehbare Leistung mit Skalierbarkeit bietet.
- AWS CloudTrail — CloudTrail ist ein AWS-Service, der Sie bei der Steuerung, Einhaltung von Vorschriften sowie der Betriebs- und Risikoprüfung Ihres AWS-Kontos unterstützt. Aktionen, die von einem Benutzer, einer Rolle oder einem AWS-Service ausgeführt werden, werden als Ereignisse in aufgezeichnet CloudTrail.
- Amazon CloudWatch Events — Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit.
- AWS Lambda — Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne dass Server bereitgestellt oder verwaltet werden müssen. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice, der für eine Vielzahl von Speicherlösungen verwendet werden kann, darunter Websites, mobile Anwendungen, Backups und Data Lakes.

- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) ist ein Webservice, der es Anwendungen, Endbenutzern und Geräten ermöglicht, sofort Benachrichtigungen aus der Cloud zu senden und zu empfangen.

Code

- Eine ZIP-Datei des Projekts ist als Anhang verfügbar.

Epen

Definieren Sie den S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Wählen oder erstellen Sie auf der Amazon S3 S3-Konsole einen S3-Bucket mit einem eindeutigen Namen, der keine führenden Schrägstriche enthält. Dieser S3-Bucket hostet die Lambda-Code-.zip-Datei. Ihr S3-Bucket muss sich in derselben AWS-Region befinden wie die DynamoDB-Ressource, die überwacht wird.	Cloud-Architekt

Laden Sie den Lambda-Code in den S3-Bucket hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Lambda-Code in den S3-Bucket hoch.	Laden Sie die Lambda-Code-ZIP-Datei, die im Abschnitt Anlagen bereitgestellt wird, in den S3-Bucket hoch. Der S3-Bucket muss sich in derselben	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Region befinden wie die DynamoDB-Ressource, die überwacht wird.	

Stellen Sie die CloudFormation AWS-Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation AWS-Vorlage bereit.	Stellen Sie auf der CloudFormation AWS-Konsole die CloudFormation AWS-Vorlage bereit, die im Abschnitt Anlagen bereitgestellt wird. Geben Sie im nächsten Epic Werte für die Parameter an.	Cloud-Architekt

Vervollständigen Sie die Parameter in der CloudFormation AWS-Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Nennen Sie den S3-Bucket.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epic erstellt oder ausgewählt haben.	Cloud-Architekt
Geben Sie den Amazon S3 S3-Schlüssel ein.	Geben Sie den Speicherort der Lambda-Code-ZIP-Datei in Ihrem S3-Bucket an, ohne vorangestellte Schrägstriche (z. B.). `<folder>/<file-name>.zip`	Cloud-Architekt
Geben Sie eine E-Mail-Adresse an	Geben Sie eine aktive E-Mail-Adresse an, um Amazon SNS	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SNS-Benachrichtigungen zu erhalten.	
Definieren Sie die Protokollierungsebene.	Definieren Sie die Protokollierungsebene und die Häufigkeit für Ihre Lambda-Funktion. `Info`bezeichnet detaillierte Informationsmeldungen über den Fortschritt der Anwendung. `Error`bezeichnet Fehlerereignisse, die es der Anwendung dennoch ermöglichen könnten, weiter zu laufen. `Warning`bezeichnet potenziell schädliche Situationen.	Cloud-Architekt
Geben Sie die erforderlichen DynamoDB-Tagschlüssel ein.	Achten Sie darauf, dass die Tags durch Kommas getrennt sind und keine Leerzeichen dazwischen stehen (z. B.). `ApplicationId,CreatedBy,Environment,Organization` Das Ereignis CloudWatch Ereignisse sucht nach diesen Tags und sendet eine Benachrichtigung, wenn sie nicht gefunden werden.	Cloud-Architekt

Bestätigen Sie das Abonnement.

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail an die von Ihnen angegebene E-Mail-Adresse. Um Benachrichtigungen über Verstöße zu erhalten, müssen Sie dieses E-Mail-Abonnement bestätigen.	Cloud-Architekt

Zugehörige Ressourcen

- Erstellen eines S3-Buckets
- Dateien in einen S3-Bucket hochladen
- Ressourcen in DynamoDB taggen
- Erstellen einer CloudWatch Ereignisregel, die bei einem AWS-API-Aufruf mit AWS ausgelöst wird CloudTrail

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Implementieren Sie regionsübergreifende Notfallwiederherstellung mit AWS DMS und Amazon Aurora

Erstellt von Mark Hudson (AWS)

Übersicht

Naturkatastrophen oder vom Menschen verursachte Katastrophen können jederzeit eintreten und sich auf die Verfügbarkeit von Services und Workloads auswirken, die in einer bestimmten AWS-Region ausgeführt werden. Um die Risiken zu minimieren, müssen Sie einen Notfallwiederherstellungsplan (DR) entwickeln, der die integrierten regionsübergreifenden Funktionen der AWS-Services beinhaltet. Für AWS-Services, die von Natur aus keine regionsübergreifende Funktionalität bieten, muss der DR-Plan auch eine Lösung für deren Failover in allen AWS-Regionen bieten.

Dieses Muster führt Sie durch ein Disaster Recovery-Setup mit zwei Amazon Aurora MySQL-Compatible Edition-Datenbankclustern in einer einzigen Region. Um die DR-Anforderungen zu erfüllen, sind die Datenbankcluster so konfiguriert, dass sie die globale Datenbankfunktion von Amazon Aurora verwenden, wobei sich eine einzige Datenbank über mehrere AWS-Regionen erstreckt. Eine AWS Database Migration Service (AWS DMS) -Aufgabe repliziert Daten zwischen den Clustern in der lokalen Region. AWS DMS unterstützt derzeit jedoch kein Task-Failover zwischen Regionen. Dieses Muster umfasst die Schritte, die erforderlich sind, um diese Einschränkung zu umgehen und AWS DMS in beiden Regionen unabhängig zu konfigurieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ausgewählte primäre und sekundäre AWS-Regionen, die globale Amazon Aurora Aurora-Datenbanken unterstützen.
- Zwei unabhängige Amazon Aurora MySQL-Compatible Edition-Datenbankcluster in einem einzigen Konto in der primären Region.
- Datenbank-Instance-Klasse db.r5 oder höher (empfohlen).
- Eine AWS-DMS-Aufgabe in der primären Region, die eine fortlaufende Replikation zwischen den vorhandenen Datenbankclustern durchführt.
- Ressourcen der DR-Region sind vorhanden, um die Anforderungen für die Erstellung von Datenbank-Instances zu erfüllen. Weitere Informationen finden Sie unter Arbeiten mit einer DB-Instance in einer VPC.

Einschränkungen

- Eine vollständige Liste der globalen Amazon Aurora Aurora-Datenbankbeschränkungen finden Sie unter Einschränkungen der globalen Amazon Aurora Aurora-Datenbanken.

Produktversionen

- Amazon Aurora MySQL-kompatible Edition 5.7 oder 8.0. Weitere Informationen finden Sie unter Amazon Aurora Aurora-Versionen.

Architektur

Zieltechnologie-Stack

- Globaler Datenbankcluster Amazon Aurora MySQL-Compatible Edition
- AWS DMS

Zielarchitektur

Das folgende Diagramm zeigt eine globale Datenbank für zwei AWS-Regionen, eine mit den primären Haupt- und Reporterdatenbanken und der AWS-DMS-Replikation und eine mit den sekundären Haupt- und Reporterdatenbanken.

Automatisierung und Skalierung

Sie können AWS verwenden CloudFormation , um die erforderliche Infrastruktur in der sekundären Region zu erstellen, z. B. die Virtual Private Cloud (VPC), Subnetze und Parametergruppen. Sie können AWS auch verwenden CloudFormation , um die sekundären Cluster in der DR-Region zu erstellen und sie der globalen Datenbank hinzuzufügen. Wenn Sie CloudFormation Vorlagen verwendet haben, um die Datenbankcluster in der primären Region zu erstellen, können Sie diese aktualisieren oder mit einer zusätzlichen Vorlage erweitern, um die globale Datenbankressource zu erstellen. Weitere Informationen finden Sie unter Erstellen eines Amazon Aurora Aurora-DB-Clusters mit zwei DB-Instances und Erstellen eines globalen Datenbank-Clusters für Aurora MySQL.

Schließlich können Sie die AWS-DMS-Aufgaben in den primären und sekundären Regionen mithilfe von Ereignissen CloudFormation nach dem Auftreten von Failover- und Failback-Ereignissen erstellen. Weitere Informationen finden Sie unter AWS::DMS::ReplicationTask.

Tools

- Amazon Aurora ist eine vollständig verwaltete relationale Datenbank-Engine, die mit MySQL und PostgreSQL kompatibel ist. Dieses Muster verwendet Amazon Aurora MySQL-Compatible Edition.
- Die globalen Datenbanken von Amazon Aurora sind für global verteilte Anwendungen konzipiert. Eine einzelne globale Amazon Aurora Aurora-Datenbank kann sich über mehrere AWS-Regionen erstrecken. Sie repliziert Ihre Daten ohne Auswirkungen auf die Datenbankleistung. Es ermöglicht außerdem schnelle lokale Lesevorgänge mit geringer Latenz in jeder Region und ermöglicht die Notfallwiederherstellung nach regionsweiten Ausfällen.
- AWS DMS bietet eine einmalige Migration oder eine fortlaufende Replikation. Eine fortlaufende Replikationsaufgabe sorgt dafür, dass Ihre Quell- und Zieldatenbanken synchron bleiben. Nach der Einrichtung wendet die laufende Replikationsaufgabe kontinuierlich Quelländerungen mit minimaler Latenz auf das Ziel an. Alle Funktionen von AWS DMS, wie Datenvalidierung und Transformationen, sind für jede Replikationsaufgabe verfügbar.

Epen

Bereiten Sie die vorhandenen Datenbankcluster in der primären Region vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Parameter gruppe des Datenbank-Clusters.	Aktivieren Sie in der vorhandenen Parameter gruppe des Datenbank-Clusters die binäre Protokoll ierung auf Zeilenebene, indem Sie den **`binlog_format`** Parameter auf den Wert row setzen. AWS DMS erfordert binäre Protokollierung auf Zeilenebe ne für MySQL-kompatible Datenbanken, wenn laufende Replikationen oder Change Data Capture (CDC) durchgeführt werden. Weitere	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Informationen finden Sie unter Verwenden einer von AWS verwalteten MySQL-kompatiblen Datenbank als Quelle für AWS DMS.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisieren Sie den Aufbewahrungszeitraum für das Binärprotokoll der Datenbank.	Führen Sie mithilfe eines auf Ihrem Endbenutzergerät installierten MySQL-Clients oder einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance die folgende von Amazon Relational Database Service (Amazon RDS) bereitgestellte gespeicherte Prozedur auf dem Writer-Node des Haupt-Datenbank-Clusters aus, wobei die Anzahl der Stunden für die Aufbewahrung der Protokolle angegeben XX ist.
	`call mysql.rds_set_configuration('binlog retention hours', XX)`
	Bestätigen Sie die Einstellung, indem Sie den folgenden Befehl ausführen.
	`call mysql.rds_show_configuration;`
	MySQL-kompatible Datenbanken, die von AWS verwaltet werden, löschen die Binärprotokolle so schnell wie möglich. Daher muss der Aufbewahrungszeitraum lang genug sein, um sicherzustellen, dass die Protokolle nicht gelöscht
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	werden, bevor die AWS DMS-Aufgabe ausgeführt wird. Ein Wert von 24 Stunden ist normalerweise ausreichend, der Wert sollte jedoch auf der Zeit basieren, die für die Einrichtung der AWS DMS-Aufgabe in der DR-Region erforderlich ist.	

Aktualisieren Sie die bestehende AWS DMS-Aufgabe in der primären Region

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Notieren Sie den ARN der AWS-DMS-Aufgabe.	Verwenden Sie den Amazon Resource Name (ARN), um den AWS DMS-Aufga bennamen für die spätere Verwendung abzurufen. Um den ARN der AWS-DMS-A ufgabe abzurufen, zeigen Sie die Aufgabe in der Konsole an oder führen Sie den folgenden Befehl aus.
	`aws dms describe-replication-tasks`
	Ein ARN sieht wie folgt aus.
	`arn:aws:dms:us-east-1:<accountid>:task:AN6HFFMPM246XOZVEUHCNSOVF7MQCLTOZUIRAMY`
		AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Die Zeichen nach dem letzten Doppelpunkt entsprechen dem Aufgabennamen, der in einem späteren Schritt verwendet wird.	
Ändern Sie die bestehende AWS DMS-Aufgabe, um den Checkpoint aufzuzeichnen.	AWS DMS erstellt Prüfpunkte, die Informationen enthalten, sodass die Replikationsengine den Wiederherstellungspunkt für den Change-Stream kennt. Um Checkpoint-Informationen aufzuzeichnen, führen Sie die folgenden Schritte in der Konsole aus: 1. Beenden Sie die AWS DMS-Aufgabe. 2. Verwenden Sie den JSON-Editor in der Aufgabe, um den TaskRecoveryTableEnabled Parameter auf true zu setzen. 3. Starten Sie die AWS DMS-Aufgabe.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Checkpoint-Informationen.	Verwenden Sie einen MySQL-Client, der mit dem Writer-Endpunkt für den Cluster verbunden ist, und fragen Sie die neue Metadatentabelle im Reporter-Datenbank-Cluster ab, um zu überprüfen, ob sie existiert und die Informationen zum Replikationsstatus enthält. Führen Sie den folgenden Befehl aus. `select * from awsdms_control.awsdms_txn_state;` Der Aufgabenname aus dem ARN sollte in dieser Tabelle in der `Task_Name` Spalte zu finden sein.	DBA

Erweitern Sie beide Amazon Aurora Aurora-Cluster auf eine DR-Region

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schaffen Sie eine Basisinfrastruktur in der DR-Region.	Erstellen Sie die Basiskomponenten, die für die Erstellung von und den Zugriff auf die Amazon Aurora Aurora-Cluster erforderlich sind: • Virtual Private Cloud (VPC) • Subnetze • Sicherheitsgruppe	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Listen zur Kontrolle des Netzwerkzugriffs • Subnetzgruppe • DB-Parametergruppe • DB-Cluster-Paramet ergruppe Stellen Sie sicher, dass die Konfiguration beider Parametergruppen mit der Konfiguration in der primären Region übereinstimmt.	
Fügen Sie die DR-Region zu beiden Amazon Aurora Aurora-Clustern hinzu.	Fügen Sie eine sekundäre Region (die DR-Region) zu den Haupt- und Reporter-Clustern von Amazon Aurora hinzu. Weitere Informationen finden Sie unter Hinzufügen einer AWS-Region zu einer globalen Amazon Aurora Aurora-Datenbank.	AWS-Administrator

Führen Sie ein Failover durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beenden Sie die AWS DMS-Aufgabe.	Die AWS-DMS-Aufgabe in der primären Region funktioni ert nach einem Failover nicht ordnungsgemäß und sollte gestoppt werden, um Fehler zu vermeiden.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie ein verwaltetes Failover durch.	Führen Sie einen verwaltet en Failover des Hauptdate nbankclusters zur DR-Region durch. Anweisungen finden Sie unter Durchführen von verwalteten geplanten Failovers für globale Amazon Aurora Aurora-Datenbanken . Nachdem das Failover auf dem Haupt-Datenbank-Cluster abgeschlossen ist, führen Sie dieselbe Aktivität auf dem Reporter-Datenbank-Cluster durch.	AWS-Administrator, DBA
Daten in die Hauptdatenbank laden.	Fügen Sie Testdaten in den Writer-Knoten der Hauptdate nbank im DR-Datenbankcluste r ein. Diese Daten werden verwendet, um zu überprüfen, ob die Replikation ordnungsg emäß funktioniert.	DBA
Erstellen Sie die AWS DMS-Replikationsinstanz.	Informationen zum Erstellen der AWS DMS-Replikationsin stanz in der DR-Region finden Sie unter Erstellen einer Replikationsinstanz.	AWS-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die AWS DMS-Quell- und Zielendpunkte.	Informationen zum Erstellen der AWS DMS-Quell- und Zielendpunkte in der DR-Region finden Sie unter Quell- und Zielendpunkte erstellen. Die Quelle sollte auf die Writer-Instance des Haupt-Datenbank-Clusters verweisen. Das Ziel sollte auf die Writer-Instanz des Reporter-Datenbank-Clusters verweisen.	AWS-Administrator, DBA
Besorgen Sie sich den Replikationsprüfpunkt.	Um den Replikationsprüfpunkt zu erhalten, verwenden Sie einen MySQL-Client, um die Metadatentabelle abzufragen, indem Sie Folgendes für den Writer-Knoten im Reporter-Datenbank-Cluster in der DR-Region ausführen. `select * from awsdms_control.awsdms_txn_state;` Suchen Sie in der Tabelle nach dem Wert task_name, der dem ARN der AWS-DMS-Aufgabe entspricht, der in der primären Region existiert und den Sie im zweiten Epic abgerufen haben.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS DMS-Aufgabe.	Erstellen Sie mit der Konsole eine AWS DMS-Aufgabe in der DR-Region. Geben Sie in der Aufgabe die Migration smethode Nur Datenände rungen replizieren an. Weitere Informationen finden Sie unter Aufgabe erstellen. 1. Verwenden Sie den Assistenten, um in den Aufgabeneinstellungen Folgendes anzugeben: • CDC-Startmodus für Quelltransaktionen — Aktivieren Sie den benutzerdefinierten CDC-Startmodus • Benutzerdefinierter CDC-Startpunkt für Quelltran saktionen — Geben Sie einen Wiederherstellungs prüfpunkt an 2. Geben Sie in das Feld Wiederherstellungs-Checkpoint den Wert für den Replikationsprüfpunkt ein, der zuvor durch die Datenbankabfrage in der Tabelle abgerufen wurde. `awsdms_txn_state` 3. Wählen Sie im Bereich mit den Aufgabeneinstellungen den JSON-Editor aus und	AWS-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	setzen Sie den TaskRecov eryTableEnabledParameter auf true. Stellen Sie die Einstellu ng AWS DMS-Aufgabe Migrationsaufgabe starten auf Automatisch bei Erstellung ein.	
Notieren Sie den ARN der AWS-DMS-Aufgabe.	Verwenden Sie den ARN, um den AWS DMS-Aufga bennamen für die spätere Verwendung abzurufen. Führen Sie den folgenden Befehl aus, um den ARN für die AWS-DMS-Aufgabe abzurufen. `aws dms describe-replication-tasks`	AWS-Administrator, DBA
Validieren Sie die replizierten Daten.	Fragen Sie den Reporter-Datenbankcluster in der DR-Region ab, um zu bestätige n, dass die Testdaten, die Sie in den Haupt-Datenbank-Cl uster geladen haben, repliziert wurden.	DBA

Führen Sie ein Failback durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beenden Sie die AWS DMS-Aufgabe.	Die AWS-DMS-Aufgabe in der DR-Region funktioniert nach einem Failback nicht ordnungsgemäß und sollte gestoppt werden, um Fehler zu vermeiden.	AWS-Administrator
Führen Sie ein verwaltetes Failback durch.	Führen Sie ein Failback des Haupt-Datenbank-Clusters auf die primäre Region durch. Anweisungen finden Sie unter Durchführen von verwalteten geplanten Failovers für globale Amazon Aurora Aurora-Datenbanken. Nachdem das Failback auf dem Haupt-Datenbank-Cluster abgeschlossen ist, führen Sie dieselbe Aktivität auf dem Reporter-Datenbank-Cluster durch.	AWS-Administrator, DBA
Besorgen Sie sich den Replikationsprüfpunkt.	Um den Replikationsprüfpunkt zu erhalten, verwenden Sie einen MySQL-Client, um die Metadatentabelle abzufragen, indem Sie Folgendes für den Writer-Knoten im Reporter-Datenbank-Cluster in der DR-Region ausführen. `select * from awsdms_control.awsdms_txn_state;`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Suchen Sie in der Tabelle nach dem `task_name` Wert, der dem ARN der AWS-DMS-Aufgabe entspricht, der in der DR-Region existiert und den Sie im vierten Epic erhalten haben.	
Aktualisieren Sie die AWS-DMS-Quell- und Zielendpunkte.	Nachdem die Datenbank cluster ausgefallen sind, überprüfen Sie die Cluster in der primären Region, um festzustellen, welche Knoten die Writer-Instances sind. Stellen Sie anschließend sicher, dass die vorhandenen AWS-DMS-Quell- und Zielendpunkte in der primären Region auf die Writer-Instances verweisen. Falls nicht, aktualisieren Sie die Endpunkte mit den DNS-Namen (Domain Name System) der Writer-Instance.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS DMS-Aufgabe.	Erstellen Sie mit der Konsole eine AWS DMS-Aufgabe in der primären Region. Geben Sie in der Aufgabe die Migrationsmethode Nur Datenänderungen replizieren an. Weitere Informationen finden Sie unter Aufgabe erstellen. 1. Verwenden Sie in den Aufgabeneinstellungen den Assistenten und geben Sie Folgendes an: • CDC-Startmodus für Quelltransaktionen — Aktivieren Sie den benutzerdefinierten CDC-Startmodus • Benutzerdefinierter CDC-Startpunkt für Quelltransaktionen — Geben Sie einen Wiederherstellungsprüfpunkt an 2. Geben Sie in das Feld Wiederherstellungs-Checkpoint den Wert für den Replikationsprüfpunkt ein, der zuvor durch die Datenbankabfrage in der Tabelle abgerufen wurde. `awsdms_txn_state` 3. Wählen Sie ebenfalls im Bereich mit den Aufgabene	AWS-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	instellungen den JSON-Editor aus und setzen Sie den TaskRecoveryTableEnabledParameter auf true. 4. Stellen Sie abschließend die Einstellung AWS DMS-Aufgabe Migrationsaufgabe starten auf Automatisch bei Erstellung ein.	
Notieren Sie die AWS-DMS-Aufgabe Amazon Resource Name (ARN).	Verwenden Sie den ARN, um den AWS DMS-Aufga bennamen für die spätere Verwendung abzurufen. Führen Sie den folgenden Befehl aus, um den ARN für die AWS-DMS-Aufgabe abzurufen: `aws dms describe-replication-tasks` Der Aufgabenname wird bei der Durchführung eines weiteren verwalteten Failovers oder während eines DR-Szenarios benötigt.	AWS-Administrator, DBA
Löschen Sie AWS DMS-Aufgaben.	Löschen Sie die ursprüngliche (derzeit angehaltene) AWS DMS-Aufgabe in der primären Region und die bestehende AWS DMS-Aufgabe (derzeit gestoppt) in der sekundären Region.	AWS-Administrator

Zugehörige Ressourcen

- Konfiguration Ihres Amazon Aurora Aurora-DB-Clusters
- Verwenden von Amazon Aurora Global Databases
- Arbeiten mit Amazon Aurora MySQL
- Arbeiten mit einer AWS DMS-Replikationsinstanz
- Arbeiten mit AWS DMS-Endpunkten
- Arbeiten mit AWS DMS-Aufgaben
- Was ist AWS CloudFormation?

Zusätzliche Informationen

Die globalen Datenbanken von Amazon Aurora werden in diesem Beispiel für DR verwendet, da sie ein effektives Recovery Time Objective (RTO) von 1 Sekunde und ein Recovery Point Objective (RPO) von weniger als 1 Minute bieten. Beides ist niedriger als bei herkömmlichen replizierten Lösungen und ideal für DR-Szenarien.

Die globalen Datenbanken von Amazon Aurora bieten viele weitere Vorteile, darunter die folgenden:

- Globale Lesevorgänge mit lokaler Latenz — Verbraucher auf der ganzen Welt können mit lokaler Latenz auf Informationen in einer lokalen Region zugreifen.
- Skalierbare sekundäre Amazon Aurora Aurora-DB-Cluster — Sekundäre Cluster können unabhängig voneinander skaliert werden, sodass bis zu 16 schreibgeschützte Replikate hinzugefügt werden können.
- Schnelle Replikation vom primären zum sekundären Amazon Aurora Aurora-DB-Cluster — Die Replikation hat nur geringe Auswirkungen auf die Leistung des primären Clusters. Sie erfolgt auf der Speicherebene mit typischen regionsübergreifenden Replikationslatenzen von weniger als 1 Sekunde.

Dieses Muster verwendet auch AWS DMS für die Replikation. Amazon Aurora Aurora-Datenbanken bieten die Möglichkeit, Read Replicas zu erstellen, was den Replikationsprozess und die DR-Einrichtung vereinfachen kann. AWS DMS wird jedoch häufig zur Replikation verwendet, wenn Datentransformationen erforderlich sind oder wenn die Zieldatenbank zusätzliche Indizes benötigt, über die die Quelldatenbank nicht verfügt.

Migrieren Sie Oracle-Funktionen und -Prozeduren mit mehr als 100 Argumenten nach PostgreSQL

Erstellt von Srinivas Potlachervoo (AWS)

Übersicht

Dieses Muster zeigt, wie Oracle-Datenbankfunktionen und -prozeduren mit mehr als 100 Argumenten nach PostgreSQL migriert werden. Sie können dieses Muster beispielsweise verwenden, um Oracle-Funktionen und -Prozeduren auf einen der folgenden PostgreSQL-kompatiblen AWS-Datenbankservices zu migrieren:

- Amazon Relational Database Service (Amazon RDS) für PostgreSQL
- Amazon Aurora PostgreSQL-Compatible Edition

PostgreSQL unterstützt keine Funktionen oder Prozeduren mit mehr als 100 Argumenten. Um das Problem zu umgehen, können Sie einen neuen Datentyp definieren, der Typfelder enthält, die den Argumenten der Quellfunktion entsprechen. Anschließend können Sie eine PL/pgSQL-Funktion erstellen und ausführen, die den benutzerdefinierten Datentyp als Argument verwendet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Amazon RDS-Oracle-Datenbank-Instance (DB)
- Eine Amazon RDS for PostgreSQL PostgreSQL-DB-Instance oder eine Aurora PostgreSQL-kompatible DB-Instance

Produktversionen

- Amazon RDS Oracle DB-Instance-Versionen 10.2 und höher
- Amazon RDS PostgreSQL-DB-Instance-Versionen 9.4 und höher oder Aurora PostgreSQL-kompatible DB-Instance-Versionen 9.4 und höher
- Oracle SQL Developer Version 18 und höher
- pgAdmin Version 4 und höher

Architektur

Quelltechnologie-Stack

- Amazon RDS Oracle DB-Instance-Versionen 10.2 und höher

Zieltechnologie-Stack

- Amazon RDS PostgreSQL-DB-Instance-Versionen 9.4 und höher oder Aurora PostgreSQL-kompatible DB-Instance-Versionen 9.4 und höher

Tools

AWS-Services

- Amazon Relational Database Service (Amazon RDS) für PostgreSQL unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen PostgreSQL-Datenbank in der AWS-Cloud.
- Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt.

Andere Dienste

- Oracle SQL Developer ist eine integrierte Entwicklungsumgebung, die die Entwicklung und Verwaltung von Oracle-Datenbanken sowohl in herkömmlichen als auch in Cloud-basierten Bereitstellungen vereinfacht.
- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL. Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, verwalten und verwenden können.

Bewährte Methoden

Stellen Sie sicher, dass der Datentyp, den Sie erstellen, mit den Typfeldern übereinstimmt, die in der Oracle-Quellfunktion oder -prozedur enthalten sind.

Epen

Führen Sie eine Oracle-Funktion oder -Prozedur mit mehr als 100 Argumenten aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen oder identifizieren Sie eine bestehende Oracle/PLSQL-Funktion oder -Prozedur mit mehr als 100 Argumenten.	Erstellen Sie eine Oracle/PLSQL-Funktion oder -Prozedur mit mehr als 100 Argumenten. –oder– Identifizieren Sie eine bestehende Oracle/PLSQL-Funktion oder -Prozedur mit mehr als 100 Argumenten. Weitere Informationen finden Sie in den Abschnitten 14.7 CREATE FUNCTION-Anweisung und 14.11 CREATE PROCEDURE-Anweisung in der Oracle-Datenbankdokumentation.	Oracle/PLSQL-Kenntnisse
Kompilieren Sie die Oracle/PLSQL-Funktion oder -Prozedur.	Kompilieren Sie die Oracle/PLSQL-Funktion oder -Prozedur. Weitere Informationen finden Sie in der Oracle Database-Dokumentation unter Funktion kompilieren.	Oracle/PLSQL-Kenntnisse
Führen Sie die Oracle/PLSQL-Funktion aus.	Führen Sie die Oracle/PLSQL-Funktion oder -Prozedur aus. Speichern Sie dann die Ausgabe.	Oracle/PLSQL-Kenntnisse

Definieren Sie einen neuen Datentyp, der den Argumenten der Quellfunktion oder -prozedur entspricht

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie einen neuen Datentyp in PostgreSQL.	Definieren Sie einen neuen Datentyp in PostgreSQL, der dieselben Felder enthält, die in den Argumenten der Oracle-Quellfunktion oder -prozedur vorkommen. Weitere Informationen finden Sie unter CREATE TYPE in der PostgreSQL-Dokumentation.	PostgreSQL PL/PgSQL-Kenntnisse

Erstellen Sie eine PostgreSQL-Funktion, die das neue TYPE-Argument enthält

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine PostgreSQL-Funktion, die den neuen Datentyp enthält.	Erstellen Sie eine PostgreSQL-Funktion, die das neue TYPE Argument enthält. Eine Beispielfunktion finden Sie im Abschnitt Zusätzliche Informationen dieses Musters.	PostgreSQL PL/PgSQL-Kenntnisse
Kompilieren Sie die PostgreSQL-Funktion.	Kompilieren Sie die Funktion in PostgreSQL. Wenn die neuen Datentypfelder mit den Argumenten der Quellfunktion oder -prozedur übereinstimmen, wird die Funktion erfolgreich kompiliert.	PostgreSQL PL/PgSQL-Kenntnisse

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die PostgreSQL-Funktion aus.	Führen Sie die PostgreSQL-Funktion aus.	PostgreSQL PL/PgSQL-Kenntnisse

Fehlerbehebung

Problem	Lösung
Die Funktion gibt den folgenden Fehler zurück: FEHLER: Syntaxfehler in der Nähe von „“ <statement>	Stellen Sie sicher, dass alle Anweisungen der Funktion mit einem Semikolon () enden. `;`
Die Funktion gibt den folgenden Fehler zurück: FEHLER: „“ ist keine bekannte Variable <variable>	Stellen Sie sicher, dass die Variable, die im Funktionshauptteil verwendet wird, im `DECLARE` Abschnitt der Funktion aufgeführt ist.

Zugehörige Ressourcen

- Arbeiten mit Amazon Aurora PostgreSQL (Amazon Aurora Aurora-Benutzerhandbuch für Aurora)
- CREATE TYPE (PostgreSQL-Dokumentation)

Zusätzliche Informationen

Beispiel für eine PostgreSQL-Funktion, die ein TYPE-Argument enthält

```
CREATE OR REPLACE FUNCTION test_proc_new
(
    IN p_rec type_test_proc_args
)
RETURNS void
AS
$BODY$
BEGIN

    /*
```

```
    **************
    The body would contain code to process the input values.
    For our testing, we will display couple of values.
    ***************
    */
    RAISE NOTICE USING MESSAGE = CONCAT_WS('', 'p_acct_id: ', p_rec.p_acct_id);
    RAISE NOTICE USING MESSAGE = CONCAT_WS('', 'p_ord_id: ', p_rec.p_ord_id);
    RAISE NOTICE USING MESSAGE = CONCAT_WS('', 'p_ord_date: ', p_rec.p_ord_date);

END;
$BODY$
LANGUAGE plpgsql
COST 100;
```

Migrieren Sie Amazon RDS for Oracle DB-Instances zu anderen Konten, die AMS verwenden

Erstellt von Pinesh Singal (AWS)

Übersicht

Dieses Muster zeigt Ihnen, wie Sie eine Amazon Relational Database Service (Amazon RDS) für Oracle DB-Instance von einem AWS-Konto zu einem anderen AWS-Konto migrieren. Das Muster gilt für Szenarien, in denen das AWS-Quellkonto keine AWS Managed Services (AMS) verwendet, das Zielkonto jedoch AMS. Sie können die Migration abschließen, indem Sie einen Request for Change (RFC) in AMS verwenden, anstatt die AWS-Managementkonsole für Datenbankoperationen zu verwenden. Dieser Ansatz bietet minimale Ausfallzeiten für eine Oracle-Quelldatenbank mit mehreren Terabyte und einer hohen Anzahl von Transaktionen. Beispielsweise könnte die Ausfallzeit für eine 400-900-GB-Datenbank etwa zwei oder drei Stunden dauern. Die Zeit für die Datenbankmigration ist direkt proportional zur Größe der Amazon RDS for Oracle Oracle-DB-Instance.

> **Important**
>
> Dieses Muster erfordert, dass Sie einen Datenbank-Snapshot der Amazon RDS for Oracle Oracle-DB-Instance in einem Quellkonto erstellen, den Snapshot auf ein Zielkonto kopieren, das AMS verwendet, und dann aus diesem Snapshot durch Raising eine neue DB-Instance erstellen RFCs.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto für das Quellkonto
- Ein aktives AWS-Konto, das AMS für das Zielkonto verwendet
- Amazon RDS für Oracle-DB-Instance, betriebsbereit

Einschränkungen

- Dieselben Eigenschaften oder Konfigurationen für die DB-Instances im Quellkonto werden auf eine neue Ziel-DB-Instance auf AMS kopiert.

- Die RFC-Methode, die in diesem Migrationsansatz verwendet wird, bietet nur begrenzte Funktionen zur Unterstützung von Amazon RDS for Oracle. Sie können auf alle Funktionen von Amazon RDS for Oracle zugreifen, indem Sie eine CloudFormation AWS-Vorlage verwenden, um die Datenbankmigration durchzuführen.
- Es kann zu einem Anwendungsausfall für mehrere Stunden kommen, da die Migration während der geplanten Ausfallzeit abgeschlossen werden muss. Während der Ausfallzeit beenden Sie die DB-Instance im Quellkonto und schalten dann eine neue DB-Instance im Zielkonto live.
- Dieser Migrationsansatz gilt nicht für die Migration einer DB-Instance von einer AWS-Region in eine andere Region innerhalb desselben AWS-Kontos.

Produktversionen

- Oracle Database Standard Edition 2 (SE2) 12.1.0.2.v2-Instance und höher auf Amazon RDS for Oracle
- Amazon RDS for Oracle 11g wird nicht mehr unterstützt (Weitere Informationen finden Sie unter Amazon RDS for Oracle in der Amazon RDS-Dokumentation.)

Architektur

Quelltechnologie-Stack

- Oracle Database SE2 12.1.0.2.v2-Instanz auf Amazon RDS for Oracle
- Amazon RDS-Subnetzgruppe
- Amazon RDS-Optionsgruppe (falls erforderlich)
- Amazon RDS-Parametergruppe (falls erforderlich)
- Sicherheitsgruppe Amazon Virtual Private Cloud (Amazon VPC)
- AWS Key Management Service (AWS KMS) mit von AWS verwalteten Schlüsseln oder vom Kunden verwalteten Schlüsseln
- Rolle AWS Identity and Access Management (IAM) (falls erforderlich)

Zieltechnologie-Stack

- Oracle Database SE2 12.1.0.2.v2-Instanz auf Amazon RDS for Oracle
- Amazon RDS-Subnetzgruppe
- Amazon RDS-Optionsgruppe (falls erforderlich)

- Amazon RDS-Parametergruppe (falls erforderlich)
- Amazon VPC-Sicherheitsgruppe
- AWS Managed Services (AMS)
- AWS KMS mit von AWS verwalteten Schlüsseln und vom Kunden verwalteten Schlüsseln
- IAM-Rolle (falls erforderlich)

Quell- und Ziel-Migrationsarchitektur

Das folgende Diagramm zeigt die Migration einer Amazon RDS for Oracle DB-Instance in einem AWS-Konto zu einer Amazon RDS for Oracle DB-Instance in einem anderen AWS-Konto, das AMS verwendet.

Das Diagramm zeigt den folgenden Workflow:

1. Erstellen Sie einen Datenbank-Snapshot der Amazon RDS for Oracle Oracle-DB-Instance im Quellkonto.
2. Kopieren Sie den Snapshot auf AMS im Zielkonto.
3. Erstellen Sie eine neue Amazon RDS for Oracle DB-Instance aus dem Snapshot im Zielkonto.

Automatisierung und Skalierung

Sie können die Migration automatisieren und skalieren, indem Sie CloudFormation Vorlagen verwenden und RFCs in AMS erstellen. CloudFormation ermöglicht es Ihnen, alle Funktionen von Amazon RDS for Oracle zu nutzen, einschließlich der Möglichkeit, die DB-Instance zu konfigurieren und wiederherzustellen, wenn Sie eine Amazon RDS for Oracle Oracle-DB-Instance aus einem Snapshot erstellen.

Tools

- Amazon Relational Database Service (Amazon RDS) für Oracle unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Oracle-Datenbank in der AWS-Cloud.
- AWS Key Management Service (AWS KMS) unterstützt Sie bei der Erstellung und Kontrolle kryptografischer Schlüssel, um Ihre Daten zu schützen.
- Mit AWS Managed Services (AMS) können Sie Ihre AWS-Infrastruktur effizienter und sicherer betreiben.

Epen

Bereiten Sie sich auf die Umstellung auf das Zielkonto vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen benutzerdefinierten AWS-KMS-Schlüssel.	1. Rufen Sie einen automatisierten RFC namens Create KMS key auf, um einen benutzerdefinierten KMS-Schlüssel von Ihrem Zielkonto aus zu erstellen. 2. **Note** Teilen Sie Ihren benutzerdefinierten KMS-Schlüssel mit dem Quellkonto. : Sie können Amazon RDS for Oracle Oracle-DB-Instances, die den von AWS verwalteten Standardschlüssel für Amazon RDS (`aws/rds`) verwenden, nicht gemeinsam nutzen. Teilen Sie stattdessen die DB-Instance, indem Sie die DB-Instance anhand Ihres KMS-Schlüssels erneut verschlüsseln.	AWS, AMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Sicherheitsgruppe.	Rufen Sie einen automatisierten RFC namens Create security group auf, um von Ihrem Zielkonto aus eine Sicherheitsgruppe für Ihre VPC zu erstellen. Stellen Sie sicher, dass Sie Folgendes angeben: • Neuer Name der Sicherheitsgruppe • Regeln für ein- und ausgehenden TCP- und UDP-Eingang • Standardkennzeichnungen	AWS, AMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Überprüfen Sie Ihre Amazon RDS-Ressourcen.	Die folgenden Ressourcen werden erstellt, wenn eine Amazon RDS for Oracle DB-Instance erstellt wird: • Amazon RDS-Subnetzgruppe (basierend auf der Subnetz-ID) • Amazon RDS-Optionsgruppe (basierend auf dem Snapshot der Quell-DB-Instance) • Amazon RDS-Parametergruppe (basierend auf dem Snapshot der DB-Instance) Wenn Sie die Amazon RDS-Ressourcen überprüfen möchten, die bei der Erstellung Ihrer DB-Instance erstellt wurden, können Sie eine Verbindung zu Ihrer Oracle-DB-Instance herstellen und Ihre Subnetzgruppe, Optionsgruppe und Parametergruppe in der Amazon RDS-Konsole suchen.	AWS

Übersteigen Sie das Quellkonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stoppen Sie die Anwendung.	Stoppen Sie die Anwendung und ihre abhängigen Dienste. Sie müssen den gesamten Datenverkehr zur Datenbank im Quellkonto beenden.	Besitzer der App
Machen Sie einen manuellen Schnappschuss.	Erstellen Sie manuell einen DB-Snapshot der Amazon RDS for Oracle Oracle-DB-Instance im Quellkonto.	AWS
Stoppen Sie die DB-Instance.	Stoppen Sie die Amazon RDS for Oracle DB-Instance.	AWS
Kopieren Sie den Snapshot.	Kopieren Sie den DB-Snapshot in dasselbe Quellkonto und verwenden Sie dann den vom Zielkonto gemeinsam genutzten benutzerdefinierten KMS-Schlüssel, um die kopierte DB-Snapshot-Datei erneut zu verschlüsseln.	AWS
Teilen Sie den Snapshot.	Teilen Sie den neuen Snapshot (mit dem benutzerdefinierten KMS-Schlüssel kopiert) mit dem Zielkonto.	AWS

Überspringen Sie das Zielkonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopieren Sie den Snapshot.	Rufen Sie einen automatisierten RFC namens Copy RDS snapshot auf, um den DB-Snapshot auf dasselbe Zielkonto zu kopieren und den standardmäßigen AWS-verwalteten KMS-Schlüssel zu verwenden, der für die erneute Verschlüsselung erstellt wurde. Dies ist erforderlich, um das Zielkonto zum Eigentümer des neuen Snapshots zu machen und um zu ermöglichen, dass die aus dem Snapshot erstellte Amazon RDS for Oracle Oracle-DB-Instance bei Bedarf der Optionsgruppe zugeordnet werden kann.	AWS, AMS
Erstellen Sie eine DB-Instance aus dem Snapshot.	Rufen Sie einen automatisierten RFC namens Create DB from snapshot auf, um aus dem Snapshot eine Amazon RDS for Oracle Oracle-DB-Instance zu erstellen. Stellen Sie sicher, dass Sie Folgendes angeben: • Im vorherigen Schritt wurde eine neue Snapshot-ID erstellt	AWS, AMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• VPC-ID • Subnetz-ID • RDS-Instanz-ID • Standardkennzeichnungen	
Hängen Sie die Instance an die Sicherheitsgruppe an und führen Sie Konfigurationsaktualisierungen durch.	1. Rufen Sie einen manuellen RFC namens Update Other auf, um die Amazon RDS for Oracle DB-Instance, die Sie zuvor erstellt haben, mit der zuvor erstellten VPC-Sicherheitsgruppe zu verknüpfen. 2. Nehmen Sie weitere Änderungen an der Konfiguration der Amazon RDS for Oracle Oracle-DB-Instance vor.	AWS, AMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die DB-Instance.	Testen Sie die Endpunktk onnektivität der neuen Amazon RDS for Oracle DB-Instance, indem Sie sich bei einer beliebigen Instance oder einem Anwendung sserver anmelden, der auf derselben Sicherheitsgruppe gehostet wird, und indem Sie Telnet verwenden, um eine Verbindung zum 1521-Port herzustellen. Weitere Informationen finden Sie unter Verbindung zu einer Amazon RDS-DB-Instance in der Amazon RDS-Dokumentation. **Note** Wenn die Anmeldeda ten des primären Benutzers verfügbar sind, können Sie die Amazon RDS for Oracle DB-Instance testen, indem Sie sich von einem beliebige n SQL-Client (z. B. Oracle SQL Developer) aus anmelden.	AWS, DBA

Zugehörige Ressourcen

- AWS Managed Services (AWS-Dokumentation)

- So RFCs funktionieren Sie (Dokumentation zu AWS Managed Services)
- Verschlüsselte Snapshots teilen (Amazon RDS-Benutzerhandbuch)
- Wie kann ich einen verschlüsselten Amazon RDS-DB-Snapshot mit einem anderen Konto teilen? (AWS-Wissenszentrum)
- Was ist Amazon Relational Database Service (Amazon RDS)? (Amazon RDS-Benutzerhandbuch)
- Amazon RDS for Oracle (Amazon RDS-Benutzerhandbuch)
- Verwenden der AMS-Konsolen (Dokumentation zu AWS Managed Services)

Zusätzliche Informationen

Machen Sie die Migration rückgängig

Wenn Sie die Migration rückgängig machen möchten, führen Sie die folgenden Schritte aus:

1. Rufen Sie einen manuellen RFC (Update Other) vom Zielkonto aus, um den im Zielkonto erstellten Datenbank-Stack zu löschen.
2. Aktualisieren Sie die Anwendungskonfiguration so, dass sie auf die Amazon RDS for Oracle DB-Instance im Quellkonto verweist.
3. Starten Sie die Amazon RDS for Oracle DB-Instance im Quellkonto.

Migrieren Sie Oracle OUT-Bind-Variablen in eine PostgreSQL-Datenbank

Erstellt von Bikash Chandra Rout (AWS) und Vinay Paladi (AWS)

Übersicht

Dieses Muster zeigt, wie Oracle OUT Database-Bindungsvariablen zu einem der folgenden PostgreSQL-kompatiblen AWS-Datenbankservices migriert werden:

- Amazon Relational Database Service (Amazon RDS) für PostgreSQL
- Amazon Aurora PostgreSQL-Compatible Edition

PostgreSQL unterstützt keine OUT Bind-Variablen. Um dieselbe Funktionalität in Ihren Python-Anweisungen zu erhalten, können Sie eine benutzerdefinierte PL/pgSQL-Funktion erstellen, die stattdessen die Paketvariablen GET und **SET**verwendet. Um diese Variablen anzuwenden, verwendet das in diesem Muster bereitgestellte Beispiel-Wrapper-Funktionsskript ein AWS Schema Conversion Tool (AWS SCT) -Erweiterungspaket.

> **Note**
>
> Wenn es sich bei der EXECUTE IMMEDIATE SELECT Oracle-Anweisung um eine Anweisung handelt, die höchstens eine Zeile zurückgeben kann, hat es sich bewährt, wie folgt vorzugehen:

- Fügen Sie OUT Bind-Variablen (Definitionen) in die INTO Klausel ein
- Fügen Sie IN Bind-Variablen in die USING Klausel ein

Weitere Informationen finden Sie in der Oracle-Dokumentation unter EXECUTE IMMEDIATE-Anweisung.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle Database 10g-Quelldatenbank (oder neuer) in einem lokalen Rechenzentrum

- Eine Amazon RDS for PostgreSQL PostgreSQL-DB-Instance oder eine Aurora PostgreSQL-kompatible DB-Instance

Architektur

Quelltechnologie-Stack

- Lokale Oracle Database 10g-Datenbank (oder neuer)

Zieltechnologie-Stack

- Eine Amazon RDS for PostgreSQL PostgreSQL-DB-Instance oder eine Aurora PostgreSQL-kompatible DB-Instance

Zielarchitektur

Das folgende Diagramm zeigt einen Beispiel-Workflow für die Migration von Oracle 0UT Database-Bindungsvariablen in eine PostgreSQL-kompatible AWS-Datenbank.

Das Diagramm zeigt den folgenden Workflow:

1. AWS SCT konvertiert das Quelldatenbankschema und einen Großteil des benutzerdefinierten Codes in ein Format, das mit der PostgreSQL-kompatiblen AWS-Zieldatenbank kompatibel ist.
2. Alle Datenbankobjekte, die nicht automatisch konvertiert werden können, werden von der PL/pgSQL-Funktion gekennzeichnet. Objekte, die markiert sind, werden dann manuell konvertiert, um die Migration abzuschließen.

Tools

- Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt.
- Amazon Relational Database Service (Amazon RDS) für PostgreSQL unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen PostgreSQL-Datenbank in der AWS-Cloud.

- Das AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein mit der Zieldatenbank kompatibles Format konvertiert werden.
- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL. Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, verwalten und verwenden können.

Epen

Migrieren Sie Oracle OUT-Bind-Variablen mithilfe einer benutzerdefinierten PL/pgSQL-Funktion und AWS SCT

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Connect zu Ihrer PostgreSQL-kompatiblen AWS-Datenbank her.	Nachdem Sie Ihre DB-Instance erstellt haben, können Sie jede Standard-SQL-Client-Anwendung verwenden, um eine Verbindung zu einer Datenbank in Ihrem DB-Cluster herzustellen. Sie können beispielsweise pgAdmin verwenden, um eine Verbindung zu Ihrer DB-Instance herzustellen. Weitere Informationen finden Sie in einer der folgenden Seiten: • Herstellen einer Verbindung zu einer Amazon RDS-DB-Instance im Amazon RDS-Benutzerhandbuch • Herstellen einer Verbindung zu einem Amazon Aurora Aurora-DB-Cluster im	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon Aurora Aurora-Benutzerhandbuch	
Fügen Sie das Beispiel-Wrapper-Funktionsskript aus diesem Muster zum Hauptschema der Zieldatenbank hinzu.	Kopieren Sie das Beispiel für ein PL/pgSQL-Wrapper-Funktionsskript aus dem Abschnitt Zusätzliche Informationen dieses Musters. Fügen Sie dann die Funktion zum Hauptschema der Zieldatenbank hinzu. Weitere Informationen finden Sie im Abschnitt CREATE FUNCTION der PostgreSQL-Dokumentation.	Ingenieur für Migration
(Optional) Aktualisieren Sie den Suchpfad im Hauptschema der Zieldatenbank, sodass er das Test_PG-Schema enthält.	Um die Leistung zu verbessern, können Sie die PostgreSQL-Variable search_path so aktualisieren, dass sie den Schemanamen test_PG enthält. Wenn Sie den Schemanamen in den Suchpfad aufnehmen, müssen Sie den Namen nicht jedes Mal angeben, wenn Sie die PL/pgSQL-Funktion aufrufen. Weitere Informationen finden Sie in Abschnitt 5.9.3 Der Schemasuchpfad in der PostgreSQL-Dokumentation.	Migrationsingenieur

Zugehörige Ressourcen

- AWS-Schemakonvertierungstool
- OUT-Bindungsvariablen (Oracle-Dokumentation)
- Verbessern Sie die Leistung von SQL-Abfragen mithilfe von Bind-Variablen (Oracle-Blog)

Zusätzliche Informationen

Beispiel für eine PL/pgSQL-Funktion

```
/* Oracle */

CREATE or replace PROCEDURE test_pg.calc_stats_new1 (
                                                a NUMBER,
                                                b NUMBER,
                                                result out NUMBER
                                               )

IS
BEGIN
result:=a+b;
END;
/
/* Testing */
set serveroutput on
DECLARE
  a NUMBER := 4;
  b NUMBER := 7;
  plsql_block VARCHAR2(100);
  output number;
BEGIN
  plsql_block := 'BEGIN test_pg.calc_stats_new1(:a, :b,:output); END;';
  EXECUTE IMMEDIATE plsql_block USING a, b,out output;  -- calc_stats(a, a, b, a)
  DBMS_OUTPUT.PUT_LINE('output:'||output);
END;

output:11


PL/SQL procedure successfully completed.

--Postgres--
```

```
/* Example : 1 */
CREATE OR REPLACE FUNCTION test_pg.calc_stats_new1(
                                                    w integer,
                                                    x integer
                                                  )
RETURNS integer
AS
$BODY$
begin
      return w + x ;
end;
$BODY$
LANGUAGE  plpgsql;


CREATE OR REPLACE FUNCTION aws_oracle_ext.set_package_variable(
                                                                 package_name name,
                                                                 variable_name name,
                                                                 variable_value
 anyelement
                                                               )
    RETURNS void
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
begin
    perform set_config
      ( format( '%s.%s',package_name, variable_name )
      , variable_value::text
      , false );
  end;
$BODY$;

CREATE OR REPLACE FUNCTION aws_oracle_ext.get_package_variable_record(
                                                                       package_name
 name,
                                                                       record_name name
                                                                     )
RETURNS text
LANGUAGE 'plpgsql'
    COST 100
```

```
    VOLATILE
AS $BODY$
begin
    execute 'select ' || package_name || '$Init()';

    return aws_oracle_ext.get_package_variable
        (
         package_name := package_name
        , variable_name := record_name || '$REC' );
end;
$BODY$;

--init()--
CREATE OR REPLACE FUNCTION test_pg.init()
RETURNS void
AS
$BODY$
BEGIN
if aws_oracle_ext.is_package_initialized('test_pg' ) then
      return;
    end if;
    perform aws_oracle_ext.set_package_initialized
      ('test_pg' );
PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_output', NULL::INTEGER);
PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_status', NULL::text);
END;
$BODY$
LANGUAGE  plpgsql;

/* callable for 1st Example */

DO $$
declare
v_sql text;
v_output_loc int;
a integer :=1;
b integer :=2;
BEGIN
perform  test_pg.init();
--raise notice 'v_sql %',v_sql;
execute 'do $a$ declare v_output_l int; begin select * from test_pg.calc_stats_new1('||
a||','||b||') into v_output_l;
PERFORM aws_oracle_ext.set_package_variable(''test_pg'', ''v_output'', v_output_l) ;
 end; $a$'  ;
```

```
v_output_loc := aws_oracle_ext.get_package_variable('test_pg', 'v_output');
raise notice 'v_output_loc %',v_output_loc;
END ;
$$

/*In above Postgres example we have set the value of v_output using v_output_l in the
 dynamic anonymous block to mimic the
  behaviour of oracle out-bind variable .*/

--Postgres Example : 2 --
CREATE OR REPLACE FUNCTION test_pg.calc_stats_new2(
 w integer,
 x integer,
inout status text,
 out result integer)
AS
$BODY$
DECLARE
begin
result :=  w + x ;
status := 'ok';
end;
$BODY$
LANGUAGE  plpgsql;

/* callable for 2nd Example */
DO $$
declare
v_sql text;
v_output_loc int;
v_staus text:= 'no';
a integer :=1;
b integer :=2;
BEGIN
perform  test_pg.init();
execute 'do $a$ declare v_output_l int; v_status_l text; begin select * from
 test_pg.calc_stats_new2('||a||','||b||','''||v_staus||''') into v_status_l,v_output_l;
PERFORM aws_oracle_ext.set_package_variable(''test_pg'', ''v_output'', v_output_l) ;
PERFORM aws_oracle_ext.set_package_variable(''test_pg'', ''v_status'', v_status_l) ;
end; $a$'  ;
v_output_loc := aws_oracle_ext.get_package_variable('test_pg', 'v_output');
v_staus := aws_oracle_ext.get_package_variable('test_pg', 'v_status');
raise notice 'v_output_loc %',v_output_loc;
raise notice 'v_staus %',v_staus;
```

```
END ;
$$
```

Migrieren Sie SAP HANA zu AWS mithilfe von SAP HSR mit demselben Hostnamen

Erstellt von Pradeep Puliyampatta (AWS)

Übersicht

SAP HANA-Migrationen zu Amazon Web Services (AWS) können mit mehreren Optionen durchgeführt werden, darunter Sicherung und Wiederherstellung, Export und Import sowie SAP HANA System Replication (HSR). Die Auswahl einer bestimmten Option hängt von der Netzwerkkonnektivität zwischen Quell- und Ziel-SAP-HANA-Datenbanken, der Größe der Quelldatenbank, Überlegungen zu Ausfallzeiten und anderen Faktoren ab.

Die SAP HSR-Option für die Migration von SAP HANA-Workloads zu AWS funktioniert gut, wenn ein stabiles Netzwerk zwischen Quell- und Zielsystem besteht und die gesamte Datenbank (SAP HANA DB-Replikationssnapshot) innerhalb eines Tages vollständig repliziert werden kann, wie von SAP für die Netzwerkdurchsatzanforderungen für SAP HSR festgelegt. Die Ausfallzeiten bei diesem Ansatz beschränken sich auf die Durchführung der Übernahme in der AWS Zielumgebung, die Sicherung der SAP HANA-DB und Aufgaben nach der Migration.

SAP HSR unterstützt die Verwendung verschiedener Hostnamen (Hostnamen, die unterschiedlichen IP-Adressen zugeordnet sind) für den Replikationsverkehr zwischen dem Primär- oder Quell- und dem Sekundär- oder Zielsystem. Sie können dies tun, indem Sie diese spezifischen Gruppen von Hostnamen im Abschnitt unter definieren. `[system_replication_hostname_resolution]` `global.ini` In diesem Abschnitt müssen alle Hosts des primären und des sekundären Standorts auf jedem Host definiert werden. Detaillierte Konfigurationsschritte finden Sie in der SAP-Dokumentation.

Eine wichtige Erkenntnis aus dieser Konfiguration ist, dass sich die Hostnamen im Primärsystem von den Hostnamen im Sekundärsystem unterscheiden müssen. Andernfalls können die folgenden Fehler beobachtet werden.

- `"each site must have a unique set of logical hostnames"`
- `"remoteHost does not match with any host of the source site. All hosts of source and target site must be able to resolve all hostnames of both sites correctly"`

Die Anzahl der Schritte nach der Migration kann jedoch reduziert werden, indem derselbe SAP HANA DB-Hostname in der AWS Zielumgebung verwendet wird.

Dieses Muster bietet eine Problemumgehung für die Verwendung desselben Hostnamens in Quell- und Zielumgebungen, wenn Sie die SAP HSR-Option verwenden. Mit diesem Muster können Sie die Option SAP HANA Hostname Rename verwenden. Sie weisen der SAP HANA-Zieldatenbank einen temporären Hostnamen zu, um die Eindeutigkeit des Hostnamens für SAP HSR zu gewährleisten. Nachdem die Migration den Meilenstein der Übernahme in der SAP HANA-Zielumgebung abgeschlossen hat, können Sie den Hostnamen des Zielsystems wieder auf den Hostnamen des Quellsystems zurücksetzen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver. AWS-Konto
- Eine Virtual Private Cloud (VPC) mit einem Virtual Private Network (VPN) -Endpunkt oder einem Router.
- AWS Client VPN oder AWS Direct Connect so konfiguriert, dass Dateien von der Quelle zum Ziel übertragen werden.
- SAP HANA-Datenbanken sowohl in der Quell- als auch in der Zielumgebung. Das Ziel-Patch-Level für SAP HANA DB sollte innerhalb derselben SAP HANA Platform-Edition dem Quell-Patch-Level der SAP HANA-DB entsprechen oder höher sein. Beispielsweise kann die Replikation nicht zwischen HANA 1.0- und HANA 2.0-Systemen eingerichtet werden. Weitere Informationen finden Sie unter Frage 15 in SAP-Hinweis: 1999880 — Häufig gestellte Fragen: SAP HANA-Systemreplikation.
- SAP-Anwendungsserver in der Zielumgebung.
- Amazon Elastic Block Store (Amazon EBS) -Volumes in der Zielumgebung.

Einschränkungen

Die folgende Liste von SAP-Dokumenten behandelt bekannte Probleme im Zusammenhang mit dieser Problemumgehung, einschließlich Einschränkungen in Bezug auf dynamisches Tiering und Scale-out-Migrationen für SAP HANA:

- 2956397 — Das Umbenennen des SAP HANA-Datenbanksystems ist fehlgeschlagen

- 2222694 — Beim Versuch, das HANA-System umzubenennen, wird der folgende Fehler angezeigt: „Die Quelldateien gehören nicht dem ursprünglichen sidadm-Benutzer (uid = xxxx)“
- 2607227 — hdblcm: register_rename_system: Das Umbenennen der SAP HANA-Instanz ist fehlgeschlagen
- 2630562 — Die Umbenennung des HANA-Hostnamens ist fehlgeschlagen und HANA wird nicht gestartet
- 2935639 — sr_register verwendet nicht den Hostnamen, der unter system_replication_hostname_resolution im Abschnitt global.ini angegeben ist
- 2710211 — Fehler: Quellsystem und Zielsystem haben überlappende logische Hostnamen
- 2693441 — Ein SAP HANA-System konnte aufgrund eines Fehlers nicht umbenannt werden
- 2519672 — Die primäre und die sekundäre Version von HANA haben unterschiedliche System-PKI-SSFS-Daten und -Schlüssel oder können nicht überprüft werden
- 2457129 — Das Umbenennen von SAP HANA-Systemhosts ist nicht zulässig, wenn dynamisches Tiering Teil der Landschaft ist
- 2473002 — Verwendung der HANA-Systemreplikation zur Migration von Scale-Out-Systemen (Es gibt keine Einschränkungen, die SAP bei der Verwendung dieses Ansatzes zur Umbenennung von Hostnamen für Scale-out-SAP-HANA-Systeme vorsieht. Das Verfahren muss jedoch auf jedem einzelnen Host wiederholt werden. Für diesen Ansatz gelten auch andere Einschränkungen bei der Scale-Out-Migration.)

Produktversionen

- Diese Lösung gilt für die SAP HANA DB Platform Edition 1.0 und 2.0.

Architektur

Einrichtung der Quelle

In der Quellumgebung ist eine SAP HANA-Datenbank installiert. Alle SAP-Anwendungsserververbindungen und DB-Schnittstellen verwenden denselben Hostnamen für Client-Verbindungen. Das folgende Diagramm zeigt den Beispiel-Hostnamen der Quelle `hdbhost` und die entsprechende IP-Adresse.

Ziel-Setup

Die AWS Cloud Zielumgebung verwendet denselben Hostnamen, um eine SAP HANA-Datenbank auszuführen. Die Zielumgebung auf AWS umfasst Folgendes:

- SAP HANA-Datenbank
- SAP-Anwendungsserver
- EBS-Datenträger

Zwischenkonfiguration

In der folgenden Abbildung wird der Hostname in der AWS Zielumgebung vorübergehend umbenannt, `temp-host` sodass die Hostnamen in der Quelle und im Ziel eindeutig sind. Nachdem die Migration den Meilenstein der Übernahme in der Zielumgebung abgeschlossen hat, wird der virtuelle Hostname des Zielsystems unter Verwendung des ursprünglichen Namens, umbenannt. `hdbhost`

Die Zwischenkonfiguration umfasst eine der folgenden Optionen:

- AWS Client VPN mit einem Client-VPN-Endpunkt
- AWS Direct Connect Verbindung zu einem Router herstellen

SAP-Anwendungsserver in der AWS Zielumgebung können entweder vor der Einrichtung der Replikation oder nach der Übernahme installiert werden. Die Installation der Anwendungsserver vor der Einrichtung der Replikation kann jedoch dazu beitragen, die Ausfallzeiten während der Installation, der Konfiguration der Hochverfügbarkeit und der Backups zu reduzieren.

Tools

AWS-Services

- AWS Client VPNist ein verwalteter clientbasierter VPN-Dienst, mit dem Sie sicher auf AWS Ressourcen und Ressourcen in Ihrem lokalen Netzwerk zugreifen können.
- AWS Direct Connectverbindet Ihr internes Netzwerk über ein Standard-Ethernet-Glasfaserkabel mit einem AWS Direct Connect Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen

direkt zur Öffentlichkeit AWS-Services einrichten und dabei Internetdienstanbieter in Ihrem Netzwerkpfad umgehen.

- Amazon Elastic Block Store (Amazon EBS) bietet Speichervolumen auf Blockebene zur Verwendung mit Amazon Elastic Compute Cloud (Amazon EC2) -Instances. EBS-Volumes verhalten sich wie unformatierte Blockgeräte. Sie können diese Volumes als Geräte auf Ihren Instances mounten.

Andere Tools

- SAP-Anwendungsserver — SAP-Anwendungsserver bieten Programmierern die Möglichkeit, Geschäftslogik auszudrücken. Der SAP-Anwendungsserver führt die Datenverarbeitung auf der Grundlage der Geschäftslogik durch. Die eigentlichen Daten werden in einer Datenbank gespeichert, die eine separate Komponente ist.
- SAP HANA Cockpit und SAP HANA Studio — Sowohl SAP HANA Cockpit als auch SAP HANA Studio bieten eine administrative Schnittstelle zur SAP HANA-Datenbank. In SAP HANA Studio ist die SAP HANA-Verwaltungskonsole die Systemansicht, die relevante Inhalte für die SAP HANA-Datenbankadministration bereitstellt.
- SAP HANA-Systemreplikation — Die SAP HANA-Systemreplikation (SAP HSR) ist das von SAP bereitgestellte Standardverfahren für die Replikation von SAP HANA-Datenbanken. Die erforderlichen ausführbaren Dateien für SAP HSR sind Teil des SAP HANA-Serverkerns selbst.

Epen

Bereiten Sie die Quell- und Zielumgebung vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren und konfiguri eren Sie die SAP HANA-Date nbanken.	Stellen Sie in der Quell- und Zielumgebung sicher, dass die SAP HANA DB gemäß den bewährten Methoden von SAP HANA installiert und konfiguri ert ist. Weitere Informationen finden Sie unter SAP HANA unter AWS.	SAP-Basisverwaltung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ordnen Sie die IP-Adresse zu.	Stellen Sie in der Zielumgebung sicher, dass der temporäre Hostname einer internen IP-Adresse zugewiesen ist. 1. Weisen Sie der EC2 Instance in der AWS-Managementkonsole eine sekundäre IPv4 Adresse zu, indem Sie zu Instance EC2, Actions, Networking, IP-Adresse verwalten, Neue IP-Adresse zuweisen navigieren. 2. Um dem EC2 Netzwerkadapter (NIC) dieselbe Adresse vom Betriebssystem aus als Root-Benutzer zuzuweisen, führen Sie den Befehl `ip addr add <IP>/32 dev eth0` aus und `<IP>` ersetzen Sie ihn durch die IP-Adresse aus Schritt 1.	AWS-Verwaltung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ziel-Hostnamen auflösen	Vergewissern Sie sich in der sekundären SAP HANA DB, dass beide Hostnamen (`hdbhostundtemp-host`) für die SAP HANA-Replikationsnetzwerke aufgelöst wurden, indem Sie die entsprechenden Hostnamen in der Datei aktualisieren. `/etc/hosts`	Linux-Verwaltung
Sichern Sie die Quell- und Zieldatenbanken von SAP HANA.	Verwenden Sie SAP HANA Studio oder das SAP HANA Cockpit, um Backups auf den SAP HANA-Datenbanken durchzuführen.	SAP-Basisverwaltung
PKI-Zertifikate des Exchange-Systems.	(Gilt nur für SAP HANA 2.0 und höher) Exchange-Zertifikate im sicheren Speicher der Public-Key-Infrastruktur (PKI) des Systems im Dateisystemspeicher (SSFS) zwischen der primären und der sekundären Datenbank. Weitere Informationen finden Sie im SAP-Hinweis 2369981 — Erforderliche Konfigurationsschritte für die Authentifizierung mit SAP HANA System Replication.	SAP-Basisverwaltung

Benennen Sie die Zieldatenbank SAP HANA um

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stoppen Sie die Verbindungen mit den Zielclients.	Fahren Sie in der Zielumgebung die SAP-Anwendungsserver und andere Client-Verbindungen herunter.	SAP-Basisverwaltung

Benennen Sie die Ziel-SAP HANA-Datenbank in den temporären Hostnamen um.	1. Benennen Sie als Root-Benutzer den Zielhostnamen der SAP HANA-DB mithilfe von resident in den temporären Hostnamen um. `hdblcm`
	`root $> cd /hana/shared/<SID/hdblcm`
	`root $> ./hdblcm`
	2. Wählen Sie eine Option. 9 `| rename_system | Rename the SAP HANA Database System`
	3. Geben Sie den neuen Namen ein: `temp-host .`
	4. Sie können andere Optionen nach Bedarf validieren. Achten Sie jedoch darauf, dass Sie die Host-Umbenennung nicht mit einer SID-Änderung verwechseln (SAP-Hinweis 2598814 — hdblcm: SID-Umbenennung schlägt fehl).
		SAP-Basisverwaltung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Das Stoppen und Starten der SAP HANA-DB wird von gesteuert. `hdblcm`	
Weisen Sie Replikationsnetzwerke zu.	Geben Sie in der `global.ini` Datei des Quellsystems unter dem `[system_replication_hostname_resolution]` Header die Details zum Quell- und Zielreplikationsnetzwerk an. Kopieren Sie dann die Einträge in die `global.ini` Datei auf dem Zielsystem.	SAP-Basisverwaltung
Aktivieren Sie die Replikation auf der Primärseite.	Führen Sie den folgenden Befehl aus, um die Replikation auf der SAP HANA-Quelldatenbank zu aktivieren. `hdbnsutil -sr_enable --name=siteA`	SAP-Basisverwaltung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Registrieren Sie die Ziel-SAP HANA DB als Sekundärs ystem.	Um die Ziel-SAP-HANA-DB als sekundäres Quellsyst em für SAP HSR zu registrie ren, wählen Sie asynchrone Replikation.
	`(sid)adm $> HDB stop`
	`(sid)adm $> hdbnsutil -sr_register –name=sitеB –remotehost=hdbhost /`
	`--remoteInstance=00 –replicationMode=async –operationMode=logreplay`
	`(sid)adm $> HDB start`
	Alternativ können Sie die `–online` Option zur Registrie rung wählen. In diesem Fall müssen Sie die SAP HANA DB nicht stoppen und starten.
		SAP-Basisverwaltung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Synchronisation validieren.	Stellen Sie in der SAP HANA-Quelldatenbank sicher, dass alle Protokolle auf das Zielsystem angewende t werden (da es sich um eine asynchrone Replikation handelt).
	
	Um die Replikation zu überprüfen, führen Sie auf der Quelle die folgenden Befehle aus.
	
	`(sid)adm $> cdpy`
	`(sidadm $> python systemReplicationStatus.py`
		SAP-Basisverwaltung

Fahren Sie die SAP-Quell anwendung und die SAP HANA DB herunter.	Führen Sie während der Umstellung auf die Migration das Quellsystem (die SAP-Anwendung und die SAP HANA-Datenbank) herunter.	SAP-Basisverwaltung
Führen Sie eine Übernahme am Zielort durch.	Führen Sie den Befehl aus, um eine Übernahme am Ziel auf AWS durchzufü hrenhdbnsutil -sr_takeover .	SAP-Basisverwaltung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schalten Sie auf der Ziel-SAP HANA-Datenbank die Replikation aus.	Um die Replikationsmetadaten zu löschen, beenden Sie die Replikation auf dem Zielsystem, indem Sie den Befehl ausführen`hdbnsutil -sr_disable` . **Note** Dies entspricht dem SAP-Hinweis 2693441 — Ein SAP HANA-System konnte aufgrund eines Fehlers nicht umbenannt werden.	SAP-Basisverwaltung
Sichern Sie die Ziel-SAP HANA-Datenbank.	Nach erfolgreicher Übernahme empfehlen wir, ein vollständiges SAP HANA DB-Backup durchzuführen.	SAP-Basisverwaltung

Kehren Sie zum ursprünglichen Hostnamen im Zielsystem zurück

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Setzen Sie den Hostnamen der SAP HANA DB-Zieldatenbank auf den ursprünglichen Hostnamen zurück.	1. Um den Zielhostnamen der SAP HANA-DB auf den ursprünglichen virtuellen Hostnamen zurückzusetzen, verwenden Sie resident. `hdblcm`	SAP-Basisverwaltung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	``` root $> cd /hana/sha red/<SID>/hdblcm root $> ./hdblcm ``` 2. Wählen Sie eine Option. 9 `| rename_system | Rename the SAP HANA Database System` 3. Geben Sie den neuen Namen ein:`hdbhost`. Sie können andere Optionen nach Bedarf validieren. Achten Sie jedoch darauf, dass Sie die Host-Umbenennung nicht mit einer SID-Änderung verwechseln (SAP-Hinweis 2598814 — hdblcm: SID-Umbenennung schlägt fehl).	
Passen Sie hdbuserstore an.	Passen Sie die `hdbuserstore` Details an, die auf die Quelldetails verweisen. `schema/user` Die detaillierten Schritte finden Sie in der SAP-Dokumentation. Führen Sie den Befehl aus, um diesen Schritt zu validieren`R3trans -d`. Das Ergebnis sollte eine erfolgreiche Verbindung zur SAP HANA-Datenbank widerspiegeln.	SAP-Basisverwaltung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Client-Verbindungen.	Starten Sie in der Zielumgebung die SAP-Anwendungsserver und andere Client-Verbindungen.	SAP-Basisverwaltung

Zugehörige Ressourcen

SAP-Referenzen

Referenzen zur SAP-Dokumentation werden häufig von SAP aktualisiert. Um auf dem Laufenden zu bleiben, lesen Sie den SAP-Hinweis 2407186 — Anleitungen und Whitepapers für SAP HANA High Availability.

Zusätzliche SAP-Hinweise

- 2550327 — So benennen Sie ein SAP HANA-System um
- 1999880 — Häufig gestellte Fragen: SAP HANA-Systemreplikation
- 2078425 — Hinweis zur Fehlerbehebung für das Lifecycle-Management-Tool hdblcm für die SAP HANA-Plattform
- 2592227 — Änderung des FQDN-Suffixes in HANA-Systemen
- 2048681 — Durchführung von Verwaltungsaufgaben für das Lebenszyklusmanagement der SAP HANA-Plattform auf Systemen mit mehreren Hosts ohne SSH- oder Root-Anmeldeinformationen

SAP-Dokumente

- Netzwerkverbindung zur Systemreplikation
- Auflösung des Hostnamens für die Systemreplikation

AWS Verweise

- Migration von SAP HANA von anderen Plattformen auf AWS

Zusätzliche Informationen

Die Änderungen, die im `hdblcm` Rahmen der Aktivität zur Umbenennung von Hostnamen vorgenommen wurden, werden im folgenden ausführlichen Protokoll zusammengefasst.

Migrieren Sie SQL Server mithilfe verteilter Verfügbarkeitsgruppen zu AWS

Erstellt von Praveen Marthala (AWS)

Übersicht

Microsoft SQL Server Always On-Verfügbarkeitsgruppen bieten eine Hochverfügbarkeits- (HA) und Notfallwiederherstellungslösung (DR) für SQL Server. Eine Verfügbarkeitsgruppe besteht aus einem primären Replikat, das Lese-/Schreibverkehr akzeptiert, und bis zu acht sekundären Replikaten, die Leseverkehr akzeptieren. Eine Verfügbarkeitsgruppe wird auf einem Windows Server Failover Cluster (WSFC) mit zwei oder mehr Knoten konfiguriert.

Verteilte Verfügbarkeitsgruppen von Microsoft SQL Server Always On bieten eine Lösung für die Konfiguration von zwei separaten Verfügbarkeitsgruppen zwischen zwei unabhängigen WFSCs. Die Verfügbarkeitsgruppen, die Teil der verteilten Verfügbarkeitsgruppe sind, müssen sich nicht im selben Rechenzentrum befinden. Eine Verfügbarkeitsgruppe kann sich vor Ort befinden, und die andere Verfügbarkeitsgruppe kann sich in der Amazon Web Services (AWS) Cloud auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances in einer anderen Domain befinden.

Dieses Muster beschreibt die Schritte zur Verwendung einer verteilten Verfügbarkeitsgruppe zur Migration von lokalen SQL Server-Datenbanken, die Teil einer vorhandenen Verfügbarkeitsgruppe sind, zu SQL Server mit auf Amazon EC2 eingerichteten Verfügbarkeitsgruppen. Wenn Sie diesem Muster folgen, können Sie die Datenbanken mit minimalen Ausfallzeiten während der Umstellung in die AWS-Cloud migrieren. Die Datenbanken sind unmittelbar nach der Umstellung auf AWS hochverfügbar. Sie können dieses Muster auch verwenden, um das zugrunde liegende Betriebssystem von lokal auf AWS umzustellen und dabei dieselbe Version von SQL Server beizubehalten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS Direct Connect oder AWS Site-to-Site VPN
- Dieselbe Version von SQL Server ist lokal und auf den beiden Knoten auf AWS installiert

Produktversionen

- SQL Server Version 2016 und höher

- SQL Server Enterprise Edition

Architektur

Quelltechnologie-Stack

- Microsoft SQL Server-Datenbank mit lokalen Always-On-Verfügbarkeitsgruppen

Zieltechnologie-Stack

- Microsoft SQL Server-Datenbank mit Always-On-Verfügbarkeitsgruppen EC2 auf Amazon in der AWS-Cloud

Migrationsarchitektur

Terminologie

- WSFC 1 — WSFC vor Ort
- WSFC 2 — WSFC in der AWS-Cloud
- AG 1 — Erste Verfügbarkeitsgruppe, die sich in WSFC 1 befindet
- AG 2 — Zweite Verfügbarkeitsgruppe, die sich in WSFC 2 befindet
- Primäres SQL Server-Replikat — Knoten in AG 1, der als globaler primärer Knoten für alle Schreibvorgänge gilt
- SQL Server-Forwarder — Knoten in AG 2, der Daten asynchron vom primären SQL Server-Replikat empfängt
- Sekundäres SQL Server-Replikat — Knoten in AG 1 oder AG 2, die Daten synchron vom primären Replikat oder der Weiterleitung empfangen

Tools

- AWS Direct Connect — AWS Direct Connect verbindet Ihr internes Netzwerk über ein Standard-Ethernet-Glasfaserkabel mit einem AWS Direct Connect Connect-Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt zu öffentlichen AWS-Services erstellen und dabei Internetdienstanbieter in Ihrem Netzwerkpfad umgehen.

- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können Amazon verwenden EC2 , um so viele oder so wenige virtuelle Server zu starten, wie Sie benötigen, und Sie können nach oben oder unten skalieren.
- Site-to-SiteAWS-VPN — AWS Site-to-Site VPN unterstützt die Erstellung eines site-to-site virtuellen privaten Netzwerks (VPN). Sie können das VPN so konfigurieren, dass es Datenverkehr zwischen Instances, die Sie auf AWS starten, und Ihrem eigenen Remote-Netzwerk weiterleitet.
- Microsoft SQL Server Management Studio — Microsoft SQL Server Management Studio (SSMS) ist eine integrierte Umgebung für die Verwaltung der SQL Server-Infrastruktur. Es bietet eine Benutzeroberfläche und eine Gruppe von Tools mit umfangreichen Skripteditoren, die mit SQL Server interagieren.

Epen

Richten Sie eine zweite Verfügbarkeitsgruppe auf AWS ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine WSFC auf AWS.	Erstellen Sie WSFC 2 auf EC2 Amazon-Instances mit zwei Knoten für HA. Sie verwenden diesen Failover-Cluster, um die zweite Verfügbar keitsgruppe (AG 2) auf AWS zu erstellen.	Systemadministrator, SysOps Administrator
Erstellen Sie die zweite Verfügbarkeitsgruppe auf WSFC 2.	Erstellen Sie mithilfe von SSMS AG 2 auf zwei Knoten in WSFC 2. Der erste Knoten in WSFC 2 fungiert als Forwarder. Der zweite Knoten in WSFC 2 wird als sekundäre s Replikat von AG 2 fungieren. Derzeit sind in AG 2 keine Datenbanken verfügbar. Dies ist der Ausgangspunkt für	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Einrichtung der verteilten Verfügbarkeitsgruppe.	
Erstellen Sie Datenbanken ohne Wiederherstellungsoption auf AG 2.	Sichern Sie Datenbanken in der lokalen Verfügbarkeitsgruppe (AG 1). Stellen Sie die Datenbanken sowohl auf dem Forwarder als auch auf dem sekundären Replikat von AG 2 ohne Wiederherstellungsoption wieder her. Geben Sie beim Wiederherstellen der Datenbanken einen Speicherort mit ausreichend Speicherplatz für die Datenbankdatendateien und die Protokolldateien an. Zu diesem Zeitpunkt befinden sich die Datenbanken im Wiederherstellungsstatus. Sie sind nicht Teil von AG 2 oder der Distributed Availability Group und werden nicht synchronisiert.	DBA, Entwickler

Konfigurieren Sie die verteilte Verfügbarkeitsgruppe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die verteilte Verfügbarkeitsgruppe auf AG 1.	Um die verteilte Verfügbarkeitsgruppe auf AG 1 zu erstellen, verwenden Sie die	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`CREATE AVAILABILITY GROUP DISTRIBUTED` Option with. 1. Verwenden Sie `LISTENER_URL` Endpunktadressen für AG 1 und AG 2. 2. Für`AVAILABILITY-MODE`, verwenden, `ASYNCHRONOUS_COMMIT` um Netzwerklatenz zu vermeiden, falls vorhanden. Dies hat keine Auswirkungen auf die Leistung der Datenbank. 3. Geben Sie als `FAILOVER_MODE` `MANUAL`ein. Dies ist der einzige Verfügbarkeitsmodus, der mit verteilten Verfügbarkeitsgruppen funktioniert. 4. Um die Datenbanken auf AG 2 manuell wiederherzustellen und größere Datenbanken besser kontrollieren zu können, verwenden Sie `MANUAL` for`SEEDING_MODE` .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die verteilte Verfügbarkeitsgruppe auf AG 2.	Verwenden Sie die `DISTRIBUTED` Option, um die verteilte Verfügbar keitsgruppe auf AG 2 `ALTER AVAILABILITY GROUP` zu erstellen. 1. Verwenden Sie `LISTENER_URL` Endpunktadressen für AG 1 und AG 2. 2. Für`AVAILABILITY-MODE`, verwenden, `ASYNCHRONOUS_COMMIT` um Netzwerklatenz zu vermeiden, falls vorhanden . Dies hat keine Auswirkun gen auf die Leistung der Datenbank. 3. Geben Sie als `FAILOVER_MODE` `MANUAL`ein. Dies ist der einzige Verfügbar keitsmodus, der mit verteilte n Verfügbarkeitsgruppen funktioniert. 4. Um die Datenbanken auf AG 2 manuell wiederher zustellen und größere Datenbanken besser kontrollieren zu können, verwenden Sie `MANUAL` for`SEEDING_MODE` .	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Die verteilte Verfügbar keitsgruppe wird zwischen AG 1 und AG 2 erstellt. Die Datenbanken in AG 2 sind noch nicht so konfiguriert, dass sie am Datenfluss von AG 1 nach AG 2 teilnehmen.	
Fügen Sie dem Forwarder und dem sekundären Replikat auf AG 2 Datenbanken hinzu.	Fügen Sie die Datenbank en der verteilten Verfügbar keitsgruppe hinzu, indem Sie `ALTER DATABASE` die `SET HADR AVAILABIL ITY GROUP` Option sowohl im Forwarder als auch im sekundären Replikat auf AG 2 verwenden. Dadurch wird der asynchron e Datenfluss zwischen Datenbanken auf AG 1 und AG 2 gestartet. Der globale Primärserver nimmt Schreibvorgänge vor, sendet Daten synchron an das sekundäre Replikat auf AG 1 und sendet Daten asynchron an den Forwarder auf AG 2. Der Forwarder auf AG 2 sendet Daten synchron an das sekundäre Replikat auf AG 2.	DBA, Entwickler

Überwachen Sie den asynchronen Datenfluss zwischen AG 1 und AG 2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
DMVs Verwendungs- und SQL Server-Protokolle.	Überwachen Sie den Status des Datenflusses zwischen zwei Verfügbarkeitsgrup pen mithilfe dynamischer Verwaltungsansichten (DMVs) und SQL Server-Protokollen. DMVs zu den für die Überwachung von Interesse sind, gehören `sys.dm_ha dr_availability_re plica_states` und`sys.dm_hadr_automa tic_seeding` . Den Status der Weiterlei tungssynchronisierung finden Sie im SQL Server-Protokoll auf der Weiterleitung anhand des synchronisierten Status.	DBA, Entwickler

Führen Sie Umstellungsaktivitäten für die endgültige Migration durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stoppt den gesamten Datenverkehr zum primären Replikat.	Stoppen Sie den eingehenden Datenverkehr zum primären Replikat in AG 1, sodass keine Schreibaktivitäten in den Datenbanken stattfinden und die Datenbanken für die Migration bereit sind.	Besitzer der App, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie den Verfügbar keitsmodus der verteilten Verfügbarkeitsgruppe auf AG 1.	Stellen Sie auf dem primären Replikat den Verfügbar keitsmodus der verteilten Verfügbarkeitsgruppe auf synchron ein. Nachdem Sie den Verfügbar keitsmodus auf synchron geändert haben, werden die Daten synchron vom primären Replikat in AG 1 an den Forwarder in AG 2 gesendet.	DBA, Entwickler
Überprüfen Sie die LSNs in beiden Verfügbarkeitsgruppen.	Überprüfen Sie die letzten Protokollsequenznummern (LSNs) sowohl in AG 1 als auch in AG 2. Da im primären Replikat in AG 1 keine Schreibvorgänge stattfinden, werden die Daten synchronisiert, und die letzten Daten sollten LSNs für beide Verfügbarkeitsgruppen übereinstimmen.	DBA, Entwickler
Aktualisieren Sie AG 1 auf die sekundäre Rolle.	Wenn Sie AG 1 auf die sekundäre Rolle aktualisi eren, verliert AG 1 die primäre Replikatrolle und akzeptiert keine Schreibvorgänge, und der Datenfluss zwischen zwei Verfügbarkeitsgruppen wird gestoppt.	DBA, Entwickler

Führen Sie einen Failover zur zweiten Verfügbarkeitsgruppe durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Manuelles Failover zu AG 2.	Ändern Sie auf dem Forwarder in AG 2 die Distributed Availability Group, um Datenverlust zu verhinder n. Da Sie bereits überprüft und bestätigt haben, dass die letzten LSNs auf AG 1 und AG 2 übereinstimmen, ist Datenverlust kein Problem. Wenn Sie Datenverlust auf dem Forwarder in AG 2 zulassen, ändern sich die Rollen von AG 1 und AG 2: • AG 2 wird zur Verfügbar keitsgruppe mit dem primären Replikat und dem sekundären Replikat. • AG 1 wird zur Verfügbar keitsgruppe mit dem Forwarder und dem sekundären Replikat.	DBA, Entwickler
Ändern Sie den Verfügbar keitsmodus der verteilten Verfügbarkeitsgruppe auf AG 2.	Ändern Sie auf dem primären Replikat in AG 2 den Verfügbarkeitsmodus in asynchron. Dadurch wird die Datenbewe gung von AG 2 nach AG 1 von synchron zu asynchron geändert. Dieser Schritt ist erforderlich, um Netzwerkl	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	atenz zwischen AG 2 und AG 1 zu vermeiden, falls vorhanden, und beeinträchtigt nicht die Leistung der Datenbank.	
Beginnen Sie mit dem Senden von Datenverkehr an das neue primäre Replikat.	Aktualisieren Sie die Verbindungszeichenfolge, sodass der Listener-URL-Endpunkt auf AG 2 für das Senden von Datenverkehr an die Datenbanken verwendet wird. AG 2 akzeptiert jetzt Schreibvorgänge und sendet Daten an den Forwarder in AG 1 sowie das Senden von Daten an sein eigenes sekundäres Replikat in AG 2. Daten werden asynchron von AG 2 zu AG 1 übertragen.	Besitzer der App, Entwickler

Führen Sie Aktivitäten nach der Umstellung durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die verteilte Verfügbarkeitsgruppe auf AG 2.	Überwachen Sie die Migration für den geplanten Zeitraum. Löschen Sie dann die verteilte Verfügbarkeitsgruppe auf AG 2, um die Einrichtung verteilter Verfügbarkeitsgruppen zwischen AG 2 und AG 1 zu entfernen. Dadurch wird	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Konfiguration der verteilten Verfügbarkeitsgruppe entfernt und der Datenfluss von AG 2 zu AG 1 wird gestoppt. Derzeit ist AG 2 auf AWS hochverfügbar, mit einem primären Replikat, das Schreibvorgänge akzeptier t, und einem sekundäre n Replikat in derselben Verfügbarkeitsgruppe.	
Nehmen Sie die lokalen Server außer Betrieb.	Nehmen Sie die lokalen Server in WSFC 1 außer Betrieb, die Teil von AG 1 sind.	Systemadministrator, Administrator SysOps

Zugehörige Ressourcen

- Verteilte Verfügbarkeitsgruppen
- SQL-Dokumente: Verteilte Verfügbarkeitsgruppen
- SQL Docs: AlwaysOn-Verfügbarkeitsgruppen: eine Hochverfügbarkeits- und Disaster-Recovery-Lösung

Migrieren Sie mithilfe von AWS DMS von Oracle 8i oder 9i zu Amazon RDS for Oracle SharePlex

Erstellt von Ramu Jagini (AWS)

Übersicht

Dieses Muster beschreibt, wie eine lokale Oracle 8i- oder 9i-Datenbank zu einer Amazon Relational Database Service (Amazon RDS) für Oracle-Datenbank migriert wird. Sie können dieses Muster verwenden, um Ihre Migration mit reduzierten Ausfallzeiten abzuschließen, indem Sie Quest SharePlex für die synchrone Replikation verwenden.

Sie müssen für Ihre Migration eine Oracle-Datenbankzwischeninstanz verwenden, da der AWS Database Migration Service (AWS DMS) Oracle 8i oder 9i nicht als Quellumgebung unterstützt. Sie können SharePlex 7.6.3 verwenden, um von früheren Oracle-Datenbankversionen auf spätere Oracle-Datenbankversionen zu replizieren. Die Oracle-Zwischeninstanz ist als Ziel für SharePlex 7.6.3 kompatibel und wird als Quelle für AWS DMS oder neuere Versionen von unterstützt. SharePlex Diese Unterstützung ermöglicht die Weiterreplikation von Daten in die Zielumgebung von Amazon RDS for Oracle.

Beachten Sie, dass sich mehrere veraltete Datentypen und Funktionen auf eine Migration von Oracle 8i oder 9i zur neuesten Version von Oracle Database auswirken können. Um diese Auswirkungen zu minimieren, verwendet dieses Muster Oracle 11.2.0.4 als Datenbankzwischenversion, um den Schemacode vor der Migration zur Amazon RDS for Oracle Oracle-Zielumgebung zu optimieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle 8i- oder 9i-Quelldatenbank in einer lokalen Umgebung
- Oracle Database 12c Version 2 (12CR2) für das Staging auf Amazon Elastic Compute Cloud (Amazon) EC2
- Quest SharePlex 7.6.3 (kommerzielle Qualität)

Einschränkungen

- Einschränkungen von RDS für Oracle

Produktversionen

- Oracle 8i oder 9i für die Quelldatenbank
- Oracle 12 CR2 für die Staging-Datenbank (muss mit der Version von Amazon RDS for Oracle übereinstimmen)
- Oracle 12 CR2 oder höher für die Zieldatenbank (Amazon RDS for Oracle)

Architektur

Quelltechnologie-Stack

- Oracle 8i- oder 9i-Datenbank
- SharePlex

Zieltechnologie-Stack

- Amazon RDS für Oracle

Migrationsarchitektur

Das folgende Diagramm zeigt, wie eine Oracle 8i- oder 9i-Datenbank von einer lokalen Umgebung zu einer Amazon RDS for Oracle DB-Instance in der AWS-Cloud migriert wird.

Das Diagramm zeigt den folgenden Workflow:

1. Aktivieren Sie die Oracle-Quelldatenbank mit Archivprotokollmodus, erzwungener Protokollierung und zusätzlicher Protokollierung.
2. Stellen Sie die Oracle-Staging-Datenbank mithilfe von Recovery Manager (RMAN) point-in-time Recovery und FLASHBACK_SCN aus der Oracle-Quelldatenbank wieder her.
3. Konfigurieren Sie SharePlex das Lesen von Redo-Logs aus der Oracle-Quelldatenbank mithilfe von (wird in RMAN verwendet). `FLASHBACK_SCN`
4. Starten Sie die SharePlex Replikation, um Daten aus der Oracle-Quelldatenbank mit der Oracle-Staging-Datenbank zu synchronisieren.
5. Stellen Sie die Amazon RDS for Oracle Oracle-Zieldatenbank mithilfe von EXPDP und IMPDP mit wieder her. `FLASHBACK_SCN`

6. Konfigurieren Sie AWS DMS und seine Quellaufgaben als Oracle-Staging-Datenbank und Amazon RDS for Oracle als Zieldatenbank, indem Sie `FLASHBACK_SCN` (wird in EXPDP verwendet) verwenden.
7. Starten Sie AWS DMS-Aufgaben, um Daten aus der Oracle-Staging-Datenbank mit der Oracle-Zieldatenbank zu synchronisieren.

Tools

- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der AWS-Cloud.
- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS-Cloud oder zwischen Kombinationen von Cloud- und lokalen Setups.
- Quest SharePlex ist ein Oracle-to-Oracle Datenreplikationstool zum Verschieben von Daten mit minimalen Ausfallzeiten und ohne Datenverlust.
- Recovery Manager (RMAN) ist ein Oracle Database-Client, der Sicherungs- und Wiederherstellungsaufgaben für Ihre Datenbanken ausführt. Er vereinfacht das Sichern, Wiederherstellen und Wiederherstellen von Datenbankdateien erheblich.
- Mit Data Pump Export können Sie Daten und Metadaten in eine Reihe von Betriebssystemdateien hochladen, die als Dump-Dateisatz bezeichnet werden. Der Dump-Dateisatz kann nur mit dem Data Pump Import Utility oder dem Paket DBMS_DATAPUMP importiert werden.

Epen

Einrichtung SharePlex und Oracle-Staging-Datenbank auf Amazon EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine EC2 Instanz.	1. Erstellen Sie eine EC2 Instanz. 2. Installieren Sie Oracle 12 CR2 auf der EC2 Instance, die als Oracle-Staging-Dat enbank dienen soll.	Oracle-Verwaltung
Bereiten Sie die Staging-D atenbank vor.	Bereiten Sie die Oracle-Staging-Datenbank für	Oracle-Verwaltung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Wiederherstellung als Upgrade auf Oracle 12 vor, CR2 indem Sie das RMAN-Backup aus der Oracle 8i- oder 9i-Datenbankquellu mgebung übernehmen. Weitere Informationen finden Sie in der Oracle-Dokumentati on im Oracle 9i Recovery Manager User's Guide und im Database Backup and Recovery User's Guide.	
Konfigurieren SharePlex.	Konfigurieren Sie die SharePlex Quelle als lokale Oracle 8i- oder 9i-Datenb ank und konfigurieren Sie das Ziel als die auf Amazon gehostete Oracle CR2 12-Staging-Datenbank. EC2	SharePlex, Oracle-Verwaltung

Richten Sie Amazon RDS for Oracle als Ihre Zielumgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Oracle-DB-Instance.	Erstellen Sie eine Amazon RDS for Oracle Oracle-Da tenbank und verbinden Sie dann Oracle 12 CR2 mit der Datenbank. Weitere Informationen finden Sie in der Amazon RDS-Dokumentation unter Eine	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Oracle-DB-Instance erstellen und eine Verbindung zu einer Datenbank auf einer Oracle-DB-Instance herstellen.	
Stellen Sie Amazon RDS for Oracle aus der Staging-Datenbank wieder her.	1. Erstellen Sie ein EXPDP-Backup vom Oracle-Staging-Datenbankserver, indem Sie `FLASHBACK_SCN` 2. Stellen Sie Amazon RDS for Oracle aus der Staging-Datenbank wieder her. Weitere Informationen finden Sie unter 54 DBMS_DATAPUMP in der Oracle-Dokumentation.	DBA

AWS DMS einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Endpunkte für die Datenbanken.	Erstellen Sie einen Quellendpunkt für die Oracle-Staging-Datenbank und einen Zielendpunkt für die Amazon RDS for Oracle Oracle-Datenbank. Weitere Informationen finden Sie unter Wie erstelle ich Quell- oder Zielendpunkte	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	mit AWS DMS? im AWS Knowledge Center.	
Erstellen Sie eine Replikationsinstanz.	Verwenden Sie AWS DMS, um eine Replikationsinstanz für die Oracle-Staging-Datenbank zur Amazon RDS for Oracle Oracle-Datenbank zu starten. Weitere Informationen finden Sie unter Wie erstelle ich eine AWS DMS-Replikationsinstanz? im AWS Knowledge Center.	DBA
Erstellen und starten Sie Replikationsaufgaben.	Erstellen Sie AWS DMS-Replikationsaufgaben für Change Data Capture (CDC) mithilfe `FLASHBACK_SCN` von EXPDP (da die volle Last bereits über EXPDP erfolgt ist). Weitere Informationen finden Sie in der AWS DMS-Dokumentation unter Aufgabe erstellen.	DBA

Wechseln Sie zu Amazon RDS for Oracle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stoppen Sie die Arbeitslast der Anwendung.	Stoppen Sie die Anwendungsserver und ihre Anwendung	App-Entwickler, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en während des geplanten Umstellungsfensters.	
Überprüfen Sie die Synchronisierung der lokalen Oracle-Staging-Datenbank mit der Instanz. EC2	Stellen Sie sicher, dass alle Nachrichten für Replikationsaufgaben von der SharePlex Replikationsinstanz in die Oracle-Staging-Datenbank auf Amazon gesendet wurden, EC2 indem Sie einige Log-Switches in der lokalen Quelldatenbank durchführen. Weitere Informationen finden Sie unter 6.4.2 Eine Protokolldatei wechseln in der Oracle-Dokumentation.	DBA
Validieren Sie die Synchronisierung der Oracle-Staging-Datenbank mit der Amazon RDS for Oracle Oracle-Datenbank.	Vergewissern Sie sich, dass alle Ihre AWS DMS-Aufgaben keine Verzögerung und keine Fehler aufweisen, und überprüfen Sie dann den Validierungsstatus der Aufgaben.	DBA
Stoppen Sie die Replikation von SharePlex und Amazon RDS.	Wenn SharePlex sowohl die als auch die AWS DMS-Replikation keine Fehler anzeigen, beenden Sie beide Replizierungen.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ordnen Sie die Anwendung Amazon RDS neu zu.	Teilen Sie die Amazon RDS for Oracle Oracle-Endpunktdetails mit dem Anwendungsserver und seinen Anwendungen und starten Sie dann die Anwendung, um den Geschäftsbetrieb wieder aufzunehmen.	App-Entwickler, DBA

Testen Sie die AWS-Zielumgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Oracle-Staging-Datenbankumgebung auf AWS.	1. Testen Sie die SharePlex Replikation und stellen Sie sicher, dass es in der Oracle-Staging-Datenbank keine Synchronisierungsl ücken oder Replikati onsfehler gibt. 2. Stellen Sie anhand von in der lokalen Umgebung definierten Benchmark s sicher, dass sich die Anwendung erwartung sgemäß verhält.	SharePlex, Oracle-Verwaltung
Testen Sie die Amazon RDS-Umgebung.	1. Stellen Sie sicher, dass alle Daten, die nach der Replikation an Amazon RDS weitergegeben werden, fehlerfrei sind.	Oracle-Verwaltung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Verweisen Sie eine andere Anwendung auf die Amazon RDS-DB-Instance und führen Sie dann Leistungs tests durch, um das erwartete Verhalten zu überprüfen. Weitere Informationen finden Sie unter Amazon RDS for Oracle in der Amazon RDS-Dokumentation.	

Zugehörige Ressourcen

- Migrieren Sie mit Zuversicht
- Amazon EC2
- Amazon RDS für Oracle
- AWS Database Migration Service
- Debuggen Ihrer AWS DMS-Migrationen: Was tun, wenn etwas schief geht (Teil 1)
- Debuggen Ihrer AWS DMS-Migrationen: Was tun, wenn etwas schief geht (Teil 2)
- Debuggen Ihrer AWS DMS-Migrationen: Was tun, wenn etwas schief geht? (Teil 3)
- SharePlex für Datenbankreplikation
- SharePlex: Datenbankreplikation für jede Umgebung

Überwachen Sie Amazon Aurora auf Instances ohne Verschlüsselung

Erstellt von Mansi Suratwala (AWS)

Übersicht

Dieses Muster stellt eine Amazon Web Services (AWS) CloudFormation -Vorlage bereit, die Sie einsetzen können, um automatische Benachrichtigungen einzurichten, wenn eine Amazon Aurora Aurora-Instance ohne aktivierte Verschlüsselung erstellt wird.

Aurora ist eine vollständig verwaltete, mit MySQL und PostgreSQL kompatible relationale Datenbank-Engine. Bei manchen Workloads kann Aurora einen bis zu fünfmal höheren Durchsatz als MySQL und einen bis zu dreimal höheren Durchsatz als PostgreSQL liefern, ohne dass die meisten Ihrer bestehenden Anwendungen geändert werden müssen.

Die CloudFormation Vorlage erstellt ein Amazon CloudWatch Events-Ereignis und eine AWS-Lambda-Funktion. Das Ereignis verwendet AWS CloudTrail , um die Erstellung einer Aurora-Instance oder die Wiederherstellung einer vorhandenen Instance zu einem bestimmten Zeitpunkt zu überwachen. Das Cloudwatch Events-Ereignis initiiert die Lambda-Funktion, die überprüft, ob die Verschlüsselung aktiviert ist. Wenn die Verschlüsselung nicht aktiviert ist, sendet die Lambda-Funktion eine Amazon Simple Notification Service (Amazon SNS) -Benachrichtigung, die Sie über den Verstoß informiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

Einschränkungen

- Diese Servicesteuerung funktioniert nur mit Amazon Aurora Aurora-Instances. Andere Amazon Relational Database Service (Amazon RDS) -Instances werden nicht unterstützt.
- Die CloudFormation Vorlage darf nur für `RestoreDBClusterToPointInTim` E **`CreateDBInstance`** und E bereitgestellt werden.

Produktversionen

- PostgreSQL-Versionen, die in Amazon Aurora unterstützt werden

- MySQL-Versionen, die in Amazon Aurora unterstützt werden

Architektur

Zieltechnologie-Stack

- Amazon Aurora
- AWS CloudTrail
- Amazon CloudWatch
- AWS Lambda
- Amazon Simple Storage Service (Amazon-S3)
- Amazon SNS

Zielarchitektur

Automatisierung und Skalierung

Sie können die CloudFormation Vorlage mehrfach für verschiedene Regionen und Konten verwenden. Sie müssen sie in jeder Region oder jedem Konto nur einmal ausführen.

Tools

Tools

- Amazon Aurora — Amazon Aurora ist eine vollständig verwaltete relationale Datenbank-Engine, die mit MySQL und PostgreSQL kompatibel ist.
- AWS CloudTrail — AWS CloudTrail unterstützt Sie bei der Verwaltung der Unternehmensführung, der Einhaltung von Vorschriften sowie der Betriebs- und Risikoprüfung Ihres AWS-Kontos. Aktionen, die von einem Benutzer, einer Rolle oder einem AWS-Service ausgeführt werden, werden als Ereignisse in aufgezeichnet CloudTrail.
- Amazon CloudWatch Events — Amazon CloudWatch Events liefert einen near-real-time Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben.
- AWS Lambda — AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice, den Sie für eine Vielzahl von Speicherlösungen verwenden können, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) ist ein verwalteter Service, der die Nachrichtenzustellung über Lambda, HTTP, E-Mail, mobile Push-Benachrichtigungen und mobile Textnachrichten (SMS) ermöglicht.

Code

Eine ZIP-Datei des Projekts ist als Anhang verfügbar.

Epen

Erstellen Sie den S3-Bucket für das Lambda-Skript

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Öffnen Sie die Amazon S3 S3-Konsole und wählen oder erstellen Sie einen S3-Bucket . Dieser S3-Bucket hostet die Lambda-Code-.zip-Datei. Ihr S3-Bucket muss sich in derselben Region wie Aurora befinden. Der S3-Bucket-Name darf keine führenden Schrägstriche enthalten.	Cloud-Architekt

Laden Sie den Lambda-Code in den S3-Bucket hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Lambda-Code hoch.	Laden Sie die Lambda-Code-ZIP-Datei, die im Abschnitt Anlagen bereitgestellt wird, in	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den von Ihnen definierten S3-Bucket hoch.	

Stellen Sie die CloudFormation Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation Vorlage bereit.	Stellen Sie auf der CloudFormation Konsole die `RDS_Aurora_Encryption_At_Rest.yml` CloudFormation Vorlage bereit, die als Anlage zu diesem Muster bereitgestellt wird. Geben Sie im nächsten Epos Werte für die Vorlagenparameter an.	Cloud-Architekt

Vervollständigen Sie die Parameter in der CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den S3-Bucket-Namen an.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epic erstellt oder ausgewählt haben.	Cloud-Architekt
Geben Sie den S3-Schlüssel an.	Geben Sie den Speicherort der Lambda-Code-ZIP-Datei in Ihrem S3-Bucket an, ohne vorangestellte Schrägstriche (z. B.). `<directory>/<file-name>.zip`	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine aktive E-Mail-Adresse an, um Amazon SNS SNS-Benachrichtigungen zu erhalten.	Cloud-Architekt
Definieren Sie die Protokollierungsebene.	Definieren Sie die Protokollierungsebene und die Häufigkeit für Ihre Lambda-Funktion. `Info`bezeichnet detaillierte Informationsmeldungen über den Fortschritt der Anwendung. `Error`bezeichnet Fehlerereignisse, die es der Anwendung dennoch ermöglichen könnten, weiter zu laufen. `Warning`bezeichnet potenziell schädliche Situationen.	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail-Nachricht an die angegebene E-Mail-Adresse. Um Benachrichtigungen zu erhalten, müssen Sie dieses E-Mail-Abonnement bestätigen.	Cloud-Architekt

Zugehörige Ressourcen

- Erstellen eines S3-Buckets
- Dateien in einen S3-Bucket hochladen
- Erstellen eines Amazon Aurora-DB Clusters
- Erstellen einer CloudWatch Ereignisregel, die bei einem AWS-API-Aufruf mit AWS ausgelöst wird CloudTrail

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Überwachen Sie GoldenGate Oracle-Protokolle mithilfe von Amazon CloudWatch

Erstellt von Chithra Krishnamurthy (AWS)

Übersicht

Oracle GoldenGate bietet Echtzeitreplikation zwischen Amazon Relational Database Service (Amazon RDS) für Oracle-Datenbanken oder zwischen Oracle-Datenbanken, die auf Amazon Elastic Compute Cloud (Amazon EC2) gehostet werden. Es unterstützt sowohl unidirektionale als auch bidirektionale Replikation.

Bei der Replikation ist die Überwachung von entscheidender Bedeutung, um sicherzustellen, dass der GoldenGate Prozess ordnungsgemäß ausgeführt wird und ob die Quell- und Zieldatenbanken synchron sind. GoldenGate

Dieses Muster erklärt die Schritte zur Implementierung der CloudWatch Amazon-Überwachung für ein GoldenGate Fehlerprotokoll und wie Alarme eingerichtet werden, um Benachrichtigungen für bestimmte Ereignisse zu senden, z. B. `STOP ABEND` damit Sie geeignete Maßnahmen ergreifen können, um die Replikation schnell wieder aufzunehmen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- GoldenGate auf einer EC2 Instanz installiert und konfiguriert, sodass Sie die CloudWatch Überwachung für diese EC2 Instanzen einrichten können. Wenn Sie die bidirektionale Replikation GoldenGate in allen AWS-Regionen überwachen möchten, müssen Sie den CloudWatch Agenten in jeder EC2 Instanz installieren, in der der GoldenGate Prozess ausgeführt wird.

Einschränkungen

- Dieses Muster erklärt, wie der GoldenGate Prozess mithilfe von überwacht wird CloudWatch. CloudWatch überwacht keine Verzögerungen bei der Replikation oder Probleme mit der Datensynchronisierung während der Replikation. Sie müssen separate SQL-Abfragen ausführen, um die Replikationsverzögerung oder datenbezogene Fehler zu überwachen, wie in der GoldenGate Dokumentation beschrieben.

Produktversionen

- Dieses Dokument basiert auf der Implementierung von Oracle GoldenGate 19.1.0.0.4 für Oracle auf Linux x86-64. Diese Lösung gilt jedoch für alle Hauptversionen von. GoldenGate

Architektur

Zieltechnologie-Stack

- GoldenGate Binärdateien für Oracle, die auf einer EC2 Instanz installiert sind
- Amazon CloudWatch
- Amazon-Simple-Notification-Service (Amazon-SNS)

Zielarchitektur

Tools

AWS-Services

- Amazon CloudWatch ist ein Überwachungsdienst, der in diesem Muster zur Überwachung von GoldenGate Fehlerprotokollen verwendet wird.
- Amazon SNS ist ein Benachrichtigungsservice, der in diesem Muster zum Senden von E-Mail-Benachrichtigungen verwendet wird.

Andere Tools

- Oracle GoldenGate ist ein Datenreplikationstool, das Sie für Amazon RDS for Oracle Oracle-Datenbanken oder Oracle-Datenbanken verwenden können, die auf Amazon gehostet werden EC2.

Implementierungsschritte auf hoher Ebene

1. Erstellen Sie eine AWS Identity and Access Management (IAM) -Rolle für den CloudWatch Agenten.
2. Ordnen Sie die IAM-Rolle der EC2 Instance zu, in der GoldenGate Fehlerprotokolle generiert werden.
3. Installieren Sie den CloudWatch Agenten auf der EC2 Instanz.

4. Konfigurieren Sie die CloudWatch Agenten-Konfigurationsdateien: `awscli.conf` und`awslogs.conf`.
5. Starten Sie den CloudWatch Agenten.
6. Erstellen Sie Metrikfilter in der Protokollgruppe.
7. Richten Sie Amazon SNS ein.
8. Erstellen Sie einen Alarm für die metrischen Filter. Amazon SNS sendet E-Mail-Benachrichtigungen, wenn diese Filter Ereignisse erfassen.

Eine ausführliche Anleitung finden Sie im nächsten Abschnitt.

Epen

Schritt 1. Erstellen Sie eine IAM-Rolle für den Agenten CloudWatch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Rolle.	Für den Zugriff auf AWS-Ressourcen sind Berechtigungen erforderlich. Daher erstellen Sie IAM-Rollen, die die Berechtigungen enthalten, die für jeden Server zur Ausführung des CloudWatch Agenten erforderlich sind. So erstellen Sie die IAM-Rolle: 1. Melden Sie sich in der AWS-Managementkonsole an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/. 2. Wählen Sie im Navigationsbereich Rollen und dann Rolle erstellen.	AWS allgemein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie für Vertrauen swürdigen Entitätstyp die Option AWS-Service aus. 4. Wählen EC2Sie für Allgemeine Anwendung sfälle die Option und dann Weiter aus. 5. Aktivieren Sie in der Liste der Richtlinien das Kontrollk ästchen neben CloudWatc hAgentServerPolicy. Verwenden Sie ggf. das Suchfeld, um die Richtlinie zu finden. 6. Wählen Sie Weiter aus. 7. Geben Sie unter Role name (Rollenname) einen Namen für Ihre neue Rolle, wie z. B. `goldengate-cw-monitoring-role` , oder einen anderen von Ihnen bevorzugten Namen ein. 8. (Optional) Geben Sie im Feld Role description (Rollenbeschreibung) eine Beschreibung ein. 9. Vergewissern Sie sich, dass dies unter Richtlinienname CloudWatchAgentSer verPolicyangezeigt wird. 10. (Optional) Fügen Sie ein oder mehrere Tags	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(Schlüssel-Wert-Paare) hinzu, um den Zugriff für diese Rolle zu organisieren, nachzuverfolgen oder zu kontrollieren, und wählen Sie dann Rolle erstellen aus.	

Schritt 2. Ordnen Sie der Instance die IAM-Rolle zu GoldenGate EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ordnen Sie die IAM-Rolle der EC2 Instanz zu, in der GoldenGate Fehlerprotokolle generiert werden.	Die von generierten Fehlerprotokolle GoldenGate müssen mit Daten gefüllt CloudWatch und überwacht werden. Daher müssen Sie die in Schritt 1 erstellte IAM-Rolle der EC2 Instance zuordnen, auf der sie ausgeführt GoldenGate wird. Um einer Instance eine IAM-Rolle zuzuweisen: 1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/. 2. Wählen Sie im Navigationsbereich Instances aus und suchen Sie dann die Instance, auf der ausgeführt GoldenGate wird. 3. Wählen Sie die Instanz aus und wählen Sie dann	AWS allgemein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Aktionen, Sicherheit, IAM-Rolle ändern aus. 4. Wählen Sie die im ersten Schritt erstellte IAM-Rolle aus, um sie an Ihre Instance anzuhängen, und klicken Sie dann auf Speichern.	

Schritte 3—5. Installieren und konfigurieren Sie den CloudWatch Agenten auf der Goldengate-Instanz EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den CloudWatch Agenten auf der GoldenGate EC2 Instanz.	Führen Sie den folgenden Befehl aus, um den Agenten zu installieren: `sudo yum install -y awslogs`	AWS allgemein

Bearbeiten Sie die Agenten-Konfigurationsdateien.	1. Führen Sie den folgenden Befehl aus.
	`sudo su -`
	2. Bearbeiten Sie diese Datei, um die AWS-Region nach Bedarf zu aktualisieren.
	`cat /etc/awslogs/conf`
	`[plugins]`
	`cwlogs = cwlogs`
	`[default]`
	`region = us-east-1`
		AWS allgemein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	3. Bearbeiten Sie die `/etc/awslogs/awslogs.conf` Datei, um den Dateinamen und den Namen der Protokollgruppe date/time format. You must specify the date/time zu aktualisieren und dem Datumsformat in zu entsprechen. `ggserror.log` Andernfalls fließt der Log-Stream nicht hinein CloudWatch. Zum Beispiel:
	`datetime_format = %Y-%m-%dT%H:%M:%S%z`
	`file = /u03/oracle/oragg/ggserr.log`
	`log_group_name = goldengate_monitor`	

Starten Sie den CloudWatch Agenten.	Verwenden Sie den folgenden Befehl, um den Agenten zu starten. `$ sudo service awslogsd start` Nachdem Sie den Agenten gestartet haben, können Sie die Protokollgruppe in der CloudWatch Konsole anzeigen. Der Protokollstream wird den Inhalt der Datei enthalten.	AWS allgemein

Schritt 6: Erstellen Sie Metrikfilter für die Protokollgruppe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie metrische Filter für die Schlüsselwörter ABEND und STOPPED.	Wenn Sie Metrikfilter für die Protokollgruppe erstellen, wird jedes Mal, wenn die Filter im Fehlerprotokoll identifiziert werden, ein Alarm ausgelöst und eine E-Mail-Benachricht igung gesendet, die auf der Amazon SNS SNS-Konfi guration basiert. So erstellen Sie Metrikfilter: 1. Öffnen Sie die CloudWatc h Konsole unter https:// console.aws.amazon.com/ cloudwatch/. 2. Wählen Sie den Namen der Protokollgruppe aus. 3. Wählen Sie Aktionen und dann Metrikfilter erstellen. 4. Geben Sie für das Filtermus ter ein Muster an, z. `ABEND` B. 5. Wählen Sie Next (Weiter) aus und geben Sie einen Namen für Ihren Metrikfilter ein. 6. Geben Sie unter Metrikdet ails für Metrik-Namespace einen Namen für den CloudWatch Namespace ein, in dem die Metrik	CloudWatch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	veröffentlicht wird. Wenn der Namespace noch nicht vorhanden ist, stellen Sie sicher, dass Create new (Neu erstellen) ausgewählt ist. 7. Geben Sie für Metrikwert den Wert ein1, weil Ihr Metrikfilter das Vorkommen der Schlüsselwörter im Filter zählt. 8. Stellen Sie „Einheit“ auf „Keine“ ein. 9. Wählen Sie Metrikfilter erstellen aus. Sie finden den Metrikfilter, den Sie über den Navigationsbereich erstellt haben. 10. Erstellen Sie einen weiteren metrischen Filter für das `STOPPED` Muster. Innerhalb einer Protokollgruppe können Sie mehrere Metrikfilter erstellen und Alarme einzeln festlegen.	

Schritt 7. Einrichten von Amazon SNS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein SNS-Thema.	In diesem Schritt konfigurieren Sie Amazon SNS so,	Amazon SNS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dass Alarme für die metrische n Filter erstellt werden. Um ein SNS-Thema zu erstellen: 1. Melden Sie sich zu https://console.aws.amazon.com/sns/Hause bei der Amazon SNS-Konsole an. 2. Geben Sie im Feld Thema erstellen einen Themennam en ein, z. B.`goldengat e-alert` , und wählen Sie dann Nächster Schritt aus. 3. Wählen Sie unter Type (Typ) die Option Standard aus. 4. Scrollen Sie zum Ende des Formulars und wählen Sie Create topic (Erstelle n eines Themas) aus. In der Konsole wird die Seite Details geöffnet.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Abonnement.	Um ein Abonnement für das Thema zu erstellen: 1. Wählen Sie im linken Navigationsbereich Subscriptions (Abonnements). 2. Wählen Sie auf der Seite Subscriptions (Abonnements) die Option Create subscription (Abonnement erstellen)aus. 3. Wählen Sie auf der Seite Abonnement erstellen das Feld Themen-ARN aus, um eine Liste der Themen in Ihrem AWS-Konto anzuzeigen. 4. Wählen Sie das Mesh aus, das Sie im vorherigen Schritt erstellt haben. 5. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus. 6. Geben Sie unter Endpoint (Endpunkt) eine E-Mail-Adresse ein, um die Benachrichtigungen zu empfangen. 7. Wählen Sie Abonnement erstellen aus. Die Konsole öffnet die Detailseite des neuen Abonnements.	Amazon SNS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Suchen Sie in Ihrem E-Mail-Posteingang nach einer Nachricht von AWS Notifications und wählen Sie dann in der E-Mail Abonnement bestätigen aus. Amazon SNS öffnet Ihren Webbrowser und zeigt eine Abonnementbestätigung mit Ihrer Abonnement-ID an.	

Schritt 8. Erstellen Sie einen Alarm, um Benachrichtigungen für die Metrikfilter zu senden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Alarm für das SNS-Thema.	So erstellen Sie einen Alarm, der auf einem Metrikfilter für Protokollgruppen basiert: 1. Öffnen Sie die CloudWatch Konsole unter. https://console.aws.amazon.com/cloudwatch/ 2. Wählen Sie ausgehend vom Navigationsbereich Logs (Protokolle) und dann Log groups (Protokollgruppen) aus. 3. Wählen Sie die Protokoll gruppe aus, die Ihren Metrikfilter enthält.	CloudWatch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie Metric filters (Metrikfilter) aus. 5. Aktivieren Sie auf der Registerkarte Metrische Filter das Kontrollkästchen für den metrischen Filter, auf dem Ihr Alarm basieren soll. 6. Wählen Sie Alarm erstellen aus. 7. Geben Sie unter Bedingungen in jedem Abschnitt Folgendes an: • Wählen Sie für Threshold type (Schwellenwerttyp) die Option Static (Statisch) aus. • Für Wann immer es ist. <metric-name> , wählen Sie Größer. • Für als. , geben Sie 0 an. 8. Wählen Sie Weiter aus. 9. Unter Benachrichtigung: • Wählen Sie für Alarmstatusauslöser die Option Im Alarm aus. • Wählen Sie unter Benachrichtigung an das folgende SNS-Thema senden die Option Bestehendes Thema auswählen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wählen Sie im E-Mail-Feld das Amazon SNS SNS-Thema aus, das Sie im vorherigen Schritt erstellt haben. 10. Wählen Sie Weiter aus. 11. Geben Sie unter Name und Beschreibung einen Namen und eine Beschreibung für Ihren Alarm ein. **Note** Für die Beschreib ung können Sie den Instanznamen angeben, sodass die Benachric htigungs-E-Mail beschreibend ist. 12. Überprüfen Sie bei Vorschau und Erstellen, ob Ihre Konfiguration korrekt ist, und wählen Sie dann Alarm erstellen aus. Nach diesen Schritten erhalten Sie jedes Mal, wenn diese Muster in der GoldenGat e Fehlerprotokolldatei (`ggserr.log`), die Sie überwachen, erkannt werden, eine E-Mail-Benachrichtigung.	

Fehlerbehebung

Problem	Lösung
Der Protokollstream aus dem GoldenGate Fehlerprotokoll fließt nicht hinein CloudWatch.	Überprüfen Sie die `/etc/awslogs/awslogs.conf` Datei, um zu überprüfen, ob der Dateiname und der date/time format. You must specify the date/time Protokollgruppenname dem Datumsformat entsprechen`ggserror.log` . Andernfalls fließt der Protokollstream nicht hinein CloudWatch.

Zugehörige Ressourcen

- CloudWatch Amazon-Dokumentation
- Erfassung von Metriken und Protokollen mit dem CloudWatch Agenten
- Amazon SNS SNS-Dokumentation

Replatform Oracle Database Enterprise Edition auf Standard Edition 2 auf Amazon RDS for Oracle

Erstellt von Lanre (Lan-Ray) showunmi (AWS) und Tarun Chawla (AWS)

Übersicht

Oracle Database Enterprise Edition (EE) ist in vielen Unternehmen eine beliebte Wahl für die Ausführung von Anwendungen. In einigen Fällen verwenden Anwendungen jedoch nur wenige oder gar keine Funktionen von Oracle Database EE, sodass es an Rechtfertigungen für enorme Lizenzkosten mangelt. Sie können Kosteneinsparungen erzielen, indem Sie solche Datenbanken bei der Migration zu Amazon RDS auf Oracle Database Standard Edition 2 (SE2) herabstufen.

Dieses Muster beschreibt, wie ein Downgrade von Oracle Database EE auf Oracle Database durchgeführt wird, SE2 wenn von einer lokalen Umgebung zu Amazon RDS for Oracle migriert wird. Die in diesem Muster beschriebenen Schritte gelten auch, wenn Ihre EE-Oracle-Datenbank bereits auf Amazon RDS oder auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance läuft.

Weitere Informationen finden Sie im AWS Prescriptive Guidance Guide zur Evaluierung des Downgrades von Oracle-Datenbanken auf Standard Edition 2 auf AWS.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Oracle Database Enterprise Edition
- Ein Client-Tool, wie Oracle SQL Developer oder SQL*Plus, zum Herstellen einer Verbindung mit SQL-Befehlen und zum Ausführen von SQL-Befehlen in einer Oracle-Datenbank
- Datenbankbenutzer für die Durchführung der Bewertung, z. B. einer der folgenden Benutzer:
  - Benutzer mit ausreichenden Rechten für die Ausführung der AWS Schema Conversion Tool (AWS SCT) -Bewertung
  - Benutzer mit ausreichenden Rechten, um SQL-Abfragen in Oracle-Datenbank-Wörterbuchtabellen auszuführen
- Datenbankbenutzer für die Durchführung der Datenbankmigration, z. B. einer der folgenden Benutzer:
  - Benutzer mit ausreichenden Rechten für die Ausführung von AWS Database Migration Service (AWS DMS)

- Benutzer mit ausreichenden Rechten für den Export und Import von Oracle Data Pump
- Benutzer mit ausreichenden Rechten zum Ausführen von Oracle GoldenGate

Einschränkungen

- Amazon RDS for Oracle hat eine maximale Datenbankgröße. Weitere Informationen finden Sie unter Amazon-RDS-DB-Instance Speicher.

Produktversionen

Die in diesem Dokument beschriebene allgemeine Logik gilt für Oracle-Versionen ab 9i. Unterstützte Versionen von selbstverwalteten Datenbanken und Datenbanken von Amazon RDS for Oracle finden Sie in der AWS DMS-Dokumentation.

Um die Funktionsnutzung in Fällen zu identifizieren, in denen AWS SCT nicht unterstützt wird, führen Sie SQL-Abfragen in der Quelldatenbank aus. Verwenden Sie die Oracle Export- und Import-Dienstprogramme, um von früheren Versionen von Oracle zu migrieren, in denen AWS DMS und Oracle Data Pump nicht unterstützt werden.

Eine aktuelle Liste der unterstützten Versionen und Editionen finden Sie in der AWS-Dokumentation unter Oracle on Amazon RDS. Einzelheiten zu Preisen und unterstützten Instance-Klassen finden Sie unter Amazon RDS für Oracle – Preise.

Architektur

Quelltechnologie-Stack

- Oracle Database Enterprise Edition läuft vor Ort oder auf Amazon EC2

Zieltechnologie-Stack mit nativen Oracle-Tools

- Amazon RDS for Oracle mit Oracle-Datenbank SE2

1. Exportieren Sie Daten mithilfe von Oracle Data Pump.
2. Kopieren Sie Dumpdateien über einen Datenbank-Link nach Amazon RDS.

3. Importieren Sie Dump-Dateien mithilfe von Oracle Data Pump in Amazon RDS.

Zieltechnologie-Stack mit AWS DMS

- Amazon RDS for Oracle mit Oracle-Datenbank SE2
- AWS DMS

1. Exportieren Sie Daten mithilfe von Oracle Data Pump mit FLASHBACK_SCN.
2. Kopieren Sie Dumpdateien über einen Datenbank-Link nach Amazon RDS.
3. Importieren Sie Dump-Dateien mithilfe von Oracle Data Pump in Amazon RDS.
4. Verwenden Sie AWS DMS Change Data Capture (CDC).

Tools

AWS-Services

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS-Cloud oder zwischen Kombinationen von Cloud- und lokalen Setups.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der AWS-Cloud. Dieses Muster verwendet Amazon RDS for Oracle.
- AWS SCT bietet eine projektbasierte Benutzeroberfläche, mit der Sie das Datenbankschema Ihrer Oracle-Quelldatenbank automatisch bewerten, konvertieren und in ein mit Amazon RDS for Oracle kompatibles Format kopieren können. Mit AWS SCT können Sie potenzielle Kosteneinsparungen analysieren, die durch die Änderung Ihres Lizenztyps von Enterprise auf Standard Edition von Oracle erzielt werden können. Der Abschnitt Lizenzbewertung und Cloud-Support des AWS SCT-Berichts enthält detaillierte Informationen zu den verwendeten Oracle-Funktionen, sodass Sie bei der Migration zu Amazon RDS for Oracle eine fundierte Entscheidung treffen können.

Andere Tools

- Native Oracle-Import- und Exportprogramme unterstützen das Verschieben von Oracle-Daten in und aus Oracle-Datenbanken. Oracle bietet zwei Arten von Dienstprogrammen für

Datenbankimport und -export: Original Export und Import (für frühere Versionen) und Oracle Data Pump Export and Import (verfügbar in Oracle Database 10g, Version 1 und höher).

- Oracle GoldenGate bietet Funktionen zur Replikation in Echtzeit, sodass Sie Ihre Zieldatenbank nach einem ersten Ladevorgang synchronisieren können. Diese Option kann dazu beitragen, die Ausfallzeiten von Anwendungen während der Inbetriebnahme zu reduzieren.

Epen

Machen Sie vor der Migration eine Bewertung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Datenbank anforderungen für Ihre Anwendungen.	Stellen Sie sicher, dass Ihre Anwendungen für die Ausführung auf Oracle Database zertifiziert sind SE2. Erkundigen Sie sich direkt beim Softwarea nbieter, Entwickler oder in der Anwendungsdokumentation.	App-Entwickler, DBA, App-Besitzer
Untersuchen Sie die Verwendung von EE-Funkti onen direkt in der Datenbank.	Gehen Sie wie folgt vor, um die Nutzung der EE-Funktion zu ermitteln: • Generieren Sie einen AWS SCT-Bewertungsbericht für Ihre Oracle EE-Datenb ank. In dem Bericht erfahren Sie, welche Funktionen aus Ihrer aktuellen EE-Datenb ank entfernt werden sollten, wenn Sie die Lizenztypen ändern möchten. • Wenn Sie ein Oracle Support-Konto haben, rufen Sie das Skript `options_p`	App-Besitzer, DBA, App-Entwi ckler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`acks_usage_statistics.sql` im Support-Dokument 1317265.1 ab und führen Sie es aus, um einen Bericht über die Optionen und Funktionen zu generieren, die in Ihrer Oracle-Datenbank verwendet werden. • Fragen Sie DBA_FEATURE_USAGE_STATISTICS ab, um Details zu allen Funktionen anzuzeigen, die verwendet werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Verwendung von EE-Funktionen für betriebliche Aktivitäten.	Datenbank- oder Anwendungsadministratoren verlassen sich bei betrieblichen Aktivitäten manchmal auf reine EE-Funktionen. Zu den häufigsten Beispielen gehören Online-Wartungsaktivitäten (Indexneuerstellung, Tabellenverschiebung) und die Verwendung von Parallelität durch Batch-Jobs. Diese Abhängigkeiten können verringert werden, indem Sie Ihre Betriebsabläufe nach Möglichkeit ändern. Identifizieren Sie die Verwendung dieser Funktionen und treffen Sie eine Entscheidung auf der Grundlage der Kosten im Vergleich zu den Vorteilen. Verwenden Sie die Tabelle zum Vergleich von Oracle Database EE und SE2 Funktionen als Leitfaden, um die Funktionen zu identifizieren, die in Oracle Database verfügbar sind SE2.	App-Entwickler, DBA, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Workload-Muster der EE Oracle-Datenbank.	Oracle Database beschränkt die Nutzung SE2 automatisch auf maximal 16 CPU-Threads zu einem beliebigen Zeitpunkt. Wenn Ihre Oracle EE-Datenbank für die Verwendung des Oracle Diagnostic Pack lizenziert ist, verwenden Sie das Tool Automatic Workload Repository (AWR) oder DBA_HIST_*-Views, um die Workload-Muster der Datenbank zu analysieren und festzustellen, ob sich die maximale Grenze von 16 CPU-Threads negativ auf die Service Levels auswirkt, wenn Sie auf. SE2 Stellen Sie sicher, dass Ihre Bewertung Perioden mit hoher Aktivität abdeckt, wie z. B. die Verarbeitung am Ende eines Tages, eines Monats oder eines Jahres.	App-Besitzer, DBA, App-Entwickler

Bereiten Sie die Zielinfrastruktur auf AWS vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Netzwerkinfrastruktur bereit und konfigurieren Sie sie.	Erstellen Sie eine Virtual Private Cloud (VPC) und Subnetze, Sicherheitsgruppen	AWS-Administrator, Cloud-Architekt, Netzwerkadministrator, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und Netzwerkzugriffskontrolllisten.	
Stellen Sie die Amazon RDS for Oracle SE2 Oracle-Datenbank bereit.	Stellen Sie die Amazon RDS for Oracle SE2 Oracle-Zieldatenbank bereit, um die Leistungs-, Verfügbarkeits- und Sicherheitsanforderungen Ihrer Anwendungen zu erfüllen. Wir empfehlen eine Multi-AZ-Konfiguration für Produktionsworkloads. Um die Migrationsleistung zu verbessern, können Sie die Aktivierung von Multi-AZ jedoch bis nach der Datenmigration verschieben.	Cloud-Administrator, Cloud-Architekt, DBA, DevOps Ingenieur, AWS-Administrator
Passen Sie die Amazon RDS-Umgebung an.	Konfigurieren Sie benutzerdefinierte Parameter und Optionen und aktivieren Sie zusätzliche Überwachung. Weitere Informationen finden Sie unter Bewährte Methoden für die Migration zu Amazon RDS for Oracle.	AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator, DBA, Cloud-Architekt

Führen Sie den Migrationstestlauf und die Anwendungstests durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie die Daten (Probelauf).	Migrieren Sie Daten von der Oracle EE-Quelldatenbank zur Amazon RDS for Oracle SE2 Oracle-Datenbank-Instance	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	mit dem Ansatz, der für Ihre spezifische Umgebung am besten geeignet ist. Wählen Sie eine Migrationsstrategie aus, die auf Faktoren wie Größe, Komplexität und verfügbarem Ausfallzeitfenster basiert. Verwenden Sie eine oder eine Kombination der folgenden Optionen: • Systemeigene Oracle-Tools wie Oracle Data Pump (empfohlen), Oracle Import-Export Utilities und Oracle. GoldenGate • AWS DMS, Nutzung der vollen Last mit kontinuierlicher Replikation über CDC.	
Validieren Sie die Zieldatenbank.	Führen Sie nach der Migration eine Validierung von Datenbankspeicher- und Codeobjekten durch. Überprüfen Sie die Migrationsprotokolle und beheben Sie alle identifizierten Probleme. Weitere Informationen finden Sie im Leitfaden Migration von Oracle-Datenbanken in die AWS-Cloud.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Anwendungen.	Anwendungs- und Datenbankadministratoren sollten gegebenenfalls Funktions-, Leistungs- und Betriebstests durchführen. Weitere Informationen finden Sie unter Bewährte Methoden für die Migration zu Amazon RDS for Oracle. Lassen Sie sich abschließend von den Beteiligten die Zustimmung zu den Testergebnissen einholen.	App-Entwickler, App-Besitzer, DBA, Migrationsingenieur, Migrationsleiter

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Daten aus Oracle Database EE aktualisieren.	Wählen Sie einen Ansatz zur Datenaktualisierung, der auf den Anforderungen an die Anwendungsverfügbarkeit basiert. Weitere Informationen finden Sie in den Migrationsmethoden unter Strategien für die Migration von Oracle-Datenbanken zu AWS. Beispielsweise können Sie fast keine Ausfallzeiten erreichen, indem Sie Tools wie Oracle GoldenGate oder AWS DMS mit laufender Replikation verwenden. Wenn das	App-Besitzer, Leiter der Umstellung, DBA, Migrationsingenieur, Migrationsleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ausfallzeitfenster dies zulässt, können Sie die endgültige Datenübernahme mithilfe von Offline-Methoden wie Oracle Data Pump oder Original Export-Import durchführen.	
Verweisen Sie Anwendungen auf die Zieldatenbankinstanz.	Aktualisieren Sie die Verbindungsparameter in Anwendungen und anderen Clients so, dass sie auf die Amazon RDS for Oracle SE2 Oracle-Datenbank verweisen.	App-Entwickler, App-Besitzer, Migrationsingenieur, Migration sleiter, Cutover-Leiter
Führen Sie Aktivitäten nach der Migration durch.	Führen Sie Aufgaben nach der Datenmigration durch, z. B. die Aktivierung von Multi-AZ, Datenvalidierung und andere Prüfungen.	DBA, Migrationsingenieur
Führen Sie eine Überwachung nach der Umstellung durch.	Verwenden Sie Tools wie Amazon CloudWatch und Amazon RDS Performance Insights, um die Amazon RDS for Oracle SE2 Oracle-Da tenbank zu überwachen.	App-Entwickler, App-Besit zer, AWS-Administrator, DBA, Migrationsingenieur

Zugehörige Ressourcen

AWS Prescriptive Guidance

- Migration von Oracle-Datenbanken in die AWS-Cloud (Anleitung)
- Evaluieren Sie das Downgrade von Oracle-Datenbanken auf Standard Edition 2 auf AWS (Leitfaden)
- Migrieren Sie eine lokale Oracle-Datenbank zu Amazon RDS for Oracle (Muster)

- Migrieren Sie eine On-Premises-Oracle-Datenbank zu Amazon RDS für Oracle mit Oracle Data Pump (Muster)

Blog-Posts

- Migration von Oracle-Datenbanken mit AWS DMS nahezu ohne Ausfallzeiten
- Analyse des Leistungsmanagements in Oracle SE mit Amazon RDS for Oracle
- Verwaltung Ihres SQL-Plans in Oracle SE mit Amazon RDS for Oracle
- Implementierung der Tabellenpartitionierung in Oracle Standard Edition: Teil 1

Replizieren Sie Mainframe-Datenbanken mithilfe von Precisely Connect nach AWS

Erstellt von Lucio Pereira (AWS), Balaji Mohan (AWS) und Sayantan Giri (AWS)

Übersicht

Dieses Muster beschreibt die Schritte zur Replikation von Daten aus Mainframe-Datenbanken in Amazon-Datenspeicher nahezu in Echtzeit mithilfe von Precisely Connect. Es implementiert eine ereignisbasierte Architektur mit Amazon Managed Streaming for Apache Kafka (Amazon MSK) und benutzerdefinierten Datenbank-Konnektoren in der Cloud, um Skalierbarkeit, Belastbarkeit und Leistung zu verbessern.

Precisely Connect ist ein Replikationstool, das Daten von älteren Mainframe-Systemen erfasst und in Cloud-Umgebungen integriert. Daten werden durch Change Data Capture (CDC) von Mainframes auf AWS repliziert, wobei Nachrichtenflüsse nahezu in Echtzeit mit heterogenen Datenpipelines mit niedriger Latenz und hohem Durchsatz verwendet werden.

Dieses Muster deckt auch eine Notfallwiederherstellungsstrategie für belastbare Datenpipelines mit Datenreplikation und Failover-Routing in mehreren Regionen ab.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine bestehende Mainframe-Datenbank — z. B. IBM DB2, IBM Information Management System (IMS) oder Virtual Storage Access Method (VSAM) —, die Sie in die AWS-Cloud replizieren möchten
- Ein aktives AWS-Konto
- AWS Direct Connect oder AWS Virtual Private Network (AWS VPN) von Ihrer Unternehmensumgebung zu AWS
- Eine virtuelle private Cloud mit einem Subnetz, das über Ihre Legacy-Plattform erreichbar ist

Architektur

Quelltechnologie-Stack

Eine Mainframe-Umgebung, die mindestens eine der folgenden Datenbanken umfasst:

- IBM IMS-Datenbank
- DB2 IBM-Datenbank
- VSAM-Dateien

Zieltechnologie-Stack

- Amazon MSK
- Amazon Elastic Kubernetes Service (Amazon EKS) und Amazon EKS Anywhere
- Docker
- Eine relationale AWS-Datenbank oder NoSQL-Datenbank wie die folgende:
  - Amazon-DynamoDB
  - Amazon Relational Database Service (Amazon RDS) für Oracle, Amazon RDS for PostgreSQL oder Amazon Aurora
  - Amazon ElastiCache für Redis
  - Amazon Keyspaces (für Apache Cassandra)

Zielarchitektur

Replizieren von Mainframe-Daten in AWS-Datenbanken

Das folgende Diagramm veranschaulicht die Replikation von Mainframe-Daten in eine AWS-Datenbank wie DynamoDB, Amazon RDS, Amazon oder Amazon ElastiCache Keyspaces. Die Replikation erfolgt nahezu in Echtzeit, indem Sie Precisely Capture and Publisher in Ihrer lokalen Mainframe-Umgebung, Precisely Dispatcher auf Amazon EKS Anywhere in Ihrer lokalen verteilten Umgebung und Precisely Apply Engine und Datenbank-Konnektoren in der AWS-Cloud verwenden.

Das Diagramm zeigt den folgenden Workflow:

1. Precisiely Capture ruft Mainframe-Daten aus CDC-Protokollen ab und verwaltet die Daten im internen Transientenspeicher.
2. Precisely Publisher überwacht Änderungen im internen Datenspeicher und sendet CDC-Datensätze über eine TCP/IP-Verbindung an Precisely Dispatcher.
3. Precisely Dispatcher empfängt die CDC-Datensätze von Publisher und sendet sie an Amazon MSK. Der Dispatcher erstellt Kafka-Schlüssel auf der Grundlage der Benutzerkonfiguration und

mehrerer Worker-Tasks, um Daten parallel zu übertragen. Der Dispatcher sendet eine Bestätigung an Publisher zurück, wenn Datensätze in Amazon MSK gespeichert wurden.

4. Amazon MSK speichert die CDC-Aufzeichnungen in der Cloud-Umgebung. Die Partitionsgröße der Themen hängt von den Durchsatzanforderungen Ihres Transaktionsverarbeitungssystems (TPS) ab. Der Kafka-Schlüssel ist für die weitere Transformation und die Reihenfolge der Transaktionen erforderlich.
5. Die Precisely Apply Engine hört sich die CDC-Datensätze von Amazon MSK an und transformiert die Daten (z. B. durch Filtern oder Zuordnen) basierend auf den Anforderungen der Zieldatenbank. Sie können den Precisely SQD-Skripts benutzerdefinierte Logik hinzufügen. (SQD ist die eigene Sprache von Precisely.) Die Precisely Apply Engine wandelt jeden CDC-Datensatz in das Apache Avro- oder JSON-Format um und verteilt ihn je nach Ihren Anforderungen an verschiedene Themen.
6. Die Ziel-Kafka-Themen enthalten CDC-Datensätze in mehreren Themen, die auf der Zieldatenbank basieren, und Kafka erleichtert die Transaktionsreihenfolge auf der Grundlage des definierten Kafka-Schlüssels. Die Partitionsschlüssel sind auf die entsprechenden Partitionen abgestimmt, um einen sequentiellen Prozess zu unterstützen.
7. Datenbank-Connectors (maßgeschneiderte Java-Anwendungen) hören die CDC-Datensätze von Amazon MSK ab und speichern sie in der Zieldatenbank.
8. Sie können eine Zieldatenbank entsprechend Ihren Anforderungen auswählen. Dieses Muster unterstützt sowohl NoSQL- als auch relationale Datenbanken.

Wiederherstellung nach einem Notfall

Geschäftskontinuität ist der Schlüssel zum Erfolg Ihres Unternehmens. Die AWS-Cloud bietet Funktionen für Hochverfügbarkeit (HA) und Disaster Recovery (DR) und unterstützt die Failover- und Fallback-Pläne Ihres Unternehmens. Dieses Muster folgt einer aktiven/passiven DR-Strategie und bietet umfassende Leitlinien für die Implementierung einer DR-Strategie, die Ihren RTO- und RPO-Anforderungen entspricht.

Das folgende Diagramm veranschaulicht den DR-Workflow.

Das Diagramm zeigt Folgendes:

1. Ein halbautomatisches Failover ist erforderlich, falls in AWS-Region 1 ein Fehler auftritt. Im Falle eines Fehlers in Region 1 muss das System Routing-Änderungen einleiten, um den Precisely Dispatcher mit Region 2 zu verbinden.

2. Amazon MSK repliziert Daten durch Spiegelung zwischen Regionen. Aus diesem Grund muss der Amazon MSK-Cluster in Region 2 während eines Failovers als primärer Leader befördert werden.
3. Die Precisely Apply Engine und die Datenbank-Konnektoren sind zustandslose Anwendungen, die in jeder Region funktionieren können.
4. Die Datenbanksynchronisierung hängt von der Zieldatenbank ab. DynamoDB kann beispielsweise globale Tabellen und globale ElastiCache Datenspeicher verwenden.

Verarbeitung mit niedriger Latenz und hohem Durchsatz durch Datenbankkonnektoren

Datenbankkonnektoren sind wichtige Komponenten dieses Musters. Connectors verfolgen einen Listener-basierten Ansatz, um Daten von Amazon MSK zu sammeln und Transaktionen durch Verarbeitung mit hohem Durchsatz und niedriger Latenz für unternehmenskritische Anwendungen (Stufen 0 und 1) an die Datenbank zu senden. Das folgende Diagramm veranschaulicht diesen Prozess.

Dieses Muster unterstützt die Entwicklung einer maßgeschneiderten Anwendung mit Single-Thread-Nutzung über eine Multithread-Verarbeitungs-Engine.

1. Der Haupt-Thread des Connectors verwendet CDC-Datensätze von Amazon MSK und sendet sie zur Verarbeitung an den Thread-Pool.
2. Threads aus dem Thread-Pool verarbeiten CDC-Datensätze und senden sie an die Zieldatenbank.
3. Wenn alle Threads ausgelastet sind, werden die CDC-Einträge von der Thread-Warteschlange in der Warteschleife gehalten.
4. Der Haupt-Thread wartet darauf, dass alle Datensätze aus der Thread-Warteschlange gelöscht werden, und überträgt Offsets in Amazon MSK.
5. Die untergeordneten Threads behandeln Fehler. Wenn bei der Verarbeitung Fehler auftreten, werden die fehlgeschlagenen Nachrichten an das Thema DLQ (Dead Letter Queue) gesendet.
6. Die untergeordneten Threads initiieren bedingte Aktualisierungen (siehe Bedingungsausdrücke in der DynamoDB-Dokumentation) auf der Grundlage des Mainframe-Zeitstempels, um Duplikate oder out-of-order Aktualisierungen in der Datenbank zu vermeiden.

Informationen zur Implementierung einer Kafka-Consumer-Anwendung mit Multithreading-Funktionen finden Sie im Blogbeitrag Multi-Threading Message Consumption with the Apache Kafka Consumer auf der Confluent-Website.

Tools

AWS-Services

- Amazon Managed Streaming for Apache Kafka (Amazon MSK) ist ein vollständig verwalteter Service, der Sie beim Erstellen und Ausführen von Anwendungen unterstützt, die Apache Kafka zur Verarbeitung von Streaming-Daten verwenden.
- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen, Kubernetes auf AWS auszuführen, ohne Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten zu müssen.
- Amazon EKS Anywhere unterstützt Sie bei der Bereitstellung, Verwendung und Verwaltung von Kubernetes-Clustern, die in Ihren eigenen Rechenzentren ausgeführt werden.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der AWS-Cloud.
- Amazon ElastiCache unterstützt Sie bei der Einrichtung, Verwaltung und Skalierung verteilter In-Memory-Cache-Umgebungen in der AWS-Cloud.
- Amazon Keyspaces (für Apache Cassandra) ist ein verwalteter Datenbankservice, der Sie bei der Migration, Ausführung und Skalierung Ihrer Cassandra-Workloads in der AWS-Cloud unterstützt.

Andere Tools

- Precisely Connect integriert Daten aus älteren Mainframe-Systemen wie VSAM-Datensätzen oder IBM Mainframe-Datenbanken in Cloud- und Datenplattformen der nächsten Generation.

Bewährte Methoden

- Finden Sie die beste Kombination aus Kafka-Partitionen und Multithread-Konnektoren, um ein optimales Verhältnis von Leistung und Kosten zu erzielen. Mehrere Precisely Capture- und Dispatcher-Instanzen können aufgrund des höheren MIPS-Verbrauchs (Millionen Befehle pro Sekunde) die Kosten in die Höhe treiben.
- Vermeiden Sie es, den Datenbankkonnektoren Datenmanipulations- und Transformationslogik hinzuzufügen. Verwenden Sie zu diesem Zweck die Precisely Apply Engine, die Verarbeitungszeiten in Mikrosekunden angibt.

- Erstellen Sie in Datenbank-Konnektoren regelmäßige Anfragen oder Integritätsprüfungen an die Datenbank (Heartbeats), um die Verbindung häufig aufzuwärmen und die Latenz zu reduzieren.
- Implementieren Sie die Threadpool-Validierungslogik, um die ausstehenden Aufgaben in der Thread-Warteschlange zu verstehen und warten Sie, bis alle Threads abgeschlossen sind, bevor Sie mit der nächsten Kafka-Abfrage beginnen. Auf diese Weise können Datenverluste vermieden werden, wenn ein Knoten, ein Container oder ein Prozess abstürzt.
- Stellen Sie Latenzmetriken über Integritätsendpunkte zur Verfügung, um die Beobachtbarkeit mithilfe von Dashboards und Nachverfolgungsmechanismen zu verbessern.

Epen

Bereiten Sie die Quellumgebung vor (vor Ort)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie den Mainframe-Prozess (Batch- oder Online-Utility) ein, um den CDC-Prozess von Mainframe-Datenbanken aus zu starten.	1. Identifizieren Sie die Mainframe-Umgebung. 2. Identifizieren Sie die Mainframe-Datenbanken, die am CDC-Prozess beteiligt sein werden. 3. Entwickeln Sie in der Mainframe-Umgebung einen Prozess, der das CDC-Tool startet, um Änderungen in der Quelldatenbank zu erfassen. Anweisungen finden Sie in Ihrer Mainframe-Dokumentation. 4. Dokumentieren Sie den CDC-Prozess, einschließlich der Konfiguration. 5. Stellen Sie den Prozess sowohl in Test- als auch in	Mainframe-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Produktionsumgebungen bereit.	
Aktivieren Sie die Logstreams der Mainframe-Datenbank.	1. Konfigurieren Sie Protokoll streams in der Mainframe -Umgebung, um CDC-Protokolle zu erfassen. Anweisungen finden Sie in Ihrer Mainframe-Dokument ation. 2. Testen Sie die Log-Strea ms, um sicherzustellen, dass sie die erforderlichen Daten erfassen. 3. Stellen Sie die Protokoll streams in Test- und Produktionsumgebungen bereit.	Spezialist für Mainframe-Datenbanken

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie die Capture-Komponente, um CDC-Datensätze zu erfassen.	1. Installieren und konfigurieren Sie die Precisely Capture-Komponente in der Mainframe-Umgebung. Anweisungen finden Sie in der Precisely Dokumentation. 2. Testen Sie die Konfiguration, um sicherzustellen, dass die Capture-Komponente ordnungsgemäß funktioniert. 3. Richten Sie einen Replikationsprozess ein, um die erfassten CDC-Datensätze über die Capture-Komponente zu replizieren. 4. Dokumentieren Sie die Capture-Konfiguration für jede Quelldatenbank. 5. Entwickeln Sie ein Überwachungssystem, um sicherzustellen, dass die Capture-Komponente die Protokolle im Laufe der Zeit ordnungsgemäß sammelt. 6. Stellen Sie die Installation und Konfigurationen in der Test- und Produktionsumgebung bereit.	Mainframe-Ingenieur, Precisely Connect SME

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Publisher-Komponente so, dass sie die Capture-Komponente abhört.	1. Installieren und konfigurieren Sie die Precisely Publisher-Komponente in der Mainframe-Umgebung. Anweisungen finden Sie in der Precisely Dokumentation. 2. Testen Sie die Konfiguration, um sicherzustellen, dass die Publisher-Komponente ordnungsgemäß funktioniert. 3. Richten Sie einen Replikationsprozess ein, um die CDC-Datensätze von Publisher in der Precisely Dispatcher-Komponente zu veröffentlichen. 4. Dokumentieren Sie die Publisher-Konfiguration. 5. Entwickeln Sie ein Überwachungssystem, um sicherzustellen, dass die Publisher-Komponente im Laufe der Zeit ordnungsgemäß funktioniert. 6. Stellen Sie die Installation und Konfigurationen in der Test- und Produktionsumgebung bereit.	Mainframe-Ingenieur, Precisely Connect SME

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Amazon EKS Anywhere in der lokalen verteilten Umgebung bereit.	1. Installieren Sie Amazon EKS Anywhere auf der lokalen Infrastruktur und stellen Sie sicher, dass diese ordnungsgemäß konfiguriert ist. Anweisungen finden Sie in der Amazon EKS Anywhere Anywhere-Dokumentation. 2. Richten Sie eine sichere Netzwerkumgebung für den Kubernetes-Cluster ein, einschließlich Firewalls. 3. Implementieren und testen Sie die Bereitstellung der Beispielanwendung im Amazon EKS Anywhere Anywhere-Cluster. 4. Implementieren Sie automatische Skalierungsfunktionen für den Cluster. 5. Entwicklung und Implementierung von Sicherungs- und Notfallwiederherstellungsverfahren.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Dispatcher-Komponente in der verteilten Umgebung bereit und konfiguri eren Sie sie, um die Themen in der AWS-Cloud zu veröffent lichen.	1. Konfigurieren und container isieren Sie die Precisely Dispatcher-Komponente. Anweisungen finden Sie in der Precisely Dokumenta tion. 2. Stellen Sie das Dispatcher-Docker-Image in der lokalen Amazon EKS Anywhere Anywhere-Umgebung bereit. 3. Richten Sie eine sichere Verbindung zwischen der AWS-Cloud und dem Dispatcher ein. 4. Entwickeln Sie ein Überwachungssystem, um sicherzustellen, dass die Dispatcher-Komponente im Laufe der Zeit ordnungsg emäß funktioniert. 5. Stellen Sie die Installation und die Konfigurationen in der Test- und Produktio nsumgebung bereit.	DevOps Ingenieur, Precisely Connect SME

Bereiten Sie die Zielumgebung vor (AWS)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie einen Amazon EKS-Cluster in der angegeben en AWS-Region bereit.	1. Melden Sie sich bei Ihrem AWS-Konto an und konfigurieren Sie es, um	DevOps Ingenieur, Netzwerka dministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	sicherzustellen, dass die erforderlichen Berechtigungen für die Erstellung und Verwaltung des Amazon EKS-Clusters vorhanden sind. 2. Erstellen Sie eine Virtual Private Cloud (VPC) und Subnetze in der ausgewählten AWS-Region. Anweisungen finden Sie in der Amazon EKS-Dokumentation. 3. Erstellen und konfigurieren Sie die erforderlichen Netzwerksicherheitsgruppen, um die Kommunikation zwischen dem Amazon EKS-Cluster und anderen Ressourcen in der VPC zu ermöglichen. Weitere Informationen finden Sie in der Amazon EKS-Dokumentation. 4. Erstellen Sie den Amazon EKS-Cluster und konfigurieren Sie ihn mit der richtigen Knotengruppengröße und den richtigen Instance-Typen. 5. Validieren Sie den Amazon EKS-Cluster, indem Sie eine Beispielanwendung bereitstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie einen MSK-Cluster bereit und konfigurieren Sie die entsprechenden Kafka-Themen.	1. Konfigurieren Sie Ihr AWS-Konto, um sicherzustellen, dass die erforderlichen Berechtigungen für die Erstellung und Verwaltung des MSK-Clusters vorhanden sind. 2. Erstellen und konfigurieren Sie die erforderlichen Netzwerksicherheitsgruppen, um die Kommunikation zwischen dem MSK-Cluster und anderen Ressourcen in der VPC zu ermöglichen. Weitere Informationen finden Sie in der Amazon VPC-Dokumentation. 3. Erstellen Sie den MSK-Cluster und konfigurieren Sie ihn so, dass er die Kafka-Themen enthält, die von der Anwendung verwendet werden. Weitere Informationen finden Sie in der Amazon MSK-Dokumentation.	DevOps Ingenieur, Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Apply Engine-Komponente so, dass sie sich die replizierten Kafka-Themen anhört.	1. Konfigurieren und containerisieren Sie die Precisely Apply Engine-Komponente. 2. Stellen Sie das Apply Engine Docker-Image im Amazon EKS-Cluster in Ihrem AWS-Konto bereit. 3. Richten Sie die Apply Engine so ein, dass sie MSK-Themen abhört. 4. Entwickeln und konfigurieren Sie ein SQD-Skript in der Apply Engine für die Filterung und Transformation. Weitere Informationen finden Sie in der Dokumentation Precisely. 5. Stellen Sie die Apply Engine in Test- und Produktionsumgebungen bereit.	Precisely Connect SME

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie DB-Instances in der AWS-Cloud bereit.	1. Konfigurieren Sie Ihr AWS-Konto, um sicherzustellen, dass die erforderlichen Berechtigungen für die Erstellung und Verwaltung von DB-Clustern und -Tabellen vorhanden sind. Anweisungen finden Sie in der AWS-Dokumentation für den AWS-Datenbankservice, den Sie verwenden möchten. (Links finden Sie im Abschnitt Ressourcen.) 2. Erstellen Sie eine VPC und Subnetze in der ausgewählten AWS-Region. 3. Erstellen und konfigurieren Sie die erforderlichen Netzwerksicherheitsgruppen, um die Kommunikation zwischen den DB-Instances und anderen Ressourcen in der VPC zu ermöglichen. 4. Erstellen Sie die Datenbanken und konfigurieren Sie sie so, dass sie die Tabellen enthalten, die die Anwendung verwenden wird. 5. Entwerfen und validieren Sie die Datenbankschemas.	Dateningenieur, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren und implementieren Sie Datenbank-Konnektoren, um sich die von der Apply Engine veröffentlichten Themen anzuhören.	1. Entwerfen Sie Datenbank-Konnektoren, um die Kafka-Themen mit den AWS-Datenbanken zu verbinden, die Sie in den vorherigen Schritten erstellt haben. 2. Entwickeln Sie die Konnektoren auf der Grundlage der Zieldatenbank. 3. Konfigurieren Sie die Konnektoren so, dass sie sich die Kafka-Themen anhören, die von der Apply Engine veröffentlicht werden. 4. Stellen Sie die Konnektoren im Amazon EKS-Cluster bereit.	App-Entwickler, Cloud-Architekt, Dateningenieur

Richten Sie Geschäftskontinuität und Disaster Recovery ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie Ziele für die Notfallwiederherstellung für Ihre Geschäftsanwendungen.	1. Definieren Sie die RPO- und RTO-Ziele für CDC-Pipelines auf der Grundlage Ihrer Geschäftsanforderungen und der Folgenanalyse. 2. Definieren Sie die Kommunikations- und Benachrichtigungsv	Cloud-Architekt, Dateningenieur, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	erfahren, um sicherzus tellen, dass alle Beteiligten über den Notfallwiederherst ellungsplan informiert sind. 3. Ermitteln Sie das Budget und die Ressourcen, die für die Umsetzung des Notfallwiederherstellungspl ans erforderlich sind. 4. Dokumentieren Sie die Ziele für die Notfallwi ederherstellung, einschlie ßlich der RPO- und RTO-Ziele.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entwerfen Sie Strategien für die Notfallwiederherstellung auf der Grundlage eines definierten RTO/RPO.	1. Ermitteln Sie die am besten geeigneten Strategien für die Notfallwiederherstellung für CDC-Pipelines auf der Grundlage Ihrer Kritikalität und Ihrer Wiederherstellungsanforderungen. 2. Definieren Sie die Disaster Recovery-Architektur und -Topologie. 3. Definieren Sie die Failover- und Failback-Verfahren für CDC-Pipelines, um sicherzustellen, dass diese schnell und nahtlos in die Backup-Region umgestellt werden können. 4. Dokumentieren Sie die Strategien und Verfahren für die Notfallwiederherstellung und stellen Sie sicher, dass alle Beteiligten ein klares Verständnis des Entwurfs haben.	Cloud-Architekt, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Disaster Recovery-Cluster und Konfigurationen bereit.	1. Stellen Sie eine sekundäre AWS-Region für die Notfallwiederherstellung bereit. 2. Erstellen Sie in der sekundären AWS-Region eine Umgebung, die mit der primären AWS-Region identisch ist. 3. Konfigurieren Sie Apache Kafka MirrorMaker zwischen der primären und der sekundären Region. Weitere Informationen finden Sie in der Amazon MSK-Dokumentation. 4. Konfigurieren Sie Standby-Anwendungen in der sekundären Region. 5. Konfigurieren Sie Datenbankreplikationen zwischen der primären und der sekundären Region.	DevOps Ingenieur, Netzwerkadministrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die CDC-Pipeline für die Notfallwiederherstellung.	1. Definieren Sie den Umfang und die Ziele des Disaster Recovery-Tests für die CDC-Pipeline, einschließlich der Testszenarien und der zu erreichenden RTO. 2. Identifizieren Sie die Testumgebung und die Infrastruktur für die Durchführung des Disaster Recovery-Tests. 3. Bereiten Sie die Testdatensätze und das Skript vor, um Ausfallszenarien zu simulieren. 4. Überprüfen Sie die Datenintegrität und -konsistenz, um sicherzustellen, dass es nicht zu Datenverlusten kommt.	App-Besitzer, Dateningenieur, Cloud-Architekt

Zugehörige Ressourcen

AWS-Ressourcen

- Amazon-DynamoDB
- Bedingungsausdrücke mit Amazon DynamoDB
- Amazon EKS
- Amazon EKS Anywhere
- Amazon ElasticCache
- Amazon Keyspaces
- Amazon MSK

- Amazon RDS und Amazon Aurora
- Amazon VPC

Ressourcen präzise Connect

- Precisiely Connect im Überblick
- Datenerfassung ändern mit Precisely Connect

Konfluente Ressourcen

- Nachrichtenverarbeitung in mehreren Threads mit dem Apache Kafka Consumer

Planen Sie Jobs für Amazon RDS for PostgreSQL und Aurora PostgreSQL mithilfe von Lambda und Secrets Manager

Erstellt von Yaser Raja (AWS)

Übersicht

Für lokale Datenbanken und Datenbanken, die auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances gehostet werden, verwenden Datenbankadministratoren häufig das Cron-Hilfsprogramm, um Jobs zu planen.

Beispielsweise kann ein Job für die Datenextraktion oder ein Job für das Löschen von Daten einfach mit Cron geplant werden. Für diese Jobs sind die Datenbankanmeldedaten in der Regel entweder fest codiert oder in einer Eigenschaftendatei gespeichert. Wenn Sie jedoch zu Amazon Relational Database Service (Amazon RDS) oder Amazon Aurora PostgreSQL-Compatible Edition migrieren, verlieren Sie die Möglichkeit, sich bei der Host-Instance anzumelden, um Cron-Jobs zu planen.

Dieses Muster beschreibt, wie Jobs für Amazon RDS for PostgreSQL AWS Lambda - und AWS Secrets Manager Aurora PostgreSQL-kompatible Datenbanken nach der Migration verwendet und geplant werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Eine Amazon RDS for PostgreSQL- oder Aurora PostgreSQL-kompatible Datenbank

Einschränkungen

- Ein Job muss innerhalb von 15 Minuten abgeschlossen sein. Dies ist das Timeout-Limit für Lambda-Funktionen. Weitere Grenzwerte finden Sie in der AWS Lambda Dokumentation.
- Der Jobcode muss in einer von Lambda unterstützten Sprache geschrieben sein.

Architektur

Quelltechnologie-Stack

Dieser Stack enthält Jobs, die in Sprachen wie Bash, Python und Java geschrieben wurden. Datenbankanmeldedaten werden in der Eigenschaftendatei gespeichert, und der Job wird mithilfe von Linux-Cron geplant.

Zieltechnologie-Stack

Dieser Stack hat eine Lambda-Funktion, die die in Secrets Manager gespeicherten Anmeldeinformationen verwendet, um eine Verbindung mit der Datenbank herzustellen und die Aktivität auszuführen. Die Lambda-Funktion wird im geplanten Intervall mithilfe von Amazon CloudWatch Events initiiert.

Zielarchitektur

Tools

- Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS Ressourcen beschreiben, nahezu in Echtzeit. Mithilfe einfacher Regeln, die Sie schnell einrichten können, können Sie Ereignisse zuordnen und sie an eine oder mehrere Zielfunktionen oder Streams weiterleiten. CloudWatch Events erkennt betriebliche Änderungen, sobald sie eintreten. Es reagiert auf diese betrieblichen Änderungen und ergreift bei Bedarf Korrekturmaßnahmen, indem es Nachrichten sendet, um auf die Umgebung zu reagieren, Funktionen aktiviert, Änderungen vornimmt und Statusinformationen erfasst. Sie können CloudWatch Ereignisse auch verwenden, um mithilfe von Cron - oder Rate-Ausdrücken automatisierte Aktionen zu planen, die zu bestimmten Zeiten von selbst initiiert werden.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie zahlen nur für die Rechenzeit, die Sie verbrauchen. Es fallen keine Gebühren an, wenn Ihr Code nicht ausgeführt wird. Mit Lambda können Sie Code für praktisch jede Art von Anwendung oder Backend-Service ohne Verwaltungsaufwand ausführen. Lambda führt Ihren Code auf einer hochverfügbaren Recheninfrastruktur aus und verwaltet alle Rechenressourcen, einschließlich Server- und Betriebssystemwartung, Kapazitätsbereitstellung und automatische Skalierung, Codeüberwachung und Protokollierung. Sie müssen lediglich Ihren Code in einer der Sprachen bereitstellen, die Lambda unterstützt.
- AWS Secrets Managerhilft Ihnen dabei, Geheimnisse für den Zugriff auf Ihre Anwendungen, Dienste und IT-Ressourcen zu schützen. Sie können Datenbankanmeldedaten, API-Schlüssel und andere Geheimnisse während ihres gesamten Lebenszyklus problemlos rotieren, verwalten

und abrufen. Benutzer und Anwendungen rufen Geheimnisse ab, indem sie Secrets Manager aufrufen. Dadurch entfällt die Notwendigkeit APIs, vertrauliche Informationen im Klartext fest zu codieren. Secrets Manager bietet geheime Rotation mit integrierter Integration für Amazon RDS, Amazon Redshift und Amazon DocumentDB. Der Service ist auf andere Arten von Geheimnissen erweiterbar, einschließlich API-Schlüsseln und Tokens. OAuth Secrets Manager ermöglicht es Ihnen, den Zugriff auf geheime Daten mithilfe detaillierter Berechtigungen zu kontrollieren und die Rotation von Geheimnissen zentral für Ressourcen in den AWS Cloud Diensten von Drittanbietern und vor Ort zu überwachen.

Epen

Speichern Sie Datenbankanmeldedaten in Secrets Manager

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Datenbankbenutzer für die Lambda-Funktion.	Es empfiehlt sich, separate Datenbankbenutzer für verschiedene Teile Ihrer Anwendung zu verwenden. Wenn für Ihre Cron-Jobs bereits ein separater Datenbankbenutzer existiert, verwenden Sie diesen. Andernfalls erstellen Sie einen neuen Datenbankbenutzer. Weitere Informationen finden Sie unter PostgreSQL-Benutzer und -Rollen verwalten (AWS Blogbeitrag).	DBA
Speichern Sie Datenbankanmeldedaten als geheim in Secrets Manager.	Folgen Sie den Anweisungen unter Create a database secret (Secrets Manager-Dokumentation).	DBA, DevOps

Verfassen Sie den Code für die Lambda-Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie eine von Lambda unterstützte Programmi ersprache.	Eine Liste der unterstützten Sprachen finden Sie unter Lambda-Laufzeiten (Lambda-Dokumentation).	Developer
Schreiben Sie die Logik zum Abrufen der Datenbank anmeldedaten von Secrets Manager.	Beispielcode finden Sie unter So stellen Sie Datenbank anmeldedaten sicher für Lambda-Funktionen bereit, indem Sie AWS Secrets Manager(AWS Blogbeitrag) verwenden.	Developer
Schreiben Sie die Logik zur Ausführung der geplanten Datenbankaktivität.	Migrieren Sie Ihren vorhanden en Code für den Schedulin g-Job, den Sie vor Ort verwenden, auf die Lambda-Funktion. Weitere Informati onen finden Sie unter Deployment von Lambda-Funktionen (Lambda-D okumentation).	Developer

Stellen Sie den Code bereit und erstellen Sie die Lambda-Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Lambda-Fu nktionsbereitstellungspaket.	Dieses Paket enthält den Code und seine Abhängigk eiten. Weitere Informationen finden Sie unter Bereitste	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	llungspakete (Lambda-D okumentation).	
So erstellen Sie die Lambda-Funktion:	Wählen Sie in der Lambda-Konsole Create function aus, geben Sie einen Funktions namen ein, wählen Sie die Laufzeitumgebung aus und wählen Sie dann Create function aus.	DevOps
Laden Sie das Bereitste llungspaket hoch.	Wählen Sie die Lambda-Fu nktion aus, die Sie erstellt haben, um ihre Konfiguration zu öffnen. Sie können Ihren Code direkt in den Codeberei ch schreiben oder Ihr Bereitste llungspaket hochladen. Um Ihr Paket hochzuladen, gehen Sie zum Abschnitt Funktionscode, wählen Sie den Eintragstyp Code aus, um eine ZIP-Datei hochzuladen, und wählen Sie dann das Paket aus.	DevOps
Konfigurieren Sie die Lambda-Funktion gemäß Ihren Anforderungen.	Sie können beispielsweise den Timeout-Parameter auf die Dauer festlegen, die Ihre Lambda-Funktion voraussichtlich dauern wird. Weitere Informationen finden Sie unter Konfiguration von Funktionsoptionen (Lambda-D okumentation).	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie die Berechtigungen für die Lambda-Funktionsrolle für den Zugriff auf Secrets Manager fest.	Anweisungen finden Sie unter Verwenden von Geheimnissen in AWS Lambda Funktionen (Secrets Manager Manager-Dokumentation).	DevOps
Testen Sie die Lambda-Funktion.	Initiieren Sie die Lambda-Funktion manuell, um sicherzustellen, dass sie wie erwartet funktioniert.	DevOps

Planen Sie die Lambda-Funktion mithilfe von Ereignissen CloudWatch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Regel, damit die Lambda-Funktion nach einem Zeitplan ausgeführt wird.	Planen Sie die Lambda-Funktion mithilfe von CloudWatch Events. Anweisungen finden Sie unter Lambda-Funktionen mithilfe von CloudWatch Ereignissen planen (CloudWatch Events-Tutorial).	DevOps

Zugehörige Ressourcen

- AWS Secrets Manager
- Erste Schritte mit Lambda
- Eine CloudWatch Ereignisregel erstellen, die bei einem Ereignis ausgelöst wird
- AWS Lambda Beschränkungen
- Fragen Sie Ihre AWS Datenbank von Ihrer serverlosen Anwendung aus ab (Blogbeitrag)

Senden Sie Benachrichtigungen für eine Amazon RDS for SQL Server Server-Datenbank-Instance mithilfe eines lokalen SMTP-Servers und Datenbank-E-Mail

Erstellt von Nishad Mankar (AWS)

Übersicht

Datenbank-E-Mail (Microsoft-Dokumentation) sendet E-Mail-Nachrichten, wie Benachrichtigungen oder Warnungen, aus einer Microsoft SQL Server-Datenbank mithilfe eines SMTP-Servers (Simple Mail Transfer Protocol). Die Dokumentation zu Amazon Relational Database Service (Amazon RDS) für Microsoft SQL Server enthält Anweisungen zur Verwendung von Amazon Simple Email Service (Amazon SES) als SMTP-Server für Datenbank-Mail. Weitere Informationen finden Sie unter Using Database Mail on Amazon RDS for SQL Server (Verwenden von Database Mail auf Amazon RDS für SQL Server). Als alternative Konfiguration erklärt dieses Muster, wie Database Mail so konfiguriert wird, dass E-Mails von einer Amazon RDS for SQL Server Server-Datenbank-Instance (DB) gesendet werden, indem ein lokaler SMTP-Server als Mail-Server verwendet wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Amazon RDS-DB-Instance, auf der eine Standard- oder Enterprise Edition von SQL Server ausgeführt wird
- Die IP-Adresse oder der Hostname des lokalen SMTP-Servers
- Eine Sicherheitsgruppenregel für eingehenden Datenverkehr, die Verbindungen mit der Amazon RDS for SQL Server-DB-Instance von der IP-Adresse des SMTP-Servers aus ermöglicht
- Eine Verbindung, z. B. eine AWS Direct Connect Connect-Verbindung, zwischen Ihrem lokalen Netzwerk und der Virtual Private Cloud (VPC), die die Amazon RDS-DB-Instance enthält

Einschränkungen

- Express-Editionen von SQL Server werden nicht unterstützt.
- Weitere Informationen zu Einschränkungen finden Sie unter Einschränkungen bei der Verwendung von Datenbank-Mail auf Amazon RDS for SQL Server in der Amazon RDS-Dokumentation.

Produktversionen

- Standard- und Enterprise-Editionen der SQL Server-Versionen, die in RDS unterstützt werden

Architektur

Zieltechnologie-Stack

- Amazon RDS for SQL Server Server-Datenbank-Instance
- Amazon Route 53 53-Weiterleitungsregel
- Datenbank-E-Mail
- Lokaler SMTP-Server
- Microsoft SQL Server Management Studio (SSMS)

Zielarchitektur

Die folgende Abbildung zeigt die Zielarchitektur für dieses Muster. Wenn ein Ereignis oder eine Aktion eintritt, die eine Benachrichtigung oder Warnung bezüglich der Datenbank-Instance auslöst, verwendet Amazon RDS for SQL Server Database Mail, um eine E-Mail-Benachrichtigung zu senden. Database Mail verwendet den lokalen SMTP-Server, um die E-Mail zu senden.

Tools

AWS-Services

- Amazon Relational Database Service (Amazon RDS) für Microsoft SQL Server unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen SQL Server-Datenbank in der AWS-Cloud.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.

Andere Tools

- Datenbank-E-Mail ist ein Tool, das E-Mail-Nachrichten, wie Benachrichtigungen und Warnungen, von der SQL Server Database Engine (Datenbankmodul) an Benutzer sendet.
- Microsoft SQL Server Management Studio (SSMS) ist ein Tool für die Verwaltung von SQL Server, einschließlich des Zugriffs auf, der Konfiguration und der Verwaltung von SQL Server-

Komponenten. In diesem Muster verwenden Sie SSMS, um die SQL-Befehle auszuführen, um Database Mail auf einer Amazon RDS for SQL Server-DB-Instance einzurichten.

Epen

Aktivieren Sie die Netzwerkkonnektivität mit dem lokalen SMTP-Server

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie Multi-AZ aus der RDS-DB-Instance.	Wenn Sie eine Multi-Zone-RDS-DB-Instance verwenden , konvertieren Sie die Multi-AZ-Instance in eine Single-AZ -Instance. Wenn Sie mit der Konfiguration von Database Mail fertig sind, konvertieren Sie die DB-Instance wieder in eine Multi-AZ-Bereitste llung. Die Database Mail-Konfiguration funktioniert dann sowohl im primären als auch im sekundären Knoten. Anweisungen finden Sie unter Multi-AZ aus einer Microsoft SQL Server-DB-Instance entfernen.	DBA
Erstellen Sie eine Zulassung sliste für den Amazon RDS-Endpunkt oder die IP-Adresse auf dem lokalen SMTP-Server.	Der SMTP-Server befindet sich außerhalb des AWS-Netzwerks. Erstellen Sie auf dem lokalen SMTP-Server eine Zulassungsliste, die es dem Server ermöglicht, mit dem ausgehenden Endpunkt oder der IP-Adresse für die Amazon RDS-Instance oder die Amazon Elastic Compute	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Cloud (Amazon EC2) - Instance zu kommunizieren, die auf Amazon RDS gehostet wird. Dieses Verfahren ist von Organisation zu Organisat ion unterschiedlich. Weitere Informationen zum DB-Instance-Endpunkt finden Sie unter Finden des DB-Instance-Endpunkts und der Portnummer.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die Einschränkungen für Port 25.	Standardmäßig schränkt AWS Port 25 für EC2 Instances ein. Gehen Sie wie folgt vor, um die Beschränkung auf Port 25 aufzuheben: 1. Melden Sie sich mit Ihrem AWS-Konto an und öffnen Sie dann das Formular Anfrage zur Aufhebung der Einschränkungen beim Senden von E-Mails. 2. Geben Sie Ihre E-Mail-Adresse ein, damit der AWS Support Sie mit aktuellen Informationen zu Ihrer Anfrage kontaktieren kann. 3. Geben Sie die erforderlichen Informationen in das Feld Beschreibung des Anwendungsfalls ein. 4. Wählen Sie Absenden aus. Note • Wenn Sie Instances in mehr als einer AWS-Region haben, reichen Sie für jede Region eine separate Anfrage ein.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Die Bearbeitung Ihrer Anfrage kann bis zu 48 Stunden dauern.	
Fügen Sie eine Route 53 53-Regel hinzu, um DNS-Abfragen für den SMTP-Server aufzulösen.	Verwenden Sie Route 53, um DNS-Abfragen zwischen Ihren AWS-Ressourcen und dem lokalen SMTP-Server zu lösen. Sie müssen eine Regel erstellen, die die DNS-Abfragen an die SMTP-Serverdomäne weiterleitet, z. B. `example.com` Anweisungen finden Sie in der Route 53 53-Dokumentation unter Erstellen von Weiterleitungsregeln.	Netzwerkadministrator

Datenbank-E-Mail auf der Amazon RDS for SQL Server-DB-Instance einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Datenbank-E-Mail aktivieren.	Erstellen Sie eine Parametergruppe für Datenbank-E-Mail, legen Sie den `database mail xps` Parameter auf fest1, und ordnen Sie dann die Datenbank-E-Mail-Parametergruppe der Ziel-RDS-DB-Instance zu. Anweisungen finden Sie unter Enabling Database Mail in der Amazon RDS-Dokumentation. Fahren Sie in dieser Anleitung nicht mit dem Abschnitt Konfiguration von Datenbank-Mail fort. Die	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Konfiguration für den lokalen SMTP-Server unterscheidet sich von der von Amazon SES.	
Stellen Sie eine Verbindung mit der DB-Instance her.	Verwenden Sie von einem Bastion-Host aus Microsoft SQL Server Managemen t Studio (SSMS), um eine Verbindung zur Amazon RDS for SQL Server Server-Da tenbank-Instance herzustel len. Anweisungen finden Sie unter Verbindung zu einer DB-Instance herstelle n, auf der die Microsoft SQL Server-Datenbank-Engine ausgeführt wird. Falls Sie auf Fehler stoßen, finden Sie im Abschnitt Verwandte Ressourcen die Hinweise zur Fehlerbehebung bei Verbindungen.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Profil.	Geben Sie in SSMS die folgende SQL-Anweisung ein, um das Datenbank-E-Mail-Profil zu erstellen. Ersetzen Sie die folgenden Werte: • Geben Sie für `profile_name` einen Namen für das neue Profil ein. • Geben Sie für `description` eine kurze Beschreibung des neuen Profils ein. Weitere Informationen zu dieser gespeicherten Prozedur und ihren Argumenten finden Sie in der Microsoft-Dokumentation unter sysmail_add_profile_sp. `EXECUTE msdb.dbo.sysmail_add_profile_sp @profile_name = 'SQL Alerts profile', @description = 'Profile used for sending outgoing notifications using OM SMTP Server.';`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie dem Profil Principals hinzu.	Geben Sie die folgende SQL-Anweisung ein, um dem Datenbank-E-Mail-Profil öffentliche oder private Prinzipale hinzuzufügen. Ein Prinzipal ist eine Entität, die SQL Server-Ressourcen anfordern kann. Ersetzen Sie die folgenden Werte: • Geben Sie für `profile_name` den Namen des Profils ein, das Sie zuvor erstellt haben. • Geben Sie für `principal_name` den Namen des Datenbankbenutzers oder der Datenbankrolle ein. Dieser Wert muss einem SQL Server-Authentifizierungsbenutzer, einem Windows-Authentifizierungsbenutzer oder einer Windows-Authentifizierungsgruppe zugeordnet sein. Weitere Informationen zu dieser gespeicherten Prozedur und ihren Argumenten finden Sie in der Microsoft-Dokumentation unter sysmail_add_principalprofile_sp.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`EXECUTE msdb.dbo.sysmail_add_principalprofile_sp @profile_name = 'SQL Alerts profile', @principal_name = 'public', @is_default = 1 ;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Konto.	Geben Sie die folgende SQL-Anweisung ein, um das Datenbank-E-Mail-Konto zu erstellen. Ersetzen Sie die folgenden Werte: • Geben Sie für `account_name` einen Namen für das neue Konto ein. • Geben Sie für `description` eine kurze Beschreibung des neuen Kontos ein. • Geben Sie für die E-Mail-Adresse ein `email_address`, von der aus die Datenbank-E-Mail-Nachrichten gesendet werden sollen. • Geben Sie für einen Anzeigenamen ein `display_address`, der für ausgehende Nachrichten für dieses Konto verwendet werden soll, z. `SQL Server Automated Notification` B. Sie können auch den Wert verwenden, für den Sie eingegeben haben `email_address`. • Geben Sie für `mailserver_name` den Namen oder die IP-Adresse des SMTP-Mailservers ein.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Belassen Sie für `port` den Wert von. `25` • Lassen Sie den Wert für `enable_ssl` stehen `1` oder geben Sie ein, `0` wenn Datenbank-E-Mail die Kommunikation nicht mit SSL verschlüsseln soll. • Geben Sie für `username` den Benutzernamen für die Anmeldung am SMTP-Mailserver ein. Wenn für den Server keine Authentif izierung erforderlich ist, geben Sie ein`NULL`. • Geben Sie für `password` das Passwort für die Anmeldung am SMTP-Mailserver ein. Wenn für den Server keine Authentif izierung erforderlich ist, geben Sie ein`NULL`. Weitere Informationen zu dieser gespeicherten Prozedur und ihren Argumenten finden Sie in der Microsoft -Dokumentation unter sysmail_add_account_sp. `EXECUTE msdb.dbo.sysmail_add_accoun t_sp @account_name = 'SQL Alerts account',`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>@description = 'Database Mail account for sending outgoing notifications.', @email_address = 'xyz@example.com', @display_name = 'xyz@example.com', @mailserver_name = 'test_smtp.example.com', @port = 25, @enable_ssl = 1, @username = 'SMTP-username', @password = 'SMTP-password';</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie das Konto dem Profil hinzu.	Geben Sie die folgende SQL-Anweisung ein, um das Datenbank-E-Mail-Konto zum Datenbank-E-Mail-Profil hinzuzufügen. Ersetzen Sie die folgenden Werte: • Geben Sie für `profile_name` den Namen des Profils ein, das Sie zuvor erstellt haben. • Geben Sie für `account_name` den Namen des Kontos ein, das Sie zuvor erstellt haben. Weitere Informationen zu dieser gespeicherten Prozedur und ihren Argumenten finden Sie in der Microsoft-Dokumentation unter sysmail_add_profileaccount_sp. `EXECUTE msdb.dbo.sysmail_add_profileaccount_sp @profile_name = 'SQL Alerts profile', @account_name = 'SQL Alerts account', @sequence_number = 1;`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Fügen Sie Multi-AZ zur RDS-DB-Instance hinzu.	Wenn Sie Multi-AZ mit Datenbankspiegelung (DBM) oder AlwaysOn-Verfügbar keitsgruppen (AGs) hinzufüge n möchten, lesen Sie die Anweisungen unter Hinzufüge n von Multi-AZ zu einer Microsoft SQL Server-DB-Instance.	DBA

Zugehörige Ressourcen

- Verwenden von Database Mail auf Amazon RDS for SQL Server (Amazon RDS-Dokumentation)
- Arbeiten mit Dateianhängen (Amazon RDS-Dokumentation)
- Problembehandlung bei Verbindungen zu Ihrer SQL Server-DB-Instance (Amazon RDS-Dokumentation)
- Es kann keine Verbindung zur Amazon RDS-DB-Instance hergestellt werden (Amazon RDS-Dokumentation)

Disaster Recovery für SAP auf IBM Db2 auf AWS einrichten

Erstellt von Ambarish Satarkar (AWS) und Debasis Sahoo (AWS)

Übersicht

Dieses Muster beschreibt die Schritte zur Einrichtung eines Disaster Recovery-Systems (DR) für SAP-Workloads mit IBM Db2 als Datenbankplattform, das in der Amazon Web Services (AWS) Cloud ausgeführt wird. Ziel ist die Bereitstellung einer kostengünstigen Lösung zur Gewährleistung der Geschäftskontinuität im Falle eines Ausfalls.

Das Muster verwendet den Pilotlampenansatz. Durch die Implementierung von Pilot Light DR auf AWS können Sie Ausfallzeiten reduzieren und die Geschäftskontinuität aufrechterhalten. Der Pilot-Light-Ansatz konzentriert sich auf die Einrichtung einer minimalen DR-Umgebung in AWS, einschließlich eines SAP-Systems und einer Standby-Db2-Datenbank, die mit der Produktionsumgebung synchronisiert ist.

Diese Lösung ist skalierbar. Sie können sie nach Bedarf auf eine umfassende Notfallwiederherstellungsumgebung erweitern.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine SAP-Instance, die auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance läuft
- Eine IBM Db2-Datenbank
- Ein Betriebssystem, das von der SAP Product Availability Matrix (PAM) unterstützt wird
- Verschiedene physische Datenbank-Hostnamen für Produktions- und Standby-Datenbank-Hosts
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket in jeder AWS-Region mit aktivierter regionsübergreifender Replikation (CRR)

Produktversionen

- IBM Db2-Datenbank Version 11.5.7 oder höher

Architektur

Zieltechnologie-Stack

- Amazon EC2
- Amazon Simple Storage Service (Amazon-S3)
- Amazon Virtual Private Cloud (VPC-Peering)
- Amazon Route 53
- IBM Db2 Disaster Recovery (HADR) mit hoher Verfügbarkeit

Zielarchitektur

Diese Architektur implementiert eine DR-Lösung für SAP-Workloads mit Db2 als Datenbankplattform. Die Produktionsdatenbank wird in AWS-Region 1 bereitgestellt und eine Standby-Datenbank wird in einer zweiten Region bereitgestellt. Die Standby-Datenbank wird als DR-System bezeichnet. Db2-Datenbank unterstützt mehrere Standby-Datenbanken (bis zu drei). Es verwendet Db2 HADR für die Einrichtung der DR-Datenbank und die Automatisierung des Protokollversands zwischen der Produktions- und der Standby-Datenbank.

Im Notfall, bei dem Region 1 nicht verfügbar ist, übernimmt die Standby-Datenbank in der DR-Region die Rolle der Produktionsdatenbank. SAP-Anwendungsserver können im Voraus oder mithilfe von AWS Elastic Disaster Recovery oder einem Amazon Machine Image (AMI) erstellt werden, um die RTO-Anforderungen (Recovery Time Objective) zu erfüllen. Dieses Muster verwendet ein AMI.

Db2 HADR implementiert ein Produktions-Standby-Setup, bei dem die Produktion als primärer Server fungiert und alle Benutzer mit ihm verbunden sind. Alle Transaktionen werden in Protokolldateien geschrieben, die mithilfe von TCP/IP auf den Standby-Server übertragen werden. Der Standby-Server aktualisiert seine lokale Datenbank, indem er die übertragenen Protokolldatensätze weiterleitet. Dadurch wird sichergestellt, dass die Datenbank mit dem Produktionsserver synchron bleibt.

VPC-Peering wird verwendet, damit Instances in der Produktionsregion und der DR-Region miteinander kommunizieren können. Amazon Route 53 leitet Endbenutzer zu Internetanwendungen weiter.

1. Erstellen Sie ein AMI des Anwendungsservers in Region 1 und kopieren Sie das AMI in Region 2. Verwenden Sie das AMI, um im Notfall Server in Region 2 zu starten.
2. Richten Sie die Db2-HADR-Replikation zwischen der Produktionsdatenbank (in Region 1) und der Standby-Datenbank (in Region 2) ein.
3. Ändern Sie im EC2 Notfall den Instanztyp so, dass er der Produktionsinstanz entspricht.

4. In Region 1 `LOGARCHMETH1` ist auf eingestelltdb2remote: S3 path.
5. In Region 2 `LOGARCHMETH1` ist auf gesetztdb2remote: S3 path.
6. Die regionsübergreifende Replikation wird zwischen den S3-Buckets durchgeführt.

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS. Dieses Muster verwendet VPC-Peering.

Bewährte Methoden

- Das Netzwerk spielt eine Schlüsselrolle bei der Entscheidung über den HADR-Replikationsmodus. Für DR in allen AWS-Regionen empfehlen wir, den Modus Db2 HADR ASYNC oder SUPERASYNC zu verwenden.
- Weitere Informationen zu den Replikationsmodi für Db2 HADR finden Sie in der IBM-Dokumentation.
- Sie können die AWS-Managementkonsole oder die AWS-Befehlszeilenschnittstelle (AWS CLI) verwenden, um ein neues AMI Ihres vorhandenen SAP-Systems zu erstellen. Anschließend können Sie das AMI verwenden, um Ihr vorhandenes SAP-System wiederherzustellen oder einen Clone zu erstellen.
- AWS Systems Manager Automation kann Sie bei den allgemeinen Wartungs- und Bereitstellungsaufgaben von EC2 Instances und anderen AWS-Ressourcen unterstützen.
- AWS bietet mehrere native Services zur Überwachung und Verwaltung Ihrer Infrastruktur und Anwendungen auf AWS. Dienste wie Amazon CloudWatch und AWS CloudTrail können verwendet

werden, um Ihre zugrunde liegende Infrastruktur bzw. API-Operationen zu überwachen. Weitere Informationen finden Sie unter SAP on AWS — IBM Db2 HADR with Pacemaker.

Epen

Bereite die Umgebung vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie das System und die Protokolle.	1. Vergewissern Sie sich, dass das Produktionssystem SAP auf Db2 eingerichtet ist. 2. Vergewissern Sie sich, dass die Protokollsicherung aktiviert und so konfiguriert ist, dass die Protokolle im S3-Bucket gespeichert werden. Dies kann mit dem Db2-Parameter `LOGARCHMETH1` überprüft werden. 3. Erstellen Sie ein AMI des zusätzlichen Anwendungsservers.	AWS-Administrator, SAP-Basisadministrator

Richten Sie die Server und die Replikation ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die SAP- und Datenbankserver.	1. Verwenden Sie ein CloudFormation AWS-Skript oder ein AMI der Produktionsinstanz, um die Infrastruktur für die DR-Region bereitzustellen. Im	SAP-Basisadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Rahmen des Pilotprojekts können Sie eine kleinere EC2 Instance in derselben Familie wie die Produktio nsinstanz verwenden. Wenn Ihr Produktions-Instance-Typ beispiels weise ist `r6i.12xla rge` , können Sie den `r6i.xlarge` Instance-Typ für den DR-Build verwenden. Stellen Sie jedoch sicher, dass Sie der DR-Instance dieselbe Speicherkapazität zuweisen, um das Backup der Produktionsdatenbank wiederherzustellen. 2. Erstellen Sie Bereitste llungspunkte für `/sapmnt/ <SID>/` das Amazon Elastic File System (Amazon EFS) und stellen Sie sicher, dass die Replikation vom Primärsys tem aus konfiguriert ist. 3. Erstellen Sie ein VOLLSTÄNDIGES Datenbank-Backup (online oder offline) vom Produktio nssystem. Sie werden dieses Backup verwenden , um die DR-Datenbank zu erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Verwenden Sie im DR-System die Systemkopiermethode SAP Software Provisioning Manager (SWPM) mit der Option Systemkopie verwenden, um das DR-SAP-System zu erstellen. backup/restore for HA/DR 5. Wenn Sie von SWPM dazu aufgefordert werden, stellen Sie die Datenbank in DR mit dem Backup wieder her, das Sie aus der Produktion erstellt haben. Die DR-Datenbank wird sich im Status „Rollforward ausstehend“ befinden. Der Status „Rollforward ausstehend“ ist standardmäßig festgelegt, nachdem die vollständige Sicherung wiederhergestellt wurde. Der Status „Rollforward ausstehend“ gibt an, dass die Datenbank gerade wiederhergestellt wird und dass möglicherweise einige Änderungen übernommen werden müssen. Weitere Informationen finden Sie in der IBM-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Konfiguration.	1. Um die Protokollarchivierung für HADR einzurichten, müssen sowohl die Produktions- als auch die DR-Datenbank in der Lage sein, Protokolle automatisch von allen Protokollarchivspeicherorten abzurufen. Stellen Sie sicher, dass der `LOGARCHMETH1` Parameter in der DR-Datenbank auf denselben Speicherort wie in der Produktionsdatenbank gesetzt ist. Wenn auf denselben Standort aufgrund regionaler Beschränkungen nicht zugegriffen werden kann, stellen Sie sicher, dass das DR-System automatisch Protokolle vom Primärsystem abrufen kann. 2. Um TCP/IP-Ports für die Aktivierung der Datenbankreplikation zu aktivieren, ändern Sie `/etc/services` die Produktions- und DR-Hosts, indem Sie die folgenden beiden Einträge hinzufügen. `<SID>`Bezieht sich im Code auf die System-ID (SID) der Db2-Datenbank (z. B.). `PR1`	AWS-Administrator, SAP-Basisadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<SID>_HADR_1 55001/tcp # DB2 HADR Port1 <SID>_HADR_2 55002/tcp # DB2 HADR Port2 Vergewissern Sie sich, dass beide Ports eingehenden und ausgehenden Verkehr zwischen dem Primär- und dem Standby-Port zulassen. 3. Überprüfen Sie `/etc/hosts` die Produktions- und DR-Hosts, um sicherzustellen, dass die Hostnamen sowohl für die Produktions- als auch für die Standby-Hosts auf die richtigen IP-Adressen verweisen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie die Replikation von der Produktions-Datenbank zur DR-DB ein (im ASYNC-Modus).	1. Führen Sie in der Produktionsdatenbank die folgenden Befehle aus, um die Parameter zu aktualisieren.
	`db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_HOST HOST1`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_SVC <SID>_HADR_1`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_HOST HOST2`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_SVC <SID>_HADR_2`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_INST db2<sid>`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_TIMEOUT 120`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_SYNCMODE ASYNC`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_SPOOL_LIMIT 1000`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_PEER_WINDOW 240`
	`db2 UPDATE DB CFG FOR <SID> USING indexrec RESTART logindexbuild ON`
	2. Führen Sie in der DR-Datenbank die folgenden
		SAP-Basisadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Befehle aus, um die Parameter zu aktualisieren.
	
	`db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_HOST HOST2`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_SVC <SID>_HADR_2`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_HOST HOST1`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_SVC <SID>_HADR_1`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_INST db2<sid>`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_TIMEOUT 120`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_SYNCMODE ASYNC`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_SPOOL_LIMIT 1000`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_PEER_WINDOW 240`
	`db2 UPDATE DB CFG FOR <SID> USING indexrec RESTART logindexbuild ON`
	
	Diese Parameter sind erforderlich, um HADR-bezogene Informationen für beide Datenbanken bereitzustellen. In der Db2-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Datenbank wird HADR auf der Grundlage der Werte für jeden der zuvor festgeleg ten Parameter aktiviert. Weitere Informationen zu diesen Parametern finden Sie in der IBM-Dokum entation.
	3. Starten Sie HADR zunächst in der neu erstellten Standby-Datenbank, indem Sie den folgenden Befehl verwenden.
	`db2 deactivate db <SID>`
	`db2 start hadr on db <SID> as standby`
	4. Starten Sie HADR in der Produktionsdatenbank mit dem folgenden Befehl.
	`db2 deactivate db <SID>`
	`db2 start hadr on db <SID> as primary`
	5. Überprüfen Sie, ob die Produktions- und Standby-Db2-Datenbanken synchron sind und ob der Protokoll versand läuft.
	Verwenden Sie den folgenden db2pd Befehl, um den HADR-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Replikationsstatus zu überwachen. `db2pd -d <SID> -hadr` Weitere Informationen zur Überwachung von HADR finden Sie in der IBM-Dokumentation.	

Testen Sie DR-Failover-Aufgaben

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Planen Sie die Ausfallzeiten des Produktionsbetriebs für den DR-Test ein.	Stellen Sie sicher, dass Sie die erforderlichen Betriebsausfälle in der Produktionsumgebung einplanen, um das DR-Failover-Szenario zu testen.	SAP-Basisadministrator
Erstellen Sie einen Testbenutzer.	Erstellen Sie einen Testbenutzer (oder beliebige Teständerungen), der auf dem DR-Host validiert werden kann, um die Protokollreplikation nach einem DR-Failover zu bestätigen.	SAP-Basisadministrator
Stoppen Sie auf der Konsole die EC2 Produktionsinstanzen.	In diesem Schritt wird ein unsachgemäßes Herunterfahren eingeleitet, um ein Katastrophenszenario nachzuahmen.	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Skalieren Sie die EC2 DR-Instance entsprechend den Anforderungen.	Ändern Sie auf der EC2 Konsole den Instance-Typ in der DR-Region. 1. Stoppen Sie die Instance: Wenn die Instance läuft, müssen Sie sie beenden, bevor Sie ihren Instance-Typ ändern können. Wählen Sie auf der EC2 Konsole die Instance aus und klicken Sie auf Stopp. 2. Ändern Sie den Instanztyp: Wählen Sie auf der EC2 Konsole die Instance aus und klicken Sie dann auf Actions, Instance Settings, Change Instance Type. Wählen Sie den Instanztyp aus, der der primären Instance entspricht, und klicken Sie auf Anwenden. 3. Starten Sie die Instance: Nachdem die Änderung des Instance-Typs abgeschlossen ist, starten Sie die Instance von der EC2 Konsole aus, indem Sie die Instanz auswählen und Start wählen. 4. Verwenden Sie den folgenden Befehl, um die Db2-Datenbank zu starten.	SAP-Basis-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`db2start` `db2 start HADR on db <SID> as standby`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Übernahme einleiten.	Initiieren Sie vom DR-System (`host2`) aus den Übernahme prozess und rufen Sie die DR-Datenbank als primäre Datenbank auf.
	`db2 takeover hadr on database <SID> by force`
	Optional können Sie die folgenden Parameter festlegen, um die Speicherzuweisung der Datenbank automatisch an den Instance-Typ anzupassen. Der `INSTANCE_MEMORY` Wert kann auf der Grundlage des dedizierten Speicherbereichs festgelegt werden, der der Db2-Datenbank zugewiesen werden soll.
	`db2 update db cfg for <SID> using INSTANCE_MEMORY <FIXED VALUE> IMMEDIATE;`
	`db2 get db cfg for <SID> | grep -i DATABASE_MEMORY AUTOMATIC IMMEDIATE;`
	`db2 update db cfg for <SID> using self_tuning_mem ON IMMEDIATE;`
	Überprüfen Sie die Änderung mithilfe der folgenden Befehle.
		SAP-Basisadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`db2 get db cfg for <SID> | grep -i MEMORY` `db2 get db cfg for <SID> | grep -i self_tuning_mem`	
Starten Sie den Anwendungsserver für SAP in der DR-Region.	Starten Sie mithilfe des AMI, das Sie aus dem Produktionssystem erstellt haben, einen neuen zusätzlichen Anwendungsserver in der DR-Region.	SAP-Basisadministrator
Führen Sie eine Validierung durch, bevor Sie die SAP-Anwendung starten.	1. Validieren Sie die `/etc/fstab` Einträge `/etc/hosts` und. 2. `/sapmnt/<SID>/` Auf dem DR-System montieren. 3. Stellen Sie sicher, dass das DR-Dateisystem mit der Produktion `/sapmnt/<SID>/` synchronisiert `/sapmnt/<SID>/` ist. 4. Melden Sie sich beim `<sid>adm` Benutzer an`R3trans -d`, führen Sie die Ausführung aus und überprüfen Sie die Ausgabe in der `trans.log` Datei. Die `trans.log` Datei wird an derselben Stelle generiert, an der Sie den `R3trans -d` Befehl ausgeführt haben.	AWS-Administrator, SAP-Basisadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Starten Sie die SAP-Anwendung auf dem DR-System.	Starten Sie die SAP-Anwendung auf dem DR-System mithilfe von `<sid>adm` user. Verwenden Sie den folgenden Code, der die XX Instanznummer Ihres SAP ABAP SAP Central Services (ASCS) - Servers und die Instanznummer Ihres SAP-Anwendungsservers YY darstellt.
	`sapconrol -nr XX -function StartService <SID>`
	`sapconrol -nr XX -function StartSystem`
	`sapconrol -nr YY -function StartService <SID>`
	`sapconrol -nr YY -function StartSystem`
		SAP-Basisadministrator

Führen Sie die SAP-Validierung durch.	Dies wird als DR-Test durchgeführt, um Beweise zu liefern oder um den Erfolg der Datenreplikation in die DR-Region zu überprüfen.	Testingenieur

Führen Sie DR-Failback-Aufgaben aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Produktions-SAP- und Datenbankserver.	Starten Sie auf der Konsole die EC2 Instanzen, die	SAP-Basisadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SAP und die Datenbank im Produktionssystem hosten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Starten Sie die Produktionsdatenbank und richten Sie HADR ein.	Melden Sie sich beim Produktionssystem (`host1`) an und stellen Sie mithilfe des folgenden Befehls sicher, dass sich die Datenbank im Wiederherstellungsmodus befindet.
	`db2start`
	`db2 start HADR on db P3V as standby`
	`db2 connect to <SID>`
	Stellen Sie sicher, dass der HADR-Status lautet`connected` . Der Replikationsstatus sollte sein. `peer`
	`db2pd -d <SID> -hadr`
	Wenn die Datenbank nicht inkonsistent ist und sich nicht im `connected peer` Status N befindet, sind möglicher weise eine Sicherung und Wiederherstellung erforderl ich, um die Datenbank mit der aktuell aktiven Datenbank (`host2`in der DR-Region) zu synchronisieren (aktiviert). `host1` Stellen Sie in diesem Fall das DB-Backup aus der Datenbank in der `host2` DR-Region auf die Datenbank in
		SAP-Basisadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der `host1` Produktionsregion wieder her.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie ein Failback der Datenbank auf die Produktio nsregion durch.	In einem normalen business-as-usual Szenario wird dieser Schritt während einer geplanten Ausfallze it ausgeführt. Anwendung en, die auf dem DR-System ausgeführt werden, werden gestoppt, und für die Datenbank wird ein Failback in die Produktionsregion (Region 1) durchgeführt, um den Betrieb von der Produktionsregion aus wieder aufzunehmen. 1. Melden Sie sich beim SAP-Anwendungsserver in der DR-Region an und beenden Sie die SAP-Anwendung. 2. Trennen Sie die `/sapmnt/<SID>` Installation vom DR-System und stellen Sie sicher, dass die Änderunge n auf das Produktio nssystem rückwirke nd repliziert werden. `/sapmnt/<SID>` 3. Melden Sie sich beim Datenbankserver (`host1`) in der Produktionsregion an, und führen Sie die Übernahme durch.	SAP-Basisadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`db2 takeover hadr on database <SID>`
	4. Überprüfen Sie den HADR-Status: `HADR_ROLE` sollte aktiviert `host1` und `PRIMARY` `StandBy` aktiviert `host2` sein.
	`db2pd -d <SID> -hadr`	

Führen Sie eine Validierung durch, bevor Sie die SAP-Anwendung starten.	1. Validieren Sie die `/etc/fstab` Einträge `/etc/hosts` und. 2. `/sapmnt/<SID>/` Auf dem Produktionssystem montieren. 3. Stellen Sie sicher, dass es mit dem DR-System synchronisiert ist`/sapmnt/<SID>/` . 4. Melden Sie sich beim `<sid>adm` Benutzer an`R3trans -d`, führen Sie die `trans.log` Datei aus und überprüfen Sie die Ausgabe. Die `trans.log` Datei wird an derselben Stelle generiert, an der Sie den `R3trans -d` Befehl ausgeführt haben.	AWS-Administrator, SAP-Basisadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Starten Sie die SAP-Anwendung.	1. Starten Sie die SAP-Anwendung auf dem Produktionssystem mit dem `<sid>adm` Benutzer. Verwenden Sie den folgenden Code, der die XX Instanznummer Ihres SAP ASCS-Servers und die Instanznummer Ihres SAP-Anwendungsservers YY darstellt.
	`sapconrol -nr XX -function StartService <SID>`
	`sapconrol -nr XX -function StartSystem`
	`sapconrol -nr YY -function StartService <SID>`
	`sapconrol -nr YY -function StartSystem`
	2. Um zu überprüfen, ob Anwendungsserver verfügbar sind, melden Sie sich bei SAP an und führen Sie mithilfe von SICK und SM51 Transaktionen Prüfungen durch.
		SAP-Basisadministrator

Fehlerbehebung

Problem	Lösung
Wichtige Protokolldateien und Befehle zur Behebung von Problemen im Zusammenhang mit HADR	• `db2 get db cfg | grep -i hadr` • `db2pd -d sid -hadr` • `Db2diag.log` (Diese Datei befindet sich in der Regel innerhalb des `db2dump` Verzeichnisses, und der `db2dump` Pfad wird durch den Parameter `DIAGPATH` definiert.)
SAP-Hinweis zur Behebung von HADR-Problemen auf Db2 UDB	Weitere Informationen finden Sie im SAP-Hinweis 1154013 - DB6: DB-Probleme in der HADR-Umgebung. (Sie benötigen Anmeldeinformationen für das SAP-Portal, um auf diesen Hinweis zugreifen zu können.)

Zugehörige Ressourcen

- Ansätze zur Notfallwiederherstellung für Db2-Datenbanken auf AWS (Blogbeitrag)
- SAP on AWS — IBM Db2 HADR mit Pacemaker
- Schrittweises Verfahren zum Einrichten der HADR-Replikation zwischen Datenbanken DB2
- Db2 HADR Wiki

Zusätzliche Informationen

Mit diesem Muster können Sie ein Disaster-Recovery-System für ein SAP-System einrichten, das auf der Db2-Datenbank läuft. In einer Notfallsituation sollte das Geschäft in der Lage sein, die von Ihnen definierten Anforderungen an das Recovery Time Objective (RTO) und das Recovery Point Objective (RPO) einzuhalten:

- RTO ist die maximal zulässige Verzögerung zwischen der Betriebsunterbrechung und der Wiederherstellung des Dienstes. Damit wird festgelegt, was als akzeptables Zeitfenster gilt, wenn der Service nicht verfügbar ist.

- RPO ist die maximal zulässige Zeitspanne seit dem letzten Datenwiederherstellungspunkt. Damit wird festgelegt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Serviceunterbrechung gilt.

FAQs Weitere Informationen zu HADR finden Sie im SAP-Hinweis #1612105 - DB6: Häufig gestellte Fragen zu Db2 High Availability Disaster Recovery (HADR). (Sie benötigen Zugangsdaten für das SAP-Portal, um auf diesen Hinweis zugreifen zu können.)

Richten Sie mithilfe von Terraform eine CI/CD-Pipeline für die Datenbankmigration ein

Erstellt von Dr. Rahul Sharad Gaikwad (AWS), Aarti Rajput (AWS), Ashish Bhatt (AWS), Aniket Dekate (AWS), Naveen Suthar (AWS), Nadeem Rahaman (AWS), Ruchika Modi (AWS) und Tamilselvan P (AWS)

Übersicht

Bei diesem Muster geht es darum, eine CI/CD-Pipeline (Continuous Integration and Continuous Deployment) einzurichten, um Datenbankmigrationen zuverlässig und automatisiert zu verwalten. Es behandelt den Prozess der Bereitstellung der erforderlichen Infrastruktur, der Migration von Daten und der Anpassung von Schemaänderungen mithilfe von Terraform, einem Infrastructure-as-Code-Tool (IaC).

Insbesondere richtet das Muster eine CI/CD-Pipeline ein, um eine lokale Microsoft SQL Server-Datenbank auf Amazon Relational Database Service (Amazon RDS) zu migrieren. AWS Sie können dieses Muster auch verwenden, um eine SQL Server-Datenbank, die sich auf einer virtuellen Maschine (VM) oder in einer anderen Cloud-Umgebung befindet, zu Amazon RDS zu migrieren.

Dieses Muster befasst sich mit den folgenden Herausforderungen im Zusammenhang mit der Datenbankverwaltung und -bereitstellung:

- Manuelle Datenbankbereitstellungen sind zeitaufwändig, fehleranfällig und nicht einheitlich in allen Umgebungen.
- Die Koordination von Infrastrukturbereitstellung, Datenmigrationen und Schemaänderungen kann komplex und schwierig zu verwalten sein.
- Die Sicherstellung der Datenintegrität und die Minimierung von Ausfallzeiten bei Datenbankaktualisierungen sind für Produktionssysteme von entscheidender Bedeutung.

Dieses Muster bietet die folgenden Vorteile:

- Optimiert den Prozess der Aktualisierung und Bereitstellung von Datenbankänderungen durch die Implementierung einer CI/CD-Pipeline für Datenbankmigrationen. Dadurch wird das Fehlerrisiko reduziert, die Konsistenz in allen Umgebungen gewährleistet und Ausfallzeiten minimiert.
- Trägt zur Verbesserung der Zuverlässigkeit, Effizienz und Zusammenarbeit bei. Ermöglicht eine schnellere Markteinführung und geringere Ausfallzeiten bei Datenbankaktualisierungen.

- Unterstützt Sie bei der Einführung moderner DevOps Methoden für das Datenbankmanagement, was zu mehr Agilität, Zuverlässigkeit und Effizienz Ihrer Softwarebereitstellungsprozesse führt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Terraform 0.12 oder höher ist auf Ihrem lokalen Computer installiert (Anweisungen finden Sie in der Terraform-Dokumentation)
- Terraform AWS Provider Version 3.0.0 oder höher von HashiCorp (siehe das Repository für diesen Anbieter) GitHub
- IAM-Richtlinie AWS Identity and Access Management (Least Privilege) (siehe den Blogbeitrag Techniken zum Schreiben von IAM-Richtlinien mit den geringsten Rechten)

Architektur

Dieses Muster implementiert die folgende Architektur, die die komplette Infrastruktur für den Datenbankmigrationsprozess bereitstellt.

In dieser Architektur:

- Die Quelldatenbank ist eine SQL Server-Datenbank, die sich vor Ort, auf einer virtuellen Maschine (VM) befindet oder von einem anderen Cloud-Anbieter gehostet wird. Das Diagramm geht davon aus, dass sich die Quelldatenbank in einem lokalen Rechenzentrum befindet.
- Das lokale Rechenzentrum und ich AWS sind über ein VPN oder AWS Direct Connect eine Verbindung verbunden. Dies ermöglicht eine sichere Kommunikation zwischen der Quelldatenbank und der AWS Infrastruktur.
- Die Zieldatenbank ist eine Amazon RDS-Datenbank, die mithilfe einer Datenbankbereitstellungspipeline in der Virtual Private Cloud (VPC AWS) gehostet wird.
- AWS Database Migration Service (AWS DMS) repliziert Ihre lokale Datenbank auf. AWS Es wird verwendet, um die Replikation der Quelldatenbank in die Zieldatenbank zu konfigurieren.

Das folgende Diagramm zeigt die Infrastruktur, die mit verschiedenen Ebenen des Datenbankmigrationsprozesses eingerichtet wurde, der die Bereitstellung, AWS DMS Einrichtung und Validierung umfasst.

In diesem Prozess:

- Die Validierungspipeline validiert alle Prüfungen. Die integrierte Pipeline geht zum nächsten Schritt über, wenn alle erforderlichen Validierungen abgeschlossen sind.
- Die DB-Bereitstellungspipeline besteht aus verschiedenen AWS CodeBuild Phasen, in denen Terraform-Aktionen für den bereitgestellten Terraform-Code für die Datenbank ausgeführt werden. Wenn diese Schritte abgeschlossen sind, werden Ressourcen im Ziel bereitgestellt. AWS-Konto
- Die AWS DMS Pipeline besteht aus verschiedenen CodeBuild Phasen, in denen Tests durchgeführt und anschließend die AWS DMS Infrastruktur für die Durchführung der Migration mithilfe von IaC bereitgestellt wird.

Tools

AWS-Services und Tools

- AWS CodeBuildist ein vollständig verwalteter Dienst für kontinuierliche Integration, der Quellcode kompiliert, Tests durchführt und ready-to-deploy Softwarepakete produziert.
- AWS CodePipelineist ein vollständig verwalteter Continuous Delivery-Service, der Sie bei der Automatisierung Ihrer Release-Pipelines für schnelle und zuverlässige Anwendungs- und Infrastrukturupdates unterstützt.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der. AWS Cloud
- Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice, der Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet.
- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen von Cloud- und lokalen Konfigurationen.

Andere Dienste

- Terraform ist ein IaC-Tool von HashiCorp , mit dem Sie Cloud- und lokale Ressourcen erstellen und verwalten können.

Code-Repository

Der Code für dieses Muster ist im GitHub Database Migration DevOps Framework unter Verwendung des Terraform-Beispiel-Repositorys verfügbar.

Bewährte Methoden

- Implementieren Sie automatisierte Tests für Ihre Datenbankmigration, um die Richtigkeit von Schemaänderungen und die Datenintegrität zu überprüfen. Dazu gehören Komponententests, Integrationstests und end-to-end Tests.
- Implementieren Sie eine robuste Sicherungs- und Wiederherstellungsstrategie für Ihre Datenbanken, insbesondere vor der Migration. Dies gewährleistet die Datenintegrität und bietet eine Ausweichoption im Falle von Ausfällen.
- Implementieren Sie eine robuste Rollback-Strategie, um Datenbankänderungen rückgängig zu machen, falls während der Migration Fehler oder Probleme auftreten. Dies könnte ein Rollback zu einem früheren Datenbankstatus oder das Zurücksetzen einzelner Migrationsskripten beinhalten.
- Richten Sie Überwachungs- und Protokollierungsmechanismen ein, um den Fortschritt und den Status von Datenbankmigrationen zu verfolgen. Auf diese Weise können Sie Probleme schnell identifizieren und lösen.

Epen

Richten Sie Ihre lokale Workstation ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richte Git auf deiner lokalen Workstation ein und konfiguri ere es.	Installieren und konfiguri eren Sie Git auf Ihrer lokalen Workstation, indem Sie den Anweisungen in der Git-Dokumentation folgen.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie einen Projektordner und fügen Sie die Dateien aus dem GitHub Repository hinzu.	1. Öffnen Sie das GitHub Repository für dieses Muster.
	2. Wählen Sie Code, um die Klonoptionen zu sehen, und kopieren Sie die auf der Registerkarte HTTPS angegebene URL.
	3. Erstellen Sie einen Ordner für Ihr Projekt auf Ihrer Workstation.
	4. Öffnen Sie ein Terminal und navigieren Sie zu diesem Ordner.
	5. Klonen Sie das GitHub Repository:
	`git clone <github-repository-url>`
	wo `<github-repository-url>` ist die URL, die Sie in Schritt 2 kopiert haben.
	6. Wenn das Klonen abgeschlossen ist, wechseln Sie zum geklonten Repository in Ihrem Projektordner:
	`cd <folder-name>/aws-terraform-db-migration-framework-samples`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Öffnen Sie dieses Projekt in einer integrierten Entwicklungsumgebung (IDE) Ihrer Wahl.	

Stellen Sie die Zielarchitektur bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die erforderlichen Parameter.	In der `ssm-parameters.sh` Datei werden alle erforderlichen AWS Systems Manager Parameter gespeichert. Sie können diese Parameter mit den benutzerdefinierten Werten für Ihr Projekt konfigurieren. Öffnen Sie die `ssm-parameters.sh` Datei in dem `setup/db-ssm-params` Ordner auf Ihrer lokalen Workstation und legen Sie diese Parameter fest, bevor Sie die CI/CD-Pipeline ausführen.	DevOps Ingenieur
Initialisieren Sie die Terraform-Konfiguration.	Geben Sie im `db-cicd-integration` Ordner den folgenden Befehl ein, um Ihr Arbeitsverzeichnis zu initialisieren, das die Terraform-Konfigurationsdateien enthält:	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`terraform init`	
Sehen Sie sich eine Vorschau des Terraform-Plans an.	Geben Sie den folgenden Befehl ein, um einen Terraform-Plan zu erstellen: `terraform plan -var-file ="terraform.sample"` Terraform wertet die Konfigura tionsdateien aus, um den Zielstatus für die deklarier ten Ressourcen zu ermitteln . Anschließend wird der Zielstatus mit dem aktuellen Status verglichen und ein Plan erstellt.	DevOps Ingenieur
Überprüfen Sie den Plan.	Überprüfen Sie den Plan und stellen Sie sicher, dass er die erforderliche Architekt ur in Ihrem Ziel AWS-Konto konfiguriert.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Lösung bereit.	1. Geben Sie den folgenden Befehl ein, um den Plan anzuwenden: `terraform apply -var-file="terraform.sample"` 2. Geben Sie `yes` zur Bestätigung ein. Terraform erstellt, aktualisiert oder zerstört die Infrastruktur, um den in den Konfigurationsdateien angegebenen Zielstatus zu erreichen. Weitere Informationen zur Sequenz finden Sie im Abschnitt Architektur dieses Musters.	DevOps Ingenieur

Überprüfen der Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Bereitstellung.	Überprüfen Sie den Status der `db-cicd-integration` Pipeline, um sicherzustellen, dass die Datenbankmigration abgeschlossen ist. 1. Melden Sie sich bei der an AWS Management Console, und öffnen Sie dann die AWS CodePipeline Konsole.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie im Navigation sbereich Pipelines aus. 3. Wählen Sie die `db-cicd-integration` Pipeline aus. 4. Stellen Sie sicher, dass die Pipeline-Ausführung erfolgreich abgeschlossen wurde.	

Reinigen Sie die Infrastruktur nach dem Gebrauch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Säubere die Infrastruktur.	1. Nachdem Ihr Projekt abgeschlossen ist, bereinigen Sie die von Ihnen erstellte Infrastruktur mit dem folgenden Befehl: `terraform destroy --var-file=terraform.sample` 2. Geben Sie `yes` zur Bestätigung ein.	DevOps Ingenieur

Zugehörige Ressourcen

AWS Dokumentation

- Erste Schritte mit einem Terraform-Produkt

Terraform-Dokumentation

- Terraform-Installation

- Terraform-Backend-Konfiguration
- Terraform Provider-Dokumentation AWS

Richten Sie eine HA/DR-Architektur für Oracle E-Business Suite auf Amazon RDS Custom mit einer aktiven Standby-Datenbank ein

Erstellt von Simon Cunningham (AWS) und Nitin Saxena

Übersicht

Dieses Muster beschreibt, wie Sie Ihre Oracle E-Business-Lösung auf Amazon Relational Database Service (Amazon RDS) Custom für Hochverfügbarkeit (HA) und Disaster Recovery (DR) aufbauen können, indem Sie eine Amazon RDS Custom Read Replica-Datenbank in einer anderen Amazon Web Services (AWS) Availability Zone einrichten und sie in eine aktive Standby-Datenbank konvertieren. Die Erstellung der Amazon RDS Custom Read Replica erfolgt vollständig automatisiert über die AWS-Managementkonsole.

In diesem Muster werden die Schritte zum Hinzufügen zusätzlicher Anwendungsebenen und gemeinsam genutzter Dateisysteme, die auch Teil einer HA/DR-Architektur sein können, nicht behandelt. Weitere Informationen zu diesen Themen finden Sie in den folgenden Oracle Support Notes: 1375769.1, 1375670.1 und 1383621.1 (Abschnitt 5, Erweiterte Cloning-Optionen). (Für den Zugriff ist ein Oracle Support-Konto erforderlich.)

Informationen zur Migration des E-Business Suite-Systems zu einer einstufigen Single-AZ-Architektur auf Amazon Web Services (AWS) finden Sie im Muster Oracle E-Business Suite to Amazon RDS Custom migrieren.

Die Oracle E-Business Suite ist eine ERP-Lösung (Enterprise Resource Planning) zur Automatisierung unternehmensweiter Prozesse wie Finanzen, Personalwesen, Lieferketten und Fertigung. Sie hat eine dreistufige Architektur: Client, Anwendung und Datenbank. Bisher mussten Sie Ihre E-Business Suite-Datenbank auf einer selbst verwalteten Amazon Elastic Compute Cloud (Amazon EC2) -Instance ausführen, aber jetzt können Sie von Amazon RDS Custom profitieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine bestehende E-Business Suite-Installation auf Amazon RDS Custom; siehe Muster Oracle E-Business Suite zu Amazon RDS Custom migrieren
- Wenn Sie die Read Replica auf schreibgeschützt umstellen und damit Reporting in den Standby-Modus verlagern möchten, benötigen Sie eine Oracle Active Data Guard-Datenbanklizenz (siehe Preisliste für Oracle Technology Commercial)

Einschränkungen

- Einschränkungen und nicht unterstützte Konfigurationen für Oracle-Datenbanken auf Amazon RDS Custom
- Einschränkungen im Zusammenhang mit Amazon RDS Custom for Oracle Read Replicas

Produktversionen

Informationen zu Oracle-Datenbankversionen und Instance-Klassen, die von Amazon RDS Custom unterstützt werden, finden Sie unter Anforderungen und Einschränkungen für Amazon RDS Custom for Oracle.

Architektur

Das folgende Diagramm zeigt eine repräsentative Architektur für E-Business Suite auf AWS, die mehrere Availability Zones und Anwendungsstufen in einer aktiven/passiven Konfiguration umfasst. Die Datenbank verwendet eine Amazon RDS Custom DB-Instance und eine Amazon RDS Custom Read Replica. Die Read Replica verwendet Active Data Guard, um in eine andere Availability Zone zu replizieren. Sie können die Read Replica auch verwenden, um den Lesetraffic auf die Primärdatenbank auszulagern und zu Berichtszwecken.

Weitere Informationen finden Sie unter Arbeiten mit Read Replicas für Amazon RDS Custom for Oracle in der Amazon RDS-Dokumentation.

Die Amazon RDS Custom Read Replica wird standardmäßig so erstellt, wie sie bereitgestellt wird. Wenn Sie jedoch einige Ihrer schreibgeschützten Workloads in die Standby-Datenbank auslagern möchten, um die Belastung Ihrer Primärdatenbank zu reduzieren, können Sie den Modus der bereitgestellten Replikate manuell in schreibgeschützt ändern, indem Sie die Schritte im Abschnitt Epics befolgen. Ein typischer Anwendungsfall hierfür wäre, Ihre Berichte von der Standby-Datenbank aus auszuführen. Für die Umstellung auf schreibgeschützt ist eine aktive Standby-Datenbanklizenz erforderlich.

Wenn Sie eine Read Replica auf AWS erstellen, verwendet das System unter dem Deckmantel den Oracle Data Guard Broker. Diese Konfiguration wird automatisch generiert und im Modus „Maximale Leistung“ wie folgt eingerichtet:

```
DGMGRL> show configuration
```

```
Configuration - rds_dg
  Protection Mode: MaxPerformance
  Members:
  vis_a - Primary database
    vis_b - Physical standby database
Fast-Start Failover: DISABLED
Configuration Status:
SUCCESS   (status updated 58 seconds ago)
```

Tools

AWS-Services

- Amazon RDS Custom for Oracle ist ein verwalteter Datenbankservice für ältere, benutzerdefinierte und verpackte Anwendungen, die Zugriff auf das zugrunde liegende Betriebssystem und die Datenbankumgebung benötigen. Er automatisiert Aufgaben und Operationen der Datenbankverwaltung und ermöglicht es Ihnen als Datenbankadministrator gleichzeitig, auf Ihre Datenbankumgebung und Ihr Betriebssystem zuzugreifen und diese anzupassen.

Andere Tools

- Oracle Data Guard ist ein Tool, mit dem Sie Oracle-Standby-Datenbanken erstellen und verwalten können. Dieses Muster verwendet Oracle Data Guard, um eine aktive Standby-Datenbank auf Amazon RDS Custom einzurichten.

Epen

Erstellen eines Lesereplikats

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Read Replica der Amazon RDS Custom DB-Instance.	Um eine Read Replica zu erstellen, folgen Sie den Anweisungen in der Amazon RDS-Dokumentation und verwenden Sie die Amazon RDS Custom DB-Instance, die Sie erstellt haben (siehe	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Abschnitt Voraussetzungen), als Quelldatenbank. Standardmäßig wird die Amazon RDS Custom Read Replica als physisches Standby erstellt und befindet sich im gemounteten Zustand. Dies dient dazu, die Einhaltung der Oracle Active Data Guard-Lizenz sicherzustellen. Folgen Sie den nächsten Schritten, um die Read Replica in den Nur-Lese-Modus zu konvertieren.	

Ändern Sie die Read Replica in eine schreibgeschützte aktive Standby-Version

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Connect zur Amazon RDS Custom Read Replica her.	Verwenden Sie die folgenden Befehle, um Ihre physische Standby-Datenbank in eine aktive Standby-Datenbank zu konvertieren. **Important** Für diese Befehle ist eine aktive Oracle-Standby-Lizenz erforderlich. Um eine Lizenz zu erhalten, wenden Sie	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	sich an Ihren Oracle-Vertreter.
	
	`$ sudo su - rdsdb`
	`-bash-4.2$ sql`
	`SQL> select process,s`
	`tatus,sequence# from v`
	`$managed_standby;`
	
	`PROCESS STATUS`
	`SEQUENCE#`
	`--------- ------------`
	`----------`
	`ARCH CLOSING`
	`3956`
	`ARCH CONNECTED`
	`0`
	`ARCH CLOSING`
	`3955`
	`ARCH CLOSING`
	`3957`
	`RFS IDLE`
	`0`
	`RFS IDLE`
	`3958`
	`MRP0 APPLYING_LOG`
	`3958`
	`SQL> select name,`
	`database_role,`
	`open_mode from v`
	`$database;`
	
	`NAME DATABASE_`
	`ROLE OPEN_MODE`
	`--------- ---------`
	`------- ---------`
	`----------`
	`VIS PHYSICAL`
	`STANDBY MOUNTED`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SQL> alter database recover managed standby database cancel; Database altered. Open the standby database SQL> alter database open; Database altered. SQL> select name, database_role, open_mode from v $database; NAME DATABASE_ ROLE OPEN_MODE --------- --------- ------- --------- ----------- VIS PHYSICAL STANDBY READ ONLY	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Starten Sie die Medienwie derherstellung mit Log Apply in Echtzeit.	Verwenden Sie die folgenden Befehle, um die Funktion zum Einspielen von Protokollen in Echtzeit zu aktivieren. Diese konvertieren und validieren die Standby-Datenbank (Read Replica) als aktive Standby-Datenbank, sodass Sie eine Verbindung herstellen und schreibgeschützte Abfragen ausführen können.
	`SQL>  alter database recover managed standby database using current logfile disconnect from session;`
	`Database altered`
		DBA

Überprüfen Sie den Datenbankstatus.	Verwenden Sie den folgenden Befehl, um den Status der Datenbank zu überprüfen.
	`SQL> select name, database_role, open_mode from v$database;`
	`NAME DATABASE_ROLE OPEN_MODE`
	`--------- --------- ------- --------- -----------`
	`VIS PHYSICAL STANDBY READ ONLY WITH APPLY`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktivieren Sie den Modus „Redo Apply“.	Verwenden Sie den folgenden Befehl, um den Redo Apply-Modus zu überprüfen.
	
	`SQL> select process,s tatus,sequence# from v $managed_standby;`
	`PROCESS STATUS SEQUENCE#`
	`--------- ------------ ----------`
	`ARCH CLOSING 3956`
	`ARCH CONNECTED 0`
	`ARCH CLOSING 3955`
	`ARCH CLOSING 3957`
	`RFS IDLE 0`
	`RFS IDLE 3958`
	`MRP0 APPLYING_LOG 3958`
	
	`SQL> select open_mode from v$database;`
	`OPEN_MODE`
	`--------------------`
	`READ ONLY WITH APPLY`
		DBA

Zugehörige Ressourcen

- Migrieren Sie die Oracle E-Business Suite zu Amazon RDS Custom (AWS Prescriptive Guidance)
- Arbeiten mit Amazon RDS Custom (Amazon RDS-Dokumentation)
- Arbeiten mit Read Replicas für Amazon RDS Custom for Oracle (Amazon RDS-Dokumentation)

- Amazon RDS Custom for Oracle — Neue Kontrollfunktionen in der Datenbankumgebung (AWS-News-Blog)
- Migration der Oracle E-Business Suite auf AWS (AWS-Whitepaper)
- Architektur der Oracle E-Business Suite auf AWS (AWS-Whitepaper)

Richten Sie die Datenreplikation zwischen Amazon RDS for MySQL und MySQL auf Amazon EC2 mithilfe von GTID ein

Erstellt von Rajesh Madiwale (AWS)

Übersicht

Dieses Muster beschreibt, wie die Datenreplikation in der Amazon Web Services (AWS) -Cloud zwischen einer Amazon Relational Database Service (Amazon RDS) für MySQL-DB-Instance und einer MySQL-Datenbank auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance mithilfe der MySQL Native Global Transaction Identifier (GTID) -Replikation eingerichtet wird.

Mit werden Transaktionen identifiziert und nachverfolgt GTIDs, wenn sie auf dem ursprünglichen Server festgeschrieben und von Replikaten übernommen werden. Sie müssen nicht auf Protokolldateien zurückgreifen, wenn Sie während eines Failovers ein neues Replikat starten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine bereitgestellte Amazon Linux-Instance

Einschränkungen

- Für dieses Setup muss ein internes Team die schreibgeschützten Abfragen ausführen.
- Die Quell- und Zielversion von MySQL müssen identisch sein.
- Die Replikation wird in derselben AWS-Region und in derselben Virtual Private Cloud (VPC) eingerichtet.

Produktversionen

- Amazon RDS-Versionen 5.7.23 und höher, welche Versionen unterstützen GTID

Architektur

Quelltechnologie-Stack

- Amazon RDS für MySQL

Zieltechnologie-Stack

- MySQL auf Amazon EC2

Zielarchitektur

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Relational Database Service (Amazon RDS) for MySQL unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen MySQL-Datenbank in der AWS-Cloud.

Andere Dienste

- Globale Transaktions-Identifikatoren (GTIDs) sind eindeutige Identifikatoren, die für festgeschriebene MySQL-Transaktionen generiert werden.
- mysqldump ist ein Client-Hilfsprogramm zur Durchführung logischer Backups durch die Erstellung von SQL-Anweisungen, die ausgeführt werden können, um die Objektdefinitionen und Tabellendaten der Quelldatenbank zu reproduzieren.
- mysql ist der Befehlszeilenclient für MySQL.

Epen

Erstellen und Vorbereiten der Amazon RDS for MySQL MySQL-DB-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die RDS for MySQL-Instanz.	Um die RDS for MySQL-Ins tance zu erstellen, folgen Sie	DBA, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den Schritten in der Amazon RDS-Dokumentation und verwenden Sie dabei die Parameterwerte, die in der nächsten Aufgabe behandelt werden.	
Aktivieren Sie GTID-bezogene Einstellungen in der DB-Parametergruppe.	Aktivieren Sie die folgenden Parameter in der Parametergruppe Amazon RDS for MySQL DB. Auf `enforce_gtid_consistency` einstellen `on` und `gtid-mode` auf einstellen`on`.	DBA
Starten Sie die Amazon RDS for MySQL MySQL-Instance neu.	Ein Neustart ist erforderlich, damit die Parameteränderungen wirksam werden.	DBA

Erstellen Sie einen Benutzer und gewähren Sie ihm Replikationsberechtigungen.	Verwenden Sie die folgenden Befehle, um MySQL zu installieren.
	
	`CREATE USER 'repl'@'%' IDENTIFIED BY 'xxxx';`
	`GRANT REPLICATION SLAVE ON *.* TO 'repl'@'%' ;`
	`FLUSH PRIVILEGES;`
		DBA

Installieren und bereiten Sie MySQL auf der EC2 Amazon-Instance vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie MySQL auf Amazon Linux.	Verwenden Sie die folgenden Befehle, um MySQL zu installieren.
	`sudo yum update`
	`sudo wget https://dev.mysql.com/get/mysql57-community-release-el7-11.noarch.rpm`
	`sudo yum localinstall mysql57-community-release-el7-11.noarch.rpm`
	`sudo yum install mysql-community-server`
	`sudo systemctl start mysqld`
		DBA

Melden Sie sich auf der EC2 Instanz bei MySQL an und erstellen Sie die Datenbank.	Der Datenbankname sollte mit dem Datenbanknamen in Amazon RDS for MySQL identisch sein. Im folgenden Beispiel lautet der Datenbank name`replication` . `create database replication;`	DBA
Bearbeiten Sie die MySQL-Konfigurationsdatei und starten Sie die Datenbank neu.	Bearbeiten Sie die `my.conf` Datei, die sich in befindet, `/etc/` indem Sie die folgenden Parameter hinzufügen. `server-id=3`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`gtid_mode=ON enforce_gtid_consistency=ON replicate-ignore-db=mysql binlog-format=ROW log_bin=mysql-bin`
	
	Starten Sie dann den `mysqld` Dienst neu.
	
	`systemctl mysqld restart`	

Replikation einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Exportieren Sie den Datendump aus der Amazon RDS for MySQL MySQL-Datenbank.	Verwenden Sie den folgenden Befehl, um den Dump aus Amazon RDS for MySQL zu exportieren. `mysqldump --single-transaction -h mydb.xxxxxxx.amazonaws.com -uadmin -p --databases replication > replication-db.sql`	DBA
Stellen Sie die .sql-Dump-Datei in der MySQL-Datenbank bei Amazon wieder her. EC2	Verwenden Sie den folgenden Befehl, um den Dump in die MySQL-Datenbank auf Amazon EC2 zu importieren.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`mysql -D replication -uroot -p < replication-db.sql`	

Konfigurieren Sie die MySQL-Datenbank auf Amazon EC2 als Replikat.	Um die Replikation zu starten und den Replikationsstatus zu überprüfen, melden Sie sich bei der MySQL-Datenbank bei Amazon EC2 an und verwenden Sie den folgenden Befehl.
	`CHANGE MASTER TO MASTER_HOST="mydb.xxxxxxx.amazonaws.com", MASTER_USER="repl", MASTER_PASSWORD="rep123", MASTER_PORT=3306, MASTER_AUTO_POSITION = 1;`
	`START SLAVE;`
	`SHOW SLAVE STATUS\G`
		DBA

Zugehörige Ressourcen

- EC2 Amazon-Benutzerhandbuch für Linux-Instances
- Installation von MySQL unter Linux mithilfe des MySQL Yum-Repositorys
- Replikation mit globalen Transaktions-Identifikatoren
- Verwendung der GTID-basierten Replikation für Amazon RDS for MySQL

Rollen für eine PeopleSoft Oracle-Anwendung auf Amazon RDS Custom for Oracle wechseln

Erstellt von sampath kathirvel (AWS)

Übersicht

Um die Oracle PeopleSoft Enterprise Resource Planning (ERP) -Lösung auf Amazon Web Services (AWS) auszuführen, können Sie Amazon Relational Database Service (Amazon RDS) oder Amazon RDS Custom for Oracle verwenden, das ältere, benutzerdefinierte und verpackte Anwendungen unterstützt, die Zugriff auf das zugrunde liegende Betriebssystem (OS) und die Datenbankumgebung benötigen. Wichtige Faktoren, die bei der Planung einer Migration zu berücksichtigen sind, finden Sie unter Strategien zur Oracle-Datenbankmigration in AWS Prescriptive Guidance.

Dieses Muster konzentriert sich auf die Schritte zur Durchführung eines Oracle Data Guard-Switchovers oder Rollenübergangs für eine PeopleSoft Anwendungsdatenbank, die auf Amazon RDS Custom als Primärdatenbank mit einer Read Replica-Datenbank läuft. Das Muster umfasst Schritte zur Konfiguration des Fast-Start-Failovers (FSFO). Während dieses Vorgangs funktionieren die Datenbanken in der Oracle Data Guard-Konfiguration weiterhin in ihren neuen Rollen. Typische Anwendungsfälle für Oracle Data Guard Switchover sind Notfallwiederherstellungsübungen (DR), geplante Wartungsaktivitäten an Datenbanken und fortlaufende Patches zum Einspielen von Standby-First-Patches. Weitere Informationen finden Sie im Blogbeitrag Reduzieren Sie die Ausfallzeiten beim Datenbank-Patching in Amazon RDS Custom.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Abschluss von Add HA to Oracle PeopleSoft on Amazon RDS Custom mithilfe eines Read Replica-Musters.

Einschränkungen

- Einschränkungen und nicht unterstützte Konfigurationen für RDS Custom for Oracle
- Einschränkungen im Zusammenhang mit Amazon RDS Custom for Oracle Read Replicas

Produktversionen

- Informationen zu Oracle-Datenbankversionen, die von Amazon RDS Custom unterstützt werden, finden Sie unter RDS Custom for Oracle.
- Informationen zu Oracle-Datenbankinstanzklassen, die von Amazon RDS Custom unterstützt werden, finden Sie unter DB-Instance-Klassenunterstützung für RDS Custom for Oracle.

Architektur

Technologie-Stack

- Amazon RDS Custom für Oracle

Zielarchitektur

Das folgende Diagramm zeigt eine Amazon RDS Custom DB-Instance und eine Amazon RDS Custom Read Replica. Oracle Data Guard ermöglicht den Rollenwechsel während des Failovers für DR

Eine repräsentative Architektur mit Oracle PeopleSoft auf AWS finden Sie unter Eine hochverfügbare PeopleSoft Architektur auf AWS einrichten.

Tools

AWS-Services

- Amazon RDS Custom for Oracle ist ein verwalteter Datenbankservice für ältere, benutzerdefinierte und verpackte Anwendungen, die Zugriff auf das zugrunde liegende Betriebssystem und die Datenbankumgebung benötigen.
- AWS Secrets Manager hilft Ihnen dabei, hartcodierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Geheimnis programmgesteuert abzurufen. In diesem Muster rufen Sie die Datenbankbenutzerkennwörter aus Secrets Manager für `RDS_DATAGUARD` mit dem geheimen Namen `abdo-not-delete-rds-custom-+<<RDS Resource ID>>+-dg`.

Andere Dienste

- Oracle Data Guard unterstützt Sie bei der Erstellung, Wartung, Verwaltung und Überwachung von Standby-Datenbanken. Dieses Muster verwendet Oracle Data Guard Maximum Performance für den Rollenwechsel (Oracle Data Guard Switchover).

Bewährte Methoden

Für Ihre Produktionsbereitstellung empfehlen wir, die Observer-Instance in einer dritten Availability Zone zu starten, getrennt von den Primär- und Read Replica-Knoten.

Epen

Initiieren Sie den Rollenwechsel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Unterbrechen Sie die Datenbankautomatisierung sowohl für das Primär- als auch für das Replikat.	Obwohl das RDS Custom Automation Framework den Rollenübergangsprozess nicht beeinträchtigt, empfiehlt es sich, die Automatisierung während des Oracle Data Guard-Switchovers zu unterbrechen. Um die benutzerdefinierte RDS-Datenbankautom atisierung anzuhalten und wieder aufzunehmen, folgen Sie den Anweisungen unter Anhalten und Wiederauf nehmen der benutzerdefinierte n RDS-Automatisierung.	Cloud-Administrator, DBA
Überprüfen Sie den Status von Oracle Data Guard.	Um den Status von Oracle Data Guard zu überprüfe n, melden Sie sich bei der Primärdatenbank an. Dieses Muster enthält Code für die	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Verwendung einer Multitenant-Container-Datenbank (CDB) oder einer Nicht-CDB-Instance .
	
	Nicht-CDB
	
	`-bash-4.2$ dgmgrl RDS_DATAGUARD@RDS_CUSTOM_ORCL_A`
	`DGMGRL for Linux: Release 19.0.0.0.0 - Production on Mon Nov 28 20:55:50 2022`
	`Version 19.10.0.0.0`
	`Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved.`
	`Welcome to DGMGRL, type "help" for informati on.`
	`Password:`
	`Connected to "ORCL_A"`
	`Connected as SYSDG.`
	`DGMGRL> show configura tion`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
	`orcl_a - Primary database`
	`orcl_d - Physical standby database`
	`Fast-Start Failover: Disabled`
	`Configuration Status:`
	`SUCCESS (status updated 59 seconds ago)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	DGMGRL> CDB CDB-bash-4.2$ dgmgrl C##RDS_DATAGUARD@R DS_CUSTOM_RDSCDB_A DGMGRL for Linux: Release 19.0.0.0.0 - Production on Wed Jan 18 06:13:07 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Welcome to DGMGRL, type "help" for informati on. Password: Connected to "RDSCDB_A " Connected as SYSDG. DGMGRL> show configura tion Configuration - rds_dg Protection Mode: MaxAvailability Members: rdscdb_a - Primary database rdscdb_b - Physical standby database Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 52 seconds ago) DGMGRL>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Instanzrolle.	Öffnen Sie die AWS-Management konsole und navigieren Sie zur Amazon RDS-Konsole. Überprüfen Sie im Abschnitt Replikation der Datenbank auf der Registerkarte Konnektivität und Sicherheit die Instance-Rolle für die Primärinstanz und das Replikat. Die primäre Rolle sollte mit der primären Oracle Data Guard-Datenbank übereinstimmen, und die Replikatrolle sollte mit der physischen Standby-Datenbank von Oracle Data Guard übereinstimmen.	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Führen Sie den Switchover durch.	Um den Switchover durchzuführen, stellen Sie vom primären Knoten DGMGRL aus eine Verbindung zu her.
	
	Nicht-CDB
	
	`DGMGRL> switchover to orcl_d;`
	`Performing switchover NOW, please wait...`
	`Operation requires a connection to database "orcl_d"`
	`Connecting ...`
	`Connected to "ORCL_D"`
	`Connected as SYSDG.`
	`New primary database "orcl_d" is opening...`
	`Operation requires start up of instance "ORCL" on database "orcl_a"`
	`Starting instance "ORCL"...`
	`Connected to an idle instance.`
	`ORACLE instance started.`
	`Connected to "ORCL_A"`
	`Database mounted.`
	`Database opened.`
	`Connected to "ORCL_A"`
	`Switchover succeeded, new primary is "orcl_d"`
	`DGMGRL>`
	
	CDB
	
	`DGMGRL> switchover to rdscdb_b`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`Performing switchover NOW, please wait...`
	`New primary database "rdscdb_b" is opening...`
	`Operation requires start up of instance "RDSCDB" on database "rdscdb_a"`
	`Starting instance "RDSCDB"...`
	`Connected to an idle instance.`
	`ORACLE instance started.`
	`Connected to "RDSCDB_A"`
	`Database mounted.`
	`Database opened.`
	`Connected to "RDSCDB_A"`
	`Switchover succeeded, new primary is "rdscdb_b"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Oracle Data Guard-Verbindung.	Überprüfen Sie nach dem Switchover die Oracle Data Guard-Verbindung vom primären Knoten zu`DGMGRL`.
	
	Nicht-CDB
	
	`DGMGRL> show configura tion;`
	`Configuration - rds_dg`
	`Protection Mode:`
	`MaxAvailability`
	`Members:`
	`orcl_d - Primary`
	`database`
	`orcl_a - Physical`
	`standby database`
	`Fast-Start Failover:`
	`Disabled`
	`Configuration Status:`
	`SUCCESS (status updated`
	`60 seconds ago)`
	`DGMGRL>`
	
	`DGMGRL> show configura tion lag;`
	`Configuration - rds_dg`
	`Protection Mode:`
	`MaxAvailability`
	`Members:`
	`orcl_d - Primary`
	`database`
	`orcl_a - Physical`
	`standby database`
	`Transport Lag: 0`
	`seconds (computed 0`
	`seconds ago)`
	`Apply Lag: 0 seconds`
	`(computed 0 seconds`
	`ago)`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
Fast-Start Failover:
 Disabled
Configuration Status:
SUCCESS (status updated
 44 seconds ago)
DGMGRL>
```

CDB

```
DGMGRL> show configura
tion
DGMGRL> show configura
tion
Configuration - rds_dg
  Protection Mode:
 MaxAvailability
  Members:
  rdscdb_b - Primary
 database
    rdscdb_a - Physical
 standby database
Fast-Start Failover:
 Disabled
Configuration Status:
SUCCESS   (status
 updated 52 seconds ago)
DGMGRL>

DGMGRL> show configura
tion lag
Configuration - rds_dg
  Protection Mode:
 MaxAvailability
  Members:
  rdscdb_b - Primary
 database
    rdscdb_a - Physical
 standby database
              Transport
 Lag:      0 seconds
```

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 53 seconds ago) DGMGRL>	
Überprüfen Sie die Instance-Rolle auf der Amazon RDS-Konsole.	Nachdem Sie den Rollenwechsel durchgeführt haben, zeigt die Amazon RDS-Konsole die neuen Rollen im Abschnitt Replikation auf der Registerkarte Konnektivität und Sicherheit unter Datenbanken an. Es kann einige Minuten dauern, bis der Replikationsstatus von „leer“ auf „Replizierend“ aktualisiert wird.	DBA

FSFO konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Setzen Sie den Switchover zurück.	Stellen Sie den Switchover wieder auf den Primärknoten zurück.	DBA
Installieren und starten Sie den Observer.	Ein Observer-Prozess ist eine DGMGRL Client-Komponente,	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die normalerweise auf einem anderen Computer als die Primär- und Standby-D atenbank ausgeführt wird. Die ORACLE HOME-Inst allation für den Observer kann eine Oracle Client Administr ator-Installation sein, oder Sie können entweder Oracle Database Enterprise Edition oder Personal Edition installie ren. Weitere Informationen zur Observer-Installation für Ihre Datenbank-Version finden Sie unter Observer installieren und starten. Um Hochverfügbarkeit für den Observer-Prozess zu konfigurieren, sollten Sie wie folgt vorgehen: • Aktivieren Sie die automatis che EC2 Instance-Wiederherstellung für die EC2 Instance, auf der Ihr Observer ausgeführ t wird. Sie müssen den Observer-Startvorgang als Teil des Betriebssystemstar ts automatisieren. • Stellen Sie einen Observer in der EC2 Instance bereit und konfigurieren Sie eine Amazon EC2 Auto Scaling Scaling-Gruppe der Größe eins (1). Im Falle eines EC2	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Instance-Ausfalls startet die automatische Skalierungsgruppe automatisch eine weitere EC2 Instance. Für Oracle 12c Release 2 und höher können Sie bis zu drei Observer einsetzen. Ein Beobachter ist der primäre Beobachter, und die anderen sind Ersatzbeobachter. Wenn der primäre Beobachter ausfällt, übernimmt einer der Ersatzbeobachter die primäre Rolle.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie vom Observer-Host aus eine Connect zu DGMGRL her.	Der Observer-Host ist mit `tnsnames.ora` Einträgen für die Primär- und Standby-Datenbankkonnektivität konfiguriert. Sie können FSFO mit dem Schutzmodus für maximale Leistung aktiviere n, solange der Datenverl ust innerhalb der FastStart FailoverLagLimitKonfigura tion liegt (Wert in Sekunden) . Sie müssen jedoch den Schutzmodus für maximale Verfügbarkeit verwenden, um Datenverlust zu vermeiden (RPO=0).
	
	Nicht-CDB
	
	`DGMGRL> show configura tion;`
	`Configuration - rds_dg`
	`Protection Mode:`
	`MaxAvailability`
	`Members:`
	`orcl_a - Primary`
	`database`
	`orcl_d - Physical`
	`standby database`
	`Fast-Start Failover:`
	`Disabled`
	`Configuration Status:`
	`SUCCESS (status updated`
	`58 seconds ago)`
	`DGMGRL> show configura tion lag`
	`Configuration - rds_dg`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
Protection Mode:
 MaxAvailability
Members:
orcl_a - Primary
 database
orcl_d - Physical
 standby database
Transport Lag: 0
 seconds (computed 1
 second ago)
Apply Lag: 0 seconds
 (computed 1 second ago)
Fast-Start Failover:
 Disabled
Configuration Status:
SUCCESS (status updated
 5 seconds ago)
DGMGRL>
```

CDB

```
-bash-4.2$ dgmgrl
 C##RDS_DATAGUARD@R
DS_CUSTOM_RDSCDB_A
DGMGRL for Linux:
 Release 19.0.0.0.0 -
 Production on Wed Jan
 18 06:55:09 2023
Version 19.16.0.0.0
Copyright (c) 1982,
 2019, Oracle and/or
 its affiliates.  All
 rights reserved.
Welcome to DGMGRL, type
 "help" for informati
on.
Password:
Connected to "RDSCDB_A
"
Connected as SYSDG.
```

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`DGMGRL> show configura tion Configuration - rds_dg Protection Mode: MaxAvailability Members: rdscdb_a - Primary database rdscdb_b - Physical standby database Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 18 seconds ago) DGMGRL>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Ändern Sie die Standby-Datenbank als Failover-Ziel.	Stellen Sie entweder vom Primärknoten oder vom Beobachterknoten eine Connect zu einer Standby-Datenbank her. (Obwohl Ihre Konfiguration mehrere Standby-Datenbanken enthalten könnte, müssen Sie zu diesem Zeitpunkt nur eine Verbindung herstellen.)
	
	Nicht-CDB
	
	`DGMGRL> edit database orcl_a set property FastStartFailoverTarget='orcl_d';`
	`Property "faststartfailovertarget" updated`
	`DGMGRL> edit database orcl_d set property FastStartFailoverTarget='orcl_a';`
	`Property "faststartfailovertarget" updated`
	`DGMGRL> show database orcl_a FastStartFailoverTarget;`
	`FastStartFailoverTarget = 'orcl_d'`
	`DGMGRL> show database orcl_d FastStartFailoverTarget;`
	`FastStartFailoverTarget = 'orcl_a'`
	`DGMGRL>`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	CDB
	
	`DGMGRL> edit database orcl_a set property FastStartFailoverTarget='rdscdb_b';`
	`Object "orcl_a" was not found`
	`DGMGRL> edit database rdscdb_a set property FastStartFailoverTarget='rdscdb_b';`
	`Property "faststartfailovertarget" updated`
	`DGMGRL> edit database rdscdb_b set property FastStartFailoverTarget='rdscdb_a';`
	`Property "faststartfailovertarget" updated`
	`DGMGRL> show database rdscdb_a FastStartFailoverTarget;`
	`FastStartFailoverTarget = 'rdscdb_b'`
	`DGMGRL> show database rdscdb_b FastStartFailoverTarget;`
	`FastStartFailoverTarget = 'rdscdb_a'`
	`DGMGRL>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie FastStart FailoverThreshold die Verbindung zu DGMGRL.	Der Standardwert in Oracle 19c ist 30 Sekunden und der Mindestwert ist 6 Sekunden. Ein niedrigerer Wert kann das Recovery Time Objective (RTO) während des Failovers möglicherweise verkürzen. Ein höherer Wert trägt dazu bei, die Wahrscheinlichkeit unnötiger vorübergehender Failoverfehler in der Primärdat enbank zu verringern. Das RDS Custom for Oracle Automation Framework überwacht den Zustand der Datenbank und führt alle paar Sekunden Korrektur maßnahmen durch. Daher empfehlen wir die Einstellung FastStartFailoverThreshold auf einen Wert von mehr als 10 Sekunden. Im folgenden Beispiel wird der Schwellen wert auf 35 Sekunden konfiguriert. Kein CBD oder CDB `DGMGRL> edit configura tion set property FastStartFailoverT hreshold=35; Property "faststar tfailoverthreshold" updated`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`DGMGRL> show configura tion FastStart FailoverThreshold; FastStartFailover Threshold = '35' DGMGRL>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktivieren Sie FSFO, indem Sie vom Primär- oder Beobachterknoten aus eine Verbindung zu DGMGRL herstellen.	Wenn für die Datenbank Flashback Database nicht aktiviert ist, wird die Warnmeldung angezeigt. `ORA-16827` Die optionale Flashback-Datenbank hilft dabei, ausgefallene Primärdat enbanken automatisch bis zu einem Zeitpunkt vor dem Failover wiederherzustellen, wenn die FastStartFailoverA utoReinstateKonfigura tionseigenschaft auf gesetzt ist `TRUE` (was die Standarde instellung ist).
	
	Nicht-CDB
	
	`DGMGRL> enable fast_star t failover;`
	`Warning: ORA-16827:`
	`Flashback Database is disabled`
	`Enabled in Zero Data Loss Mode.`
	`DGMGRL>`
	`DGMGRL> show configura tion`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
	`orcl_a - Primary database`
	`Warning: ORA-16819: fast-start failover observer not started`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	orcl_d - (*) Physical
	 standby database
	Warning: ORA-16819:
	 fast-start failover
	 observer not started
	Fast-Start Failover:
	 Enabled in Zero Data
	 Loss Mode
	Configuration Status:
	WARNING (status updated
	 29 seconds ago)
	DGMGRL>
	
	CDB
	
	DGMGRL> enable fast_star
	t failover;
	Warning: ORA-16827:
	 Flashback Database is
	 disabled
	Enabled in Zero Data
	 Loss Mode.
	DGMGRL> show configura
	tion;
	Configuration - rds_dg
	  Protection Mode:
	 MaxAvailability
	  Members:
	  rdscdb_a - Primary
	 database
	  Warning: ORA-16819
	: fast-start failover
	 observer not started
	  rdscdb_b - (*)
	 Physical standby
	 database
	Fast-Start Failover:
	 Enabled in Zero Data
	 Loss Mode
	Configuration Status:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`WARNING (status updated 11 seconds ago)` `DGMGRL>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Starten Sie den Observer für die FSFO-Überwachung und überprüfen Sie den Status.	Sie können den Observer vor oder nach der Aktivierung von FSFO starten. Wenn FSFO bereits aktiviert ist, beginnt der Observer sofort mit der Überwachung des Status und der Verbindungen zu den primären und Ziel-Standby-Datenbanken. Wenn FSFO nicht aktiviert ist, beginnt der Observer erst mit der Überwachung, nachdem FSFO aktiviert wurde.
	
	Wenn Sie den Observer starten, wird die primäre DB-Konfiguration ohne Fehlermeldungen angezeigt, wie der vorherige Befehl zeigt. `show configuration`
	
	Nicht-CDB
	
	`DGMGRL> start observer;`
	`[W000 2022-12-01T06:16:51.271+00:00]`
	`FSFO target standby is orcl_d`
	`Observer 'ip-10-0-1-89' started`
	`[W000 2022-12-01T06:16:51.352+00:00]`
	`Observer trace level is set to USER`
	
	`DGMGRL> show configuration`
	`Configuration - rds_dg`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Protection Mode: MaxAvailability Members: orcl_a - Primary database orcl_d - (*) Physical standby database Fast-Start Failover: Enabled in Zero Data Loss Mode Configuration Status: SUCCESS (status updated 56 seconds ago) DGMGRL> DGMGRL> show observer Configuration - rds_dg Primary: orcl_a Active Target: orcl_d Observer "ip-10-0- 1-89" - Master Host Name: ip-10-0-1 -89 Last Ping to Primary: 1 second ago Last Ping to Target: 1 second ago DGMGRL> CDB DGMGRL> start observer; Succeeded in opening the observer file "/home/oracle/fsfo _ip-10-0-1-56.dat". [W000 2023-01-1 8T07:31:32.589+00:00] FSFO target standby is rdscdb_b	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Observer 'ip-10-0-1-56' started The observer log file is '/home/oracle/observer_ip-10-0-1-56.log'. DGMGRL> show configuration Configuration - rds_dg Protection Mode: MaxAvailability Members: rdscdb_a - Primary database rdscdb_b - (*) Physical standby database Fast-Start Failover: Enabled in Zero Data Loss Mode Configuration Status: SUCCESS (status updated 12 seconds ago) DGMGRL> DGMGRL> show observer; Configuration - rds_dg Primary: rdscdb_a Active Target: rdscdb_b Observer "ip-10-0-1-56" - Master Host Name: ip-10-0-1-56 Last Ping to Primary: 1 second ago Last Ping to Target: 2 seconds ago DGMGRL>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Failover.	In diesem Szenario kann ein Failover-Test durchgeführt werden, indem die primäre EC2 Instanz manuell gestoppt wird. Bevor Sie die EC2 Instance beenden, verwenden Sie den `tail` Befehl, um die Observer-Protokolldatei auf der Grundlage Ihrer Konfiguration zu überwache n. Wird verwendet`DGMGRL`, um sich `orcl_d` mit dem Benutzer `RDS_DATAGUARD` bei der Standby-Datenbank anzumelden und den Status von Oracle Data Guard zu überprüfen. Es sollte zeigen, dass es `orcl_d` sich um die neue Primärdatenbank handelt. **Note** In diesem Failover-Testszenario `orcl_d` handelt es sich um die Nicht-CDB-Datenbank. Vor dem Failover wurde die Flashback-Datenbank aktiviert. `orcl_a` Nachdem die frühere Primärdatenbank wieder online ist und ihren `MOUNT` Status aktiviert hat,	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	nimmt der Observer sie wieder in eine neue Standby-D atenbank auf. Die wiederher gestellte Datenbank dient als FSFO-Ziel für die neue Primärdatenbank. Sie können die Details in Observer-Protokollen überprüfen.
	
	`DGMGRL> show configura tion`
	`Configuration - rds_dg`
	`Protection Mode:`
	`MaxAvailability`
	`Members:`
	`orcl_d - Primary`
	`database`
	`Warning: ORA-16824`
	`: multiple warnings,`
	`including fast-star t failover-related`
	`warnings, detected for`
	`the database`
	`orcl_a - (*) Physical`
	`standby database`
	`(disabled)`
	`ORA-16661: the standby`
	`database needs to be`
	`reinstated`
	`Fast-Start Failover:`
	`Enabled in Zero Data`
	`Loss Mode`
	`Configuration Status:`
	`WARNING (status updated`
	`25 seconds ago)`
	`DGMGRL>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Im Folgenden sehen Sie ein Beispiel für die Ausgabe in `observer.log` .
	
	`$ tail -f /tmp/obse rver.log`
	`Unable to connect to database using rds_custom_orcl_a`
	`[W000 2023-01-1 8T07:50:32.589+00:00] Primary database cannot be reached.`
	`[W000 2023-01-1 8T07:50:32.589+00:00] Fast-Start Failover threshold has expired.`
	`[W000 2023-01-1 8T07:50:32.590+00:00] Try to connect to the standby.`
	`[W000 2023-01-1 8T07:50:32.590+00: 00] Making a last connection attempt to primary database before proceeding with Fast-Start Failover.`
	`[W000 2023-01-1 8T07:50:32.591+00:00] Check if the standby is ready for failover.`
	`[S002 2023-01-1 8T07:50:32.591+00:00] Fast-Start Failover started...`
	`2023-01-18T07:50 :32.591+00:00`
	`Initiating Fast-Star t Failover to database "orcl_d"...`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	[S002 2023-01-18T07:50:32.592+00:00] Initiating Fast-start Failover. Performing failover NOW, please wait... Failover succeeded, new primary is "orcl_d" 2023-01-18T07:55:32.101+00:00 [S002 2023-01-18T07:55:32.591+00:00] Fast-Start Failover finished... [W000 2023-01-18T07:55:32.591+00:00] Failover succeeded. Restart pinging. [W000 2023-01-18T07:55:32.603+00:00] Primary database has changed to orcl_d. [W000 2023-01-18T07:55:33.618+00:00] Try to connect to the primary. [W000 2023-01-18T07:55:33.622+00:00] Try to connect to the primary rds_custom_orcl_d. [W000 2023-01-18T07:55:33.634+00:00] The standby orcl_a needs to be reinstated [W000 2023-01-18T07:55:33.654+00:00] Try to connect to the new standby orcl_a. [W000 2023-01-18T07:55:33.654+00:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`00] Connection to the primary restored! [W000 2023-01-18T07:55:35.654+00:00] Disconnecting from database rds_custom_orcl_d. [W000 2023-01-18T07:55:57.701+00:00] Try to connect to the new standby orcl_a. ORA-12170: TNS:Connect timeout occurred`	

Konfigurieren Sie die Konnektivität zwischen der Oracle Peoplesoft-Anwendung und der Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und starten Sie den Dienst in der Primärdatenbank.	Sie können Änderungen der Anwendungskonfiguration während eines Rollenwechsels vermeiden, indem Sie einen TNS-Eintrag verwenden, der sowohl den Primär- als auch den Standby-Datenbank-Endpunkt in der Konfiguration enthält. Sie können zwei rollenbasierte Datenbankdienste definieren, um sowohl Lese-/Schreib-Workloads als auch schreibgeschützte Workloads zu unterstützen. Im folgenden Beispiel `orcl_rw` ist der Lese-/Schreibdienst in der Primärdatenbank aktiv. `orcl_r`oist der schreibge	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	schützte Dienst und ist in der Standby-Datenbank aktiv, die im schreibgeschützten Modus geöffnet wurde. `SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- --------- ----------- ORCL READ WRITE SQL> exec dbms_serv ice.create_service ('orcl_rw','orcl_r w'); PL/SQL procedure successfully completed . SQL> exec dbms_serv ice.create_service ('orcl_ro','orcl_r o'); PL/SQL procedure successfully completed .`  `SQL> exec dbms_serv ice.start_service('orcl_rw'); PL/SQL procedure successfully completed . SQL>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den Dienst in der Standby-Datenbank.	Verwenden Sie den folgenden Code, um den Dienst in der schreibgeschützten Standby-Datenbank zu starten. `SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- ---------- ----------- ORCL READ ONLY WITH APPLY SQL> exec dbms_serv ice.start_service( 'orcl_ro'); PL/SQL procedure successfully completed . SQL>`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Automatisieren Sie den Start des Dienstes, wenn die primäre Datenbank neu gestartet wird.	Verwenden Sie den folgenden Code, um den Dienst beim Neustart automatisch in der Primärdatenbank zu starten. `SQL> CREATE OR REPLACE TRIGGER TrgDgServices after startup on database DECLARE db_role VARCHAR(30); db_open_mode VARCHAR(30); BEGIN SELECT DATABASE_ROLE, OPEN_MODE INTO db_role, db_open_mode FROM V$DATABASE; IF db_role = 'PRIMARY' THEN DBMS_SERV 2 ICE.START_SERVICE('orcl_rw'); END IF; IF db_role = 'PHYSICAL STANDBY' AND db_open_mode LIKE 'READ ONLY%' THEN DBMS_SERVICE.START_SERVICE('orcl_ro'); END IF; END; / Trigger created. SQL>`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie eine Verbindung zwischen den Datenbanken mit Lese-/Schreibzugriff und schreibgeschützten Datenbanken.	Sie können das folgende Anwendungskonfigurationsbeispiel für die Verbindung mit Lese-/Schreibzugriff und Schreibschutz verwenden. `ORCL_RW = (DESCRIPTION = (CONNECT_TIMEOUT= 120)(RETRY_COUNT=20)(RETRY_DELAY=3)(TRANSPORT_CONNECT_TIMEOUT=3) (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST=devpsftdb.******.us-west-2.rds.amazonaws.com) (PORT=1521)) (ADDRESS = (PROTOCOL = TCP)(HOST=psftread.******.us-west-2.rds.amazonaws.com) (PORT=1521))) (CONNECT_DATA=(SERVICE_NAME = orcl_rw))) ORCL_RO = (DESCRIPTION = (CONNECT_TIMEOUT= 120)(RETRY_COUNT=20)(RETRY_DELAY=3)(TRANSPORT_CONNECT_TIMEOUT=3) (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST=devpsftdb.******.us-west-2`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`.rds.amazonaws.com)(PORT=1521))(ADDRESS = (PROTOCOL = TCP)(HOST=psftread.******.us-west-2.rds.amazonaws.com)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME = orcl_ro))`	

Zugehörige Ressourcen

- Aktivierung von Hochverfügbarkeit mit Data Guard auf Amazon RDS Custom for Oracle (AWS-Technischer Leitfaden)
- Konfiguration von Amazon RDS als PeopleSoft Oracle-Datenbank (AWS-Whitepaper)
- Handbuch zu Oracle Data Guard Broker (Oracle-Referenzdokumentation)
- Konzepte und Verwaltung von Data Guard (Oracle-Referenzdokumentation)
- Spezifische FAN- und FCF-Konfigurationsanforderungen für Oracle Data Guard (Oracle-Referenzdokumentation)

Daten aus einem Amazon Redshift Redshift-Cluster kontenübergreifend nach Amazon S3 entladen

Erstellt von Andrew Kamel (AWS)

Übersicht

Wenn Sie Anwendungen testen, ist es hilfreich, Produktionsdaten in Ihrer Testumgebung zu haben. Mithilfe von Produktionsdaten können Sie die Anwendung, die Sie entwickeln, genauer einschätzen.

Dieses Muster extrahiert Daten aus einem Amazon Redshift Redshift-Cluster in einer Produktionsumgebung in einen Amazon Simple Storage Service (Amazon S3) -Bucket in einer Entwicklungsumgebung auf Amazon Web Services (AWS).

Das Muster führt Schritt für Schritt die Einrichtung von DEV- und PROD-Konten durch, einschließlich der folgenden Schritte:

- Erforderliche -Ressourcen
- AWS Identity and Access Management (IAM) -Rollen
- Netzwerkanpassungen an Subnetzen, Sicherheitsgruppen und der Virtual Private Cloud (VPC) zur Unterstützung der Amazon Redshift Redshift-Verbindung
- Eine AWS Lambda Beispielfunktion mit einer Python-Laufzeit zum Testen der Architektur

Um Zugriff auf den Amazon Redshift Redshift-Cluster AWS Secrets Manager zu gewähren, speichert das Muster die entsprechenden Anmeldeinformationen. Der Vorteil besteht darin, dass Sie über alle erforderlichen Informationen verfügen, um eine direkte Verbindung zum Amazon Redshift Redshift-Cluster herzustellen, ohne wissen zu müssen, wo sich der Amazon Redshift Redshift-Cluster befindet. Darüber hinaus können Sie die Verwendung des Geheimnisses überwachen.

Das in Secrets Manager gespeicherte Geheimnis umfasst den Host, den Datenbanknamen, den Port und die entsprechenden Anmeldeinformationen des Amazon Redshift Redshift-Clusters.

Informationen zu Sicherheitsaspekten bei der Verwendung dieses Musters finden Sie im Abschnitt Bewährte Methoden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein Amazon Redshift Redshift-Cluster, der im PROD-Konto ausgeführt wird
- Ein S3-Bucket, der im DEV-Konto erstellt wurde
- VPC-Peering zwischen den DEV- und PROD-Konten mit entsprechend angepassten Routentabellen
- DNS-Hostnamen und DNS-Auflösung sind für beide Peering-Verbindungen aktiviert VPCs

Einschränkungen

- Abhängig von der Datenmenge, die Sie abfragen möchten, kann es bei der Lambda-Funktion zu einem Timeout kommen.

  Wenn Ihre Ausführung länger als das maximale Lambda-Timeout (15 Minuten) dauert, verwenden Sie einen asynchronen Ansatz für Ihren Lambda-Code. Das Codebeispiel für dieses Muster verwendet die psycopg2-Bibliothek für Python, die derzeit keine asynchrone Verarbeitung unterstützt.
- Einige AWS-Services sind nicht in allen verfügbar. AWS-Regionen Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie auf der Seite Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Architektur

Das folgende Diagramm zeigt die Zielarchitektur mit DEV- und PROD-Konten.

Das Diagramm zeigt den folgenden Workflow:

1. Die Lambda-Funktion im DEV-Konto übernimmt die IAM-Rolle, die für den Zugriff auf die Amazon Redshift Redshift-Anmeldeinformationen in Secrets Manager im PROD-Konto erforderlich ist.

   Die Lambda-Funktion ruft dann das Amazon Redshift Redshift-Clustergeheimnis ab.
2. Die Lambda-Funktion im DEV-Konto verwendet die Informationen, um über das Peered-Konto eine Verbindung zum Amazon Redshift Redshift-Cluster im PROD-Konto herzustellen. VPCs

   Die Lambda-Funktion sendet dann einen Entladebefehl, um den Amazon Redshift Redshift-Cluster im PROD-Konto abzufragen.

3. Der Amazon Redshift Redshift-Cluster im PROD-Konto übernimmt die entsprechende IAM-Rolle für den Zugriff auf den S3-Bucket im DEV-Konto.

   Der Amazon Redshift Redshift-Cluster entlädt die abgefragten Daten in den S3-Bucket im DEV-Konto.

Daten von Amazon Redshift abfragen

Das folgende Diagramm zeigt die Rollen, die zum Abrufen der Amazon Redshift Redshift-Anmeldeinformationen und zum Herstellen einer Verbindung mit dem Amazon Redshift Redshift-Cluster verwendet werden. Der Workflow wird durch die Lambda-Funktion initiiert.

Das Diagramm zeigt den folgenden Workflow:

1. Das Konto „`CrossAccount-SM-Read-Role`Im DEV“ setzt das Konto „`SM-Read-Role`Im PROD“ voraus.
2. Die `SM-Read-Role` Rolle verwendet die angehängte Richtlinie, um das Geheimnis aus Secrets Manager abzurufen.
3. Die Anmeldeinformationen werden für den Zugriff auf den Amazon Redshift Redshift-Cluster verwendet.

Daten auf Amazon S3 hochladen

Das folgende Diagramm zeigt den kontoübergreifenden Lese- und Schreibvorgang für das Extrahieren von Daten und deren Upload auf Amazon S3. Der Workflow wird durch die Lambda-Funktion initiiert. Das Muster verkettet IAM-Rollen in Amazon Redshift. Der Befehl unload, der vom Amazon Redshift Redshift-Cluster kommt`CrossAccount-S3-Write-Role`, geht von und dann von der aus. `S3-Write-Role` Durch diese Rollenverkettung erhält Amazon Redshift Zugriff auf Amazon S3.

Der Workflow umfasst die folgenden Schritte:

1. Das Konto „`CrossAccount-SM-Read-Role`Im DEV“ setzt das Konto „`SM-Read-Role`Im PROD“ voraus.
2. Der `SM-Read-Role` ruft die Amazon Redshift Redshift-Anmeldeinformationen von Secrets Manager ab.

3. Die Lambda-Funktion stellt eine Verbindung zum Amazon Redshift Redshift-Cluster her und sendet eine Abfrage.
4. Der Amazon Redshift Redshift-Cluster geht davon aus. `CrossAccount-S3-Write-Role`
5. Das `CrossAccount-S3-Write-Role` geht davon aus, dass das `S3-Write-Role` im DEV-Konto ist.
6. Die Abfrageergebnisse werden in den S3-Bucket im DEV-Konto entladen.

Tools

AWS-Services

- AWS Key Management Service (AWS KMS) hilft Ihnen dabei, kryptografische Schlüssel zu erstellen und zu kontrollieren, um Ihre Daten zu schützen.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Redshift ist ein verwalteter Data-Warehouse-Service im Petabyte-Bereich in der AWS-Cloud.
- Mit AWS Secrets Manager können Sie fest codierte Anmeldeinformationen im Code (einschließlich Passwörter) durch einen API-Aufruf an Secrets Manager ersetzen und das Geheimnis programmgesteuert abrufen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code-Repository

Der Code für dieses Muster ist im GitHub unload-redshift-to-s3-Python-Repository verfügbar.

Bewährte Methoden

Haftungsausschluss zur Sicherheit

Bevor Sie diese Lösung implementieren, sollten Sie die folgenden wichtigen Sicherheitsempfehlungen berücksichtigen:

- Denken Sie daran, dass die Verbindung von Entwicklungs- und Produktionskonten den Umfang erhöhen und die allgemeine Sicherheitslage verringern kann. Wir empfehlen, diese Lösung nur

vorübergehend einzusetzen, den erforderlichen Teil der Daten zu extrahieren und dann die bereitgestellten Ressourcen sofort zu vernichten. Um die Ressourcen zu löschen, sollten Sie die Lambda-Funktion löschen, alle für diese Lösung erstellten IAM-Rollen und -Richtlinien entfernen und jeglichen Netzwerkzugriff widerrufen, der zwischen den Konten gewährt wurde.

- Konsultieren Sie Ihre Sicherheits- und Compliance-Teams, bevor Sie Daten aus der Produktions- in die Entwicklungsumgebung kopieren. Persönlich identifizierbare Informationen (PII), geschützte Gesundheitsinformationen (PHI) und andere vertrauliche oder regulierte Daten sollten generell nicht auf diese Weise kopiert werden. Kopieren Sie nur öffentlich zugängliche, nicht vertrauliche Informationen (z. B. öffentliche Bestandsdaten aus einem Shop-Frontend). Erwägen Sie die Tokenisierung oder Anonymisierung von Daten oder die Generierung synthetischer Testdaten, anstatt nach Möglichkeit Produktionsdaten zu verwenden. Eines der AWS Sicherheitsprinzipien besteht darin, Menschen von Daten fernzuhalten. Mit anderen Worten, Entwickler sollten keine Operationen im Produktionskonto ausführen.
- Beschränken Sie den Zugriff auf die Lambda-Funktion im Entwicklungskonto, da sie Daten aus dem Amazon Redshift Redshift-Cluster in der Produktionsumgebung lesen kann.
- Um eine Unterbrechung der Produktionsumgebung zu vermeiden, sollten Sie die folgenden Empfehlungen umsetzen:
  - Verwenden Sie ein separates, dediziertes Entwicklungskonto für Test- und Entwicklungsaktivitäten.
  - Implementieren Sie strenge Netzwerkzugriffskontrollen und beschränken Sie den Datenverkehr zwischen Konten auf das Notwendige.
  - Überwachen und prüfen Sie den Zugriff auf die Produktionsumgebung und die Datenquellen.
  - Implementieren Sie Zugriffskontrollen mit den geringsten Rechten für alle beteiligten Ressourcen und Dienste.
  - Überprüfen Sie regelmäßig Anmeldeinformationen wie AWS Secrets Manager geheime Daten und IAM-Rollenzugriffsschlüssel und wechseln Sie diese ab.
- Informationen zu den in diesem Artikel verwendeten Diensten finden Sie in der folgenden Sicherheitsdokumentation:
  - AWS Lambda Sicherheit
  - Amazon Redshift Redshift-Sicherheit
  - Amazon S3 S3-Sicherheit
  - AWS Secrets Manager Sicherheit
  - Bewährte IAM-Sicherheitsmethoden

Sicherheit hat beim Zugriff auf Produktionsdaten und Ressourcen oberste Priorität. Halten Sie sich stets an bewährte Verfahren, implementieren Sie Zugriffskontrollen mit geringsten Rechten und überprüfen und aktualisieren Sie Ihre Sicherheitsmaßnahmen regelmäßig.

Epen

Daten von Amazon Redshift abfragen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Geheimnis für den Amazon Redshift Redshift-Cluster.	Gehen Sie wie folgt vor, um das Geheimnis für den Amazon Redshift Redshift-Cluster zu erstellen: 1. Melden Sie sich im PROD-Konto bei der an und öffnen Sie die AWS Management Console Secrets Manager Manager-Konsole unter https://console.aws.amazon.com/secretsmanager/. 2. Wählen Sie Neues Geheimnis speichern. 3. Wählen Sie Anmeldeinformationen für Amazon Redshift Data Warehouse aus. 4. Geben Sie für Benutzername und Passwort Werte für Ihre Instance ein und bestätigen Sie den Wert für den Verschlüsselungsschlüssel, oder wählen Sie einen Wert aus.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Wählen Sie das Amazon Redshift Data Warehouse aus, auf das Ihr Secret zugreifen soll. 6. Geben Sie `Redshift-Creds-Secret` den geheimen Namen ein. 7. Schließen Sie die verbleibenden Erstellungsschritte mit den Standardoptionen ab und wählen Sie dann Speichern aus. 8. Sehen Sie sich Ihr Geheimnis an und notieren Sie sich den ARN ARN-Wert, der zur Identifizierung des Geheimnisses generiert wurde.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Rolle für den Zugriff auf Secrets Manager.	Gehen Sie wie folgt vor, um die Rolle zu erstellen: 1. Öffnen Sie im PROD-Konto die IAM-Konsole unter. https://console.aws.amazon.com/iam/ 2. Wählen Sie Policies (Richtlinien). 3. Wählen Sie Richtlinie erstellen aus. 4. Wählen Sie die Registerkarte JSON und geben Sie dann eine IAM-Richtlinie wie die folgende ein: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "secretsmanager:GetResourcePolicy", "secretsmanager:GetSecretValue", "secretsmanager:DescribeSecret", "secretsmanager:ListSecretVersionIds" ],`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Resource
	": [
	
	"<Redshift-Creds-S
	ecret-ARN>"
	]
	},
	{
	"Effect":
	"Allow",
	"Action":
	"secretsmanager:Li
	stSecrets",
	"Resource
	": "*"
	}
	]
	}</pre>
	`Redshift-Creds-Secret-ARN` Ersetzen Sie es durch den Amazon Resource Name (ARN) des Secrets Manager Manager-Geheimnisses, das die Informationen und Anmeldeinformationen für den Amazon Redshift Redshift-Cluster enthält.	

Daten aus Amazon S3 uploaden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Rolle für den Zugriff auf den S3-Bucket.	Gehen Sie wie folgt vor, um die Rolle für den Zugriff auf den S3-Bucket zu erstellen:	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Öffnen Sie im DEV-Konto die IAM-Konsole. 2. Wählen Sie Policies (Richtlinien). 3. Wählen Sie Richtlinie erstellen aus. 4. Wählen Sie die Registerkarte JSON und geben Sie dann eine IAM-Richtlinie wie die folgende ein: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "kmsstmt", "Effect": "Allow", "Action": [ "kms:Decrypt", "kms:Encrypt", "kms:GenerateDataKey" ], "Resource": [ "<kms-key-arn>" ] }, { "Sid": "s3stmt", "Effect": "Allow", "Action": [`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"s3:PutOb
	ject",
	"s3:Get*",
	"s3:List*"
	],
	"Resource": [
	"arn:aws:
	s3:::mybucket",
	"arn:aws:
	s3:::mybucket/*"
	]
	}
	]
	}</pre> `mybucket`Ersetzen Sie es durch den Namen des S3-Buckets, auf den Sie zugreifen möchten. Wenn der S3-Bucket verschlüs selt ist, `kms-key-arn` ersetzen Sie ihn außerdem durch den ARN des AWS Key Management Service (AWS KMS) -Schlüsse ls, der zur Verschlüs selung des S3-Buckets verwendet wurde. Andernfal ls benötigen Sie den AWS KMS Abschnitt in der Richtlinie nicht.
	5. Wählen Sie Richtlinie überprüfen aus, geben Sie `S3-Write-Policy` den Namen der Richtlinie ein und wählen Sie dann Richtlinie erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Wählen Sie im Navigationsbereich Rollen aus. 7. Wählen Sie Create role (Rolle erstellen) aus. 8. Wählen Sie für die Rolle „Vertrauenswürdige Entität“ die Option Benutzerdefinierte Vertrauensrichtlinie aus. 9. Wählen Sie Weiter: Berechtigungen und dann die von Ihnen erstellte S3-Write-Policy-Richtlinie aus. 10. Geben Sie **`S3-Write-Role`** den Rollennamen ein und wählen Sie dann Rolle erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Amazon Redshift Redshift-Rolle.	Gehen Sie wie folgt vor, um die Amazon Redshift Redshift-Rolle zu erstellen:
	1. Öffnen Sie im PROD-Konto die IAM-Konsole.
	2. Wählen Sie Policies (Richtlinien).
	3. Wählen Sie Richtlinie erstellen aus.
	4. Wählen Sie die Registerk arte JSON und geben Sie dann eine IAM-Richtlinie wie die folgende ein:
	`{ "Version": "2012-10-17", "Statement": [ { "Sid": "CrossAccountPolicy", "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "S3-Write-Role-ARN" } ] }`
	`S3-Write-Role-ARN`Ersetzen Sie es durch den ARN für das `S3-`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`Write-Role` im DEV-Konto. 5. Wählen Sie Richtlinie überprüfen aus, geben Sie `S3-Write-Role-Assume-Policy` den Namen der Richtlinie ein, und wählen Sie dann Richtlinie erstellen aus. 6. Wählen Sie im Navigationsbereich Rollen und dann Rolle erstellen. 7. Wählen Sie AWS-Service als vertrauenswürdigen Entitätstyp und wählen Sie dann Redshift, Redshift — Customizable. 8. Wählen Sie Weiter: Berechtigungen und dann die von Ihnen erstellte S3-Write-Role-Assume-Policy-Richtlinie aus. 9. Geben Sie den Rollennamen ein **`CrossAccount-S3-Write-Role`** und wählen Sie dann Rolle erstellen aus. 10. Ordnen Sie die IAM-Rolle Ihrem Amazon Redshift Redshift-Cluster zu.	

Stellen Sie die Lambda-Funktion bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Lambda-Funktion bereit.	Gehen Sie wie folgt vor, um eine Lambda-Funktion in der Peering-VPC bereitzustellen: 1. Öffnen Sie die Lambda-Konsole unter https://console.aws.amazon.com/lambda/. 2. Wählen Sie Funktionen. 3. Wählen Sie Create function (Funktion erstellen). 4. Geben Sie unter Basic information (Grundlegende Informationen) bei Function name (Funktionsname) einen Namen für Ihre Funktion ein. 5. Wählen Sie für Runtime Python 3.8. 6. Erweitern Sie Standardausführungsrolle ändern, und gehen Sie dann wie folgt vor: a. Wählen Sie Bestehende Rolle verwenden aus. b. Wählen Sie für Existing role die Lambda-Rolle CrossAccount-RM-Read-Role aus, die Sie zuvor erstellt haben.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Erweitern Sie Erweiterte Einstellungen und gehen Sie wie folgt vor: a. Aktivieren Sie das Kontrollkästchen VPC aktivieren. b. Wählen Sie für VPC die gepeerte VPC im DEV-Konto aus. c. Wählen Sie für Subnetze das private Subnetz aus. d. Wählen Sie unter Security Groups (Sicherheitsgruppen) die standardmäßige Sicherheitsgruppe aus. 8. Wählen Sie Funktion erstellen. 9. Fügen Sie die psycopg2-Bibliothek als Ebene zur Lambda-Funktion hinzu. **Note** Sie können eine bereits bereitgestellte Ebene aus dem psycopg2-lambda-Layer-Repository verwenden. Stellen Sie sicher, dass Sie die URL verwenden, die auf Ihrer AWS-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Region und der Python-Laufzeit basiert.	

Testen Sie die Architektur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Importieren Sie die erforderlichen Ressourcen.	Führen Sie die folgenden Befehle aus, um die erforderlichen Ressourcen zu importieren:
	`import ast`
	`import boto3`
	`import psycopg2`
	`import base64`
	`from botocore.exceptions import ClientError`
		App-Developer

Führen Sie die Lambda-Handler-Funktion aus.	Die Lambda-Funktion verwendet AWS Security Token Service (AWS STS) für den kontoübergreifenden Zugriff und die temporäre Verwaltung von Anmeldeinformationen. Die Funktion verwendet den AssumeRole API-Vorgang, um vorübergehend die Berechtigungen der IAM-Rolle zu übernehmen. `sm_read_role`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Verwenden Sie den folgenden Beispielcode, um die Lambda-Funktion auszuführen:
	
	`def lambda_handler(eve nt, context):`
	`  sts_client = boto3.client('sts')`
	
	`  # Secrets Manager Configurations`
	`  secret_name = "redshift_creds"`
	`  sm_region = "eu-west-1"`
	`  sm_read_role = "arn:aws:iam::PROD _ACCOUNT_NUMBER:role/ SM-Read-Role"`
	
	`  # S3 Bucket Configurations`
	`  s3_bucket_path = "s3://mybucket/"`
	`  s3_bucket_region = "eu-west-1"`
	`  s3_write_role = "arn:aws:iam::DEV_ ACCOUNT_NUMBER:role/ S3-Write-Role"`
	
	`  # Redshift Configura tions`
	`  sql_query = "select * from category"`
	`  redshift_db = "dev"`
	`  redshift_s3_write_ role = "arn:aws: iam::PROD_ACCOUNT_ NUMBER:role/CrossA ccount-S3-Write-Role"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> chained_s3_write_role = "%s,%s" % (redshift_s3_write_role, s3_write_role)
	
	    assumed_role_object = sts_client.assume_role(
	        RoleArn=sm_read_role,
	        RoleSessionName="CrossAccountRoleAssumption",
	        ExternalId="YOUR_EXTERNAL_ID",
	    )
	    credentials = assumed_role_object['Credentials']
	
	    secret_dict = ast.literal_eval(get_secret(credentials, secret_name, sm_region))
	    execute_query(secret_dict, sql_query, s3_bucket_path, chained_s3_write_role, s3_bucket_region, redshift_db)
	
	    return {
	        'statusCode': 200
	    }</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Hol dir das Geheimnis.	Verwenden Sie den folgenden Beispielcode, um das Amazon Redshift Redshift-Secret abzurufen:
	
	`def get_secret(credentials, secret_name, sm_region):`
	`  # Create a Secrets Manager client`
	`  session = boto3.session.Session()`
	`  sm_client = session.client(`
	`  service_name='secretsmanager',`
	`  aws_access_key_id=credentials['AccessKeyId'],`
	`  aws_secret_access_key=credentials['SecretAccessKey'],`
	`  aws_session_token=credentials['SessionToken'],`
	`  region_name=sm_region`
	`  )`
	
	`  try:`
	`  get_secret_value_response = sm_client.get_secret_value(`
	`  SecretId=secret_name`
	`  )`
	`  except ClientError as e:`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>print(e)
	raise e
	else:
	if 'SecretSt
	ring' in get_secre
	t_value_response:
	return
	get_secret_value_r
	esponse['SecretStr
	ing']
	else:
	return
	base64.b64decode(g
	et_secret_value_re
	sponse['SecretBina
	ry'])</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Führen Sie den Befehl unload aus.	Verwenden Sie den folgenden Beispielcode, um die Daten in den S3-Bucket zu entladen.
	
	`def execute_query(secret_dict, sql_query, s3_bucket_path, chained_s3_write_role, s3_bucket_region, redshift_db):`
	`  conn_string = "dbname='%s' port='%s' user='%s' password='%s' host='%s'" \`
	`  % (redshift_db,`
	`  secret_dict["port"],`
	`  secret_dict["username"],`
	`  secret_dict["password"],`
	`  secret_dict["host"])`
	`  con = psycopg2.connect(conn_string)`
	`  unload_command = "UNLOAD ('{}') TO '{}' IAM_ROLE '{}' DELIMITER '|' REGION '{}';" \`
	`  .format(sql_query,`
	`  s3_bucket_path + str(datetime.datetime.now()) + ".csv",`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>chained_s3_write_role,
	
	s3_bucket_region)
	
	# Opening a cursor and run query
	cur = con.cursor()
	cur.execute(unload_command)
	
	print(cur.fetchone())
	cur.close()
	con.close()</pre>	

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die Lambda-Funktion.	Um ungeplante Kosten zu vermeiden, entfernen Sie die Ressourcen und die Verbindung zwischen den Konten DEV und PROD. Gehen Sie wie folgt vor, um die Lambda-Funktion zu entfernen: 1. Öffnen Sie die AWS Lambda Konsole unter. https://console.aws.amazon.com/lambda/ 2. Suchen Sie die Lambda-Funktion, die Sie erstellt	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	haben, und wählen Sie sie aus. 3. Wählen Sie Aktionen und anschließend Löschen aus. 4. Bestätigen Sie das Löschen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die IAM-Rollen und -Richtlinien.	Entfernen Sie die IAM-Rollen und -Richtlinien aus den DEV- und PROD-Konten. Gehen Sie im DEV-Konto wie folgt vor: 1. Öffnen Sie die IAM-Konsole. 2. Löschen Sie die folgenden Rollen: • `S3-Write-Role` • `CrossAccount-RM-Read-Role` (Lambda-Rolle) 3. Löschen Sie die zugehörigen Richtlinien: • `S3-Write-Policy` • Die CrossAccount Richtlinie für die Übernahme von PROD-Kontorollen Gehen Sie im PROD-Konto wie folgt vor: 1. Öffnen Sie die IAM-Konsole. 2. Löschen Sie die folgenden Rollen: • `SM-Read-Role` • `CrossAccount-S3-Write-Role`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Löschen Sie die zugehörigen Richtlinien: • Die CrossAccount Richtlinie für den Zugriff auf Secrets Manager • `S3-Write-Role-Assume-Policy`	
Löschen Sie das Geheimnis in Secrets Manager.	Gehen Sie wie folgt vor, um das Geheimnis zu löschen: 1. Öffnen Sie im PROD-Konto die Secrets Manager Manager-Konsole. 2. Suchen Sie das angegebene `Redshift-Creds-Secret` Geheimnis und wählen Sie es aus. 3. Wählen Sie Actions (Aktionen) aus, und klicken Sie dann auf Delete secret (Secret löschen). 4. Bestätigen Sie das Löschen.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie VPC-Peering- und Sicherheitsgruppenregeln.	Gehen Sie wie folgt vor, um VPC-Peering- und Sicherheitsgruppenregeln zu entfernen: 1. Öffnen Sie im PROD-Konto die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/. 2. Navigieren Sie zu Sicherheitsgruppen. 3. Suchen Sie die Sicherheitsgruppe, die vom Amazon Redshift Redshift-Cluster verwendet wird. 4. Bearbeiten Sie die Regeln für eingehenden Datenverkehr und entfernen Sie die Regel, die Verbindungen von der Lambda-VPC des DEV-Kontos zulässt. 5. Navigieren Sie zu VPC Peering Connections und löschen Sie die Peering-Verbindung.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Daten aus dem S3-Bucket entfernen.	Gehen Sie wie folgt vor, um die Daten aus Amazon S3 zu entfernen: 1. Öffnen Sie im DEV-Konto die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/. 2. Suchen Sie den Bucket, den Sie für die Datenspeicherung verwendet haben. 3. Löschen Sie die Objekte innerhalb des Buckets oder löschen Sie den gesamten Bucket, falls er nicht mehr benötigt wird.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
AWS KMS Schlüssel aufräumen.	Wenn Sie benutzerdefinierte AWS KMS Schlüssel für die Verschlüsselung erstellt haben, gehen Sie wie folgt vor: 1. Öffnen Sie die AWS KMS Konsole unter https://console.aws.amazon.com/kms/. 2. Suchen Sie nach allen Schlüsseln, die für dieses Muster erstellt wurden. 3. Planen Sie das Löschen der Schlüssel ein. (Es gibt eine obligatorische Wartezeit für das Löschen von Schlüsseln).	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen und löschen Sie CloudWatch Amazon-Protokolle.	Gehen Sie wie folgt vor, um die CloudWatch Protokolle zu löschen: 1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/. 2. Suchen Sie nach Protokollgruppen, die von Ihrer Lambda-Funktion oder Ihrem Amazon Redshift Redshift-Cluster erstellt wurden. 3. Löschen Sie diese Protokollgruppen, wenn sie nicht mehr benötigt werden.	DevOps Ingenieur

Zugehörige Ressourcen

- CloudWatch Amazon-Dokumentation
- IAM-Dokumentation
- Lambda-Dokumentation
- Amazon Redshift Redshift-Dokumentation
- Amazon S3 S3-Dokumentation
- AWS Secrets Manager Dokumentation
- AWS Sicherheitsprinzipien

Zusätzliche Informationen

Nachdem Sie die Daten von Amazon Redshift nach Amazon S3 entladen haben, können Sie sie mit Amazon Athena analysieren.

Amazon Athena ist ein Big-Data-Abfrageservice, der nützlich ist, wenn Sie auf große Datenmengen zugreifen müssen. Sie können Athena verwenden, ohne Server oder Datenbanken bereitstellen zu müssen. Athena unterstützt komplexe Abfragen, und Sie können es für verschiedene Objekte ausführen.

Wie bei den meisten AWS-Services Fällen besteht der Hauptvorteil der Verwendung von Athena darin, dass es eine große Flexibilität bei der Ausführung von Abfragen ohne zusätzliche Komplexität bietet. Wenn Sie Athena verwenden, können Sie verschiedene Datentypen wie CSV und JSON in Amazon S3 abfragen, ohne den Datentyp zu ändern. Sie können Daten aus verschiedenen Quellen abfragen, auch aus externen AWS Quellen. Athena reduziert die Komplexität, da Sie keine Server verwalten müssen. Athena liest Daten direkt aus Amazon S3, ohne die Daten zu laden oder zu ändern, bevor Sie die Abfrage ausführen.

Datenbankmigrationsmuster nach Workload

Themen

- IBM
- Microsoft
- N/A
- Open-Source
- Oracle
- SAP

IBM

- Migrieren Sie mithilfe von AWS DMS eine Db2-Datenbank von Amazon EC2 zu Aurora MySQL-kompatibel
- Migrieren Sie Db2 for LUW zu Amazon mithilfe EC2 von Protokollversand, um Ausfallzeiten zu reduzieren
- Migrieren Sie Db2 for LUW zu Amazon EC2 mit Disaster Recovery mit hoher Verfügbarkeit
- Migrieren Sie mithilfe von AWS DMS und AWS SCT von IBM Db2 auf Amazon EC2 zu Aurora PostgreSQL-kompatibel
- Migrieren Sie von IBM WebSphere Application Server zu Apache Tomcat auf Amazon EC2
- Streamen Sie Daten von IBM Db2, SAP, Sybase und anderen Datenbanken nach MongoDB Atlas auf AWS

Microsoft

- Beschleunigen Sie die Erkennung und Migration von Microsoft-Workloads zu AWS
- Greifen Sie von Microsoft SQL Server auf Amazon EC2 mithilfe von Verbindungsservern auf lokale Microsoft SQL Server-Tabellen zu
- Beurteilen Sie die Abfrageleistung für die Migration von SQL Server-Datenbanken zu MongoDB Atlas auf AWS
- Automatisieren Sie Datenbankaufgaben in der SQL Server Express Edition, die auf Amazon ausgeführt wird, EC2 mithilfe eines AWS Lambda Taskplaners
- Ändern Sie Python- und Perl-Anwendungen, um die Datenbankmigration von Microsoft SQL Server zur Amazon Aurora PostgreSQL-Compatible Edition zu unterstützen
- Konfigurieren Sie das schreibgeschützte Routing in einer Always-On-Verfügbarkeitsgruppe in SQL Server auf AWS
- Erstellen Sie CloudFormation AWS-Vorlagen für AWS DMS-Aufgaben mit Microsoft Excel und Python
- Stellen Sie mithilfe von Terraform SQL Server-Failover-Cluster-Instances auf Amazon EC2 und Amazon FSx bereit
- Exportieren Sie eine Microsoft SQL Server-Datenbank mithilfe von AWS DMS nach Amazon S3
- Exportieren Sie Amazon RDS for SQL Server-Tabellen mithilfe von AWS DMS in einen S3-Bucket
- Implementieren Sie SHA1 Hashing für PII-Daten bei der Migration von SQL Server zu PostgreSQL
- EC2 Windows-Instances in ein AWS Managed Services Services-Konto aufnehmen und migrieren
- Migrieren Sie eine Messaging-Warteschlange von Microsoft Azure Service Bus zu Amazon SQS
- Migrieren Sie mithilfe von AWS DMS eine Microsoft SQL Server-Datenbank von Amazon EC2 zu Amazon DocumentDB
- Migrieren Sie eine Microsoft SQL Server-Datenbank mithilfe von AWS DMS und AWS SCT zu Aurora MySQL
- Migrieren Sie eine.NET-Anwendung von Microsoft Azure App Service zu AWS Elastic Beanstalk
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Amazon EC2
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Amazon RDS for SQL Server
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mithilfe von Verbindungsservern zu Amazon RDS for SQL Server
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mit systemeigenen Sicherungs- und Wiederherstellungsmethoden zu Amazon RDS for SQL Server

- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mit AWS DMS zu Amazon Redshift
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mithilfe von AWS SCT-Datenextraktionsagenten zu Amazon Redshift
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Microsoft SQL Server auf Amazon EC2 unter Linux
- Migrieren Sie Daten mithilfe von Rclone von Microsoft Azure Blob zu Amazon S3
- Migrieren Sie EC2 mithilfe des Application Migration Service eine lokale Microsoft SQL Server-Datenbank zu Amazon
- Migrieren Sie eine relationale Datenbank zu MongoDB Atlas am AWS
- Migrieren Sie SQL Server mithilfe verteilter Verfügbarkeitsgruppen zu AWS
- Migrieren Sie Windows-SSL-Zertifikate mithilfe von ACM zu einem Application Load Balancer
- Rehosten Sie lokale Workloads in der AWS-Cloud: Migrationscheckliste
- Verbindungsfehler nach der Migration von Microsoft SQL Server zur AWS-Cloud beheben
- Senden Sie Benachrichtigungen für eine Amazon RDS for SQL Server Server-Datenbank-Instance mithilfe eines lokalen SMTP-Servers und Datenbank-E-Mail
- Richten Sie mithilfe von Terraform eine CI/CD-Pipeline für die Datenbankmigration ein
- Richten Sie mithilfe von Amazon eine Multi-AZ-Infrastruktur für einen SQL Server Always On FCI ein FSx

N/A

- Erstellen Sie einen Genehmigungsprozess für Firewallanfragen während einer Rehost-Migration zu AWS
- Verschlüsseln Sie eine bestehende Amazon RDS for PostgreSQL PostgreSQL-DB-Instance
- Schätzung der Speicherkosten für eine Amazon DynamoDB-Tabelle
- Implementieren Sie regionsübergreifende Notfallwiederherstellung mit AWS DMS und Amazon Aurora

Open-Source

- Automatisches Generieren eines PynamoDB-Modells und CRUD-Funktionen für Amazon DynamoDB mithilfe einer Python-Anwendung
- Stellen Sie eine Connect über einen SSH-Tunnel in pgAdmin her
- Anwendungsbenutzer und Rollen in Aurora PostgreSQL-Compatible erstellen
- Verschlüsselte Verbindungen für PostgreSQL-DB-Instances in Amazon RDS aktivieren
- Migrieren Sie Amazon RDS for Oracle zu Amazon RDS for PostgreSQL mit AWS SCT und unter Verwendung von und AWS DMSAWS CLIAWS CloudFormation
- Migrieren Sie eine lokale MariaDB-Datenbank mit nativen Tools zu Amazon RDS for MariaDB
- Migrieren Sie eine lokale MySQL-Datenbank zu Amazon EC2
- Migrieren Sie eine lokale MySQL-Datenbank zu Amazon RDS for MySQL
- Migrieren Sie eine lokale MySQL-Datenbank zu Aurora MySQL
- Migrieren Sie eine lokale PostgreSQL-Datenbank zu Aurora PostgreSQL
- Migrieren Sie eine Couchbase Server-Datenbank zu Amazon EC2
- Migrieren Sie EC2 mit Auto Scaling von IBM WebSphere Application Server zu Apache Tomcat auf Amazon
- Migrieren Sie mithilfe von AWS DMS von Oracle 8i oder 9i zu Amazon RDS for Oracle SharePlex
- Migrieren Sie von Oracle GlassFish zu AWS Elastic Beanstalk
- Migrieren Sie mit pglogical von PostgreSQL auf Amazon EC2 zu Amazon RDS for PostgreSQL
- Migrieren Sie ML-Workloads zum Erstellen, Trainieren und Bereitstellen zu Amazon SageMaker mithilfe der AWS-Entwicklertools
- Migrieren Sie lokale Java-Anwendungen mit AWS App2Container zu AWS
- Migrieren Sie lokale MySQL-Datenbanken mit Percona XtraBackup, Amazon EFS und Amazon S3 zu Aurora MySQL
- Migrieren Sie externe Oracle-Tabellen zu Amazon Aurora PostgreSQL-kompatibel
- Migrieren Sie Oracle-Funktionen und -Prozeduren mit mehr als 100 Argumenten nach PostgreSQL
- Migrieren Sie Redis-Workloads zu Redis Enterprise Cloud auf AWS
- Überwachen Sie Amazon Aurora auf Instances ohne Verschlüsselung
- Starten Sie den AWS Replication Agent SELinux nach dem Neustart eines RHEL-Quellservers automatisch neu, ohne ihn zu deaktivieren.

- Planen Sie Jobs für Amazon RDS for PostgreSQL und Aurora PostgreSQL mithilfe von Lambda und Secrets Manager
- Richten Sie die Datenreplikation zwischen Amazon RDS for MySQL und MySQL auf Amazon EC2 mithilfe von GTID ein
- Transportieren Sie PostgreSQL-Datenbanken zwischen zwei Amazon RDS-DB-Instances mithilfe von pg_transport
- Daten aus einem Amazon Redshift Redshift-Cluster kontenübergreifend nach Amazon S3 entladen

Oracle

- Fügen Sie HA mithilfe einer Read Replica zu Oracle PeopleSoft auf Amazon RDS Custom hinzu
- JSON-Oracle-Abfragen in PostgreSQL-Datenbank-SQL konvertieren
- Konvertiert VARCHAR2 (1) den Datentyp für Oracle in den booleschen Datentyp für Amazon Aurora PostgreSQL
- Emulieren Sie Oracle DR mithilfe einer PostgreSQL-kompatiblen globalen Aurora-Datenbank
- Emulieren Sie Oracle RAC-Workloads mithilfe benutzerdefinierter Endpunkte in Aurora PostgreSQL
- Schätzen Sie die Größe der Amazon RDS-Engine für eine Oracle-Datenbank mithilfe von AWR-Berichten
- Behandeln Sie anonyme Blöcke in dynamischen SQL-Anweisungen in Aurora PostgreSQL
- Behandeln Sie überladene Oracle-Funktionen in Aurora PostgreSQL-kompatibel
- Schrittweise Migration von Amazon RDS for Oracle zu Amazon RDS for PostgreSQL mithilfe von Oracle SQL Developer und AWS SCT
- Laden Sie BLOB-Dateien in TEXT, indem Sie die Dateikodierung in Aurora PostgreSQL-kompatibel verwenden
- Migrieren Sie Amazon RDS for Oracle DB-Instances zu anderen Konten, die AMS verwenden
- Migrieren Sie Amazon RDS for Oracle zu Amazon RDS for PostgreSQL im SSL-Modus mithilfe von AWS DMS
- Migrieren Sie eine Amazon RDS for Oracle Oracle-Datenbank zu einer anderen AWS-Konto und AWS-Region verwenden Sie sie AWS DMS für die laufende Replikation
- Migrieren Sie eine Amazon RDS for Oracle DB-Instance zu einer anderen VPC
- Migrieren Sie eine lokale Oracle-Datenbank mithilfe EC2 von Oracle Data Pump zu Amazon
- Migrieren Sie eine lokale Oracle-Datenbank mit Logstash zu Amazon OpenSearch Service
- Migrieren Sie eine lokale Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon RDS for MySQL
- Migrieren Sie eine lokale Oracle-Datenbank zu Amazon RDS for Oracle
- Migrieren Sie eine lokale Oracle-Datenbank zu Amazon RDS for Oracle, indem Sie den direkten Oracle Data Pump-Import über einen Datenbank-Link verwenden
- Migrieren Sie eine lokale Oracle-Datenbank mit Oracle Data Pump zu Amazon RDS for Oracle
- Migrieren Sie eine lokale Oracle-Datenbank mithilfe eines Oracle-Bystanders und AWS DMS zu Amazon RDS for PostgreSQL

- Migrieren Sie eine lokale Oracle-Datenbank zu Oracle auf Amazon EC2
- Migrieren Sie mithilfe von AWS DMS und AWS SCT eine Oracle-Datenbank von Amazon EC2 zu Amazon RDS for MariaDB
- Migrieren Sie mithilfe von AWS DMS eine Oracle-Datenbank von Amazon EC2 zu Amazon RDS for Oracle
- Migrieren Sie eine Oracle-Datenbank mit AWS DMS zu Amazon DynamoDB
- Migrieren Sie eine Oracle-Datenbank mithilfe von GoldenGate Oracle-Flatfile-Adaptern zu Amazon RDS for Oracle
- Migrieren Sie eine Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon Redshift
- Migrieren Sie eine Oracle-Datenbank mit AWS DMS und AWS SCT zu Aurora PostgreSQL
- Migrieren Sie eine Oracle JD EnterpriseOne Edwards-Datenbank mithilfe von Oracle Data Pump und AWS DMS zu AWS
- Migrieren Sie eine partitionierte Oracle-Tabelle mithilfe von AWS DMS zu PostgreSQL
- Migrieren Sie eine PeopleSoft Oracle-Datenbank mithilfe von AWS DMS zu AWS
- Migrieren Sie Daten von einer lokalen Oracle-Datenbank zu Aurora PostgreSQL
- Migrieren Sie von Amazon RDS for Oracle zu Amazon RDS for MySQL
- Migrieren Sie mithilfe von Materialized Views und AWS DMS von Oracle 8i oder 9i zu Amazon RDS for PostgreSQL
- Migrieren Sie mithilfe von AWS DMS von Oracle 8i oder 9i zu Amazon RDS for PostgreSQL SharePlex
- Migrieren Sie mithilfe von Oracle von Oracle Database zu Amazon RDS for PostgreSQL GoldenGate
- Migrieren Sie mithilfe von AWS DMS und AWS SCT von Oracle auf Amazon EC2 zu Amazon RDS for MySQL
- Migrieren Sie mit AWS DMS von Oracle zu Amazon DocumentDB
- Migrieren Sie von Oracle WebLogic zu Apache Tomcat (ToMEE) auf Amazon ECS
- Migrieren Sie funktionsbasierte Indizes von Oracle nach PostgreSQL
- Migrieren Sie Legacy-Anwendungen von Oracle Pro*C zu ECPG
- Migrieren Sie Oracle CLOB-Werte in einzelne Zeilen in PostgreSQL auf AWS
- Migrieren Sie Oracle-Datenbank-Fehlercodes in eine Amazon Aurora PostgreSQL-kompatible Datenbank
- Migrieren Sie die Oracle E-Business Suite zu Amazon RDS Custom

- Migrieren Sie native Oracle-Funktionen mithilfe von Erweiterungen zu PostgreSQL
- Migrieren Sie Oracle OUT-Bind-Variablen in eine PostgreSQL-Datenbank
- Migrieren Sie Oracle PeopleSoft zu Amazon RDS Custom
- Migrieren Sie die Oracle ROWID-Funktionalität zu PostgreSQL auf AWS
- Migrieren Sie Oracle SERIALLY_REUSABLE Pragma-Pakete nach PostgreSQL
- Migrieren Sie virtuell generierte Spalten von Oracle nach PostgreSQL
- Überwachen Sie GoldenGate Oracle-Protokolle mithilfe von Amazon CloudWatch
- Replatform Oracle Database Enterprise Edition auf Standard Edition 2 auf Amazon RDS for Oracle
- Richten Sie eine HA/DR-Architektur für Oracle E-Business Suite auf Amazon RDS Custom mit einer aktiven Standby-Datenbank ein
- Richten Sie die Oracle UTL_FILE-Funktionalität auf Aurora PostgreSQL-Compatible ein
- Rollen für eine PeopleSoft Oracle-Anwendung auf Amazon RDS Custom for Oracle wechseln
- Datenbankobjekte nach der Migration von Oracle zu Amazon Aurora PostgreSQL validieren

SAP

- Automatisches Backup von SAP HANA-Datenbanken mit Systems Manager und EventBridge
- Migrieren Sie eine lokale SAP ASE-Datenbank zu Amazon EC2
- Migrieren Sie mithilfe von AWS DMS von SAP ASE zu Amazon RDS for SQL Server
- Migrieren Sie SAP ASE auf Amazon EC2 zu Amazon Aurora PostgreSQL-kompatibel mit AWS SCT und AWS DMS
- Migrieren Sie SAP HANA zu AWS mithilfe von SAP HSR mit demselben Hostnamen
- Reduzieren Sie die Umstellungszeit für homogene SAP-Migrationen mithilfe des Application Migration Service
- Disaster Recovery für SAP auf IBM Db2 auf AWS einrichten

Mehr Muster

- Greifen Sie von einem Amazon EKS-Container aus auf eine Amazon Neptune-Datenbank zu
- Mit Athena auf Amazon DynamoDB-Tabellen zugreifen, diese abfragen und verbinden
- Aggregieren Sie Daten in Amazon DynamoDB für ML-Prognosen in Athena
- Erlauben Sie EC2 Instances den Schreibzugriff auf S3-Buckets in AMS-Konten
- Analysieren und visualisieren Sie verschachtelte JSON-Daten mit Amazon Athena und Amazon QuickSight
- Authentifizieren Sie Microsoft SQL Server auf Amazon EC2 mithilfe von AWS Directory Service
- Automatisieren Sie Backups für Amazon RDS for PostgreSQL PostgreSQL-DB-Instances mithilfe von AWS Batch
- Automatisches Archivieren von Elementen in Amazon S3 mithilfe von DynamoDB TTL
- Automatically remediate unencrypted Amazon RDS DB instances and clusters
- Automatisches Stoppen und Starten einer Amazon RDS-DB-Instance mithilfe von AWS Systems Manager Maintenance Windows
- Erstellen Sie eine lose gekoppelte Architektur mit Microservices mithilfe von DevOps Praktiken und AWS Cloud9
- Erstellen Sie COBOL Db2-Programme mit und AWS Mainframe ModernizationAWS CodeBuild
- Bauen Sie mit Amazon ein Datennetz für Unternehmen auf DataZone AWS CDK, und AWS CloudFormation
- Ändern Sie Python- und Perl-Anwendungen, um die Datenbankmigration von Microsoft SQL Server zur Amazon Aurora PostgreSQL-Compatible Edition zu unterstützen
- EBCDIC-Daten mithilfe von Python in ASCII auf AWS konvertieren und entpacken
- Konvertieren Sie die temporale Funktion Teradata NORMALIZE in Amazon Redshift SQL
- Konvertieren Sie die Teradata RESET WHEN-Funktion in Amazon Redshift SQL
- Konvertiert VARCHAR2 (1) den Datentyp für Oracle in den booleschen Datentyp für Amazon Aurora PostgreSQL
- Anwendungsbenutzer und Rollen in Aurora PostgreSQL-Compatible erstellen
- Erstellen Sie CloudFormation AWS-Vorlagen für AWS DMS-Aufgaben mit Microsoft Excel und Python
- Stellen Sie DynamoDB-Datensätze mithilfe von Kinesis Data Streams und Firehose an Amazon S3 bereit mit AWS CDK

- Stellen Sie einen Cassandra-Cluster auf Amazon EC2 mit Private Static bereit, um ein IPs Rebalancing zu vermeiden
- Entwickeln Sie mithilfe von RAG und Prompting fortschrittliche, auf KI basierende Chat-Assistenten ReAct
- Emulieren Sie Oracle DR mithilfe einer PostgreSQL-kompatiblen globalen Aurora-Datenbank
- Aktivieren Sie die transparente Datenverschlüsselung in Amazon RDS for SQL Server
- Exportieren Sie eine Microsoft SQL Server-Datenbank mithilfe von AWS DMS nach Amazon S3
- Implementieren Sie SHA1 Hashing für PII-Daten bei der Migration von SQL Server zu PostgreSQL
- Schrittweise Migration von Amazon RDS for Oracle zu Amazon RDS for PostgreSQL mithilfe von Oracle SQL Developer und AWS SCT
- Laden Sie BLOB-Dateien in TEXT, indem Sie die Dateikodierung in Aurora PostgreSQL-kompatibel verwenden
- Anmeldeinformationen mit AWS Secrets Manager verwalten
- Migrieren Sie mithilfe von AWS DMS eine Db2-Datenbank von Amazon EC2 zu Aurora MySQL-kompatibel
- Migrieren Sie mithilfe von AWS DMS eine Microsoft SQL Server-Datenbank von Amazon EC2 zu Amazon DocumentDB
- Migrieren Sie eine Microsoft SQL Server-Datenbank mithilfe von AWS DMS und AWS SCT zu Aurora MySQL
- Migrieren Sie eine selbst gehostete MongoDB-Umgebung zu MongoDB Atlas am AWS
- Migrieren Sie eine Teradata-Datenbank mithilfe von AWS SCT-Datenextraktionsagenten zu Amazon Redshift
- Migrieren Sie Amazon RDS for Oracle zu Amazon RDS for PostgreSQL im SSL-Modus mithilfe von AWS DMS
- Migrieren Sie Amazon RDS for Oracle zu Amazon RDS for PostgreSQL mit AWS SCT und unter Verwendung von und AWS DMSAWS CLIAWS CloudFormation
- Migrieren Sie eine Amazon RDS-DB-Instance zu einer anderen VPC oder einem anderen Konto
- Migrieren Sie eine Amazon RDS for Oracle Oracle-Datenbank zu einer anderen AWS-Konto und AWS-Region verwenden Sie sie AWS DMS für die laufende Replikation
- Migrieren Sie eine Amazon RDS for Oracle DB-Instance zu einer anderen VPC
- Migrieren Sie einen Amazon Redshift Redshift-Cluster in eine AWS-Region in China
- Migrieren Sie eine lokale MariaDB-Datenbank mit nativen Tools zu Amazon RDS for MariaDB

- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Amazon EC2
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Amazon RDS for SQL Server
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mithilfe von Verbindungsservern zu Amazon RDS for SQL Server
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mit systemeigenen Sicherungs- und Wiederherstellungsmethoden zu Amazon RDS for SQL Server
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mit AWS DMS zu Amazon Redshift
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mithilfe von AWS SCT-Datenextraktionsagenten zu Amazon Redshift
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Microsoft SQL Server auf Amazon EC2 unter Linux
- Migrieren Sie eine lokale MySQL-Datenbank zu Amazon EC2
- Migrieren Sie eine lokale MySQL-Datenbank zu Amazon RDS for MySQL
- Migrieren Sie eine lokale MySQL-Datenbank zu Aurora MySQL
- Migrieren Sie eine lokale Oracle-Datenbank mithilfe EC2 von Oracle Data Pump zu Amazon
- Migrieren Sie eine lokale Oracle-Datenbank mit Logstash zu Amazon OpenSearch Service
- Migrieren Sie eine lokale Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon RDS for MySQL
- Migrieren Sie eine lokale Oracle-Datenbank zu Amazon RDS for Oracle
- Migrieren Sie eine lokale Oracle-Datenbank zu Amazon RDS for Oracle, indem Sie den direkten Oracle Data Pump-Import über einen Datenbank-Link verwenden
- Migrieren Sie eine lokale Oracle-Datenbank mit Oracle Data Pump zu Amazon RDS for Oracle
- Migrieren Sie eine lokale Oracle-Datenbank mithilfe eines Oracle-Bystanders und AWS DMS zu Amazon RDS for PostgreSQL
- Migrieren Sie eine lokale Oracle-Datenbank zu Oracle auf Amazon EC2
- Migrieren Sie eine lokale PostgreSQL-Datenbank zu Aurora PostgreSQL
- Migrieren Sie eine lokale SAP ASE-Datenbank zu Amazon EC2
- Migrieren Sie eine lokale ThoughtSpot Falcon-Datenbank zu Amazon Redshift
- Migrieren Sie eine lokale Vertica-Datenbank mithilfe von AWS SCT-Datenextraktionsagenten zu Amazon Redshift
- Migrieren Sie mithilfe von AWS DMS und AWS SCT eine Oracle-Datenbank von Amazon EC2 zu Amazon RDS for MariaDB

- Migrieren Sie mithilfe von AWS DMS eine Oracle-Datenbank von Amazon EC2 zu Amazon RDS for Oracle
- Migrieren Sie eine Oracle-Datenbank mit AWS DMS zu Amazon DynamoDB
- Migrieren Sie eine Oracle-Datenbank mithilfe von GoldenGate Oracle-Flatfile-Adaptern zu Amazon RDS for Oracle
- Migrieren Sie eine Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon Redshift
- Migrieren Sie eine Oracle-Datenbank mit AWS DMS und AWS SCT zu Aurora PostgreSQL
- Migrieren Sie eine Oracle JD EnterpriseOne Edwards-Datenbank mithilfe von Oracle Data Pump und AWS DMS zu AWS
- Migrieren Sie eine partitionierte Oracle-Tabelle mithilfe von AWS DMS zu PostgreSQL
- Migrieren Sie eine PeopleSoft Oracle-Datenbank mithilfe von AWS DMS zu AWS
- Migrieren Sie eine Couchbase Server-Datenbank zu Amazon EC2
- Migrieren Sie Daten von einer lokalen Oracle-Datenbank zu Aurora PostgreSQL
- Migrieren Sie Daten mithilfe AWS Cloud von Starburst auf die
- Migrieren Sie Db2 for LUW zu Amazon mithilfe EC2 von Protokollversand, um Ausfallzeiten zu reduzieren
- Migrieren Sie Db2 for LUW zu Amazon EC2 mit Disaster Recovery mit hoher Verfügbarkeit
- Migrieren Sie von Amazon RDS for Oracle zu Amazon RDS for MySQL
- Migrieren Sie von Couchbase Server zu Couchbase Capella auf AWS
- Migrieren Sie mithilfe von AWS DMS und AWS SCT von IBM Db2 auf Amazon EC2 zu Aurora PostgreSQL-kompatibel
- Migrieren Sie mithilfe von Materialized Views und AWS DMS von Oracle 8i oder 9i zu Amazon RDS for PostgreSQL
- Migrieren Sie mithilfe von AWS DMS von Oracle 8i oder 9i zu Amazon RDS for PostgreSQL SharePlex
- Migrieren Sie mithilfe von Oracle von Oracle Database zu Amazon RDS for PostgreSQL GoldenGate
- Migrieren Sie mithilfe von AWS DMS und AWS SCT von Oracle auf Amazon EC2 zu Amazon RDS for MySQL
- Migrieren Sie mit AWS DMS von Oracle zu Amazon DocumentDB
- Migrieren Sie mit pglogical von PostgreSQL auf Amazon EC2 zu Amazon RDS for PostgreSQL
- Migrieren Sie mithilfe von AWS DMS von SAP ASE zu Amazon RDS for SQL Server

- Migrieren Sie funktionsbasierte Indizes von Oracle nach PostgreSQL
- Migrieren Sie Legacy-Anwendungen von Oracle Pro*C zu ECPG
- Migrieren Sie EC2 mithilfe des Application Migration Service eine lokale Microsoft SQL Server-Datenbank zu Amazon
- Migrieren Sie lokale Cloudera-Workloads zur Cloudera Data Platform auf AWS
- Migrieren Sie lokale MySQL-Datenbanken mit Percona XtraBackup, Amazon EFS und Amazon S3 zu Aurora MySQL
- Migrieren Sie Oracle Business Intelligence 12c von lokalen Servern zur AWS-Cloud
- Migrieren Sie Oracle CLOB-Werte in einzelne Zeilen in PostgreSQL auf AWS
- Migrieren Sie Oracle-Datenbank-Fehlercodes in eine Amazon Aurora PostgreSQL-kompatible Datenbank
- Migrieren Sie die Oracle E-Business Suite zu Amazon RDS Custom
- Migrieren Sie externe Oracle-Tabellen zu Amazon Aurora PostgreSQL-kompatibel
- Migrieren Sie native Oracle-Funktionen mithilfe von Erweiterungen zu PostgreSQL
- Migrieren Sie Oracle PeopleSoft zu Amazon RDS Custom
- Migrieren Sie die Oracle ROWID-Funktionalität zu PostgreSQL auf AWS
- Migrieren Sie Oracle SERIALLY_REUSABLE Pragma-Pakete nach PostgreSQL
- Migrieren Sie Redis-Workloads zu Redis Enterprise Cloud auf AWS
- Migrieren Sie eine relationale Datenbank zu MongoDB Atlas am AWS
- Migrieren Sie SAP ASE auf Amazon EC2 zu Amazon Aurora PostgreSQL-kompatibel mit AWS SCT und AWS DMS
- Migrieren Sie virtuell generierte Spalten von Oracle nach PostgreSQL
- Richten Sie einen nutzbaren Mindestdatenraum für die gemeinsame Nutzung von Daten zwischen Organisationen ein
- ElastiCache Amazon-Cluster auf Verschlüsselung im Ruhezustand überwachen
- ElastiCache Cluster für Sicherheitsgruppen überwachen
- Abfragen von Amazon DynamoDB-Tabellen mit SQL mithilfe von Amazon Athena
- Reduzieren Sie die Umstellungszeit für homogene SAP-Migrationen mithilfe des Application Migration Service
- Datenbankanmeldedaten rotieren, ohne Container neu zu starten
- Mithilfe von AWS Fargate können Sie nachrichtengesteuerte Workloads in großem Umfang ausführen

- Sicherer und optimierter Benutzerzugriff in einer Db2-Verbunddatenbank auf AWS mithilfe vertrauenswürdiger Kontexte
- Richten Sie eine hochverfügbare PeopleSoft Architektur auf AWS ein
- Richten Sie die Oracle UTL_FILE-Funktionalität auf Aurora PostgreSQL-Compatible ein
- Streamen Sie Daten von IBM Db2, SAP, Sybase und anderen Datenbanken nach MongoDB Atlas auf AWS
- Optimieren Sie PostgreSQL-Bereitstellungen auf Amazon EKS mithilfe von PGO
- Übertragung umfangreicher Db2 z/OS-Daten in CSV-Dateien nach Amazon S3
- Transportieren Sie PostgreSQL-Datenbanken zwischen zwei Amazon RDS-DB-Instances mithilfe von pg_transport
- Datenbankobjekte nach der Migration von Oracle zu Amazon Aurora PostgreSQL validieren
- Stellen Sie sicher, dass neue Amazon Redshift Redshift-Cluster in einer VPC gestartet werden

Speicher und Backup

Themen

- Erlauben Sie EC2 Instances den Schreibzugriff auf S3-Buckets in AMS-Konten
- Automatisieren Sie die Aufnahme von Datenströmen in eine Snowflake-Datenbank mithilfe von Snowflake Snowpipe, Amazon S3, Amazon SNS und Amazon Data Firehose
- Automatisches Verschlüsseln vorhandener und neuer Amazon EBS-Volumes
- Sun SPARC-Server im Stromasys Charon-SSP-Emulator in der AWS-Cloud sichern
- Daten mit Veeam Backup & Replication auf Amazon S3 sichern und archivieren
- Konfiguration von Veritas NetBackup for VMware Cloud auf AWS
- Kopieren Sie Daten mithilfe der AWS-CLI aus einem S3-Bucket in ein anderes Konto und eine andere Region
- Kopieren Sie Daten mithilfe von S3 Batch Replication von einem S3-Bucket in ein anderes Konto und eine andere Region
- Migrieren Sie Daten mithilfe DistCp von AWS PrivateLink für Amazon S3 von einer lokalen Hadoop-Umgebung zu Amazon S3
- Mehr Muster

Erlauben Sie EC2 Instances den Schreibzugriff auf S3-Buckets in AMS-Konten

Erstellt von Mansi Suratwala (AWS)

Übersicht

AWS Managed Services (AMS) hilft Ihnen dabei, Ihre AWS Infrastruktur effizienter und sicherer zu betreiben. AMS-Konten verfügen über Sicherheitsvorkehrungen für die standardisierte Verwaltung Ihrer AWS Ressourcen. Ein Hinweis ist, dass standardmäßige Amazon Elastic Compute Cloud (Amazon EC2) -Instanzprofile keinen Schreibzugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets zulassen. Ihre Organisation verfügt jedoch möglicherweise über mehrere S3-Buckets und benötigt mehr Kontrolle über den Zugriff durch Instances. EC2 Beispielsweise möchten Sie möglicherweise Datenbank-Backups von EC2 Instances in einem S3-Bucket speichern.

Dieses Muster erklärt, wie Sie Requests for change (RFCs) verwenden, um Ihren EC2 Instances Schreibzugriff auf S3-Buckets in Ihrem AMS-Konto zu gewähren. Ein RFC ist eine Anfrage, die von Ihnen oder AMS erstellt wurde, um eine Änderung in Ihrer verwalteten Umgebung vorzunehmen, und die eine Change Type (CT) -ID für einen bestimmten Vorgang beinhaltet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein AMS Advanced-Konto. Weitere Informationen dazu finden Sie in den AMS-Betriebsplänen in der AMS-Dokumentation.
- Zugriff auf die AWS Identity and Access Management (IAM-) `customer-mc-user-role` Rolle, die eingereicht RFCs werden soll.
- AWS Command Line Interface (AWS CLI), wurde mit den EC2 Instanzen in Ihrem AMS-Konto installiert und konfiguriert.
- Kenntnisse darüber, wie das Erstellen und Einreichen RFCs in AMS funktioniert. Weitere Informationen dazu finden Sie unter Was sind AMS-Änderungstypen? in der AMS-Dokumentation.
- Ein Verständnis der manuellen und automatisierten Änderungstypen (CTs). Weitere Informationen dazu finden Sie CTs in der AMS-Dokumentation unter Automatisiert und manuell.

Architektur

Technologie-Stack

- AMS
- AWS CLI
- Amazon EC2
- Amazon S3
- IAM

Tools

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie AWS-Services über Befehle in Ihrer Befehlszeilen-Shell interagieren können.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem es kontrolliert, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Managed Services (AMS) hilft Ihnen dabei, Ihre AWS-Infrastruktur effizienter und sicherer zu betreiben.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.

Epen

Erstellen Sie einen S3-Bucket mit einem RFC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket mithilfe eines automatisierten RFC.	1. Melden Sie sich bei Ihrem AMS-Konto an, wählen Sie die Seite Änderungstyp auswählen aus RFCs, wählen Sie und wählen Sie dann Create RFC aus.	AWS-Systemadministrator, AWS-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Reichen Sie den automatisierten RFC Create S3 Bucket ein. **Note** Stellen Sie sicher, dass Sie den Namen des S3-Buckets notieren.	

Erstellen Sie ein IAM-Instanzprofil und verknüpfen Sie es mit den EC2 Instances

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Reichen Sie einen manuellen RFC ein, um eine IAM-Rolle zu erstellen.	Wenn ein AMS-Konto eingerichtet wird, wird ein Standard-IAM-Instanzprofil mit dem Namen `customer-mc-ec2-instance-profile` erstellt und jeder EC2 Instanz in Ihrem AMS-Konto zugeordnet. Das Instanzprofil hat jedoch keine Schreibberechtigungen für Ihre S3-Buckets. Um die Schreibberechtigungen hinzuzufügen, reichen Sie den RFC Create IAM Resource Manual ein, um eine IAM-Rolle mit den folgenden drei Richtlinien zu erstellen :`customer_ec2_insta`	AWS-Systemadministrator, AWS-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	nce_ , und. customer_ deny_policy customer_ ec2_s3_integration _policy **Important** Die customer_ deny_poli cy Richtlini en customer_ ec2_instance_ und sind bereits in Ihrem AMS-Konto vorhanden . Sie müssen jedoch customer_ ec2_s3_in tegration _policy mithilfe der folgenden Beispielr ichtlinie erstellen: { "Version": "2012-10-17", "Statement": [{ "Sid": "", "Effect": "Allow", "Principal": { "Service": "ec2.amazonaws.com" },	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"Action": "sts:AssumeRole" }] } Role Permissions: { "Version": "2012-10-17", "Statement": [{ "Action": ["s3:ListBucket", "s3:GetBucketLocation"], "Resource": "arn:aws:s3:::", "Effect": "Allow" }, { "Action": ["s3:GetObject", "s3:PutObject", "s3:ListMultipartUploadParts", "s3:AbortMultipartUpload"], "Resource": "arn:aws:s3:::/*", "Effect": "Allow" }</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>] }</pre>	
Reichen Sie einen manuellen RFC ein, um das IAM-Instanzprofil zu ersetzen.	Reichen Sie einen manuellen RFC ein, um die EC2 Ziel-Instances dem neuen IAM-Instanzprofil zuzuordnen.	AWS-Systemadministrator, AWS-Entwickler

Testen Sie einen Kopiervorgang in den S3-Bucket.	Testen Sie einen Kopiervorgang in den S3-Bucket, indem Sie den folgenden Befehl in der Datei ausführen AWS CLI:
	<pre>aws s3 cp test.txt s3://
	<S3 bucket>/test2.txt</pre>
		AWS-Systemadministrator, AWS-Entwickler

Zugehörige Ressourcen

- Erstellen Sie ein IAM-Instance-Profil für Ihre EC2 Amazon-Instances
- Einen S3-Bucket erstellen (mit der Amazon S3 S3-Konsole AWS SDKs,, oder AWS CLI)

Automatisieren Sie die Aufnahme von Datenströmen in eine Snowflake-Datenbank mithilfe von Snowflake Snowpipe, Amazon S3, Amazon SNS und Amazon Data Firehose

Erstellt von Bikash Chandra Rout (AWS)

Übersicht

Dieses Muster beschreibt, wie Sie Dienste in der Amazon Web Services (AWS) Cloud verwenden können, um einen kontinuierlichen Datenstrom zu verarbeiten und in eine Snowflake-Datenbank zu laden. Das Muster verwendet Amazon Data Firehose, um die Daten an Amazon Simple Storage Service (Amazon S3) zu übermitteln, Amazon Simple Notification Service (Amazon SNS), um Benachrichtigungen zu senden, wenn neue Daten empfangen werden, und Snowflake Snowpipe, um die Daten in eine Snowflake-Datenbank zu laden.

Wenn Sie diesem Muster folgen, können Sie kontinuierlich generierte Daten innerhalb von Sekunden für die Analyse zur Verfügung haben, mehrere manuelle `COPY` Befehle vermeiden und halbstrukturierte Daten beim Laden vollständig unterstützen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto.
- Eine Datenquelle, die kontinuierlich Daten an einen Firehose-Lieferstream sendet.
- Ein vorhandener S3-Bucket, der die Daten aus dem Firehose-Lieferstream empfängt.
- Ein aktives Snowflake-Konto.

Einschränkungen

- Snowflake Snowpipe stellt keine direkte Verbindung zu Firehose her.

Architektur

Technologie-Stack

- Amazon Data Firehose
- Amazon SNS
- Amazon S3
- Schneeflocke, Schneepfeife
- Snowflake-Datenbank

Tools

- Amazon Data Firehose ist ein vollständig verwalteter Service für die Bereitstellung von Echtzeit-Streaming-Daten an Ziele wie Amazon S3, Amazon Redshift, Amazon OpenSearch Service, Splunk und alle benutzerdefinierten HTTP-Endpunkte oder HTTP-Endpunkte, die unterstützten Drittanbietern gehören.
- Amazon Simple Storage Service (Amazon S3) ist Speicher für das Internet.
- Amazon Simple Notification Service (Amazon SNS) koordiniert und verwalte die Zustellung oder das Senden von Nachrichten an abonnierende Endpunkte oder Clients.
- Snowflake — Snowflake ist ein analytisches Data Warehouse, das als (SaaS) bereitgestellt wird. Software-as-a-Service
- Snowflake Snowpipe — Snowpipe lädt Daten aus Dateien, sobald sie in einer Snowflake-Phase verfügbar sind.

Epen

Richte eine Snowflake Snowpipe ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CSV-Datei in Snowflake.	Melden Sie sich bei Snowflake an und führen Sie den `CREATE FILE FORMAT` Befehl aus, um eine CSV-Datei mit einem angegeben en Feldtrennzeichen zu erstellen. Weitere Informati onen zu diesem und anderen Snowflake-Befehlen finden	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie im Abschnitt Zusätzliche Informationen.	
Erstellen Sie eine externe Snowflake-Phase.	Führen Sie den `CREATE STAGE` Befehl aus, um einen externen Snowflake-Stagingbereich zu erstellen, der auf die zuvor erstellte CSV-Datei verweist. Wichtig: Sie benötigen die URL für den S3-Bucket, Ihren AWS Zugriffsschlüssel und Ihren AWS geheimen Zugriffsschlüssel. Führen Sie den `SHOW STAGES` Befehl aus, um zu überprüfen, ob die Snowflake-Phase erstellt wurde.	Developer
Erstellen Sie die Snowflake-Zieltabelle.	Führen Sie den `CREATE TABLE` Befehl aus, um die Snowflake-Tabelle zu erstellen.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Pipe.	Führen Sie den `CREATE PIPE` Befehl aus. Vergewissern Sie sich, dass er im Befehl enthalten `auto_ingest=true` ist. Führen Sie den `SHOW PIPES` Befehl aus, um zu überprüfen, ob die Pipe erstellt wurde. Kopieren und speichern Sie den `notification_channel` Spaltenwert. Dieser Wert wird verwendet, um Amazon S3 S3-Ereignisbenachrichtigungen zu konfigurieren.	Developer

Konfigurieren Sie den S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine 30-Tage-Lebenszyklusrichtlinie für den S3-Bucket.	Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon S3 S3-Konsole. Wählen Sie den S3-Bucket aus, der die Daten von Firehose enthält. Wählen Sie dann die Registerkarte Management im S3-Bucket und wählen Sie Lebenszyklusregel hinzufügen. Geben Sie im Dialogfeld „Lebenszyklusregel“ einen Namen für Ihre Regel ein und konfigurieren Sie eine 30-Tage-Lebenszyklusregel für Ihren	Systemadministrator, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bucket. Hilfe zu dieser und anderen Geschichten finden Sie im Abschnitt Verwandte Ressourcen.	
Erstellen Sie eine IAM-Richtlinie für den S3-Bucket.	Öffnen Sie die AWS Identity and Access Management (IAM-) Konsole und wählen Sie Richtlinien aus. Wählen Sie Richtlinie erstellen und anschließend die Registerkarte JSON. Kopieren Sie die Richtlinie aus dem Abschnitt Zusätzliche Informationen und fügen Sie sie in das JSON-Feld ein. Mit dieser Richtlinie werden `PutObject` sowohl `DeleteObject` Berechtigungen als auch `GetObject` , `GetObjectVersion` , und `ListBucket` Berechtigungen erteilt. Wählen Sie Richtlinie überprüfen, geben Sie einen Richtliniennamen ein und wählen Sie dann Richtlinie erstellen aus.	Systemadministrator, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Weisen Sie die Richtlinie einer IAM-Rolle zu.	Öffnen Sie die IAM-Konsole, wählen Sie Rollen und dann Rolle erstellen aus. Wählen Sie Ein anderes AWS-Konto als vertrauenswürdige Entität aus. Geben Sie Ihre AWS-Konto ID ein und wählen Sie Externe ID erforderlich aus. Geben Sie eine Platzhalter-ID ein, die Sie später ändern werden. Wählen Sie Weiter und weisen Sie die IAM-Richtlinie zu, die Sie zuvor erstellt haben. Erstellen Sie dann die IAM-Rolle.	Systemadministrator, Entwickler
Kopieren Sie den Amazon-Ressourcennamen (ARN) für die IAM-Rolle.	Öffnen Sie die IAM-Konsole und wählen Sie Rollen aus. Wählen Sie die IAM-Rolle aus, die Sie zuvor erstellt haben, und kopieren und speichern Sie dann den Rollen-ARN.	Systemadministrator, Entwickler

Richten Sie eine Speicherintegration in Snowflake ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Speicherintegration in Snowflake.	Melden Sie sich bei Snowflake an und führen Sie den Befehl aus. `CREATE STORAGE INTEGRATION` Dadurch wird die vertrauenswürdige Beziehung geändert, der Zugriff auf Snowflake gewährt	Systemadministrator, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und die externe ID für Ihre Snowflake-Phase bereitgestellt.	
Rufen Sie die IAM-Rolle für Ihr Snowflake-Konto ab.	Führen Sie den `DESC INTEGRATION` Befehl aus, um den ARN für die IAM-Rolle abzurufen. **Important** `<integration_name>` ist der Name der Snowflake-Speicherintegration, die Sie zuvor erstellt haben.	Systemadministrator, Entwickler
Notieren Sie zwei Spaltenwerte.	Kopieren und speichern Sie die Werte für die `storage_aws_external_id` Spalten `storage_aws_iam_user_arn` und.	Systemadministrator, Entwickler

Erlauben Sie Snowflake Snowpipe, auf den S3-Bucket zuzugreifen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die IAM-Rolle nrichtlinie.	Öffnen Sie die IAM-Konsole und wählen Sie Rollen aus. Wählen Sie die IAM-Rolle aus, die Sie zuvor erstellt haben, und klicken Sie auf die Registerkarte Vertrauen	Systemadministrator, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	sbeziehungen. Wählen Sie Vertrauensstellung bearbeite n aus. Ersetzen Sie ihn `snowflake_external _id` durch den `storage_a ws_external_id` Wert, den Sie zuvor kopiert haben. `snowflake_user_arn` Ersetzen Sie ihn durch den `storage_aws_iam_us er_arn` Wert, den Sie zuvor kopiert haben. Wählen Sie dann Vertrauensrichtlinie aktualisieren.	

Schalten Sie SNS-Benachrichtigungen für den S3-Bucket ein und konfigurieren Sie sie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie die Ereignisb enachrichtigungen für den S3-Bucket.	Öffnen Sie die Amazon S3 S3-Konsole und wählen Sie Ihren Bucket aus. Wählen Sie Eigenschaften und unter Erweiterte Einstellungen die Option Ereignisse aus. Wählen Sie Benachrichtigung hinzufügen und geben Sie einen Namen für dieses Ereignis ein. Wenn Sie keinen Namen eingeben, wird eine GUID (Globally Unique Identifier) verwendet.	Systemadministrator, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Amazon SNS SNS-Benachrichtigungen für den S3-Bucket.	Wählen Sie unter Ereignisse die Option ObjectCreate (Alle) und wählen Sie dann in der Dropdownliste Senden an die Option SQS-Warteschlange aus. Wählen Sie in der SNS-Liste die Option SQS-Warteschlange ARN hinzufügen aus und fügen Sie den zuvor kopierten `notification_channel` Wert ein. Wählen Sie dann Speichern.	Systemadministrator, Entwickler
Abonnieren Sie die Snowflake-SQS-Warteschlange für das SNS-Thema.	Abonnieren Sie die Snowflake-SQS-Warteschlange für das von Ihnen erstellte SNS-Thema. Hilfe zu diesem Schritt finden Sie im Abschnitt Verwandte Ressourcen.	Systemadministrator, Entwickler

Überprüfen Sie die Snowflake-Stage-Integration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen und testen Sie Snowpipe.	Melden Sie sich bei Snowflake an und öffnen Sie die Snowflake-Stufe. Legen Sie Dateien in Ihren S3-Bucket ab und überprüfen Sie, ob sie in der Snowflake-Tabelle geladen werden. Amazon S3 sendet SNS-Benachrichtigungen an Snowpipe, wenn	Systemadministrator, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	neue Objekte im S3-Bucket erscheinen.	

Zugehörige Ressourcen

- Verwalten Ihres Speicher-Lebenszyklus
- Abonnieren Sie die Snowflake-SQS-Warteschlange für das Amazon SNS SNS-Thema

Zusätzliche Informationen

Erstellen Sie ein Dateiformat:

```
CREATE FILE FORMAT <name>
TYPE = 'CSV'
FIELD_DELIMITER = '|'
SKIP_HEADER = 1;
```

Erstellen Sie eine externe Bühne:

```
externalStageParams (for Amazon S3) ::=
  URL = 's3://[//]'

  [ { STORAGE_INTEGRATION =  } | { CREDENTIALS = ( {  { AWS_KEY_ID = `` AWS_SECRET_KEY
 = `` [ AWS_TOKEN = `` ] } | AWS_ROLE = ``  } ) ) }` ]
  [ ENCRYPTION = ( [ TYPE = 'AWS_CSE' ] [ MASTER_KEY = '' ] |
                   [ TYPE = 'AWS_SSE_S3' ] |
                   [ TYPE = 'AWS_SSE_KMS' [ KMS_KEY_ID = '' ] |
                   [ TYPE = NONE ] )
```

Erstellen Sie eine Tabelle:

```
CREATE [ OR REPLACE ] [ { [ LOCAL | GLOBAL ] TEMP[ORARY] | VOLATILE } | TRANSIENT ]
 TABLE [ IF NOT EXISTS ]
  <table_name>
    ( <col_name> <col_type> [ { DEFAULT <expr>
                              | { AUTOINCREMENT | IDENTITY } [ ( <start_num> ,
 <step_num> ) | START <num> INCREMENT <num> ] } ]
```

```
                                /* AUTOINCREMENT / IDENTITY supported only for numeric
 data types (NUMBER, INT, etc.) */
                             [ inlineConstraint ]
     [ , <col_name> <col_type> ... ]
     [ , outoflineConstraint ]
     [ , ... ] )
  [ CLUSTER BY ( <expr> [ , <expr> , ... ] ) ]
  [ STAGE_FILE_FORMAT = ( { FORMAT_NAME = '<file_format_name>'
                           | TYPE = { CSV | JSON | AVRO | ORC | PARQUET | XML }
 [ formatTypeOptions ] } ) ]
  [ STAGE_COPY_OPTIONS = ( copyOptions ) ]
  [ DATA_RETENTION_TIME_IN_DAYS = <num> ]
  [ COPY GRANTS ]
  [ COMMENT = '<string_literal>' ]
```

Etappen anzeigen:

```
SHOW STAGES;
```

Erstellen Sie eine Pipe:

```
CREATE [ OR REPLACE ] PIPE [ IF NOT EXISTS ]
  [ AUTO_INGEST = [ TRUE | FALSE ] ]
  [ AWS_SNS_TOPIC =  ]
  [ INTEGRATION = '' ]
  [ COMMENT = '' ]
  AS
```

Rohre anzeigen:

```
SHOW PIPES [ LIKE '<pattern>' ]
           [ IN { ACCOUNT | [ DATABASE ] <db_name> | [ SCHEMA ] <schema_name> } ]
```

Erstellen Sie eine Speicherintegration:

```
CREATE STORAGE INTEGRATION <integration_name>
  TYPE = EXTERNAL_STAGE
  STORAGE_PROVIDER = S3
  ENABLED = TRUE
  STORAGE_AWS_ROLE_ARN = '<iam_role>'
  STORAGE_ALLOWED_LOCATIONS = ('s3://<bucket>/<path>/', 's3://<bucket>/<path>/')
```

```
  [ STORAGE_BLOCKED_LOCATIONS = ('s3://<bucket>/<path>/', 's3://<bucket>/<path>/') ]
```

Beispiel:

```
create storage integration s3_int
  type = external_stage
  storage_provider = s3
  enabled = true
  storage_aws_role_arn = 'arn:aws:iam::001234567890:role/myrole'
  storage_allowed_locations = ('s3://amzn-s3-demo-bucket1/mypath1/', 's3://amzn-s3-
demo-bucket2/mypath2/')
  storage_blocked_locations = ('s3://amzn-s3-demo-bucket1/mypath1/sensitivedata/',
 's3://amzn-s3-demo-bucket2/mypath2/sensitivedata/');
```

Weitere Informationen zu diesem Schritt finden Sie in der Snowflake-Dokumentation unter Konfiguration einer Snowflake-Speicherintegration für den Zugriff auf Amazon S3.

Beschreiben Sie eine Integration:

```
DESC INTEGRATION <integration_name>;
```

S3-Bucket-Richtlinie:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
              "s3:PutObject",
              "s3:GetObject",
              "s3:GetObjectVersion",
              "s3:DeleteObject",
              "s3:DeleteObjectVersion"
            ],
            "Resource": "arn:aws:s3:::/*"
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::",
            "Condition": {
```

```
                "StringLike": {
                    "s3:prefix": [
                        "/*"
                    ]
                }
            }
        }
    ]
}
```

Automatisches Verschlüsseln vorhandener und neuer Amazon EBS-Volumes

Erstellt von Tony DeMarco (AWS) und Josh Joy (AWS)

Übersicht

Die Verschlüsselung von Amazon Elastic Block Store (Amazon EBS) -Volumes ist wichtig für die Datenschutzstrategie eines Unternehmens. Dies ist ein wichtiger Schritt beim Aufbau einer gut strukturierten Umgebung. Es gibt zwar keine direkte Möglichkeit, vorhandene unverschlüsselte EBS-Volumes oder -Snapshots zu verschlüsseln, aber Sie können sie verschlüsseln, indem Sie ein neues Volume oder einen neuen Snapshot erstellen. Weitere Informationen finden Sie unter EBS-Ressourcen verschlüsseln in der EC2 Amazon-Dokumentation. Dieses Muster bietet präventive und detektive Kontrollen für die Verschlüsselung Ihrer EBS-Volumes, sowohl neuer als auch vorhandener. In diesem Muster konfigurieren Sie Kontoeinstellungen, erstellen automatisierte Behebungsprozesse und implementieren Zugriffskontrollen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS) -Konto
- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert auf macOS, Linux oder Windows
- jq, installiert und konfiguriert auf macOS, Linux oder Windows
- AWS Identity and Access Management (IAM) -Berechtigungen werden für Lese- und Schreibzugriff auf AWS CloudFormation, Amazon Elastic Compute Cloud (Amazon EC2), AWS Systems Manager, AWS Config und AWS Key Management Service (AWS KMS) bereitgestellt.
- AWS Organizations ist so konfiguriert, dass alle Funktionen aktiviert sind, eine Voraussetzung für Service-Kontrollrichtlinien
- AWS Config ist in den Zielkonten aktiviert

Einschränkungen

- In Ihrem AWS-Zielkonto darf es keine AWS Config-Regeln mit dem Namen encrypted-volumes geben. Diese Lösung stellt eine Regel mit diesem Namen bereit. Bereits bestehende Regeln mit

diesem Namen können dazu führen, dass die Bereitstellung fehlschlägt und unnötige Kosten für die mehrfache Verarbeitung derselben Regel anfallen.

- Diese Lösung verschlüsselt alle EBS-Volumes mit demselben AWS-KMS-Schlüssel.
- Wenn Sie die Verschlüsselung von EBS-Volumes für das Konto aktivieren, ist diese Einstellung regionsspezifisch. Wenn Sie es für eine AWS-Region aktivieren, können Sie es nicht für einzelne Volumes oder Snapshots in dieser Region deaktivieren. Weitere Informationen finden Sie unter Standardverschlüsselung in der EC2 Amazon-Dokumentation.
- Wenn Sie bestehende, unverschlüsselte EBS-Volumes korrigieren, stellen Sie sicher, dass die EC2 Instance nicht verwendet wird. Durch diese Automatisierung wird die Instance heruntergefahren, um das unverschlüsselte Volume zu trennen und das verschlüsselte Volume anzuhängen. Während der Problembehebung kommt es zu Ausfallzeiten. Wenn es sich um einen kritischen Teil der Infrastruktur für Ihr Unternehmen handelt, stellen Sie sicher, dass manuelle oder automatische Hochverfügbarkeitskonfigurationen vorhanden sind, damit die Verfügbarkeit der auf der Instanz ausgeführten Anwendungen nicht beeinträchtigt wird. Wir empfehlen, kritische Ressourcen nur während der standardmäßigen Wartungsfenster zu reparieren.

Architektur

Arbeitsablauf bei der Automatisierung

1. AWS Config erkennt ein unverschlüsseltes EBS-Volume.
2. Ein Administrator verwendet AWS Config, um einen Behebungsbefehl an Systems Manager zu senden.
3. Die Systems Manager Manager-Automatisierung erstellt einen Snapshot des unverschlüsselten EBS-Volumes.
4. Die Systems Manager Manager-Automatisierung verwendet AWS KMS, um eine verschlüsselte Kopie des Snapshots zu erstellen.
5. Die Systems Manager Manager-Automatisierung macht Folgendes:
   a. Stoppt die betroffene EC2 Instanz, falls sie läuft
   b. Hängt die neue, verschlüsselte Kopie des Volumes an die EC2 Instance an
   c. Setzt die EC2 Instanz in ihren ursprünglichen Zustand zurück

Tools

AWS-Services

- AWS CLI — Die AWS-Befehlszeilenschnittstelle (AWS CLI) bietet direkten Zugriff auf die öffentlichen Anwendungsprogrammierschnittstellen (APIs) der AWS-Services. Sie können die Funktionen eines Services mit der AWS-CLI erkunden und Shell-Skripts zur Verwaltung Ihrer Ressourcen entwickeln. Zusätzlich zu den API-äquivalenten Low-Level-Befehlen bieten mehrere AWS-Services Anpassungen für die AWS-CLI. Anpassungen können Befehle auf einer höheren Ebene enthalten, die die Verwendung eines Services durch eine komplexe API vereinfachen.
- AWS CloudFormation — AWS CloudFormation ist ein Service, der Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen unterstützt. Sie erstellen eine Vorlage, die alle gewünschten AWS-Ressourcen beschreibt (z. B. EC2 Amazon-Instances) und diese Ressourcen für Sie CloudFormation bereitstellt und konfiguriert.
- AWS Config — AWS Config bietet eine detaillierte Ansicht der Konfiguration der AWS-Ressourcen in Ihrem AWS-Konto. Dazu gehört auch, wie die Ressourcen jeweils zueinander in Beziehung stehen und wie sie in der Vergangenheit konfiguriert wurden, damit Sie sehen können, wie sich die Konfigurationen und Beziehungen im Laufe der Zeit verändern.
- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) ist ein Webservice, der skalierbare Rechenkapazität bietet, die Sie zum Erstellen und Hosten Ihrer Softwaresysteme verwenden.
- AWS KMS — AWS Key Management Service (AWS KMS) ist ein für die Cloud skalierter Verschlüsselungs- und Schlüsselverwaltungsservice. AWS-KMS-Schlüssel und -Funktionen werden von anderen AWS-Services verwendet, und Sie können sie zum Schutz von Daten in Ihrer AWS-Umgebung verwenden.
- AWS Organizations — AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten.
- AWS Systems Manager Automation — Systems Manager Automation vereinfacht allgemeine Wartungs- und Bereitstellungsaufgaben für EC2 Amazon-Instances und andere AWS-Ressourcen.

Andere Dienste

- jq — jq ist ein leichter und flexibler Befehlszeilen-JSON-Prozessor. Sie verwenden dieses Tool, um wichtige Informationen aus der AWS-CLI-Ausgabe zu extrahieren.

Code

- Der Code für dieses Muster ist im Repository GitHub Automatisches Korrigieren unverschlüsselter EBS-Volumes mithilfe von Kunden-KMS-Schlüsseln verfügbar.

Epen

Automatisieren Sie die Wiederherstellung unverschlüsselter Volumes

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie Skripte und CloudFormation Vorlagen herunter.	Laden Sie das Shell-Skript, die JSON-Datei und die CloudFormation Vorlagen aus dem Repository GitHub Automatisches Korrigieren unverschlüsselter EBS-Volumes mithilfe von Kunden-KMS-Schlüsseln herunter.	AWS-Administrator, Allgemeines AWS
Identifizieren Sie den Administrator für den AWS-KMS-Schlüssel.	1. Melden Sie sich in der AWS-Managementkonsole an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/. 2. Identifizieren Sie einen Benutzer oder eine Rolle, der der AWS KMS KMS-Schlüsseladministrator sein wird. Wenn zu diesem Zweck ein neuer Benutzer oder eine neue Rolle erstellt werden muss, erstellen Sie sie jetzt. Weitere Informationen finden Sie unter IAM-Identitäten in der IAM-Dokumentation. Diese Automatisierung erstellt	AWS-Administrator, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	einen neuen AWS-KMS-S chlüssel. 3. Sobald Sie identifiziert sind, kopieren Sie den Amazon-Ressourcennamen (ARN) des Benutzers oder der Rolle. Weitere Informati onen finden Sie unter IAM ARNs in der IAM-Dokum entation. Sie verwenden diesen ARN im nächsten Schritt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Stack1-Vorlage CloudFormation bereit.	1. Öffnen Sie die CloudFormation AWS-Konsole unter https://console.aws.amazon.com/cloudformation/. 2. Stellen CloudFormation Sie die `Stack1.yaml` Vorlage bereit. Beachten Sie die folgenden Bereitstellungsdetails: • Geben Sie dem Stapel einen klaren und aussagekräftigen Namen. Notieren Sie sich den Stacknamen, da Sie diesen Wert im nächsten Schritt benötigen. • Fügen Sie den ARN des Schlüsseladministrators in das einzige Parameterfeld in Stack1 ein. Dieser Benutzer oder diese Rolle wird zum Administrator für den vom Stack erstellten AWS-KMS-Schlüssel. Weitere Informationen zur Bereitstellung einer CloudFormation Vorlage finden Sie in der CloudFormation Dokumentation unter	AWS-Administrator, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Arbeiten mit CloudFormation AWS-Vorlagen.	
Stellen Sie die Stack2-Vorlage CloudFormation bereit.	Stellen Sie CloudFormation die Vorlage bereit. `Stack2.yaml` Beachten Sie die folgenden Bereitstellungsdetails: • Geben Sie dem Stapel einen klaren und aussagekräftigen Namen. • Geben Sie für den einzigen Parameter von Stack2 den Namen des Stacks ein, den Sie im vorherigen Schritt erstellt haben. Dadurch kann Stack2 auf den neuen AWS-KMS-Schlüssel und die neue Rolle verweisen, die im vorherigen Schritt vom Stack bereitgestellt wurden.	AWS-Administrator, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein unverschlüsseltes Volume zum Testen.	Erstellen Sie eine EC2 Instanz mit einem unverschlüsselten EBS-Volume. Anweisungen finden Sie in der EC2 Amazon-Dokumentation unter Erstellen eines Amazon EBS-Volumes. Der Instance-Typ spielt keine Rolle, und der Zugriff auf die Instance ist nicht erforderlich. Sie können eine t2.micro-Instance erstellen, um im kostenlosen Kontingent zu bleiben, und Sie müssen kein key pair erstellen.	AWS-Administrator, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die AWS Config-Regel.	1. Öffnen Sie die AWS Config-Konsole unter https://console.aws.amazon.com/config/. Wählen Sie auf der Seite Regeln die Regel für verschlüsselte Volumes aus. 2. Vergewissern Sie sich, dass Ihre neue, unverschlüsselte Testinstanz in der Liste der nicht konformen Ressourcen erscheint. Wenn das Volume nicht sofort angezeigt wird, warten Sie einige Minuten und aktualisieren Sie die Ergebnisse. Die AWS Config-Regel erkennt die Ressourcenänderungen kurz nach der Erstellung der Instance und des Volumes. 3. Wählen Sie die Ressource und dann Remediate aus. Sie können den Fortschritt und den Status der Behebung in Systems Manager wie folgt anzeigen: 1. Öffnen Sie die AWS Systems Manager Manager-Konsole unter https://console.aws.amazon.com/systems-manager/.	AWS-Administrator, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Klicken Sie im Navigationsbereich auf Automation. 3. Wählen Sie den Link Execution ID, um die Schritte und den Status anzuzeigen.	
Konfigurieren Sie zusätzliche Konten oder AWS-Regionen.	Je nach Bedarf für Ihren Anwendungsfall wiederholen Sie diesen Vorgang für alle weiteren Konten oder AWS-Regionen.	AWS-Administrator, Allgemeines AWS

Aktivieren Sie die Verschlüsselung von EBS-Volumes auf Kontoebene

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das Aktivierungsskript aus.	1. Verwenden Sie in einer Bash-Shell den `cd` Befehl, um zum geklonten Repository zu navigieren. 2. Geben Sie den folgenden Befehl ein, um das `enable-ebs-encryption-for-account -` Skript auszuführen. `./Bash/enable-ebs-encryption-for-account.sh`	AWS-Administrator, Allgemeines AWS, Bash
Vergewissern Sie sich, dass die Einstellungen aktualisiert wurden.	1. Öffnen Sie die EC2 Amazon-Konsole unter	AWS-Administrator, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	https://console.aws.amazon.com/ec2/. 2. Wählen Sie auf der rechten Seite des Bildschirms unter Einstellungen die Option Datenschutz und Sicherheit aus. 3. Vergewissern Sie sich im Abschnitt EBS-Verschlüsselung, dass Neue EBS-Volumes immer verschlüsseln aktiviert ist und dass der Standard-Verschlüsselungsschlüssel auf den zuvor angegebenen ARN gesetzt ist. **Note** Wenn die Einstellung Neue EBS-Volumes immer verschlüsseln deaktiviert ist oder der Schlüssel immer noch auf gesetzt ist, vergewissern Sie sich alias/aws/ebs, dass Sie bei demselben Konto und derselben AWS-Region angemeldet sind, in der Sie das Shell-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Skript ausgeführ t haben, und überprüfen Sie Ihre Shell auf Fehlermel dungen.	
Konfigurieren Sie zusätzliche Konten oder AWS-Regionen.	Je nach Bedarf für Ihren Anwendungsfall wiederholen Sie diesen Vorgang für alle weiteren Konten oder AWS-Regionen.	AWS-Administrator, Allgemein es AWS

Verhindern Sie die Erstellung unverschlüsselter Instanzen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Richtlinie zur Servicesteuerung.	1. Öffnen Sie die AWS Organizations Organizat ions-Konsole in Version https://console.aw s.amazon.com/organ izations/2/. 2. Erstellen Sie eine neue Richtlinie zur Servicest euerung. Weitere Informati onen finden Sie in der Dokumentation zu AWS Organizations unter Creating a Service Control Policy. 3. Fügen Sie den Inhalt von `DenyUnencryptedEC2 .json` zur Richtlinie hinzu	AWS-Administrator, Allgemein es AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und speichern Sie sie. Sie haben diese JSON-Datei im ersten Epos aus dem GitHub Repository heruntergeladen. 4. Hängen Sie diese Richtlinie an das Stammverzeichnis der Organisation oder an alle erforderlichen Organisationseinheiten an (OUs). Weitere Informationen finden Sie unter Servicesteuerungsrichtlinien anhängen und trennen in der Dokumentation zu AWS Organizations.	

Zugehörige Ressourcen

AWS-Servicedokumentation

- AWS-CLI
- AWS Config
- AWS CloudFormation
- Amazon EC2
- AWS KMS
- AWS Organizations
- AWS Systems Manager Automation

Sonstige Ressourcen

- jq-Handbuch (jq-Website)
- jq herunterladen () GitHub

Sun SPARC-Server im Stromasys Charon-SSP-Emulator in der AWS-Cloud sichern

Erstellt von Kevin Yung (AWS), Luis Ramos (Stromasys) und Rohit Darji (AWS)

Übersicht

Dieses Muster bietet vier Optionen für die Sicherung Ihrer Sun Microsystems SPARC-Server nach einer Migration von einer lokalen Umgebung zur Amazon Web Services (AWS) Cloud. Diese Backup-Optionen helfen Ihnen bei der Implementierung eines Backup-Plans, der die Recovery Point Objective (RPO) und Recovery Time Objective (RTO) Ihres Unternehmens erfüllt, automatisierte Ansätze verwendet und Ihre Gesamtbetriebskosten senkt. Das Muster bietet einen Überblick über die vier Backup-Optionen und die Schritte zu ihrer Implementierung.

Wenn Sie einen Sun SPARC-Server verwenden, der als Gast auf einem Stromasys Charon-SSP-Emulator gehostet wird, können Sie eine der folgenden drei Backup-Optionen verwenden:

- Backup-Option 1: Virtuelles Stromasys-Band — Verwenden Sie die Charon-SSP-Funktion für virtuelle Bänder, um eine Backup-Einrichtung auf dem Sun SPARC-Server einzurichten und Ihre Sicherungsdateien mithilfe von AWS Systems Manager Automation auf Amazon Simple Storage Service (Amazon S3) und AmazonSimple Storage Service Glacier zu archivieren.
- Backup-Option 2: Stromasys-Snapshot — Verwenden Sie die Charon-SSP-Snapshot-Funktion, um eine Backup-Einrichtung für die Sun SPARC-Gastserver in Charon-SSP einzurichten.
- Backup-Option 3: Amazon Elastic Block Store (Amazon EBS) -Volume-Snapshot — Wenn Sie den Charon-SSP-Emulator auf Amazon Elastic Compute Cloud (Amazon EC2) hosten, können Sie einen Amazon EBS-Volume-Snapshot verwenden, um Backups für ein Sun SPARC-Dateisystem zu erstellen.

Wenn Sie einen Sun SPARC-Server verwenden, der als Gast auf Hardware und Charon-SSP auf Amazon gehostet wird EC2, können Sie die folgende Backup-Option verwenden:

- Backup-Option 4: AWS Storage Gateway Virtual Tape Library (VTL) — Verwenden Sie eine Backup-Anwendung mit einem Storage Gateway VTL Tape Gateway, um die Sun SPARC-Server zu sichern.

Wenn Sie einen Sun SPARC-Server verwenden, der als Branded Zone auf einem Sun SPARC-Server gehostet wird, können Sie die Backup-Optionen 1, 2 und 4 verwenden.

Stromasys bietet Software und Dienste zur Emulation älterer kritischer SPARC-, Alpha-, VAX- und PA-RISC-Systeme. Weitere Informationen zur Migration zur AWS-Cloud mithilfe der Stromasys-Emulation finden Sie im AWS-Blog unter Rehosting von SPARC-, Alpha- oder anderen Legacy-Systemen auf AWS mit Stromasys.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Bestehende Sun SPARC-Server.
- Bestehende Lizenzen für Charon-SSP. Lizenzen für Charon-SSP sind auf dem AWS Marketplace erhältlich und Lizenzen für Stromasys Virtual Environment (VE) sind bei Stromasys erhältlich. Für weitere Informationen wenden Sie sich an den Vertrieb von Stromasys.
- Vertrautheit mit Sun SPARC-Servern und Linux-Backups
- Vertrautheit mit der Charon-SSP-Emulationstechnologie. Weitere Informationen dazu finden Sie unter Stromasys Legacy-Server-Emulation in der Stromasys-Dokumentation.
- Wenn Sie die virtuelle Bandanlage oder Backup-Anwendungen für Ihre Sun SPARC-Serverdateisysteme verwenden möchten, müssen Sie die Backup-Einrichtungen für das Sun SPARC-Serverdateisystem erstellen und konfigurieren.
- Ein Verständnis von RPO und RTO. Weitere Informationen dazu finden Sie unter Disaster Recovery Objectives aus dem Whitepaper Reliability Pillar in der Dokumentation zum AWS Well-Architected Framework.
- Um Backup-Option 4 verwenden zu können, müssen Sie über Folgendes verfügen:
  - Eine softwarebasierte Backup-Anwendung, die ein Storage Gateway VTL Tape Gateway unterstützt. Weitere Informationen dazu finden Sie unter Arbeiten mit VTL-Geräten in der AWS Storage Gateway Gateway-Dokumentation.
  - Bacula Director oder eine ähnliche Backup-Anwendung, installiert und konfiguriert. Weitere Informationen dazu finden Sie in der Bacula Director-Dokumentation.

Die folgende Tabelle enthält Informationen zu den vier Backup-Optionen in diesem Muster.

Backup-Optionen	Erreicht Absturzkonsistenz?	Erreicht Anwendungskonsistenz?	Virtuelle Backup-Appliance-Lösung?	Typische Anwendungsfälle

Option 1 — Virtuelles Stromasys-Band	Ja Sie können Sun SPARC-Dateisystem-Snapshots automatisieren, um Daten auf einem virtuellen Band zu sichern. Sie können beispielsweise UFS- oder ZFS-Snapshots verwenden.	Ja Für diese Backup-Option ist ein automatisiertes Skript erforderlich, um laufende Transaktionen zu leeren, während des Dateisystem-Snapshots einen schreibgeschützten oder temporären Offline-Modus zu konfigurieren oder einen Anwendungsdaten-Dump zu erstellen. Möglicherweise benötigen Sie auch eine Ausfallzeit der Anwendung oder den Nur-Lese-Modus.	Ja	Sicherung von Sun SPARC-Serverdateisystemen mit .tar- oder .zip-Dateien Sicherung von Anwendungsdaten

Option 2 — Stromasys-Snapshot	Ja Sie müssen Charon-SSP Manager konfigurieren oder ein Startargument in der Befehlszeile verwenden, um diese Funktion zu aktivieren. Sie müssen außerdem einen Linux-Befehl ausführen, um den Charon-SSP-Emulator aufzufordern, den Sun SPARC-Gastserverstatus in einer Snapshot-Datei zu speichern. ⚠ Important Sie müssen den Sun SPARC-Gastserver	Ja Diese Backup-Option erstellt einen Snapshot des emulierten Gastservers, einschließlich seiner virtuellen Festplatten und seines Speicherabbilds. ⚠ Important Sie müssen den Sun SPARC-Gastserver während des Snapshots herunterfahren.	Nein	Sun SPARC-Server-Snapshot Sicherung der Anwendungsdaten

herunterf
ahren.

Option 3 — Amazon EBS-Volume-Snapshot	Ja Sie können AWS Backup verwenden, um den Amazon EBS-Snapshot zu automatisieren.	Ja Für diese Backup-Option ist ein automatisiertes Skript erforderlich, um laufende Transaktionen zu löschen und einen schreibgeschützten oder temporären Stopp der EC2 Instance während des Amazon EBS-Volume-Snapshots zu konfigurieren. **Important** Für diese Backup-Option ist möglicherweise eine Ausfallzeit der Anwendung oder ein Nur-Lese-Modus erforderl	Nein	Snapshot der Sun SPARC-Serverdateisysteme Sicherung von Anwendungsdaten

ich, um die Anwendungskonsistenz zu gewährleisten.

Option 4 — AWS Storage Gateway VTL	Ja Sie können mithilfe eines Backup-Agenten automatisch Backup-Daten des Sun SPARC-Dateisystems auf der VTL sichern.	Ja Für diese Backup-Option ist ein automatisiertes Skript erforderlich, um während des Dateisystem-Snapshots oder des Anwendungsdatendumps laufende Transaktionen zu löschen und einen schreibgeschützten oder temporären Offline-Modus zu konfigurieren. **Important** Für diese Backup-Option ist möglicherweise ein Ausfall der Anwendung oder ein Nur-Lese-Modus	Ja	Eine große Flotte von Sun SPARC-Serverdateisystem-Backups Sicherung von Anwendungsdaten

erforderl
ich.

Einschränkungen

- Sie können die Methoden dieses Musters verwenden, um einzelne Sun SPARC-Server zu sichern, aber Sie können diese Sicherungsoptionen auch für gemeinsam genutzte Daten verwenden, wenn Sie Anwendungen haben, die in einem Cluster ausgeführt werden.

Tools

Backup-Option 1: Virtuelles Stromasys-Band

- Stromasys Charon-SSP-Emulator — Der Charon-SSP-Emulator erstellt das virtuelle Replikat der ursprünglichen SPARC-Hardware in einem standardmäßigen 64-Bit-x86-kompatiblen Computersystem. Er führt den ursprünglichen SPARC-Binärcode aus, einschließlich Betriebssystemen (OSs) wie SunOS oder Solaris, deren mehrschichtigen Produkten und Anwendungen.
- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) ist ein Webservice, der skalierbare Rechenkapazität bietet, die Sie zum Erstellen und Hosten Ihrer Softwaresysteme verwenden.
- Amazon EFS — Amazon Elastic File System (Amazon EFS) bietet ein einfaches, serverloses, set-and-forget elastisches Dateisystem zur Verwendung mit AWS-Cloud-Services und lokalen Ressourcen.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Speicher für das Internet.
- Amazon S3 Glacier — Amazon Simple Storage Service Glacier ist eine sichere, langlebige und extrem kostengünstige Amazon S3 S3-Speicherklasse für Datenarchivierung und Langzeitsicherung.
- AWS Systems Manager Automation — Automation, eine Funktion von AWS Systems Manager, vereinfacht allgemeine Wartungs- und Bereitstellungsaufgaben von EC2 Instances und anderen AWS-Ressourcen.

Backup-Option 2: Stromasys-Snapshot

- Stromasys Charon-SSP-Emulator — Der Charon-SSP-Emulator erstellt das virtuelle Replikat der ursprünglichen SPARC-Hardware in einem standardmäßigen 64-Bit-x86-kompatiblen Computersystem. Er führt den ursprünglichen SPARC-Binärcode aus, einschließlich OSs SunOS oder Solaris, ihrer mehrschichtigen Produkte und Anwendungen.
- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) ist ein Webservice, der skalierbare Rechenkapazität bietet, die Sie zum Erstellen und Hosten Ihrer Softwaresysteme verwenden.
- Amazon EFS — Amazon Elastic File System (Amazon EFS) bietet ein einfaches, serverloses, set-and-forget elastisches Dateisystem zur Verwendung mit AWS-Cloud-Services und lokalen Ressourcen.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Speicher für das Internet.
- Amazon S3 Glacier — Amazon Simple Storage Service Glacier ist eine sichere, langlebige und extrem kostengünstige Amazon S3 S3-Speicherklasse für Datenarchivierung und Langzeitsicherung.
- AWS Systems Manager Automation — Automation, eine Funktion von AWS Systems Manager, vereinfacht allgemeine Wartungs- und Bereitstellungsaufgaben von EC2 Instances und anderen AWS-Ressourcen.

Backup-Option 3: Amazon EBS-Volume-Snapshot

- Stromasys Charon-SSP-Emulator — Der Charon-SSP-Emulator erstellt das virtuelle Replikat der ursprünglichen SPARC-Hardware in einem standardmäßigen 64-Bit-x86-kompatiblen Computersystem. Er führt den ursprünglichen SPARC-Binärcode aus, einschließlich OSs SunOS oder Solaris, ihrer mehrschichtigen Produkte und Anwendungen.
- AWS Backup — AWS Backup ist ein vollständig verwalteter Datenschutzservice, der die Zentralisierung und Automatisierung aller AWS-Services, in der Cloud und vor Ort vereinfacht.
- Amazon EBS — Amazon Elastic Block Store (Amazon EBS) bietet Speichervolumen auf Blockebene zur Verwendung mit EC2 Instances.
- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) ist ein Webservice, der skalierbare Rechenkapazität bietet, die Sie zum Erstellen und Hosten Ihrer Softwaresysteme verwenden.

Sicherungsoption 4: AWS Storage Gateway VTL

- Stromasys Charon-SSP-Emulator — Der Charon-SSP-Emulator erstellt das virtuelle Replikat der ursprünglichen SPARC-Hardware in einem standardmäßigen 64-Bit-x86-kompatiblen Computersystem. Er führt den ursprünglichen SPARC-Binärcode aus, einschließlich OSs SunOS oder Solaris, ihrer mehrschichtigen Produkte und Anwendungen.
- Bacula — Bacula ist ein Open-Source-Computer-Backup-System auf Unternehmensebene. Weitere Informationen darüber, ob Ihre bestehende Backup-Anwendung Tape Gateway unterstützt, finden Sie unter Unterstützte Backup-Anwendungen von Drittanbietern für ein Tape Gateway in der AWS Storage Gateway Gateway-Dokumentation.
- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) ist ein Webservice, der skalierbare Rechenkapazität bietet, die Sie zum Erstellen und Hosten Ihrer Softwaresysteme verwenden.
- Amazon RDS for MySQL — Amazon Relational Database Service (Amazon RDS) unterstützt DB-Instances, auf denen mehrere Versionen von MySQL ausgeführt werden.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Speicher für das Internet.
- Amazon S3 Glacier — Amazon Simple Storage Service Glacier ist eine sichere, langlebige und extrem kostengünstige Amazon S3 S3-Speicherklasse für Datenarchivierung und Langzeitsicherung.
- AWS Storage Gateway — Storage Gateway verbindet eine lokale Software-Appliance mit cloudbasiertem Speicher, um eine nahtlose Integration mit Datensicherheitsfunktionen zwischen Ihrer lokalen IT-Umgebung und der AWS-Speicherinfrastruktur zu ermöglichen.

Epen

Backup-Option 1 — Erstellen Sie ein virtuelles Stromasys-Band-Backup

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein gemeinsam genutztes Amazon EFS-Datei system für die Speicherung virtueller Banddateien.	Melden Sie sich bei der AWS-Managementkonsole an oder verwenden Sie die AWS-CLI, um ein Amazon EFS-Datei system zu erstellen. Weitere Informationen dazu finden Sie unter Erstellen eines Amazon EFS-Datei	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	systems in der Amazon EFS-Dokumentation.	
Konfigurieren Sie den Linux-Host so, dass er das gemeinsam genutzte Dateisystem mountet.	Installieren Sie den Amazon EFS-Treiber auf der Amazon EC2 Linux-Instance und konfigurieren Sie das Linux-Betriebssystem so, dass das gemeinsam genutzte Amazon EFS-Dateisystem beim Start bereitgestellt wird. Weitere Informationen dazu finden Sie unter Mounten von Dateisystemen mithilfe des EFS-Mount-Helpers in der Amazon EFS-Dokumentation.	DevOps Ingenieur
Installieren Sie den Charon-SSP Emulator.	Installieren Sie den Charon-SSP-Emulator auf der Amazon Linux-Instance. EC2 Weitere Informationen dazu finden Sie unter Einrichten einer AWS-Cloud-Instanz für Charon-SSP in der Stromasys -Dokumentation.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie für jeden Sun SPARC-Gastserver einen virtuellen Banddateicontainer im gemeinsam genutzten Dateisystem.	Führen Sie den `touch <vtape-container-name>` Befehl aus, um einen virtuellen Banddatei container im gemeinsam genutzten Dateisystem für jeden Sun SPARC-Gastserver zu erstellen, der im Charon-SSP-Emulator bereitgestellt wird.	DevOps Ingenieur
Konfigurieren Sie Charon-SSP Manager so, dass virtuelle Bandgeräte für die Sun SPARC-Gastserver erstellt werden.	Melden Sie sich bei Charon-SSP Manager an, erstellen Sie virtuelle Bandgeräte und konfigurieren Sie sie so, dass sie die virtuellen Bandcontainerdateien für jeden Sun SPARC-Gastserver verwenden. Weitere Informationen dazu finden Sie im Charon-SSP 5.2 für Linux-Benutzerhandbuch in der Stromasys-Dokumentation.	DevOps Ingenieur
Stellen Sie sicher, dass das virtuelle Bandgerät auf den Sun SPARC-Gastservern verfügbar ist.	Melden Sie sich bei jedem Sun SPARC-Gastserver an und führen Sie den `mt -f /dev/rmt/1` Befehl aus, um zu überprüfen, ob das virtuelle Bandgerät im Betriebssystem konfiguriert ist.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entwickeln Sie das Systems Manager Automation-Runbook und die Automatisierung.	Entwickeln Sie das Systems Manager Automation-Runbook und richten Sie Wartungsfenster und Verknüpfungen in Systems Manager ein, um den Backup-Prozess zu planen. Weitere Informationen dazu finden Sie unter Exemplarische Vorgehensweisen zur Automatisierung und Einrichtung von Wartungsfenstern in der Dokumentation zu AWS Systems Manager.	Cloud-Architekt
Konfigurieren Sie Systems Manager Automation so, dass rotierte virtuelle Bandcontainerdateien archiviert werden.	Verwenden Sie das Codebeispiel aus Back-Option 1 im Abschnitt Zusätzliche Informationen, um ein Systems Manager Automation-Runbook zu entwickeln, mit dem rotierte virtuelle Bandcontainerdateien in Amazon S3 und Amazon S3 Glacier archiviert werden können.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie das Systems Manager Automation-Runbook für Archivierung und Planung bereit.	Stellen Sie das Systems Manager Automation-Runbook bereit und planen Sie, dass es automatisch in Systems Manager ausgeführt wird. Weitere Informationen dazu finden Sie unter Exemplarische Vorgehensweisen zur Automatisierung in der Systems Manager Manager-Dokumentation.	Cloud-Architekt

Backup-Option 2 — Einen Stromasys-Snapshot erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein gemeinsam genutztes Amazon EFS-Dateisystem für die Speicherung virtueller Banddateien.	Melden Sie sich bei der AWS-Managementkonsole an oder verwenden Sie die AWS-CLI, um ein Amazon EFS-Dateisystem zu erstellen. Weitere Informationen dazu finden Sie unter Erstellen Sie Ihr Amazon EFS-Dateisystem in der Amazon EFS-Dokumentation.	Cloud-Architekt
Konfigurieren Sie den Linux-Host so, dass er das gemeinsam genutzte Dateisystem mountet.	Installieren Sie den Amazon EFS-Treiber in der Amazon EC2 Linux-Instance und konfigurieren Sie das Linux-Betriebssystem so, dass das gemeinsam genutzte Amazon	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	EFS-Dateisystem beim Start bereitgestellt wird. Weitere Informationen dazu finden Sie unter Mounten von Dateisystemen mithilfe des EFS-Mount-Helpers in der Amazon EFS-Dokumentation.	
Installieren Sie den Charon-SSP Emulator.	Installieren Sie den Charon-SSP-Emulator auf der Amazon Linux-Instance. EC2 Weitere Informationen dazu finden Sie unter Einrichten einer AWS-Cloud-Instanz für Charon-SSP in der Stromasys -Dokumentation.	DevOps Ingenieur
Konfigurieren Sie die Sun SPARC-Gastserver so, dass sie mit der Snapshot-Option gestartet werden.	Verwenden Sie Charon-SSP Manager, um die Snapshot-Option für jeden Sun SPARC-Gastserver einzurichten. Weitere Informationen dazu finden Sie im Charon-SSP 5.2 für Linux-Benutzerhandbuch in der Stromasys-Dokument ation.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entwickeln Sie das Systems Manager Automation-Runbook .	Verwenden Sie das Codebeispiel aus Backup-Option 2 im Abschnitt Zusätzliche Informationen, um ein Systems Manager Automation-Runbook zu entwickeln, mit dem der Snapshot-Befehl während eines Wartungsfensters remote auf einem Sun SPARC-Gastserver ausgeführt werden kann.	Cloud-Architekt
Stellen Sie das Systems Manager Automation-Runbook bereit und richten Sie die Zuordnung zu den Amazon EC2 Linux-Hosts ein.	Stellen Sie das Systems Manager Automation-Runbook bereit und richten Sie Wartungsfenster und Verknüpfungen in Systems Manager ein, um den Sicherungsvorgang zu planen. Weitere Informationen dazu finden Sie unter Exemplarische Vorgehensweisen zur Automatisierung und Einrichten von Wartungsfenstern in der Dokumentation zu AWS Systems Manager.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Archivieren Sie Schnappsc hüsse im Langzeitspeicher.	Verwenden Sie den Runbook-Beispielcode aus dem Abschnitt Zusätzliche Informati onen, um ein Systems Manager Automation-Runbook zur Archivierung von Snapshot-Dateien in Amazon S3 und Amazon S3 Glacier zu entwickeln.	Cloud-Architekt

Backup-Option 3 — Erstellen Sie einen Amazon EBS-Volume-Snapshot

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den Charon-SSP-Emulator.	Installieren Sie den Charon-SSP-Emulator auf der Amazon Linux-Instance. EC2 Weitere Informationen dazu finden Sie unter Einrichten einer AWS-Cloud-Instanz für Charon-SSP in der Stromasys -Dokumentation.	DevOps Ingenieur
Erstellen Sie EBS-Volumes für die Sun SPRAC-Gastserver.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon EBS-Konsole und erstellen Sie dann EBS-Volumes für die Sun SPRAC-Gastserver. Weitere Informationen dazu finden Sie unter Einrichten einer AWS-Cloud-Instanz für	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Charon-SSP in der Stromasys -Dokumentation.	
Hängen Sie die EBS-Volumes an die Amazon EC2 Linux-Instance an.	Hängen Sie auf der EC2 Amazon-Konsole die EBS-Volumes an die Amazon EC2 Linux-Instance an. Weitere Informationen dazu finden Sie in der EC2 Amazon-Dokumentation unter Ein Amazon EBS-Volume an eine Instance anhängen.	AWS DevOps
Ordnen Sie EBS-Volumes im Charon-SSP-Emulator als SCSI-Laufwerke zu.	Konfigurieren Sie Charon-SSP Manager so, dass die EBS-Volumes als SCSI-Laufwerke auf den Sun SPARC-Gastservern zugeordnet werden. Weitere Informationen dazu finden Sie im Abschnitt zur SCSI-Speicherkonfiguration im Handbuch Charon-SSP V5.2 für Linux in der Stromasys-Dokumentation.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den AWS-Backup-Zeitplan für die Erstellung von Snapshots der EBS-Volumes.	Richten Sie AWS-Backup-Richtlinien und Zeitpläne für Snapshots der EBS-Volumes ein. Weitere Informationen dazu finden Sie im Tutorial Amazon EBS Backup and Restore using AWS Backup in der AWS Developer Center-Do kumentation.	AWS DevOps

Backup-Option 4 — Erstellen Sie eine AWS Storage Gateway Gateway-VTL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Tape Gateway-Gerät.	Melden Sie sich bei der AWS-Managementkons ole an, öffnen Sie die AWS Storage Gateway-Konsole und erstellen Sie dann ein Tape Gateway-Gerät in einer VPC. Weitere Informationen dazu finden Sie unter Creating a Gateway in der AWS Storage Gateway Gateway-D okumentation.	Cloud-Architekt
Erstellen Sie eine Amazon RDS-DB-Instance für den Bacula-Katalog.	Öffnen Sie die Amazon RDS-Konsole und erstellen Sie eine Amazon RDS for MySQL MySQL-DB-Instance.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen dazu finden Sie unter Erstellen einer MySQL-DB-Instance und Herstellen einer Verbindung zu einer Datenbank auf einer MySQL-DB-Instance in der Amazon RDS-Dokumentation.	
Stellen Sie den Backup-Anwendungscontroller in der VPC bereit.	Installieren Sie Bacula auf der EC2 Instanz, stellen Sie den Backup-Anwendungscontroller bereit und konfigurieren Sie dann den Backup-Speicher für die Verbindung mit dem Tape Gateway-Gerät. Sie können die Beispielkonfiguration des Bacula Director-Speicher-Daemons in der `Bacula-storage-daemon-config.txt` Datei (im Anhang) verwenden. Weitere Informationen dazu finden Sie in der Bacula-Dokumentation.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Backup-Anwendung auf den Sun SPARC-Gastservern ein.	Richten Sie einen zweiten Client ein, um die Backup-Anwendung auf den Sun SPARC-Gastservern zu installieren und einzurichten, indem Sie die Bacula-Beispielkonfiguration in der `SUN-SPARC-Guest-Bacula-Config.txt` Datei (im Anhang) verwenden.	DevOps Ingenieur
Richten Sie die Backup-Konfiguration und den Zeitplan ein.	Richten Sie die Backup-Konfiguration und die Backup-Zeitpläne im Backup-Anwendungscontroller ein, indem Sie die Bacula Director-Beispielkonfiguration in der `Bacula-Directory-Config.txt` Datei (im Anhang) verwenden. Weitere Informationen dazu finden Sie in der Bacula-Dokumentation.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die Backup-Konfiguration und die Zeitpläne korrekt sind.	Folgen Sie den Anweisungen in der Bacula-Dokumentation, um die Validierung und den Backup-Test für Ihr Setup auf den Sun SPARC-Gastservern durchzuführen. Sie können beispielsweise die folgenden Befehle verwenden , um die Konfigurationsdateien zu validieren: • `bacula-dir -t -c bacula-dir.conf` • `bacula-fd -t -c bacula-fd.conf` • `bacula-sd -t -c bacula-sd.conf`	DevOps Ingenieur

Zugehörige Ressourcen

- Charon Virtual SPARC mit VE-Lizenzierung
- Charon virtuelles SPARC
- Nutzung von Cloud-Diensten und Objektspeicher mit Bacula Enterprise Edition
- Ziele der Notfallwiederherstellung (DR)
- Emulationslösungen für ältere Charon-Systeme

Zusätzliche Informationen

Backup-Option 1 — Ein virtuelles Stromasys-Band erstellen

Sie können den folgenden Systems Manager Automation-Runbook-Beispielcode verwenden, um das Backup automatisch zu starten und dann die Bänder auszutauschen:

```
...
# example backup script saved in SUN SPARC Server
 #!/usr/bin/bash
 mt -f  rewind
 tar -cvf
 mt -f  offline
...
         mainSteps:
         - action: aws:runShellScript
           name:
           inputs:
             onFailure: Abort
             timeoutSeconds: "1200"
             runCommand:
             - |
               # Validate tape backup container file exists
               if [ ! -f {{TapeBackupContainerFile}} ]; then
                 logger -s -p local3.warning "Tape backup container file is not exists
 - {{TapeBackupContainerFile}}, create a new one"
                 touch {{TapeBackupContainerFile}}
               fi
         - action: aws:runShellScript
           name: startBackup
           inputs:
             onFailure: Abort
             timeoutSeconds: "1200"
             runCommand:
             - |
               user={{BACKUP_USER}}
               keypair={{KEYPAIR_PATH}}
               server={{SUN_SPARC_IP}}
               backup_script={{BACKUP_SCRIPT}}
               ssh -i $keypair $user@$server -c "/usr/bin/bash $backup_script"
         - action: aws:runShellScript
           name: swapVirtualDiskContainer
           inputs:
             onFailure: Abort
             timeoutSeconds: "1200"
             runCommand:
             - |
               mv {{TapeBackupContainerFile}} {{TapeBackupContainerFile}}.$(date +%s)
               touch {{TapeBackupContainerFile}}
         - action: aws:runShellScript
```

```
          name: uploadBackupArchiveToS3
          inputs:
            onFailure: Abort
            timeoutSeconds: "1200"
            runCommand:
            - |
              aws s3 cp {{TapeBackupContainerFile}} s3://{{BACKUP_BUCKET}}/
{{SUN_SPARC_IP}}/$(date '+%Y-%m-%d')/
 ...
```

Backup-Option 2 — Stromasys-Snapshot

Sie können den folgenden Systems Manager Automation-Runbook-Beispielcode verwenden, um den Backup-Prozess zu automatisieren:

```
     ...

        mainSteps:
        - action: aws:runShellScript
          name: startSnapshot
          inputs:
            onFailure: Abort
            timeoutSeconds: "1200"
            runCommand:
            - |
              # You may consider some graceful stop of the application before taking a
 snapshot
              # Query SSP PID by configuration file
              # Example: ps ax | grep ssp-4 | grep Solaris10.cfg | awk '{print $1"
"$5}' | grep ssp4 | cut -f1 -d" "
              pid=`ps ax | grep ssp-4 | grep {{SSP_GUEST_CONFIG_FILE}} | awk '{print
$1" "$5}' | grep ssp4 | cut -f1 -d" "`
              if [ -n "${pid}" ]; then
                kill -SIGTSTP ${pid}
              else
                echo "No PID found for SPARC guest with config
 {{SSP_GUEST_CONFIG_FILE}}"
                exit 1
              fi
        - action: aws:runShellScript
          name: startBackup
          inputs:
            onFailure: Abort
```

```
              timeoutSeconds: "1200"
              runCommand:
              - |
                # upload snapshot and virtual disk files into S3
                aws s3 sync {{SNAPSHOT_FOLDER}} s3://{{BACKUP_BUCKET}}/$(date '+%Y-%m-
%d')/
                aws s3 cp {{VIRTUAL_DISK_FILE}} s3://{{BACKUP_BUCKET}}/$(date '+%Y-%m-
%d')/
          - action: aws:runShellScript
            name: restratSPARCGuest
            inputs:
              onFailure: Abort
              timeoutSeconds: "1200"
              runCommand:
              - |
                /opt/charon-ssp/ssp-4u/ssp4u -f {{SSP_GUEST_CONFIG_FILE}} -d -a
 {{SPARC_GUEST_NAME}} --snapshot {{SNAPSHOT_FOLDER}}
 ...
```

Sicherungsoption 4 — AWS Storage Gateway VTL

Wenn Sie nicht-globale Solaris-Zonen verwenden, um virtualisierte Sun SPARC-Legacy-Server auszuführen, kann der Backup-Ansatz auf nicht-globale Zonen angewendet werden, die auf den Sun SPARC-Servern ausgeführt werden (der Backup-Client kann beispielsweise innerhalb der nicht-globalen Zonen ausgeführt werden). Der Backup-Client kann jedoch auch auf dem Solaris-Host ausgeführt werden und Snapshots der nicht-globalen Zonen erstellen. Die Snapshots können dann auf einem Band gesichert werden.

Die folgende Beispielkonfiguration fügt das Dateisystem, das die nicht-globalen Solaris-Zonen hostet, zur Backup-Konfiguration für den Solaris-Host hinzu:

```
FileSet {
   Name = "Branded Zones"
   Include {
     Options {
       signature = MD5
     }
     File = /zones
   }
 }
```

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Daten mit Veeam Backup & Replication auf Amazon S3 sichern und archivieren

Erstellt von Jeanna James (AWS), Anthony Fiore (AWS) (AWS) und William Quigley (AWS)

Übersicht

Dieses Muster beschreibt den Prozess für das Senden von von Veeam Backup & Replication erstellten Backups an unterstützte Objektspeicherklassen von Amazon Simple Storage Service (Amazon S3) mithilfe der Veeam Scale-Out-Backup-Repository-Funktion.

Veeam unterstützt mehrere Amazon S3 S3-Speicherklassen, um Ihren spezifischen Anforderungen am besten gerecht zu werden. Sie können den Speichertyp auf der Grundlage der Anforderungen an Datenzugriff, Ausfallsicherheit und Kosten Ihrer Backup- oder Archivdaten auswählen. Sie können beispielsweise Daten, die Sie nicht für 30 Tage oder länger verwenden möchten, zu geringeren Kosten in Amazon S3 Infrequent Access (IA) speichern. Wenn Sie planen, Daten für 90 Tage oder länger zu archivieren, können Sie Amazon Simple Storage Service Glacier (Amazon S3 Glacier) Flexible Retrieval oder S3 Glacier Deep Archive mit der Archivstufe von Veeam verwenden. Sie können S3 Object Lock auch verwenden, um Backups zu erstellen, die innerhalb von Amazon S3 unveränderlich sind.

Dieses Muster behandelt nicht, wie Sie Veeam Backup & Replication mit integriertem Tape-Gateway einrichten. AWS Storage Gateway Informationen zu diesem Thema finden Sie unter Veeam Backup & Replication using AWS VTL Gateway — Deployment Guide auf der Veeam-Website.

> **Warning**
>
> Für dieses Szenario sind AWS Identity and Access Management (IAM-) Benutzer mit programmatischem Zugriff und langfristigen Anmeldeinformationen erforderlich, was ein Sicherheitsrisiko darstellt. Um dieses Risiko zu minimieren, empfehlen wir, diesen Benutzern nur die Berechtigungen zu gewähren, die sie für die Ausführung der Aufgabe benötigen, und diese Benutzer zu entfernen, wenn sie nicht mehr benötigt werden. Zugriffsschlüssel können bei Bedarf aktualisiert werden. Weitere Informationen finden Sie unter Aktualisieren von Zugriffsschlüsseln im IAM-Benutzerhandbuch.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Veeam Backup & Replication, einschließlich Veeam Availability Suite oder Veeam Backup Essentials, installiert (Sie können sich für eine kostenlose Testversion registrieren)
- Veeam Backup & Replication-Lizenz mit Enterprise- oder Enterprise Plus-Funktionalität, einschließlich Veeam Universal License (VUL)
- Ein aktiver IAM-Benutzer mit Zugriff auf einen Amazon S3 S3-Bucket
- Ein aktiver IAM-Benutzer mit Zugriff auf Amazon Elastic Compute Cloud (Amazon EC2) und Amazon Virtual Private Cloud (Amazon VPC), wenn die Archivschicht verwendet wird
- Netzwerkkonnektivität von vor Ort bis hin AWS-Services zu verfügbarer Bandbreite für Backup und Wiederherstellung des Datenverkehrs über eine öffentliche Internetverbindung oder eine AWS Direct Connect öffentliche virtuelle Schnittstelle (VIF)
- Die folgenden Netzwerkports und Endpunkte wurden geöffnet, um eine ordnungsgemäße Kommunikation mit Objektspeicher-Repositorys sicherzustellen:
  - Amazon S3 S3-Speicher — TCP — Port 443: Wird für die Kommunikation mit dem Amazon S3 S3-Speicher verwendet.
  - Amazon S3 S3-Speicher — Cloud-Endpunkte — `*.amazonaws.com` für AWS-Regionen und die oder für die AWS GovCloud (US) Regions Regionen China: Wird `*.amazonaws.com.cn` für die Kommunikation mit dem Amazon S3 S3-Speicher verwendet. Eine vollständige Liste der Verbindungsendpunkte finden Sie in der Dokumentation unter Amazon S3 S3-Endpunkte. AWS
  - Amazon S3 S3-Speicher — TCP HTTP — Port 80: Wird zur Überprüfung des Zertifikatsstatus verwendet. Beachten Sie, dass sich die Endpunkte für die Zertifikatsüberprüfung — Certificate Revocation List (CRL) URLs und Online Certificate Status Protocol (OCSP) -Server — ändern können. Die tatsächliche Adressliste finden Sie im Zertifikat selbst.
  - Amazon S3 S3-Speicher — Endpunkte zur Zertifikatsverifizierung —`*.amazontrust.com`: Wird zur Überprüfung des Zertifikatsstatus verwendet. Beachten Sie, dass sich die Endpunkte zur Zertifikatsverifizierung (CRL URLs - und OCSP-Server) ändern können. Die tatsächliche Adressliste finden Sie im Zertifikat selbst.

Einschränkungen

- Veeam unterstützt keine S3-Lifecycle-Richtlinien für S3-Buckets, die als Veeam-Objektspeicher-Repositorys verwendet werden. Dazu gehören Richtlinien mit Amazon S3 S3-

Speicherklassenübergängen und S3-Lifecycle-Ablaufregeln. Veeam muss die einzige Entität sein, die diese Objekte verwaltet. Die Aktivierung von S3 Lifecycle-Richtlinien kann zu unerwarteten Ergebnissen, einschließlich Datenverlust, führen.

Produktversionen

- Veeam Backup & Replication v9.5 Update 4 oder höher (nur Backup oder Kapazitätsstufe)
- Veeam Backup & Replication v10 oder höher (Backup oder Kapazitätsstufe und S3 Object Lock)
- Veeam Backup & Replication v11 oder höher (Backup- oder Kapazitätsstufe, Archiv- oder Archivstufe und S3 Object Lock)
- Veeam Backup & Replication v12 oder höher (Performance-Tier, Backup- oder Kapazitäts-Tier, Archiv- oder Archiv-Tier und S3 Object Lock)
- S3 Standard
- S3 Standard-IA
- S3 One Zone-IA
- S3 Glacier Flexible Retrieval (nur v11 und höher)
- S3 Glacier Deep Archive (nur v11 und höher)
- S3 Glacier Instant Retrieval (nur v12 und höher)

Architektur

Quelltechnologie-Stack

- Lokale Veeam Backup & Replication-Installation mit Konnektivität von einem Veeam-Backup-Server oder einem Veeam-Gateway-Server zu Amazon S3

Zieltechnologie-Stack

- Amazon S3
- Amazon VPC und Amazon EC2 (bei Verwendung der Archivstufe)

Zielarchitektur: SOBR

Das folgende Diagramm zeigt die Architektur des Scale-Out-Backup-Repositorys (SOBR).

Die Veeam Backup and Replication-Software schützt Daten vor logischen Fehlern wie Systemausfällen, Anwendungsfehlern oder versehentlichem Löschen. In diesem Diagramm werden Backups zuerst lokal ausgeführt und eine zweite Kopie wird direkt an Amazon S3 gesendet. Ein Backup stellt eine point-in-time Kopie der Daten dar.

Der Workflow besteht aus drei Hauptkomponenten, die für das Tiering oder Kopieren von Backups nach Amazon S3 erforderlich sind, und einer optionalen Komponente:

- Veeam Backup & Replication (1) — Der Backup-Server, der für die Koordination, Steuerung und Verwaltung der Backup-Infrastruktur, Einstellungen, Jobs, Wiederherstellungsaufgaben und anderer Prozesse verantwortlich ist.
- Veeam Gateway-Server (im Diagramm nicht dargestellt) — Ein optionaler lokaler Gateway-Server, der erforderlich ist, wenn der Veeam-Backup-Server keine ausgehende Konnektivität zu Amazon S3 hat.
- Scale-out-Backup-Repository (2) — Repository-System mit Unterstützung für horizontale Skalierung für die mehrstufige Speicherung von Daten. Das Scale-Out-Backup-Repository besteht aus einem oder mehreren Backup-Repositorys, die schnellen Zugriff auf Daten bieten und mit Amazon S3 S3-Objektspeicher-Repositorys für Langzeitspeicherung (Kapazitätsstufe) und Archivierung (Archivschicht) erweitert werden können. Veeam verwendet das Scale-Out-Backup-Repository, um Daten automatisch zwischen lokalem (Performance-Tier) und Amazon S3 S3-Objektspeicher (Kapazitäts- und Archiv-Tier) zu verteilen.

  > **Note**
  >
  > Ab Veeam Backup & Replication v12.2 macht die Direct to S3 Glacier-Funktion die S3-Kapazitätsstufe optional. Ein SOBR kann mit einer Performance-Stufe und einer S3 Glacier-Archivstufe konfiguriert werden. Diese Konfiguration ist nützlich für Benutzer, die erhebliche Investitionen in lokalen (lokalen) Speicher für die Kapazitätsstufe getätigt haben und nur eine langfristige Archivierung in der Cloud benötigen. Weitere Informationen finden Sie in der Dokumentation zu Veeam Backup & Replication.

- Amazon S3 (3) — AWS Objektspeicherservice, der Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet.

Zielarchitektur: DTO

Das folgende Diagramm zeigt die direct-to-object (DTO-) Architektur.

In diesem Diagramm werden Backup-Daten direkt an Amazon S3 gesendet, ohne dass sie zuerst vor Ort gespeichert werden. Sekundäre Kopien können in S3 Glacier gespeichert werden.

Automatisierung und Skalierung

Sie können die Erstellung von IAM-Ressourcen und S3-Buckets automatisieren, indem Sie die VeeamHub GitHub im AWS CloudFormation Repository bereitgestellten Vorlagen verwenden. Die Vorlagen enthalten sowohl Standard- als auch unveränderliche Optionen.

Tools

Tools und AWS-Services

- Veeam Backup & Replication ist eine Lösung von Veeam für den Schutz, die Sicherung, Replikation und Wiederherstellung Ihrer virtuellen und physischen Workloads.
- AWS CloudFormationhilft Ihnen dabei, Ihre AWS Ressourcen zu modellieren und einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus zu verwalten. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben und sie zusammen als Stapel zu starten und zu konfigurieren, anstatt Ressourcen einzeln zu verwalten. Sie können Stacks über mehrere und hinweg verwalten AWS-Konten und AWS-Regionen bereitstellen.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können Amazon verwenden EC2 , um so viele oder so wenige virtuelle Server zu starten, wie Sie benötigen, und Sie können nach oben oder unten skalieren.
- AWS Identity and Access Management (IAM) ist ein Webservice zur sicheren Steuerung des Zugriffs auf AWS-Services. Mit IAM können Sie Benutzer, Sicherheitsanmeldedaten wie Zugriffsschlüssel und Berechtigungen, mit denen gesteuert wird, auf welche AWS Ressourcen Benutzer und Anwendungen zugreifen können, zentral verwalten.
- Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen.
- Amazon S3 Glacier (S3 Glacier) ist ein sicherer und langlebiger Service für kostengünstige Datenarchivierung und langfristige Sicherung.
- Amazon Virtual Private Cloud (Amazon VPC) bietet einen logisch isolierten Bereich, in AWS Cloud dem Sie AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können. Dieses virtuelle Netzwerk entspricht weitgehend einem herkömmlichen Netzwerk, wie Sie es in

Ihrem Rechenzentrum betreiben, kann jedoch die Vorzüge der skalierbaren Infrastruktur von AWS nutzen.

Code

Verwenden Sie die im VeeamHub GitHub Repository bereitgestellten CloudFormation Vorlagen, um die IAM-Ressourcen und S3-Buckets für dieses Muster automatisch zu erstellen. Wenn Sie diese Ressourcen lieber manuell erstellen möchten, folgen Sie den Schritten im Abschnitt Epics.

Bewährte Methoden

- Gemäß den Best Practices für IAM empfehlen wir dringend, die langfristigen IAM-Benutzeranmeldedaten regelmäßig zu wechseln, z. B. den IAM-Benutzer, den Sie für das Schreiben von Veeam Backup & Replication-Backups auf Amazon S3 verwenden. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden in der IAM-Dokumentation.

Epen

Amazon S3 S3-Speicher in Ihrem Konto konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen IAM-Benutzer.	Folgen Sie den Anweisungen in der IAM-Dokumentation, um einen IAM-Benutzer zu erstellen. Dieser Benutzer sollte keinen AWS Konsolenzugriff haben, und Sie müssen einen Zugriffsschlüssel für diesen Benutzer erstellen. Veeam verwendet diese Entität zur Authentifizierung, um in Ihre S3-Buckets AWS zu lesen und in sie zu schreiben. Sie müssen dem Benutzer die geringsten Rechte gewähren (d. h.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	nur die für die Ausführung einer Aufgabe erforderlichen Berechtigungen), damit der Benutzer nicht über mehr Rechte verfügt, als er benötigt. Beispiele für IAM-Richtlinien, die Sie Ihrem Veeam IAM-Benutzer zuordnen können, finden Sie im Abschnitt Zusätzliche Informationen. **Note** Alternativ können Sie die im VeeamHub GitHub Repository bereitgestellten CloudFormation Vorlagen verwenden, um einen IAM-Benutzer und einen S3-Bucket für dieses Muster zu erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon S3 S3-Konsole. 2. Wenn Sie noch keinen vorhandenen S3-Bucket haben, den Sie als Zielspeicher verwenden können, wählen Sie Bucket erstellen und geben Sie einen Bucket-Namen und Bucket-Einstellungen an. AWS-Region • Wir empfehlen, dass Sie die Option „Öffentlichen Zugriff blockieren“ für den S3-Bucket aktivieren und die Zugriffs- und Benutzerberechtigungsrichtlinien so einrichten, dass sie den Anforderungen Ihrer Organisation entsprechen. Ein Beispiel finden Sie in der Amazon S3-Dokumentation. • Wir empfehlen, dass Sie S3 Object Lock aktivieren, auch wenn Sie nicht beabsichtigen, es sofort zu verwenden. Diese Einstellung kann nur zum Zeitpunkt der Erstellung des S3-Buckets aktiviert werden.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie in der Amazon S3 S3-Dokumentation unter Bucket erstellen.	

Fügen Sie Amazon S3 und S3 Glacier Flexible Retrieval (oder S3 Glacier Deep Archive) zu Veeam Backup & Replication hinzu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den Assistenten für neue Objekt-Repositorys.	Bevor Sie die Object Storage- und Scale-Out-Backup-Repositorys in Veeam einrichten, müssen Sie die Amazon S3- und S3 Glacier-Speicher-Repositorys hinzufügen, die Sie für die Kapazitäts- und Archivstufen verwenden möchten. Im nächsten Schritt verbinden Sie diese Speicher-Repositorys mit Ihrem Scale-Out-Backup-Repository. 1. Öffnen Sie auf der Veeam-Konsole die Ansicht Backup Infrastructure. 2. Wählen Sie im Inventarbereich den Knoten Backup-Repositorys und dann Repository hinzufügen aus. 3. Wählen Sie im Dialogfeld Backup-Repository hinzufügen die Option	AWS-Administrator, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Object Storage, Amazon S3 aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Amazon S3 S3-Speicher für die Kapazitätsstufe hinzu.	1. Wählen Sie im Dialogfeld Amazon Cloud Storage Services Amazon S3 aus. 2. Geben Sie im Schritt Name des Assistenten den Namen des Objektspeichers und eine kurze Beschreibung an, z. B. den Ersteller und das Erstellungsdatum. 3. Geben Sie im Schritt Konto des Assistenten das Objektspeicherkonto an. • Wählen Sie für Credentials den IAM-Benutzer aus, den Sie im ersten Epic für den Zugriff auf Ihren Amazon S3 S3-Objektspeicher erstellt haben. • Wählen Sie für die AWS-Region den AWS-Region Ort aus, an dem sich der S3-Bucket befindet. 4. Geben Sie im Bucket-Schritt des Assistenten die Objektspeichereinstellungen an. • Wählen Sie für die Rechenzentrumsregion den AWS-Region Ort aus, an dem sich der S3-Bucket befindet. • Wählen Sie für Bucket den S3-Bucket aus, den	AWS-Administrator, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie im ersten Epic erstellt haben. • Erstellen Sie für Ordner einen Cloud-Ordner, dem Sie Ihr Objektspeicher-Repository zuordnen möchten, oder wählen Sie einen aus. • Wenn Sie die Unveränderlichkeit aktivieren möchten, wählen Sie Letzte Backups für X Tage unveränderlich machen und legen Sie den Zeitraum fest, in dem Ihre Backups gesperrt werden sollen. Beachten Sie, dass die Aktivierung der Unveränderlichkeit aufgrund der erhöhten Anzahl von API-Aufrufen von Veeam an Amazon S3 zu höheren Kosten führt. 5. Überprüfen Sie im Schritt „Zusammenfassung“ des Assistenten die Konfigurationsinformationen und wählen Sie dann „Fertig stellen“.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie S3 Glacier-Speicher für die Archivstufe hinzu.	Wenn Sie eine Archivschicht erstellen möchten, verwenden Sie die IAM-Berechtigungen, die im Abschnitt Zusätzliche Informationen beschrieben sind. 1. Starten Sie den Assistenten „Neues Objekt-Repository“ wie zuvor beschrieben. 2. Wählen Sie im Dialogfeld Amazon Cloud Storage Services Amazon S3 Glacier aus. 3. Geben Sie im Schritt Name des Assistenten den Namen des Objektspeichers und eine kurze Beschreibung an, z. B. den Ersteller und das Erstellungsdatum. 4. Geben Sie im Schritt Konto des Assistenten das Objektspeicherkonto an. • Wählen Sie unter Anmeldeinformationen den IAM-Benutzer aus, den Sie im ersten Epic für den Zugriff auf Ihren S3 Glacier-Objektspeicher erstellt haben. • Wählen Sie für die AWS-Region den AWS-Region Ort aus, an dem sich der S3-Bucket befindet.	AWS-Administrator, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Geben Sie im Bucket-Schritt des Assistenten die Objektspeichereinstellungen an. • Wählen Sie für die Rechenzentrumsregion die AWS-Region. • Wählen Sie für Bucket einen S3-Bucket zum Speichern Ihrer Backup-Daten aus. Dies kann derselbe Bucket sein, den Sie für die Kapazitätsstufe verwendet haben. • Erstellen Sie für Ordner einen Cloud-Ordner, dem Sie Ihr Objektspeicher-Repository zuordnen möchten, oder wählen Sie einen aus. • Wenn Sie die Unveränderlichkeit aktivieren möchten, wählen Sie Letzte Backups für die gesamte Dauer ihrer Aufbewahrungsrichtlinie unveränderlich machen. Beachten Sie, dass die Aktivierung der Unveränderlichkeit aufgrund der erhöhten Anzahl von API-Aufrufen von Veeam an Amazon	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	S3 zu höheren Kosten führt. • Wenn Sie S3 Glacier Deep Archive als Ihre Archivspeicherklasse verwenden möchten, wählen Sie Use the Deep Archive Storage Class. 6. Konfigurieren Sie im Schritt Proxy Appliance des Assistenten die Zusatzinstanz, die für die Übertragung der Daten von Amazon S3 nach S3 Glacier verwendet wird. Sie können die Standarde instellungen verwenden oder jede Einstellung manuell konfigurieren. Um die Einstellungen manuell zu konfigurieren: • Wählen Sie Anpassen aus. • Wählen Sie zum Beispiel den EC2 Instanztyp für die Proxy-Appliance auf der Grundlage Ihrer Geschwindigkeits- und Kostenanforderungen für die Übertragung der Backup-Dateien auf die Archivebene Ihres Scale-Out-Backup-Repositorys.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wählen Sie für Amazon VPC die VPC für die Ziel-Instance aus. • Wählen Sie für Subnet das Subnetz für die Proxy-Appliance aus. • Wählen Sie unter Sicherheitsgruppe die Sicherheitsgruppe aus, die der Proxy-Appliance zugeordnet werden soll. • Geben Sie als Redirecto r-Port den TCP-Port für das Routing von Anfragen zwischen der Proxy-Appliance und den Komponenten der Backup-Infrastruktur an. • Wählen Sie OK, um Ihre Einstellungen zu bestätigen. 7. Überprüfen Sie im Schritt „Zusammenfassung“ des Assistenten die Konfigura tionsinformationen und klicken Sie dann auf Fertig stellen.	

Fügen Sie skalierbare Backup-Repositorys hinzu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den Assistenten für ein neues Scale-Out Backup Repository.	1. Öffnen Sie auf der Veeam-Konsole die Ansicht Backup Infrastructure. 2. Wählen Sie im Inventarbereich Scale-out Repositories und dann Add Scale-out Repository aus.	App-Besitzer, AWS-Systemadministrator
Fügen Sie ein Scale-Out-Backup-Repository hinzu und konfigurieren Sie Kapazitäts- und Archivstufen.	1. Geben Sie im Schritt Name des Assistenten den Namen und eine kurze Beschreibung des Scale-Out-Backup-Repositorys an. 2. Fügen Sie bei Bedarf Leistungsgrenzen hinzu. Sie können auch Ihr vorhandenes lokales Backup-Repository von Veeam als Leistungsstufe verwenden. Ab Veeam Version 12 können Sie einen S3-Bucket als Leistungserweiterung für direct-to-object (DTO-) Backups hinzufügen und so eine lokale Performance-Stufe umgehen. 3. Wählen Sie Advanced und geben Sie zusätzliche Optionen für das Scale-Out-Backup-Repository an.	App-Besitzer, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wählen Sie „Backup-Dateien pro Computer verwenden“, um für jeden Computer eine separate Backup-Datei zu erstellen und diese Dateien in mehreren Streams gleichzeitig in das Backup-Repository zu schreiben. Diese Option wird für eine bessere Nutzung von Speicher- und Rechenressourcen empfohlen. • Wählen Sie Vollständige Sicherung durchführen, wenn die erforderliche Größe offline ist, um eine vollständige Sicherungsdatei für den Fall zu erstellen, dass eine Erweiterung, die Wiederherstellungspunkte für eine inkrementelle Sicherung enthält, offline geht. Für diese Option ist freier Speicherplatz im Scale-Out-Backup-Repository erforderlich, um eine vollständige Sicherungsdatei zu hosten. 4. Geben Sie im Schritt „Richtlinie“ des Assistent	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en die Richtlinie für die Platzierung von Backups für das Repository an. • Wählen Sie Datenloka lität, um vollständige und inkrementelle Sicherungsdateien, die zu derselben Kette gehören, zusammen und mit demselben Leistungs umfang zu speichern . Sie können Dateien, die zu einer neuen Backup-Kette gehören, im gleichen oder in einem anderen Leistungs umfang speichern (es sei denn, Sie verwenden eine deduplizierende Speicher-Appliance als Leistungsumfang). • Wählen Sie Performan ce, um vollständige und inkrementelle Backup-Dateien mit unterschi edlichen Leistungsstufen zu speichern. Diese Option erfordert eine schnelle und zuverläss ige Netzwerkverbindung . Wenn Sie Leistung wählen, können Sie die Typen der zu speichern den Sicherungsdateien	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	für jede Leistungsstufe einschränken. Sie können beispielsweise vollständ ige Sicherungsdateien auf einem Extent und inkrementelle Backup-Da teien auf anderen Extents speichern. So wählen Sie Dateitypen aus: • Wählen Sie Anpassen aus. • Wählen Sie im Dialogfeld Einstellu ngen für die Backup-Platzierung einen Leistungsbereich aus, und klicken Sie dann auf Bearbeiten. • Wählen Sie den Typ der Sicherungsdateien aus, die Sie auf dem Extent speichern möchten. 5. Konfigurieren Sie im Schritt „Kapazitätsstufe“ des Assistenten die Langzeits peicherebene, die Sie dem Scale-Out-Backup-Repository zuordnen möchten. • Wählen Sie „Kapazität des Scale-out-Backup-R epositorys mit Objektspe icher erweitern“. Wählen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie für das Objektspeicher-Repository den Amazon S3 S3-Speicher für die Kapazitätsstufe aus, die Sie im vorherigen Epic hinzugefügt haben. • Wählen Sie Fenster, um ein Zeitfenster für das Verschieben oder Kopieren von Daten auszuwählen. • Wählen Sie Backups in den Objektspeicher kopieren, sobald sie erstellt wurden, um alle oder nur die kürzlich erstellten Backup-Dateien bis zur Kapazitätsgrenze zu kopieren. • Wählen Sie aus dem Fenster für betriebliche Wiederherstellungen die Option Backups nach dem Alter in den Objektspeicher verschieben aus, um inaktive Backup-Ketten in den Kapazitätsbereich zu übertragen. Geben Sie im Feld Sicherungsdateien verschieben, die älter als X Tage sind, eine Dauer an, nach deren	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ablauf die Sicherungsdateien ausgelagert werden sollen. (Geben Sie 0 Tage an, um inaktive Backup-Ketten an dem Tag auszulagern, an dem sie erstellt wurden.) Sie können auch Override wählen, um Sicherungsdateien früher zu verschieben, wenn das Scale-Out-Backup-Repository einen von Ihnen angegebenen Schwellenwert erreicht hat. • Wählen Sie In den Objektspeicher hochgeladene Daten verschlüsseln und geben Sie ein Passwort an, um alle Daten und ihre Metadaten für das Auslagern zu verschlüsseln. Wählen Sie Passwörter hinzufügen oder verwalten, um ein neues Passwort anzugeben. 6. Konfigurieren Sie im Schritt Archivierungsebene des Assistenten die Archivspeicherebene, die Sie dem Scale-Out-Backup-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Repository zuordnen möchten. (Dieser Schritt wird nicht angezeigt, wenn Sie das Hinzufügen von Amazon S3 Glacier-S peicher übersprungen haben.) • Wählen Sie Vollständ ige GFS-Backups im Objektspeicher archivier en. Wählen Sie für das Objektspeicher-Rep ository den Amazon S3 Glacier-Speicher aus, den Sie im vorherigen Epic hinzugefügt haben. • Wählen Sie für Archiv-GF S-Backups, die älter als N Tage sind, ein Zeitfenst er für das Verschieb en von Dateien in den Archivbereich. (Um inaktive Backup-Ketten an dem Tag zu archivier en, an dem sie erstellt wurden, geben Sie 0 Tage an.) 7. Überprüfen Sie im Schritt Zusammenfassung des Assistenten die Konfigura tion des Scale-Out-Backup-Repositorys und klicken Sie dann auf Fertig stellen.	

Zugehörige Ressourcen

- Einen IAM-Benutzer in Ihrer AWS-Konto (IAM-Dokumentation) erstellen
- Einen Bucket erstellen (Amazon S3 S3-Dokumentation)
- Sperren des öffentlichen Zugriffs auf Ihren Amazon S3 S3-Speicher (Amazon S3 S3-Dokumentation)
- Verwenden von S3 Object Lock (Amazon S3 S3-Dokumentation)
- Technische Dokumentation von Veeam
- So erstellen Sie eine sichere IAM-Richtlinie für die Verbindung zum S3-Objektspeicher (Veeam-Dokumentation)

Zusätzliche Informationen

In den folgenden Abschnitten finden Sie Beispiele für IAM-Richtlinien, die Sie verwenden können, wenn Sie einen IAM-Benutzer im Abschnitt Epics dieses Musters erstellen.

IAM-Richtlinie für die Kapazitätsstufe

> **Note**
>
> Ändern Sie den Namen der S3-Buckets in der Beispielrichtlinie von `<yourbucketname>` in den Namen des S3-Buckets, den Sie für Veeam-Backups auf Kapazitätsstufen verwenden möchten. Beachten Sie auch, dass die Richtlinie auf die spezifischen Ressourcen beschränkt werden sollte, die für Veeam verwendet werden (wie in der `Resource` Spezifikation in der folgenden Richtlinie angegeben), und dass der erste Teil der Richtlinie die clientseitige Verschlüsselung deaktiviert, wie im AWS Blogbeitrag Verhinderung einer unbeabsichtigten Verschlüsselung von Amazon S3 S3-Objekten beschrieben.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RestrictSSECObjectUploads",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<your-bucket-name>/*",
```

```
            "Condition": {
                "Null": {
                    "s3:x-amz-server-side-encryption-customer-algorithm": "false"
                }
            }
        },
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:GetObjectVersion",
                "s3:ListBucketVersions",
                "s3:ListBucket",
                "s3:PutObjectLegalHold",
                "s3:GetBucketVersioning",
                "s3:GetObjectLegalHold",
                "s3:GetBucketObjectLockConfiguration",
                "s3:PutObject*",
                "s3:GetObject*",
                "s3:GetEncryptionConfiguration",
                "s3:PutObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:DeleteObject*",
                "s3:DeleteObjectVersion",
                "s3:GetBucketLocation"

            ],
            "Resource": [
                "arn:aws:s3:::<yourbucketname>",
                "arn:aws:s3:::<yourbucketname>/*"
            ]
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

IAM-Richtlinie für die Archivstufe

> **Note**
>
> Ändern Sie den Namen der S3-Buckets in der Beispielrichtlinie von `<yourbucketname>` in den Namen des S3-Buckets, den Sie für Veeam-Backups auf Archivebene verwenden möchten.

So verwenden Sie Ihre vorhandenen VPC-, Subnetz- und Sicherheitsgruppen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
                "s3:PutObject",
                "s3:GetObject",
                "s3:RestoreObject",
                "s3:ListBucket",
                "s3:AbortMultipartUpload",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
                "s3:GetBucketObjectLockConfiguration",
                "s3:PutObjectRetention",
                "s3:GetObjectVersion",
                "s3:PutObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:DeleteObjectVersion",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket-name>",
                "arn:aws:s3:::<bucket-name>/*"
            ]
        }
    ]
}
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2Permissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:CreateKeyPair",
                "ec2:DescribeKeyPairs",
                "ec2:RunInstances",
                "ec2:DeleteKeyPair",
                "ec2:DescribeVpcAttribute",
                "ec2:CreateTags",
                "ec2:DescribeSubnets",
                "ec2:TerminateInstances",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
                "ec2:DescribeVpcs"
            ],
            "Resource": "arn:aws:ec2:<region>:<account-id>:*"
        }
    ]
}
```

So erstellen Sie neue VPC-, Subnetz- und Sicherheitsgruppen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
                "s3:PutObject",
                "s3:GetObject",
                "s3:RestoreObject",
                "s3:ListBucket",
                "s3:AbortMultipartUpload",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
```

```
                "s3:GetBucketLocation",
                "s3:GetBucketObjectLockConfiguration",
                "s3:PutObjectRetention",
                "s3:GetObjectVersion",
                "s3:PutObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:DeleteObjectVersion",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket-name>",
                "arn:aws:s3:::<bucket-name>/*"
            ]
        }
    ]
}

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2Permissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:CreateKeyPair",
                "ec2:DescribeKeyPairs",
                "ec2:RunInstances",
                "ec2:DeleteKeyPair",
                "ec2:DescribeVpcAttribute",
                "ec2:CreateTags",
                "ec2:DescribeSubnets",
                "ec2:TerminateInstances",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
                "ec2:DescribeVpcs",
                "ec2:CreateVpc",
                "ec2:CreateSubnet",
                "ec2:DescribeAvailabilityZones",
                "ec2:CreateRoute",
                "ec2:CreateInternetGateway",
                "ec2:AttachInternetGateway",
                "ec2:ModifyVpcAttribute",
                "ec2:CreateSecurityGroup",
```

```
                "ec2:DeleteSecurityGroup",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:DescribeRouteTables",
                "ec2:DescribeInstanceTypes"
            ],
            "Resource": "*"
        }
    ]
}
```

Konfiguration von Veritas NetBackup for VMware Cloud auf AWS

Erstellt von Shubham Salani (AWS)

Übersicht

> Hinweis: Seit dem 30. April 2024 wird VMware Cloud on AWS nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS-Vertreter zu wenden.

Viele Unternehmen verwenden Veritas NetBackup als Backup- und Wiederherstellungslösung für ihre lokalen VMware vSphere-basierten Workloads. Sobald Unternehmen ihre Workloads in softwaredefinierte Rechenzentren (SDDCs) in der VMware Cloud on Amazon Web Services (AWS) -Infrastruktur migrieren, gibt es kein klares lift-and-shift Verfahren für die Integration. NetBackup Dieses Muster beschreibt, wie Sie Veritas NetBackup in Ihrem AWS-Konto einrichten und es so konfigurieren können, dass die Workloads in Ihrem Konto gesichert werden. VMware SDDCs

Dieses Muster enthält keine Anweisungen für die Migration Ihrer Workloads. Weitere Informationen finden Sie unter VMware SDDC mithilfe VMware von HCX zur VMware Cloud auf AWS migrieren. Verwenden Sie beim Einrichten Ihrer Workloads für VMware Cloud on AWS einen ausgeweiteten Cluster (VMware Dokumentation). In dieser Konfiguration erstreckt sich Ihr Cluster über zwei AWS Availability Zones innerhalb einer einzigen Region. Dies bietet hohe Verfügbarkeit und Resilienz für den Fall, dass eine der Availability Zones nicht verfügbar ist. Elastic DRS und ein vSAN-Witness-Host (VMware Dokumentation) kopieren die Daten nahtlos in eine dritte Availability Zone, die als Fault Domain bezeichnet wird. Diese Paritätslösung kann Ihnen helfen, die Daten im Falle eines Fehlers wiederherzustellen. Da für diesen Ansatz drei Availability Zones erforderlich sind, sollten Sie bei der Auswahl einer AWS-Region für Ihre VMware Cloud-Umgebung sicherstellen, dass diese über drei oder mehr Availability Zones verfügt. Weitere Informationen finden Sie unter Regionen und Availability Zones.

In diesem Muster hat jedes SDDC einen Backup-Host, bei dem es sich um einen Proxyserver handelt. Mithilfe von Amazon Elastic Compute Cloud (Amazon EC2) -Instances richten Sie den NetBackup Master- und Medienserver in einer separaten Virtual Private Cloud (VPC) ein, einen für jedes SDDC. Da elastische Netzwerkschnittstellen eine hohe Bandbreite und geringe Latenz bieten, verwenden Sie sie, um die Konnektivität zwischen den Backup-Hosts und den entsprechenden NetBackup Master- und Medienservern zu konfigurieren. Die EC2 Instances leiten die Backups an

Amazon Elastic Block Store (Amazon EBS) -Volumes weiter, was der erste Backup-Punkt ist. Sie können AWS verwenden DataSync , um Ihre EBS-Volumes zu SDDCs synchronisieren.

Sie können auch AWS Transit Gateway und einen VPC-Schnittstellen-Endpunkt verwenden, um die EBS-Volumes mit einem anderen Speicherservice wie Amazon Simple Storage Service (Amazon S3) zu verbinden. Gemäß Ihrer Aufbewahrungsrichtlinie können Sie S3 Intelligent-Tiering S3 Glaciering-Speicherklassen verwenden, um Ihre Speicherkosten zu optimieren. Weitere Informationen finden Sie unter Verwenden von Amazon S3 S3-Speicherklassen (Amazon S3 S3-Dokumentation).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ihre VMware Cloud on AWS-Umgebung verwendet einen ausgedehnten Cluster, der sich über zwei Availability Zones erstreckt.
- Der Backup-Host muss sich in der VMware Cloud on AWS SDDC befinden, die Zugriff auf den Datenspeicher hat, in dem die VMware Virtual Machine Disk File (VMDK) -Dateien bereitgestellt werden.
- HotAdd Der Transportmodus muss auf dem NetBackup Client aktiviert sein, um virtuelle Maschinen (VMs) zu sichern und wiederherzustellen, und er muss Wiederherstellungen von benutzergesteuerten Dateien und Ordnern ermöglichen.

Einschränkungen

- Der NetBackup Masterserver muss die DNS-Auflösung für eine private IP-Adresse für den vCenter-Backup-Host im SDDC verwenden.
- Die Hosts-Dateien auf dem NetBackup Masterserver und dem Backup-Host sollten Folgendes enthalten:
  - Die private IP-Adresse und der private DNS-Name des Masterservers
  - Die private IP-Adresse und der private DNS-Name des Backup-Hosts
- Wenn Sie VPC-Schnittstellen-Endpunkte für einen S3-Bucket konfigurieren, muss die SDDC Compute Gateway-Firewall so konfiguriert sein, dass HTTPS von einer Classless Inter-Domain Routing (CIDR) -Blockquelle zugelassen wird. Weitere Informationen finden Sie unter Zugreifen auf einen S3-Bucket mithilfe eines S3-Endpunkts (Dokumentation). VMware
- VMware Cloud on AWS unterstützt nicht die folgenden Funktionen von NetBackup:
  - VM-Vorlagen sichern oder wiederherstellen

- Verwenden von NetBackup vSphere Client (HTML5 Plug-In)
- Sperren und Entsperren VMs für Backups oder Wiederherstellungen
- Backups können nicht in einem vSAN-Datenspeicher gespeichert werden
- Netzwerkblockgerät (NBD), NBDSSL und SAN-Transportmodi

Produktversionen

- VMware Cloud on AWS SDDC Version 1.0 oder höher
- Veritas NetBackup Version 8.1.2 oder höher
- Linux-Version 6.8 oder höher
- VMware vSphere Version 6.0 oder höher

Architektur

Das folgende Diagramm zeigt die Konfiguration von NetBackup for VMware Cloud on AWS. Die NetBackup Master- und Medienserver werden in einer separaten VPC bereitgestellt und über elastische Netzwerkschnittstellen mit den SDDCs Backup-Hosts verbunden. Die NetBackup Master- und Medienserver speichern die Backups auf Amazon EBS-Volumes. Sie können optional zusätzlichen Speicher in Amazon S3 S3-Buckets konfigurieren, indem Sie AWS Transit Gateway und einen VPC-Endpunkt mit PrivateLink AWS-Schnittstelle verwenden.

Tools

AWS-Services und -Tools

- Amazon Elastic Block Store (Amazon EBS) bietet Speichervolumes auf Blockebene zur Verwendung mit Amazon Elastic Compute Cloud (Amazon EC2) -Instances.
- AWS PrivateLink hilft Ihnen dabei, unidirektionale, private Verbindungen von Ihren virtuellen privaten Clouds (VPCs) zu Services außerhalb der VPC herzustellen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.

Andere Dienste

- VMware Cloud on AWS ist ein integriertes Cloud-Angebot, das gemeinsam von Amazon Web Services (AWS) und entwickelt wurde VMware.
- NetBackup für VMware Backups und Wiederherstellungen der VMware virtuellen Maschinen, die auf VMware ESXi Hosts laufen.

Epen

Konfigurieren Sie die Server NetBackup

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Firewall-Regeln.	Aktualisieren Sie die Firewallr egeln, um die Konnektiv ität zwischen dem VMware Cloud on AWS-SDDC und den NetBackup Master- und Medienservern herzustellen. Gehen Sie wie folgt vor: 1. Melden Sie sich bei VMware Cloud on AWS an unter https://vmc.vmware.com/ 2. Wählen Sie auf der Registerkarte Netzwerk und Sicherheit die Option Gateway Firewall aus. 3. Wählen Sie auf der Seite Gateway Firewall die Option Compute Gateway aus. 4. Wählen Sie Regel HINZUFÜGEN und erstellen Sie dann eine neue Regel mit den	Netzwerkadministrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	erforderlichen Firewall-Port-Einstellungen. Weitere Informationen finden Sie unter Anforderungen an NetBackup Firewall-Ports (Veritas-Dokumentation).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den NetBackup Master- und Medienserver.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/ 2. Starten Sie eine EC2 Instance (EC2 Amazon-Dokumentation) und verwenden Sie die folgenden Konfigurationsdetails: a. Wählen Sie für den NetBackup Master- und Medienserver das `NBU-Linux-GA-8-1-2-Setup-f032d23e-881b-4dee-ba70-b9ca3e915910-ami-072509a7ffc156938.4` Amazon Machine Image (AMI) aus. Dieses vorkonfigurierte AMI ist über den AWS Marketplace erhältlich. b. Wählen Sie einen Instanztyp aus. NetBackup empfiehlt `m5.2xlarge` für den Master- und Medienserver.	Cloud-Administrator, Backup-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Backup-Host für NetBackup.	1. Melden Sie sich bei VMware Cloud on AWS an unter https://vmc.vmware.com/ 2. Wählen Sie das SDDC aus. 3. Wählen Sie die Registerkarte „VCENTER öffnen“. Dadurch wird das SDDC vCenter geöffnet. 4. Notieren Sie sich den vollqualifizierten Domänennamen (FQDN) des Backup-Hosts. 5. Melden Sie sich bei der NetBackup Verwaltungskonsole an. Weitere Informationen finden Sie unter Bei der NetBackup Verwaltungskonsole anmelden (Veritas-Dokumentation). 6. Wählen Sie den Master- und den Medienserver und anschließend VMware Access Hosts aus. 7. Fügen Sie den FQDN des Backup-Hosts hinzu. 8. Wählen Sie Übernehmen und anschließend OK aus.	Cloud-Administrator, Backup-Administrator

(Optional) Amazon S3 S3-Speicher einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Speicher in Amazon S3.	1. Lesen Sie die Amazon S3 S3-Cloud-Speicheroptionen (Veritas-Dokumentation) und wählen Sie die passende Speicherklasse für Ihre Anforderungen aus. 2. Konfigurieren NetBackup Sie die Verwendung von Amazon S3 als Cloud-Speicher gemäß den Anweisungen unter Cloud-Speicher konfigurieren in NetBackup (Veritas-Dokumentation).	Cloud-Administrator, Allgemeine AWS

Zugehörige Ressourcen

AWS-Dokumentation

- Erstellen Sie einen VPC-Schnittstellen-Endpunkt (PrivateLink AWS-Dokumentation)

Veritas-Dokumentation

- NetBackup Anforderungen an den Firewall-Port

VMware Dokumentation

- Stellen Sie eine VM aus einer OVF-Vorlage in einer Inhaltsbibliothek bereit
- VMware Cloud-on-AWS-Datenübertragungsgebühren: Wie funktioniert das? (VMware Blogbeitrag)
- VMware Cloud auf AWS: Stretched Clusters

Kopieren Sie Daten mithilfe der AWS-CLI aus einem S3-Bucket in ein anderes Konto und eine andere Region

Erstellt von Appasaheb Bagali (AWS) und Purushotham G K (AWS)

Übersicht

Dieses Muster beschreibt, wie Daten von einem Amazon Simple Storage Service (Amazon S3) -Bucket in einem AWS-Quellkonto zu einem Ziel-S3-Bucket in einem anderen AWS-Konto migriert werden, entweder in derselben AWS-Region oder in einer anderen Region.

Der Quell-S3-Bucket ermöglicht den Zugriff auf AWS Identity and Access Management (IAM) mithilfe einer angehängten Ressourcenrichtlinie. Ein Benutzer im Zielkonto muss eine Rolle übernehmen, die über `GetObject` Berechtigungen für den `PutObject` Quell-Bucket verfügt. Schließlich führen `copy` Sie `sync` Befehle aus, um Daten vom S3-Quell-Bucket in den S3-Ziel-Bucket zu übertragen.

Konten sind Eigentümer der Objekte, die sie in S3-Buckets hochladen. Wenn Sie Objekte zwischen Konten und Regionen kopieren, gewähren Sie dem Zielkonto das Eigentum an den kopierten Objekten. Sie können die Eigentümerschaft eines Objekts ändern, indem Sie dessen Zugriffskontrollliste (ACL) auf ändern`bucket-owner-full-control`. Es wird jedoch empfohlen, dem Zielkonto programmgesteuerte kontoübergreifende Berechtigungen zu gewähren, da die Verwaltung mehrerer Objekte schwierig sein ACLs kann.

> **Warning**
>
> Für dieses Szenario sind IAM-Benutzer mit programmatischem Zugriff und langfristigen Anmeldeinformationen erforderlich, was ein Sicherheitsrisiko darstellt. Um dieses Risiko zu minimieren, empfehlen wir, diesen Benutzern nur die Berechtigungen zu gewähren, die sie für die Ausführung der Aufgabe benötigen, und diese Benutzer zu entfernen, wenn sie nicht mehr benötigt werden. Zugriffsschlüssel können bei Bedarf aktualisiert werden. Weitere Informationen finden Sie unter Aktualisieren von Zugriffsschlüsseln im IAM-Benut zerhandbuch.

Dieses Muster deckt eine einmalige Migration ab. Für Szenarien, die eine kontinuierliche und automatische Migration neuer Objekte von einem Quell-Bucket zu einem Ziel-Bucket erfordern, können Sie stattdessen die S3-Batch-Replikation verwenden, wie im Muster Kopieren von Daten aus

einem S3-Bucket in ein anderes Konto und eine andere Region mithilfe von S3 Batch Replication beschrieben.

Voraussetzungen und Einschränkungen

- Zwei aktive AWS-Konten in derselben oder unterschiedlichen AWS-Regionen.
- Ein vorhandener S3-Bucket im Quellkonto.
- Wenn in Ihrem Amazon S3 S3-Quell- oder Ziel-Bucket die Standardverschlüsselung aktiviert ist, müssen Sie die Schlüsselberechtigungen für den AWS Key Management Service (AWS KMS) ändern. Weitere Informationen finden Sie im AWS-re:Post-Artikel zu diesem Thema.
- Vertrautheit mit kontoübergreifenden Berechtigungen.

Architektur

Tools

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie kontrollieren, wer authentifiziert und autorisiert ist, diese zu verwenden.

Bewährte Methoden

- Bewährte Sicherheitsmethoden in IAM (IAM-Dokumentation)
- Anwenden von Berechtigungen mit den geringsten Rechten (IAM-Dokumentation)

Epen

Erstellen Sie einen IAM-Benutzer und eine IAM-Rolle im AWS-Zielkonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen IAM-Benutzer und rufen Sie den Zugriffsschlüssel ab.	1. Melden Sie sich bei der AWS-Managementkonsole an und erstellen Sie einen IAM-Benutzer mit programmatischem Zugriff. Ausführliche Schritte finden Sie in der IAM-Dokumentation unter IAM-Benutzer erstellen. Es ist nicht erforderlich, Richtlinien für diesen Benutzer anzuhängen. 2. Generieren Sie einen Zugriffsschlüssel und einen geheimen Schlüssel für diesen Benutzer. Anweisungen finden Sie in der AWS-Dokumentation unter AWS-Konto und Zugriffsschlüssel.	AWS DevOps
Erstellen Sie eine identitätsbasierte IAM-Richtlinie.	Erstellen Sie eine identitätsbasierte IAM-Richtlinie, die mit den folgenden Berechtigungen benannt `S3MigrationPolicy` ist. Ausführliche Schritte finden Sie in der IAM-Dokumentation unter Erstellen von IAM-Richtlinien. `{`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["s3:ListBucket", "s3:GetObject", "s3:GetObjectTagging", "s3:GetObjectVersion", "s3:GetObjectVersionTagging"], "Resource": ["arn:aws:s3:::amazon-s3-demo-source-bucket", "arn:aws:s3:::amazon-s3-demo-source-bucket/*"] }, { "Effect": "Allow", "Action": ["s3:ListBucket", "s3:PutObject",	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"s3:PutObjectAcl",
	"s3:PutObjectTaggi
	ng",
	"s3:GetObjectTaggi
	ng",
	"s3:GetObjectVersi
	on",
	"s3:GetObjectVersi
	onTagging"
	],
	"Resource":
	[
	"arn:aws:s3:::amazon-
	s3-demo-destination-
	bucket",
	"arn:aws:s3:::amazon-
	s3-demo-destination-
	bucket/*"
	]
	}
	]
	}</pre>
	Note
	Ändern Sie die Quell- und Ziel-Bucket-Namen entsprechend Ihrem Anwendungsfall.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Diese identitätsbasierte Richtlinie ermöglicht es dem Benutzer, der diese Rolle übernimmt, auf den Quell-Bucket und den Ziel-Bucket zuzugreifen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle.	Erstellen Sie eine IAM-Rolle, die `S3MigrationRole` nach der folgenden Vertrauensrichtlinie benannt ist, und hängen Sie dann die zuvor erstellte `S3MigrationPolicy` an. Ausführliche Schritte finden Sie in der IAM-Dokumentation unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::<destination_account>:user/<user_name>" }, "Action": "sts:AssumeRole", "Condition": {} } ] }`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Ändern Sie den Amazon-Ressourcennamen (ARN) der Ziel-IAM-Rolle oder den Benutzernamen in der Vertrauensrichtlinie entsprechend Ihrem Anwendungsfall. Diese Vertrauensrichtlinie ermöglicht es dem neu erstellten IAM-Benutzer, zu übernehmen. `S3MigrationRole`	

Erstellen Sie die S3-Bucket-Richtlinie und fügen Sie sie dem Quellkonto hinzu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine S3-Bucket-Richtlinie und fügen Sie sie an.	Melden Sie sich bei der AWS-Managementkonsole für Ihr Quellkonto an und öffnen Sie die Amazon S3 S3-Konsole. Wählen Sie Ihren S3-Quell-Bucket und dann Permissions aus. Wählen Sie unter Bucket-Richtlinie die Option Bearbeiten aus und fügen Sie dann die folgende Bucket-Richtlinie ein. Wählen Sie Save (Speichern) aus.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	{
	"Version":
	"2012-10-17",
	"Statement": [
	{
	"Sid":
	"DelegateS3Access",
	"Effect":
	"Allow",
	"Principa
	l": {"AWS": "arn:aws:
	iam::<destination_
	account>:role/<Rol
	eName>"},
	"Action":
	["s3:ListBucket",
	
	"s3:GetObject",
	
	"s3:GetObjectTaggi
	ng",
	
	"s3:GetObjectVersi
	on",
	
	"s3:GetObjectVersi
	onTagging"
	
	],
	"Resource":
	[
	
	"arn:aws:s3:::amazon-
	s3-demo-source-bucket/
	*",
	
	"arn:aws:s3:::amazon-
	s3-demo-source-bucket"
	]
	}
	]	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`}` **Note** Stellen Sie sicher, dass Sie die AWS-Konto-ID für das Zielkonto angeben und konfigurieren Sie die Bucket-Richtlinien vorlage gemäß Ihren Anforderungen. Diese ressourcenbasierte Richtlinie ermöglicht der Zielrolle den `S3MigrationRole` Zugriff auf S3-Objekte im Quellkonto.	

Konfigurieren Sie den Ziel-S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Ziel-Bucket.	Melden Sie sich bei der AWS-Managementkonsole für Ihr Zielkonto an, öffnen Sie die Amazon S3 S3-Konsole und wählen Sie dann Create Bucket aus. Erstellen Sie einen S3-Bucket gemäß Ihren Anforderungen. Weitere Informationen finden Sie unter Bucket erstellen in der	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon S3 S3-Dokumentation.	

Kopieren Sie Daten in den Ziel-S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie AWS CLI mit den neu erstellten Benutzeranmeldedaten.	1. Installieren Sie die neueste Version der AWS-CLI. Anweisungen finden Sie unter Installation oder Aktualisierung der neuesten Version der AWS-CLI in der AWS-CLI-Dokumentation. 2. Führen Sie `$ aws configure` die CLI mit dem AWS-Zugriffsschlüssel des von Ihnen erstellten Benutzers aus und aktualisieren Sie sie. Weitere Informationen finden Sie unter Konfiguration und Einstellungen für Anmeldeinformationsdateien in der AWS-CLI-Dokumentation.	AWS DevOps
Nehmen Sie die S3-Migrationsrolle an.	1. Verwenden Sie die AWS-CLI, um Folgendes anzunehmen`S3MigrationRole` : `aws sts assume-role \ --role-arn "arn:aws:iam::<des`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	tination_account>:role/S3MigrationRole" \ --role-session-name AWSCLI-Session Dieser Befehl gibt mehrere Informationen aus. Innerhalb des Anmeldeinformationsblocks benötigen Sie das `AccessKeyId` `SecretAccessKey` , und`SessionToken` . In diesem Beispiel werden die Umgebungsvariablen `RoleAccessKeyID` `RoleSecretKey` , und verwendet `RoleSessionToken` . Beachten Sie, dass der Zeitstempel des Ablaufdatums in der UTC-Zeitzone liegt. Der Zeitstempel gibt an, wann die temporären Anmeldeinformationen der IAM-Rolle ablaufen. Wenn die temporären Anmeldeinformationen ablaufen, müssen Sie die `sts:AssumeRole` API erneut aufrufen. 2. Erstellen Sie drei Umgebungsvariablen , um die IAM-Rolle zu übernehmen. Diese	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Umgebungsvariablen werden mit der folgenden Ausgabe gefüllt:
	
	`# Linux`
	`export AWS_ACCES S_KEY_ID=RoleAcces sKeyID`
	`export AWS_SECRE T_ACCESS_KEY=RoleS ecretKey`
	`export AWS_SESSI ON_TOKEN=RoleSessi onToken`
	`# Windows`
	`set AWS_ACCES S_KEY_ID=RoleAcces sKeyID`
	`set AWS_SECRE T_ACCESS_KEY=RoleS ecretKey`
	`set AWS_SESSI ON_TOKEN=RoleSessi onToken`
	
	3. Stellen Sie sicher, dass Sie die IAM-Rolle übernomme n haben, indem Sie den folgenden Befehl ausführen:
	
	`aws sts get-caller- identity`
	
	Weitere Informationen finden Sie im AWS Knowledge Center.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Kopieren und synchronisieren Sie Daten aus dem S3-Quell-Bucket in den S3-Ziel-Bucket.	Wenn Sie die Rolle übernommen haben, können `S3MigrationRole` Sie die Daten mit dem Befehl copy (cp) oder synchronize (sync) kopieren.
	
	Kopieren (Einzelheiten finden Sie in der AWS CLI Command Reference):
	
	`aws s3 cp s3://amazon-s3-demo-source-bucket/ \ s3://amazon-s3-demo-destination-bucket/ \ --recursive --source-region SOURCE-REGION-NAME --region DESTINATION-REGION-NAME`
	
	Synchronisieren (weitere Informationen finden Sie in der AWS CLI Command Reference):
	
	`aws s3 sync s3://amazon-s3-demo-source-bucket/ \ s3://amazon-s3-demo-destination-bucket/ \ --source-region SOURCE-REGION-NAME`
		Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--region DESTINATION-REGION-NAME`	

Fehlerbehebung

Problem	Lösung
Beim Aufrufen des `ListObjects` Vorgangs ist ein Fehler aufgetreten (`AccessDenied`): Zugriff verweigert	• Stellen Sie sicher, dass Sie die Rolle übernommen haben`S3MigrationRole` . • Führen Sie `aws sts get-caller-identity` den Befehl aus, um die verwendete Rolle zu überprüfen. Wenn in der Ausgabe der ARN für nicht angezeigt wird`S3MigrationRole` , nehmen Sie die Rolle erneut an und versuchen Sie es erneut.

Zugehörige Ressourcen

- Einen S3-Bucket erstellen (Amazon S3 S3-Dokumentation)
- Amazon S3 S3-Bucket-Richtlinien und Benutzerrichtlinien (Amazon S3 S3-Dokumentation)
- IAM-Identitäten (Benutzer, Gruppen und Rollen) (IAM-Dokumentation)
- Befehl cp (AWS-CLI-Dokumentation)
- Sync-Befehl (AWS-CLI-Dokumentation)

Kopieren Sie Daten mithilfe von S3 Batch Replication von einem S3-Bucket in ein anderes Konto und eine andere Region

Erstellt von Appasaheb Bagali (AWS), Lakshmikanth B D (AWS), Purushotham G K (AWS), Shubham Harsora (AWS) und Suman Rajotia (AWS)

Übersicht

Dieses Muster erklärt, wie Sie Amazon Simple Storage Service (Amazon S3) Batch Replication verwenden können, um den Inhalt eines S3-Buckets automatisch und ohne manuelles Eingreifen in einen anderen S3-Bucket zu kopieren, nachdem Sie die Buckets eingerichtet haben. Die Quell- und Ziel-Buckets können sich im selben oder in unterschiedlichen Regionen befinden AWS-Konten .

Mit S3 Batch Replication können Sie Amazon S3 S3-Objekte replizieren, die vor der Einrichtung einer Replikationskonfiguration existierten, Objekte, die zuvor repliziert wurden, und Objekte, bei denen die Replikation fehlgeschlagen ist. Diese Methode verwendet einen S3 Batch Operations Job. Wenn der Job abgeschlossen ist, erhalten Sie einen Abschlussbericht.

Sie können S3 Batch Replication in Szenarien verwenden, die eine kontinuierliche und automatische Migration neuer Objekte von einem Quell-Bucket zu einem Ziel-Bucket erfordern. Für eine einmalige Migration können Sie stattdessen AWS Command Line Interface (AWS CLI) verwenden, wie im Muster Kopieren von Daten aus einem S3-Bucket in ein anderes Konto und eine andere Region beschrieben AWS CLI.

Voraussetzungen und Einschränkungen

- Eine Quelle AWS-Konto.
- Ein Ziel AWS-Konto.
- Ein S3-Bucket im Quellkonto mit einigen Objekten (Dateien oder Ordner).
- Ein oder mehrere S3-Buckets im Zielkonto.
- Die S3-Versionierung ist für die Quell- und Ziel-Buckets aktiviert.
- AWS Identity and Access Management (IAM) -Berechtigungen zum Erstellen einer IAM-Richtlinie, einer IAM-Rolle und einer S3-Bucket-Richtlinie für die Quell- und Zielkonten.
- Die Amazon S3 S3-Lebenszyklusregeln sind deaktiviert, solange der S3-Batch-Replikationsauftrag aktiv ist. Dadurch wird die Parität zwischen Quell- und Ziel-Bucket gewährleistet. Andernfalls ist der Ziel-Bucket möglicherweise kein exaktes Replikat des Quell-Buckets.

Architektur

Tools

AWS Dienstleistungen

- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Bewährte Methoden

Im folgenden Video von AWS re:Invent 2022 werden bewährte Methoden für die Verwendung der Amazon S3 S3-Replikation zur Einhaltung gesetzlicher Vorschriften, zum Datenschutz und zur Steigerung der Anwendungsleistung beschrieben.

https://www.youtube-nocookie.com/embed/oder ISBL04? JEb Steuerungen=0

Epen

Erstellen Sie eine IAM-Richtlinie und eine Rolle für die kontenübergreifende Replikation im Quellkonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Richtlinie für die kontenübergreifende Replikation.	Im AWS Quellkonto: 1. Öffnen Sie die IAM-Konsole. 2. Erstellen Sie eine neue IAM-Richtlinie. 3. Wählen Sie im Bereich Policy-Editor die Option JSON aus und fügen Sie den folgenden Code ein. `{`	Cloud-Administrator, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"Version": "2012-10-17", "Statement": [{ "Sid": "GetSourceBucketConfiguration", "Effect": "Allow", "Action": ["s3:ListBucket", "s3:GetBucketLocation", "s3:GetBucketAcl", "s3:GetReplicationConfiguration", "s3:GetObjectVersionForReplication", "s3:GetObjectVersionAcl", "s3:GetObjectVersionTagging"], "Resource": ["arn:aws:s3:::source-bucket-name", "arn:aws:s3:::source-bucket-name/*"] }, {</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"Sid": "ReplicateToDestinationBuckets", "Effect": "Allow", "Action": ["s3:List*", "s3:*Object", "s3:ReplicateObject", "s3:ReplicateDelete", "s3:ReplicateTags"], "Resource": ["arn:aws:s3:::destination-bucket-name*", "arn:aws:s3:::destination-bucket-name/*"] }, { "Sid": "PermissionToOverrideBucketOwner", "Effect": "Allow", "Action": [	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"s3:ObjectOwnerOverrideToBucketOwner"
	            ],
	            "Resource": [
	
	"arn:aws:s3:::destination-bucket-name*",
	
	"arn:aws:s3:::destination-bucket-name/*"
	            ]
	        }
	    ]
	}</pre> Diese Richtlinie umfasst drei Aussagen:
	• `GetSourceBucketConfiguration` bietet Zugriff auf die Replikationskonfiguration und die Objektversion für die Replikation im Quell-Bucket.
	• `ReplicateToDestinationBuckets` bietet Zugriff auf die Replikation in den Ziel-Bucket. Sie können mehrere Ziel-Buckets im Array angeben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `PermissionToOverrideBucketOwner` bietet Zugriff auf, `ObjectOwnerOverridedToBucketOwner` sodass der Ziel-Bucket Eigentümer der Objekte im Zielkonto ist, die aus dem Quellkonto repliziert wurden. 4. Wählen Sie Weiter, geben Sie einen Richtliniennamen wie ein `cross-account-bucket-replication-policy` , und wählen Sie dann Richtlinie erstellen aus. Weitere Informationen finden Sie unter Erstellen von IAM-Richtlinien in der IAM-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle für die kontenübergreifende Replikation.	Im AWS Quellkonto: 1. Erstellen Sie auf der IAM-Konsole eine IAM-Rolle mit den folgenden Informationen: a. Wählen Sie für Vertrauenswürdigen Entitätstyp die Option AWS-Service aus. b. Wählen Sie als Service S3 aus. c. Wählen Sie für den Anwendungsfall S3 Batch Operations. d. Wählen Sie die Richtlinie aus, die Sie im vorherigen Schritt erstellt haben. 2. Geben Sie einen Rollennamen wie cross-account-bucket-replication -role ein und wählen Sie dann Create role aus. Weitere Informationen finden Sie in der IAM-Dokumentation unter IAM-Rollen erstellen.	Cloud-Administrator, AWS-Administrator

Erstellen Sie eine Replikationsregel im Quellkonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Replikationsregel für den Quell-Bucket im Quellkonto.	Im AWS Quellkonto: 1. Öffnen Sie die Amazon S3-Konsole. 2. Navigieren Sie zum Quell-Bucket und wählen Sie die Registerkarte Management aus. 3. Erstellen Sie eine Replikationsregel mit der folgenden Konfiguration: a. Geben Sie einen Regelnamen wies`3-replication-rule` . b. Wählen Sie für Status die Option Enabled. c. Wählen Sie unter Regelbereich die Option Gilt für alle Objekte im Bucket aus. d. Wählen Sie für Ziel die Option Spezifizieren Sie einen Bucket in einem anderen Konto aus und geben Sie dann die AWS-Konto Zielnummer und den Bucket-Namen ein. e. Wählen Sie die Option, um den Eigentümer des Objekts auf den Besitzer	AWS-Administrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	des Ziel-Buckets zu ändern. f. Wählen Sie für die IAM-Rolle die Rolle aus, die Sie zuvor im Quellkonto erstellt haben. g. Wählen Sie für Zusätzliche Replikationsoptionen alle verfügbaren Optionen aus. Diese bieten die Möglichkeit, Inhalte schnell zu replizieren, den Fortschritt der Replikation anhand von CloudWatch Amazon-Metriken zu überwachen, Löschmarkierungen zu replizieren und Metadatenänderungen zu replizieren. h. Wählen Sie Speichern. 4. Wenn Sie mehrere Ziel-Buckets haben, erstellen Sie zusätzliche Replikationsregeln. Weitere Informationen finden Sie in der Amazon S3 S3-Dokumentation unter Konfiguration der Replikation, wenn Quell- und Ziel-Buck	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ets unterschiedlichen Konten gehören.	

Wenden Sie eine Bucket-Richtlinie auf den Ziel-Bucket an

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wenden Sie eine Bucket-Richtlinie auf den Ziel-Bucket an.	Dieser Schritt muss für jeden Ziel-Bucket einzeln in den AWS Zielkonten ausgeführt werden. Im AWS Zielkonto: 1. Öffnen Sie die Amazon S3 S3-Konsole, navigieren Sie zum Ziel-Bucket und wählen Sie den Tab Permissions. 2. Bearbeiten Sie die Bucket-Richtlinie, indem Sie den folgenden JSON-Code angeben, und speichern Sie die Richtlinie: `{ "Version": "2012-10-17", "Id": "PolicyForDestinationBucket", "Statement": [ { "Sid": "Permissions on objects and buckets",`	AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::SourceAWSAccountNumber:role/IAM-Role-created-in-step1-in-source-account" }, "Action": ["s3:List*", "s3:GetBucketVersioning", "s3:PutBucketVersioning", "s3:ReplicateDelete", "s3:ReplicateObject"], "Resource": ["arn:aws:s3:::destination-bucket", "arn:aws:s3:::destination-bucket/*"] }, { "Sid": "Permission to override bucket owner", "Effect": "Allow",	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	"Principa
	l": {
	"AWS":
	"arn:aws:iam::Sour
	ceAWSAccountNumber
	:role/IAM-Role-cre
	ated-in-step1-in-s
	ource-account"
	},
	"Action":
	"s3:ObjectOwnerOve
	rrideToBucketOwner",
	"Resource
	": "arn:aws:s3:::dest
	ination-bucket/*"
	}
	]
	}
	
	Diese Richtlinie umfasst zwei Aussagen:
	
	• `Permissions on objects and bucketsgibt` an, dass der Ziel-Bucket Inhalte basierend auf der im Quellkonto definierten Rolle replizieren kann. Die Rolle stellt Berechtigungen für den Quell-Bucket bereit.
	• `Permission to override bucket ownergibt` an, dass der Ziel-Bucket berechtigt ist, die Inhaberschaft des Quellkontos außer Kraft zu setzen.	

Testen Sie die kontoübergreifende Amazon S3 S3-Replikation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die Replikation ordnungsgemäß funktioniert.	1. Fügen Sie dem Quell-Bucket ein Objekt hinzu. 2. Stellen Sie sicher, dass das neue Objekt in den S3-Buckets der Zielkonten erscheint. 3. CloudWatch Metriken anzeigen: a. Wählen Sie im Quell-Bucket die Registerkarte Metriken aus. b. Wählen Sie im Abschnitt Replikationsmetriken eine Replikationsregel aus. c. Wählen Sie Display charts (Diagramme anzeigen). Die Diagramme geben den Status der Replikation wieder, indem sie die Vorgänge, deren Replikation noch aussteht, die Replikationslatenz und die zur Replikation anstehenden Byte anzeigen. Weitere Informationen finden Sie unter Überwachen von Metriken mit Amazon	AWS-Administrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CloudWatch in der Amazon S3 S3-Dokumentation.	

Zugehörige Ressourcen

- Wann verwende ich IAM? (IAM-Dokumentation)
- So funktioniert IAM (IAM-Dokumentation)
- IAM-Rollen erstellen (IAM-Dokumentation)
- IAM-Richtlinien erstellen (IAM-Dokumentation)
- Überblick über die Zugriffsverwaltung: Berechtigungen und Richtlinien (IAM-Dokumentation)
- Amazon S3 S3-Buckets erstellen, konfigurieren und damit arbeiten (Amazon S3 S3-Dokumentation)
- Objekte in Amazon S3 hochladen, herunterladen und mit ihnen arbeiten (Amazon S3 S3-Dokumentation)
- Objekte replizieren (Amazon S3 S3-Dokumentation)

Migrieren Sie Daten mithilfe DistCp von AWS PrivateLink für Amazon S3 von einer lokalen Hadoop-Umgebung zu Amazon S3

Erstellt von Jason Owens (AWS), Andres Cantor (AWS), Jeff Klopfenstein (AWS), Bruno Rocha Oliveira (AWS) und Samuel Schmidt (AWS)

Übersicht

Dieses Muster zeigt, wie fast jede Datenmenge aus einer lokalen Apache Hadoop-Umgebung in die Amazon Web Services (AWS) -Cloud migriert werden kann, indem das Open-Source-Tool Apache DistCpmit AWS PrivateLink for Amazon Simple Storage Service (Amazon S3) verwendet wird. Anstatt das öffentliche Internet oder eine Proxy-Lösung für die Datenmigration zu verwenden, können Sie AWS PrivateLink für Amazon S3 verwenden, um Daten über eine private Netzwerkverbindung zwischen Ihrem lokalen Rechenzentrum und einer Amazon Virtual Private Cloud (Amazon VPC) zu Amazon S3 zu migrieren. Wenn Sie DNS-Einträge in Amazon Route 53 verwenden oder Einträge in der Datei /etc/hosts in allen Knoten Ihres lokalen Hadoop-Clusters hinzufügen, werden Sie automatisch zum richtigen Schnittstellenendpunkt weitergeleitet.

Dieses Handbuch enthält Anweisungen DistCp zur Migration von Daten in die AWS-Cloud. DistCp ist das am häufigsten verwendete Tool, es sind jedoch auch andere Migrationstools verfügbar. Sie können beispielsweise Offline-AWS-Tools wie AWS Snowball oder AWS Snowmobile oder Online-AWS-Tools wie AWS Storage Gateway oder AWS verwenden. DataSync Darüber hinaus können Sie andere Open-Source-Tools wie Apache verwenden. NiFi

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit einer privaten Netzwerkverbindung zwischen Ihrem lokalen Rechenzentrum und der AWS-Cloud
- Hadoop, lokal installiert mit DistCp
- Ein Hadoop-Benutzer mit Zugriff auf die Migrationsdaten im Hadoop Distributed File System (HDFS)
- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert
- Berechtigungen zum Ablegen von Objekten in einen S3-Bucket

Einschränkungen

Einschränkungen der Virtual Private Cloud (VPC) gelten PrivateLink für AWS für Amazon S3. Weitere Informationen finden Sie unter Eigenschaften und Einschränkungen von Schnittstellenendpunkten und PrivateLink AWS-Kontingente (PrivateLink AWS-Dokumentation).

AWS PrivateLink für Amazon S3 unterstützt Folgendes nicht:

- Endpunkte für den Federal Information Processing Standard (FIPS).
- Endpunkte der Website
- Globale Legacy-Endpunkte

Architektur

Quelltechnologie-Stack

- Hadoop-Cluster mit installiertem DistCp

Zieltechnologie-Stack

- Amazon S3
- Amazon VPC

Zielarchitektur

Das Diagramm zeigt, wie der DistCp Hadoop-Administrator Daten aus einer lokalen Umgebung über eine private Netzwerkverbindung wie AWS Direct Connect über einen Amazon S3-Schnittstellenendpunkt nach Amazon S3 kopiert.

Tools

AWS-Services

- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.

Andere Tools

- Apache Hadoop DistCp (Distributed Copy) ist ein Tool, das zum Kopieren großer Inter-Cluster und Intra-Cluster verwendet wird. DistCp verwendet Apache MapReduce für die Verteilung, Fehlerbehandlung und Wiederherstellung sowie für die Berichterstattung.

Epen

Daten in die AWS-Cloud migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Endpunkt für AWS PrivateLink für Amazon S3.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon VPC-Konsole. 2. Wählen Sie im Navigationsbereich Endpoints und dann Create Endpoint aus. 3. Wählen Sie für Service category die Option AWS services. 4. Geben Sie in das Suchfeld s3 ein, und drücken Sie dann die Eingabetaste. 5. Wählen Sie in den Suchergebnissen die Datei com.amazonaws aus. < your-aws-region >.s3-Dienstname, wobei der Wert in	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Spalte Typ Interface lautet. 6. Wählen Sie unter VPC Ihre VPC aus. Wählen Sie für Subnetze Ihre Subnetze aus. 7. Wählen oder erstellen Sie für Sicherheitsgruppe eine Sicherheitsgruppe, die TCP 443 zulässt. 8. Fügen Sie je nach Ihren Anforderungen Tags hinzu und wählen Sie dann Create Endpoint aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Endpunkte und suchen Sie nach den DNS-Einträgen.	1. Öffnen Sie die Amazon VPC-Konsole, wählen Sie Endpoints und dann den Endpoint aus, den Sie zuvor erstellt haben. 2. Suchen Sie auf der Registerkarte Details nach dem ersten DNS-Eintr ag für DNS-Namen. Dies ist der regionale DNS-Eintrag. Wenn Sie diesen DNS-Namen verwenden , wechseln sich Anfragen zwischen DNS-Einträgen ab, die für Availability Zones spezifisch sind. 3. Wählen Sie die Registerk arte Subnetze. Sie finden die Adresse der elastic network interface des Endpunkts in jeder Availabil ity Zone.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Firewall-Regeln und Routing-K onfigurationen.	Um zu überprüfen, ob Ihre Firewallregeln geöffnet sind und ob Ihre Netzwerkk onfiguration korrekt eingerich tet ist, testen Sie den Endpunkt mit Telnet auf Port 443. Zum Beispiel:
	
	`$ telnet vpce-<you r-VPC-endpoint-ID> .s3.us-east-2.vpce .amazonaws.com 443`
	
	`Trying 10.104.88.6...`
	
	`Connected to vpce-<you r-VPC-endpoint-ID> .s3.us-east-2.vpce .amazonaws.com.`
	
	`...`
	
	`$ telnet vpce-<you r-VPC-endpoint-ID> .s3.us-east-2.vpce .amazonaws.com 443`
	
	`Trying 10.104.71 .141...`
	
	`Connected to vpce-<you r-VPC-endpoint-ID> .s3.us-east-2.vpce .amazonaws.com.`
	
	Note
	Wenn Sie den Eintrag Regional verwenden
		Netzwerkadministrator, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	, zeigt ein erfolgrei cher Test, dass das DNS zwischen den beiden IP-Adress en wechselt, die Sie auf der Registerk arte Subnetze für Ihren ausgewähl ten Endpunkt in der Amazon VPC-Konsole sehen können.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Namensauflösung.	Sie müssen die Namensauflösung so konfigurieren, dass Hadoop auf den Amazon S3 S3-Schnittstellenendpunkt zugreifen kann. Sie können den Endpunktnamen selbst nicht verwenden. Stattdessen müssen Sie `<your-bucket-name>.s3.<your-aws-region>.amazonaws.com` oder auflösen `*.s3.<your-aws-region>.amazonaws.com`. Weitere Informationen zu dieser Namensbeschränkung finden Sie unter Einführung in den Hadoop S3A-Client (Hadoop-Website). Wählen Sie eine der folgenden Konfigurationsoptionen: • Verwenden Sie lokales DNS, um die private IP-Adresse des Endpunkts aufzulösen. Sie können das Verhalten für alle Buckets oder für ausgewählte Buckets außer Kraft setzen. Weitere Informationen finden Sie unter „Option 2: Zugriff auf Amazon S3 mithilfe von Domain Name System Response	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Policy Zones (DNS RPZ)“ in Sicherer Hybridzugriff auf Amazon S3 mit AWS PrivateLink (AWS-Blog beitrag). • Konfigurieren Sie das lokale DNS so, dass der Datenverkehr bedingt an die eingehenden Resolver-Endpunkte in der VPC weitergeleitet wird. Der Verkehr wird auf die Route 53 weitergeleitet. Weitere Informationen finden Sie unter „Option 3: Weiterlei ten von DNS-Anfragen vor Ort mithilfe von Amazon Route 53 Resolver Inbound Endpoints“ in Sicherer Hybridzugriff auf Amazon S3 mithilfe von AWS PrivateLink (AWS-Blog beitrag). • Bearbeiten Sie die Datei / etc/hosts auf allen Knoten in Ihrem Hadoop-Cluster. Dies ist eine temporäre Lösung für Tests und wird nicht für die Produktion empfohlen . Um die Datei /etc/hosts zu bearbeiten, fügen Sie einen Eintrag für entweder `<your-bucket-name> .s3.<your-aws-regi`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	on>.amazonaws.com oder s3.<your-aws-region>.amazonaws.com hinzu. Die Datei /etc/hosts darf nicht mehrere IP-Adressen für einen Eintrag haben. Sie müssen eine einzelne IP-Adresse aus einer der Availability Zones auswählen, die dann zu einer einzigen Fehlerquelle wird.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Authentifizierung für Amazon S3.	Um sich über Hadoop bei Amazon S3 zu authentifizieren, empfehlen wir, temporäre Rollenanmeldedaten in die Hadoop-Umgebung zu exportieren. Weitere Informationen finden Sie unter Authentifizierung mit S3 (Hadoop-Website). Für Jobs mit langer Laufzeit können Sie einen Benutzer erstellen und ihm eine Richtlinie zuweisen, die nur berechtigt ist, Daten in einem S3-Bucket abzulegen. Der Zugriffsschlüssel und der geheime Schlüssel können in Hadoop gespeichert werden und sind nur für den DistCp Job selbst und für den Hadoop-Administrator zugänglich. Weitere Informationen zum Speichern von Geheimnissen finden Sie unter Speichern von Geheimnissen mit Hadoop Credential Providers (Hadoop-Website). Weitere Informationen zu anderen Authentifizierungsmethoden finden Sie unter So erhalten Sie Anmeldeinformationen für eine IAM-Rolle zur Verwendung mit CLI-Zugriff auf ein AWS-Konto in der Dokumentation für AWS	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	IAM Identity Center (Nachfolger von AWS Single Sign-On).
	
	Um temporäre Anmeldeinformationen zu verwenden, fügen Sie die temporären Anmeldeinformationen zu Ihrer Anmeldeinformationsdatei hinzu oder führen Sie die folgenden Befehle aus, um die Anmeldeinformationen in Ihre Umgebung zu exportieren:
	
	`export AWS_SESSION_TOKEN=SECRET-SESSION-TOKEN`
	`export AWS_ACCESS_KEY_ID=SESSION-ACCESS-KEY`
	`export AWS_SECRET_ACCESS_KEY=SESSION-SECRET-KEY`
	
	Wenn Sie über eine herkömmliche Kombination aus Zugriffsschlüssel und geheimer Taste verfügen, führen Sie die folgenden Befehle aus:
	
	`export AWS_ACCESS_KEY_ID=my.aws.key`
	`export AWS_SECRET_ACCESS_KEY=my.secret.key`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Wenn Sie eine Kombination aus Zugriffsschlüssel und geheimem Schlüssel verwenden, ändern Sie den Anbieter der Anmeldein formationen in den DistCp Befehlen von `"org.apac he.hadoop .fs.s3a.T emporaryA WSCredent ialsProvider" bis"org.apac he.hadoop .fs.s3a.S impleAWSC redential sProvider"` .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Daten übertragen mit DistCp.	Führen Sie DistCp die folgenden Befehle aus, um Daten zu übertragen: `hadoop distcp -Dfs.s3a.aws.credentials.provider=\"org.apache.hadoop.fs.s3a.TemporaryAWSCredentialsProvider" \ -Dfs.s3a.access.key="${AWS_ACCESS_KEY_ID}" \ -Dfs.s3a.secret.key="${AWS_SECRET_ACCESS_KEY}" \ -Dfs.s3a.session.token="${AWS_SESSION_TOKEN}" \ -Dfs.s3a.path.style.access=true \ -Dfs.s3a.connection.ssl.enabled=true \ -Dfs.s3a.endpoint=s3.<your-aws-region>.amazonaws.com \ hdfs:///user/root/ s3a://<your-bucket-name>` **Note** Die AWS-Region des Endpunkts wird nicht automatisch erkannt, wenn Sie den DistCp Befehl	Migrationsingenieur, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	mit AWS PrivateLink for Amazon S3 verwenden. Hadoop 3.3.2 und spätere Versionen lösen dieses Problem, indem sie die Option aktivieren, die AWS-Region des S3-Buckets explizit festzulegen. Weitere Informationen finden Sie unter S3A, um die Option fs.s3a.endpoint.region hinzuzufügen, um die AWS-Region festzulegen (Hadoop-Website). Weitere Informationen zu zusätzlichen S3A-Anbietern finden Sie unter Allgemeine S3A-Client-Konfiguration (Hadoop-Website). Wenn Sie beispielsweise Verschlüsselung verwenden, können Sie der obigen Befehlsreihe je nach Verschlüsselungstyp die folgende Option hinzufügen: `-Dfs.s3a.server-side-encryption-algorithm=AES-256 [or SSE-C or SSE-KMS]`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Um den Schnittstellenendpunkt mit S3A zu verwenden, müssen Sie einen DNS-Alias eintrag für den S3-Regionalnamen (z. B. `s3.<your-aws-region>.amazonaws.com`) für den Schnittstellenendpunkt erstellen. Anweisungen finden Sie im Abschnitt Authentifizierung für Amazon S3 konfigurieren. Diese Problemumgehung ist für Hadoop 3.3.2 und frühere Versionen erforderlich. Zukünftige Versionen von S3A benötigen diese Problemumgehung nicht. Wenn Sie Signaturprobleme mit Amazon S3 haben, fügen Sie eine Option hinzu, um Signature Version 4 (Sigv4) zu signieren:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`-Dmapreduce.map.java.opts="-Dcom.amazonaws.services.s3.enableV4=true"`	

Mehr Muster

- Zugriff AWS-Services von IBM z/OS aus durch Installation des AWS CLI
- Automatisieren Sie ereignisgesteuerte Backups von CodeCommit zu Amazon S3 mithilfe CodeBuild von und Events CloudWatch
- Automatisches Archivieren von Elementen in Amazon S3 mithilfe von DynamoDB TTL
- Automatisches Backup von SAP HANA-Datenbanken mit Systems Manager und EventBridge
- Mainframe-Daten mithilfe von BMC AMI Cloud Data auf Amazon S3 sichern und archivieren
- Erstellen Sie eine ETL-Servicepipeline, um Daten mithilfe von AWS Glue inkrementell von Amazon S3 nach Amazon Redshift zu laden
- Konfigurieren Sie die Protokollierung von Modellaufrufen in Amazon Bedrock mithilfe von AWS CloudFormation
- EBCDIC-Daten mithilfe von Python in ASCII auf AWS konvertieren und entpacken
- Konvertiert VARCHAR2 (1) den Datentyp für Oracle in den booleschen Datentyp für Amazon Aurora PostgreSQL
- Erstellen Sie eine Amazon ECS-Aufgabendefinition und mounten Sie mithilfe von Amazon EFS ein Dateisystem auf EC2 Instances
- Stellen Sie DynamoDB-Datensätze mithilfe von Kinesis Data Streams und Firehose an Amazon S3 bereit mit AWS CDK
- Stellen Sie mithilfe von Terraform und DRA ein Lustre-Dateisystem für die Hochleistungsdatenverarbeitung bereit
- Schätzung der Speicherkosten für eine Amazon DynamoDB-Tabelle
- Identifizieren Sie öffentliche Amazon S3 S3-Buckets mithilfe AWS Organizations von Security Hub
- Migrieren Sie Amazon RDS for Oracle DB-Instances zu anderen Konten, die AMS verwenden
- Migrieren Sie einen lokalen SFTP-Server zur Verwendung von AWSAWS Transfer for SFTP
- Migrieren Sie eine partitionierte Oracle-Tabelle mithilfe von AWS DMS zu PostgreSQL
- Migrieren Sie Daten mithilfe von Rclone von Microsoft Azure Blob zu Amazon S3
- Migrieren Sie Oracle CLOB-Werte in einzelne Zeilen in PostgreSQL auf AWS
- Migrieren Sie gemeinsam genutzte Dateisysteme in einer großen AWS-Migration
- Migrieren Sie kleine Datensätze mithilfe von AWS SFTP von der lokalen Infrastruktur zu Amazon S3
- Überwachen Sie Amazon Aurora auf Instances ohne Verschlüsselung

- Verschieben Sie Mainframe-Dateien mit Transfer Family direkt nach Amazon S3
- Entfernen Sie EC2 Amazon-Einträge in derselben AWS-Konto Form AWS Managed Microsoft AD mithilfe von AWS Lambda Automatisierung
- Führen Sie statusbehaftete Workloads mit persistentem Datenspeicher aus, indem Sie Amazon EFS auf Amazon EKS mit AWS Fargate verwenden
- Erfolgreicher Import eines S3-Buckets als CloudFormation AWS-Stack
- Synchronisieren Sie Daten zwischen Amazon EFS-Dateisystemen in verschiedenen AWS-Regionen mithilfe von AWS DataSync
- EBS-Snapshot-Details für Ihr AWS-Konto oder Ihre Organisation anzeigen

Entwickler-Tools

Themen

- DevOps
- Infrastruktur
- Web- und mobile Apps

DevOps

Themen

- Automatisieren Sie den AWS Infrastrukturbetrieb mithilfe von Amazon Bedrock
- Automatisieren Sie mithilfe von Terraform CloudFront Updates, wenn sich die Load Balancer-Endpunkte ändern
- Automatisieren Sie CodeGuru Amazon-Rezensionen für AWS CDK Python-Anwendungen mithilfe von GitHub Aktionen
- Automatisieren Sie die AWS-Ressourcenbewertung
- Automatische Installation von SAP-Systemen mithilfe von Open-Source-Tools
- Automatisieren Sie das AWS Service Catalog-Portfolio und die Produktbereitstellung mithilfe von AWS CDK
- Automatisieren Sie ereignisgesteuerte Backups von CodeCommit zu Amazon S3 mithilfe CodeBuild von und Events CloudWatch
- Automatisieren Sie das Löschen von AWS CloudFormation Stacks und zugehörigen Ressourcen
- Automatisieren Sie das dynamische Pipeline-Management für die Bereitstellung von Hotfix-Lösungen in Gitflow-Umgebungen mithilfe von und AWS Service CatalogAWS CodePipeline
- Automatisieren Sie die Erfassung und Visualisierung von benutzerdefinierten Amazon MWAA-Metriken auf Amazon Managed Grafana mithilfe von Terraform
- Optimieren Sie die Entwicklung und Bereitstellung von Amazon Lex Lex-Bot mithilfe eines automatisierten Workflows
- Automatisieren Sie die Stackset-Bereitstellung mithilfe von AWS CodePipeline und AWS CodeBuild
- Automatisches Hinzufügen einer von AWS verwalteten Richtlinie für Systems Manager zu EC2 Instanzprofilen mithilfe von Cloud Custodian und AWS CDK
- Automatisches Erstellen von CI/CD-Pipelines und Amazon ECS-Clustern für Microservices mithilfe von AWS CDK
- Erstellen Sie eine lose gekoppelte Architektur mit Microservices mithilfe von DevOps Praktiken und AWS Cloud9
- Erstellen und übertragen Sie Docker-Images mithilfe von GitHub Actions und Terraform auf Amazon ECR
- Erstellen und testen Sie iOS-Apps mit AWS CodeCommit CodePipeline, AWS und AWS Device Farm

- Suchen Sie in den AWS-CDK-Anwendungen oder CloudFormation -Vorlagen nach bewährten Methoden mithilfe von cdk-nag-Regelpaketen
- Konfigurieren Sie die gegenseitige TLS-Authentifizierung für Anwendungen, die auf Amazon EKS ausgeführt werden
- Automatisieren Sie die Erstellung von AppStream 2.0-Ressourcen mit AWS CloudFormation
- Erstellen Sie einen benutzerdefinierten Protokollparser für Amazon ECS mithilfe eines Firelens-Protokollrouters
- Erstellen Sie eine Pipeline und ein AMI mit CodePipeline und HashiCorp Packer
- Erstellen Sie eine Pipeline und stellen Sie Artefaktaktualisierungen für lokale Instanzen EC2 bereit mit CodePipeline
- Automatisches Erstellen dynamischer CI-Pipelines für Java- und Python-Projekte
- Stellen Sie CloudWatch Synthetics Canaries mithilfe von Terraform bereit
- Stellen Sie eine CI/CD-Pipeline für Java-Microservices auf Amazon ECS bereit
- Stellen Sie eine ChatOps Lösung zur Verwaltung von SAST-Scanergebnissen bereit, indem Sie Amazon Q Developer in Chat-Anwendungen verwenden, benutzerdefinierte Aktionen und AWS CloudFormation
- Stellen Sie eine Firewall mit AWS Network Firewall und AWS Transit Gateway bereit
- Stellen Sie einen AWS Glue Glue-Job mit einer AWS CodePipeline CI/CD-Pipeline bereit
- Stellen Sie mithilfe eines EC2 Instanzprofils einen Amazon EKS-Cluster aus AWS Cloud9 bereit
- Stellen Sie mithilfe von AWS CodePipeline, AWS und AWS Code in mehreren CodeCommit AWS-Regionen bereit CodeBuild
- Führen Sie Amazon Redshift SQL-Abfragen mithilfe von Terraform aus
- Exportieren Sie AWS Backup Backup-Berichte aus einer gesamten Organisation in AWS Organizations als CSV-Datei
- Tags für eine Liste von EC2 Amazon-Instances in eine CSV-Datei exportieren
- Generieren Sie mithilfe von Troposphere eine CloudFormation AWS-Vorlage, die von AWS Config verwaltete Regeln enthält
- Geben Sie SageMaker Notebook-Instances temporären Zugriff auf ein CodeCommit Repository in einem anderen AWS-Konto
- Implementieren Sie eine GitHub Flow-Branching-Strategie für Umgebungen mit mehreren Konten DevOps

- Implementieren Sie eine Gitflow-Branching-Strategie für Umgebungen mit mehreren Konten DevOps
- Implementieren Sie eine Trunk-Branching-Strategie für Umgebungen mit mehreren Konten DevOps
- Implementieren Sie zentralisiertes benutzerdefiniertes Checkov-Scanning, um Richtlinien vor der Bereitstellung AWS der Infrastruktur durchzusetzen
- Automatische Erkennung von Änderungen und Initiierung verschiedener CodePipeline Pipelines für ein Monorepo in CodeCommit
- Integrieren Sie mithilfe von AWS ein Bitbucket-Repository mit AWS Amplify CloudFormation
- Starten Sie mithilfe von Step Functions und einer Lambda-Proxyfunktion ein CodeBuild Projekt für alle AWS-Konten
- Multi-AZ-Failover für EMR-Cluster mithilfe von Application Recovery Controller verwalten
- Verwalten Sie Blau/Grün-Bereitstellungen von Microservices für mehrere Konten und Regionen mithilfe von AWS-Code-Services und AWS KMS-Regionsschlüsseln für mehrere Regionen
- Überwachen Sie Amazon ECR-Repositorys mit AWS und AWS CloudFormation Config auf Platzhalterberechtigungen
- Optimieren Sie serverlose Bereitstellungen mit mehreren Konten mithilfe der AWS CDK Workflows und Aktionen GitHub
- Führen Sie benutzerdefinierte Aktionen aus CodeCommit AWS-Ereignissen durch
- Bereitstellen von AWS Service Catalog Produkten auf der Grundlage von AWS CloudFormation Vorlagen mithilfe von GitHub Aktionen
- Stellen Sie IAM-Rollen mit den geringsten Rechten bereit, indem Sie eine Rollenautomatenlösung bereitstellen
- Veröffentlichen Sie CloudWatch Amazon-Metriken in einer CSV-Datei
- Entfernen Sie EC2 Amazon-Einträge AWS Managed Microsoft AD mithilfe AWS-Konten von AWS Lambda Automatisierung
- Entfernen Sie EC2 Amazon-Einträge in derselben AWS-Konto Form AWS Managed Microsoft AD mithilfe von AWS Lambda Automatisierung
- Führen Sie Komponententests für Python-ETL-Jobs AWS Glue mithilfe des Pytest-Frameworks aus
- Richten Sie ein Helm v3-Chart-Repository in Amazon S3 ein
- Richten Sie eine CI/CD-Pipeline mithilfe von AWS CodePipeline und AWS CDK ein
- Richten Sie mithilfe von Terraform eine zentrale Protokollierung auf Unternehmensebene ein

- Richten Sie die end-to-end Verschlüsselung für Anwendungen auf Amazon EKS mithilfe von cert-manager und Let's Encrypt ein
- Vereinfachen Sie die Bereitstellung von Amazon EKS-Anwendungen für mehrere Mandanten mithilfe von Flux
- Abonnieren Sie mithilfe einer benutzerdefinierten Ressource mehrere E-Mail-Endpunkte für ein SNS-Thema
- Koordinieren Sie die Ressourcenabhängigkeit und die Aufgabenausführung mithilfe des AWS Fargate WaitCondition Hook-Konstrukts
- Verwenden Sie Git-Quell-Repositorys von Drittanbietern in AWS CodePipeline
- Erstellen Sie eine CI/CD-Pipeline zur Validierung von Terraform-Konfigurationen mithilfe von AWS CodePipeline
- Mehr Muster

Automatisieren Sie den AWS Infrastrukturbetrieb mithilfe von Amazon Bedrock

Erstellt von Ishwar Chauthaiwale (AWS) und Anand Bukkapatnam Tirumala (AWS)

Übersicht

Bei Cloud-Native-Lösungen spielt die Automatisierung gängiger Infrastrukturoperationen eine entscheidende Rolle bei der Aufrechterhaltung effizienter, sicherer und kostengünstiger Umgebungen. Die manuelle Bearbeitung von Vorgängen ist zeitaufwändig und anfällig für menschliche Fehler. Darüber hinaus müssen Teammitglieder mit unterschiedlichem AWS Fachwissen diese Aufgaben ausführen und gleichzeitig die Einhaltung der Sicherheitsprotokolle sicherstellen. Dieses Muster zeigt, wie Amazon Bedrock verwendet wird, um allgemeine AWS Infrastrukturoperationen durch Natural Language Processing (NLP) zu automatisieren.

Dieses Muster kann Unternehmen dabei helfen, wiederverwendbaren, modularen und sicheren Code für die Bereitstellung generativer KI-basierter Infrastrukturen in mehreren Umgebungen zu entwickeln. Durch seinen Fokus auf Infrastructure as Code (IaC) und Automatisierung bietet es wichtige DevOps Vorteile wie Versionskontrolle, konsistente Bereitstellungen, weniger Fehler, schnellere Bereitstellung und verbesserte Zusammenarbeit.

Das Pattern implementiert eine sichere Architektur, die es Teams ermöglicht, Abläufe in Bezug auf wichtige Aufgaben zu verwalten, darunter: AWS-Services

- Versionsverwaltung für Buckets mit Amazon Simple Storage Service (Amazon S3)
- Erstellung eines Amazon Relational Database Service (Amazon RDS) -Snapshots
- Amazon Elastic Compute Cloud (Amazon EC2) Instanzverwaltung

Die Architektur verwendet Amazon Virtual Private Cloud (Amazon VPC) -Endpunkte und private Netzwerke für eine sichere Kommunikation, wobei AWS Lambda Funktionen als Task-Executoren in privaten Subnetzen fungieren. Amazon S3 bietet Datenmanagement und implementiert umfassende AWS Identity and Access Management (IAM) -Rollen und -Berechtigungen, um angemessene Zugriffskontrollen zu gewährleisten. Diese Lösung beinhaltet keine Chat-Verlaufsfunktion und der Chat wird nicht gespeichert.

Voraussetzungen und Einschränkungen

- Ein aktiver AWS-Konto.

- Es sollten angemessene Zugangskontrollmaßnahmen getroffen werden, um den Zugang zu sichern und zu kontrollieren. Zu den Beispielen für die Zugriffskontrolle gehören die Verwendung AWS Systems Manager von Basismodellen für den Zugriff, eine IAM-Rolle für die Bereitstellung und servicebasierte Rollen, die Deaktivierung des öffentlichen Zugriffs auf Amazon S3 S3-Buckets und die Einrichtung einer Warteschlange für unzustellbare Briefe.
- Ein () vom Kunden verwalteter Schlüssel AWS Key Management Service .AWS KMS
- AWS Command Line Interface (AWS CLI) Version 2 oder höher, in der Bereitstellungsumgebung installiert und konfiguriert.
- Terraform AWS Provider Version 4 oder höher installiert und konfiguriert.
- Terraform Version 1.5.7 oder höher wurde installiert und konfiguriert.
- Überprüfen und definieren Sie OpenAPI-Schemas für die Aktionsgruppen Ihres Agenten in Amazon Bedrock, um sich vor unbefugtem Zugriff zu schützen und die Datenintegrität zu wahren.
- Der Zugriff ist in Ihrem AWS-Konto für die erforderlichen Amazon Titan Text Embeddings v2 und entweder für die Claude 3.5 Sonnet- oder Claude 3 Haiku Foundation-Modelle aktiviert. Um Bereitstellungsfehler zu vermeiden, stellen Sie sicher, dass Ihre Zielbereitstellung AWS-Region die erforderlichen Modelle unterstützt.
- Eine konfigurierte Virtual Private Cloud (VPC), die den Best Practices des AWS Well Architected Framework folgt.
- Die Überprüfung der Amazon Responsible AI-Richtlinie wurde abgeschlossen.

Produktversionen

- Amazon Titan Texteinbettungen v2
- Anthropisches Claude 3.5 Sonett oder Claude 3 Haiku
- Terraform Provider Version 4 oder höher AWS
- Terraform Version 1.5.7 oder höher

Architektur

Das folgende Diagramm zeigt den Workflow und die Architekturkomponenten für dieses Muster.

Die Lösungsarchitektur besteht aus mehreren Ebenen, die zusammenarbeiten, um Anfragen in natürlicher Sprache zu verarbeiten und entsprechende AWS Operationen auszuführen:

1. Der Benutzer stellt Betriebsanfragen über die Amazon Bedrock-Chat-Konsole.
2. Der Chatbot verwendet Amazon Bedrock Knowledge Bases für die Bearbeitung von Anfragen. Es implementiert das Amazon Titan Text Embeddings v2-Modell für die Verarbeitung natürlicher Sprache.
3. Wenn die Benutzeraufforderung eine Aktionsanfrage enthält, verwendet die Amazon Bedrock-Aktionsgruppe entweder das Anthropic Claude 3 Haiku oder das Claude 3.5 Sonnet-Modell (je nach Ihrer Wahl) für die Ausführungslogik und definiert Operationen über ein OpenAPI-Schema.
4. Die Aktionsgruppe erreicht die Amazon VPC-Endpunkte und verwendet sie AWS PrivateLink für die sichere Servicekompetenz.
5. Die AWS Lambda Funktion wird über Amazon VPC-Endpunkte für Amazon Bedrock-Services erreicht.
6. Die Lambda-Funktionen sind die primäre Ausführungs-Engine. Basierend auf der Anfrage ruft die Lambda-Funktion die API auf, um Aktionen auf der AWS-Services auszuführen. Die Lambda-Funktion kümmert sich auch um das Routing und die Ausführung von Vorgängen.
7. AWS-Services Sie rufen die API-Anfrage von der Lambda-Funktion ab und die entsprechenden Operationen werden ausgeführt.
8. Die Lambda-Funktion berechnet eine Ausgangsnutzlast, die von Amazon Bedrock verstanden wird.
9. Diese Payload wird zur sicheren Servicekommunation an Amazon Bedrock gesendet. PrivateLink Das von Amazon Bedrock verwendete Large Language Model (LLM) versteht diese Nutzlast und wandelt sie in ein für Menschen verständliches Format um.
10. Die Ausgabe wird dem Benutzer dann auf der Amazon Bedrock Chat-Konsole angezeigt.

Die Lösung ermöglicht die folgenden primären Operationen:

- Amazon S3 — Aktivieren Sie die Bucket-Versionierung für die Versionskontrolle.
- Amazon RDS — Erstellen Sie Datenbank-Snapshots für Backups.
- Amazon EC2 — Listet Instances auf und kontrolliert den Start und Stopp von Instances.

Tools

AWS-Services

- Amazon Bedrock ist ein vollständig verwalteter Service, der Ihnen leistungsstarke Basismodelle (FMs) von führenden KI-Startups und Amazon über eine einheitliche API zur Verfügung stellt.

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie AWS-Services über Befehle in Ihrer Befehlszeilen-Shell interagieren können.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon OpenSearch Serverless ist eine serverlose On-Demand-Konfiguration für Amazon OpenSearch Service.
- AWS PrivateLinkhilft Ihnen dabei, unidirektionale, private Verbindungen von Ihren virtuellen privaten Clouds (VPCs) zu Diensten außerhalb der VPC herzustellen.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der. AWS Cloud
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Systems Managerhilft Ihnen bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der ausgeführt werden. AWS Cloud Es vereinfacht das Anwendungs- und Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme und hilft Ihnen, Ihre AWS Ressourcen sicher und in großem Umfang zu verwalten.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk bereitzustellen. Dieses virtuelle Netzwerk entspricht einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben würden, mit den Vorteilen der Verwendung der skalierbaren Infrastruktur von AWS.

Andere Tools

- Git ist ein verteiltes Open-Source-Versionskontrollsystem.
- Terraform ist ein IaC-Tool (Infrastructure as Code) HashiCorp , mit dem Sie Cloud- und lokale Ressourcen erstellen und verwalten können.

Code-Repository

Der Code für dieses Muster ist im GitHub infra-ops-orchestratoraws-samples/ Repository verfügbar.

Bewährte Methoden

- Überwachen Sie regelmäßig die Lambda-Ausführungsprotokolle. Weitere Informationen finden Sie unter Überwachung und Problembehandlung von Lambda-Funktionen. Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Methoden für die Arbeit mit AWS Lambda Funktionen.
- Überprüfen Sie die Sicherheitskonfigurationen regelmäßig, um sicherzustellen, dass die Anforderungen Ihres Unternehmens eingehalten werden. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden.
- Folgen Sie dem Prinzip der geringsten Rechte und gewähren Sie die für die Ausführung einer Aufgabe erforderlichen Mindestberechtigungen. Weitere Informationen finden Sie in der IAM-Dokumentation unter Gewährung der geringsten Rechte und bewährte Methoden zur Sicherheit.

Epen

Stellen Sie die Lösung bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Klonen Sie das Repository	Führen Sie den folgenden Befehl aus, um das Repository auf Ihrem lokalen Computer zu klonen:
	`git clone "git@github.com:aws-samples/infra-ops-orchestrator.git"`
	`cd infra-ops-orchestrator`
		AWS DevOps, DevOps Ingenieur

Bearbeiten Sie die Umgebungsvariablen.	Bearbeiten Sie die `terraform.tfvars` Datei. im Stammverzeichnis	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	des geklonten Repositorys. Überprüfen Sie die Platzhalter, die mit gekennzeichnet sind `[XXXXX]`, und aktualisieren Sie sie entsprechend Ihrer Umgebung.	

Erstellen Sie die Infrastruktur.	Führen Sie die folgenden Befehle aus, um die Infrastruktur zu erstellen:
	`terraform init`
	`terraform plan`
	Überprüfen Sie den Ausführungsplan sorgfältig. Wenn die geplanten Änderungen akzeptabel sind, führen Sie den folgenden Befehl aus:
	`terraform apply --auto-approve`
		AWS DevOps, DevOps Ingenieur

Greifen Sie auf die Lösung zu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Greifen Sie auf die Lösung zu.	Gehen Sie nach erfolgreicher Bereitstellung wie folgt vor, um die Chat-basierte Oberfläche zu verwenden:	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Um auf den Infrastructure Orchestrator Assistant zuzugreifen, melden Sie sich bei der Rolle AWS Management Console Using an IAM mit Amazon Bedrock-Berechtigungen an und öffnen Sie die Amazon Bedrock-Konsole unter. https://console.aws.amazon.com/bedrock/ Wählen Sie im linken Navigationsbereich Agenten aus. Wählen Sie dann im Abschnitt Agents den Infrastructure Orchestrator Assistant aus. 2. Stellen Sie sicher, dass in Ihrer AWS Umgebung Zielressourcen für die folgenden Vorschläge vorhanden sind, und probieren Sie dann diese Beispieloperationen aus: • Erstellen Sie ein Snapshot-Backup einer Amazon RDS-Instance, indem Sie fragen: „Erstellen Sie einen Snapshot der RDS-Instance [Instance-Name]“ • Aktivieren Sie die Versionierung in einem Amazon S3 S3-Bucket	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	, indem Sie fragen: 'Versionierung für Bucket [Bucket-Name] aktivieren' • Führen Sie EC2 Amazon-Instances auf, indem Sie fragen: „Alle EC2 Instanzen auflisten“ • Starten oder stoppen Sie eine EC2 Amazon-Instance, indem Sie fragen: „ EC2 Instanz starten [Instance-ID]“ oder „ EC2 Instanz beenden [Instance-ID]“ Hinweis: Ersetzen Sie die Werte in Klammern durch die tatsächlichen Ressourcennamen oder die aus Ihrer Umgebung. IDs AWS	

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die erstellten Ressourcen.	Führen Sie den folgenden Befehl aus, um die gesamte nach diesem Muster erstellte Infrastruktur zu löschen: `terraform plan -destroy` Prüfen Sie den Vernichtungsplan sorgfältig. Wenn	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die geplanten Löschungen akzeptabel sind, führen Sie den folgenden Befehl aus: `terraform destroy` Hinweis: Mit diesem Befehl werden alle Ressourcen, die nach diesem Muster erstellt wurden, dauerhaft gelöscht. Der Befehl fordert Sie zur Bestätigung auf, bevor Ressourcen entfernt werden.	

Fehlerbehebung

Problem	Lösung
Verhalten der Agenten	Informationen zu diesem Problem finden Sie unter Testen und Beheben von Problemen mit dem Verhalten von Agenten in der Amazon Bedrock-Dokumentation.
Probleme mit dem Lambda-Netzwerk	Informationen zu diesen Problemen finden Sie unter Problembehandlung bei Netzwerkproblemen in Lambda in der Lambda-Dokumentation.
IAM-Berechtigungen	Informationen zu diesen Problemen finden Sie unter Problembehandlung bei IAM in der IAM-Dokumentation.

Zugehörige Ressourcen

- Erstellen eines DB-Snapshots für eine Single-AZ-DB-Instance für Amazon RDS
- Definieren Sie OpenAPI-Schemas für die Aktionsgruppen Ihres Agenten in Amazon Bedrock
- Aktivierung der Versionierung für Buckets
- So funktioniert Amazon Bedrock Agents
- Rufen Sie Daten ab und generieren Sie KI-Antworten mit Amazon Bedrock Knowledge Bases
- Greifen Sie sicher auf Dienste zu über AWS PrivateLink
- Stoppen und starten Sie EC2 Amazon-Instances
- Verwenden Sie Aktionsgruppen, um Aktionen zu definieren, die Ihr Agent ausführen soll

Automatisieren Sie mithilfe von Terraform CloudFront Updates, wenn sich die Load Balancer-Endpunkte ändern

Erstellt von Tamilselvan P (AWS), Mohan Annam (AWS) und Naveen Suthar (AWS)

Übersicht

Wenn Benutzer von Amazon Elastic Kubernetes Service (Amazon EKS) ihre Eingangskonfiguration über Helm-Diagramme löschen und erneut installieren, wird ein neuer Application Load Balancer (ALB) erstellt. Dies führt zu einem Problem, da Amazon CloudFront weiterhin auf den DNS-Eintrag der alten ALB verweist. Infolgedessen sind Dienste, die für diesen Endpunkt bestimmt sind, nicht erreichbar. (Weitere Informationen zu diesem problematischen Workflow finden Sie unter Zusätzliche Informationen.)

Um dieses Problem zu lösen, beschreibt dieses Muster die Verwendung einer benutzerdefinierten AWS Lambda Funktion, die mit Python entwickelt wurde. Diese Lambda-Funktion erkennt anhand von EventBridge Amazon-Regeln automatisch, wenn eine neue ALB erstellt wird. Mithilfe von aktualisiert die Funktion dann die CloudFront Konfiguration mit der DNS-Adresse der neuen ALB und stellt so sicher, dass der Datenverkehr an den richtigen Endpunkt weitergeleitet wird. AWS SDK für Python (Boto3)

Diese automatisierte Lösung gewährleistet die Servicekontinuität ohne zusätzliches Routing oder Latenz. Der Prozess trägt dazu bei, dass CloudFront immer auf den richtigen ALB-DNS-Endpunkt verwiesen wird, auch wenn sich die zugrunde liegende Infrastruktur ändert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto.
- Eine Beispiel-Webanwendung zum Testen und Validieren, die mithilfe von Helm auf Amazon EKS bereitgestellt wird. Weitere Informationen finden Sie unter Bereitstellen von Anwendungen mit Helm auf Amazon EKS in der Amazon EKS-Dokumentation.
- Konfigurieren Sie CloudFront die Konfiguration für die Weiterleitung von Anrufen an eine ALB, die von einem Helm-Ingress-Controller erstellt wurde. Weitere Informationen finden Sie unter Installieren von Load AWS Balancer Controller with Helm in der Amazon EKS-Dokumentation und Beschränken Sie den Zugriff auf Application Load Balancers in der CloudFront Dokumentation.
- Terraform wurde in einem lokalen Workspace installiert und konfiguriert.

Einschränkungen

- Einige AWS-Services sind nicht in allen verfügbar. AWS-Regionen Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie unter AWS Dienste nach Regionen. Informationen zu bestimmten Endpunkten finden Sie unter Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Produktversionen

- Terraform Version 1.0.0 oder höher
- Terraform AWS Provider Version 4.20 oder höher

Architektur

Das folgende Diagramm zeigt den Workflow und die Architekturkomponenten für dieses Muster.

Diese Lösung führt die folgenden Schritte aus:

1. Der Amazon EKS-Ingress Controller erstellt bei jedem Neustart oder einer Bereitstellung von Helm einen neuen Application Load Balancer (ALB).
2. EventBridge sucht nach Ereignissen zur ALB-Erstellung.
3. Das ALB-Erstellungsereignis löst die Lambda-Funktion aus.
4. Die Lambda-Funktion wurde auf der Grundlage von Python 3.9 bereitgestellt und verwendet zum Aufrufen die Boto3-API. AWS-Services Die Lambda-Funktion aktualisiert den CloudFront Eintrag mit dem neuesten Load Balancer-DNS-Namen, der von Create Load Balancer-Ereignissen empfangen wurde.

Tools

AWS-Services

- Amazon CloudFront beschleunigt die Verteilung Ihrer Webinhalte, indem es sie über ein weltweites Netzwerk von Rechenzentren bereitstellt, was die Latenz senkt und die Leistung verbessert.
- Mit Amazon Elastic Kubernetes Service (Amazon EKS) können Sie Kubernetes ausführen, AWS ohne dass Sie Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten müssen.

- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS Lambda Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen. AWS-Konten
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS SDK für Python (Boto3)ist ein Softwareentwicklungskit, mit dem Sie Ihre Python-Anwendung, -Bibliothek oder Ihr Skript integrieren können AWS-Services.

Andere Tools

- Python ist eine Allzweck-Computerprogrammiersprache.
- Terraform ist ein IaC-Tool (Infrastructure as Code) HashiCorp , mit dem Sie Cloud- und lokale Ressourcen erstellen und verwalten können.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub aws-cloudfront-automation-terraform-samples verfügbar.

Epen

Richten Sie eine lokale Workstation ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Git-CLI ein und konfigurieren Sie sie.	Um die Git-Befehlszeilens chnittstelle (CLI) auf Ihrer lokalen Workstation zu installie ren und zu konfigurieren, folgen Sie den Anweisung en Erste Schritte — Installat ion von Git in der Git-Dokum entation.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Projektordner und fügen Sie die Dateien hinzu.	1. Gehen Sie zum GitHub Repository des Patterns und wählen Sie die Code-Schaltfläche. 2. Wählen Sie im Dialogfeld „Klonen“ die Registerkarte „HTTPS“. Kopieren Sie unter Mithilfe der Web-URL klonen die angezeigte URL. 3. Erstellen Sie einen Ordner auf Ihrem lokalen Computer. Benennen Sie ihn mit Ihrem Projektnamen. 4. Öffnen Sie ein Terminal auf Ihrem lokalen Computer und navigieren Sie zu diesem Ordner. 5. Führen Sie den folgenden Befehl aus, um das Git-Repository dieses Musters zu klonen: `git clone https://github.com/aws-samples/aws-cloudfront-automation-terraform-samples` 6. Nachdem das Repository geklont wurde, verwenden Sie den folgenden Befehl, um zum geklonten Verzeichnis zu wechseln: `cd <directory`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`name>/cloudfront-update` Öffnen Sie dieses Projekt in einer integrierten Entwicklungsumgebung (IDE) Ihrer Wahl.	

Stellen Sie die Zielarchitektur mithilfe der Terraform-Konfiguration bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Lösung bereit.	Gehen Sie wie folgt vor AWS-Konto, um Ressourcen im Ziel bereitzustellen: 1. Rufen Sie den Ordner `cloudfront-update` auf. 2. Aktualisieren Sie die `terraform.tfvars` Datei mit dem`cloudfront_distribution_id` . 3. Führen Sie den folgenden Befehl aus, um das AWS-Region für Ihr AWS Profil festzulegen: `export AWS_REGION={{ REGION }}` 4. Führen Sie den folgenden Befehl aus, um Terraform zu initialisieren:	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`terraform init`
	5. Führen Sie den folgenden Befehl aus, um Terraform zu validieren:
	`terraform validate`
	6. Führen Sie den folgenden Befehl aus, um einen Terraform-Ausführungsplan zu erstellen:
	`terraform plan`
	7. Führen Sie den folgenden Befehl aus`terraform plan`, um die Aktionen von anzuwenden:
	`terraform apply`	

Überprüfen der Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Bereitstellung.	1. Melden Sie sich bei https://console.aws.amazon.com/cloudfront/v4/home an AWS Management Console und öffnen Sie die CloudFront Amazon-Konsole. 2. Wählen Sie im linken Navigationsbereich Distribut	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ionen aus und öffnen Sie dann die Distribution. CloudFront 3. Stellen Sie auf der Registerkarte Ursprünge sicher, dass der Ursprungs name und die Ursprungs zuordnung über den aktualisierten ALB-DNS-E intrag verfügen.	

Infrastruktur aufräumen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Säubere die Infrastruktur.	Gehen Sie wie folgt vor, um die Infrastruktur zu bereinigen, die Sie zuvor erstellt haben: 1. Führen Sie den folgenden Befehl aus: `terraform destroy` 2. Geben Sie ein, um den Befehl zum Löschen zu bestätigen`yes`.	DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Fehler beim Überprüfen der Anbietera nmeldedaten	Wenn Sie Terraform `apply` oder `destroy` Befehle von Ihrem lokalen Computer aus

Problem	Lösung
	ausführen, tritt möglicherweise ein Fehler auf, der dem folgenden ähnelt: `Error: configuring Terraform AWS Provider: error validating provider credentials: error calling sts:GetCallerIdentity: operation error STS: GetCallerIdentity, https response error StatusCode: 403, RequestID: 123456a9-fbc1-40ed-b8d8-513d0133ba7f, api error InvalidClientTokenId: The security token included in the request is invalid.` Dieser Fehler wird durch den Ablauf des Sicherheitstokens für die in der Konfiguration Ihres lokalen Computers verwendeten Anmeldeinformationen verursacht. Informationen zur Behebung des Fehlers finden Sie unter Konfigurationseinstellungen einrichten und anzeigen in der AWS Command Line Interface (AWS CLI) -Dokumentation.

Zugehörige Ressourcen

AWS Ressourcen

- Beschränken Sie den Zugriff auf Application Load Balancers
- Internetverkehr mit AWS Load Balancer Controller weiterleiten

Terraform-Dokumentation

- AWS Anbieter
- Installieren Sie Terraform
- Fernstatus

Zusätzliche Informationen

Problematischer Arbeitsablauf

Das Diagramm zeigt den folgenden Workflow:

1. Wenn der Benutzer auf die Anwendung zugreift, geht der Anruf an. CloudFront
2. CloudFront leitet die Aufrufe an den jeweiligen Application Load Balancer (ALB) weiter.
3. Der ALB enthält die Ziel-IP-Adressen, bei denen es sich um die IP-Adressen des Anwendungs-Pods handelt. Von dort aus stellt der ALB dem Benutzer die erwarteten Ergebnisse bereit.

Dieser Arbeitsablauf weist jedoch auf ein Problem hin. Die Anwendungsbereitstellungen erfolgen über Helm-Diagramme. Immer wenn es eine Bereitstellung gibt oder wenn jemand Helm neu startet, wird der entsprechende Eingang ebenfalls neu erstellt. Infolgedessen erstellt der externe Load Balancer-Controller den ALB neu. Außerdem wird die ALB bei jeder Neuerstellung mit einem anderen DNS-Namen neu erstellt. Aus diesem Grund CloudFront wird es in den Ursprungseinstellungen einen veralteten Eintrag geben. Aufgrund dieses veralteten Eintrags ist die Anwendung für den Benutzer nicht erreichbar. Dieses Problem führt zu Ausfallzeiten für Benutzer.

Alternative Lösung

Eine andere mögliche Lösung besteht darin, ein externes DNS für die ALB zu erstellen und es dann auf den Endpunkt der privaten gehosteten Zone von Amazon Route 53 zu verweisen. CloudFront Dieser Ansatz fügt dem Anwendungsablauf jedoch einen weiteren Sprung hinzu, was zu Anwendungslatenz führen kann. Die Lambda-Funktionslösung dieses Musters stört den Stromfluss nicht.

Automatisieren Sie CodeGuru Amazon-Rezensionen für AWS CDK Python-Anwendungen mithilfe von GitHub Aktionen

Erstellt von Vanitha Dontireddy (AWS) und Sarat Chandra Pothula (AWS)

Übersicht

Dieses Muster zeigt die Integration CodeGuru automatisierter Codeprüfungen von Amazon für AWS Cloud Development Kit (AWS CDK) Python-Anwendungen, die über GitHub Aktionen orchestriert werden. Die Lösung stellt eine in Python definierte serverlose Architektur bereit. AWS CDK Durch die Automatisierung der Expertencodeanalyse innerhalb der Entwicklungspipeline kann dieser Ansatz für AWS CDK Python-Projekte Folgendes bewirken:

- Verbessern Sie die Codequalität.
- Optimieren Sie Arbeitsabläufe.
- Maximieren Sie die Vorteile von serverlosem Computing.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto.
- AWS Command Line Interface (AWS CLI) Version 2.9.11 oder höher, installiert und konfiguriert.
- Ein aktives GitHub Konto und ein GitHub Repository mit Lese- und Schreib-Workflow-Berechtigungen und der Erstellung von Pull-Requests (PR) durch GitHub Actions, um sicherzustellen, dass der PR-Workflow ordnungsgemäß funktioniert.
- Eine OpenID Connect (OIDC) -Rolle in GitHub Aktionen zur Bereitstellung der Lösung in der. AWS-KontoVerwenden Sie das Konstrukt, um die Rolle zu erstellen.AWS CDK

Einschränkungen

- Amazon CodeGuru Profiler unterstützt Anwendungen, die in allen Sprachen der Java Virtual Machine (JVM) (wie Scala und Kotlin) und Runtimes sowie Python 3.6 oder höher geschrieben sind.
- Amazon CodeGuru Reviewer unterstützt Verknüpfungen mit Java- und Python-Code-Repositorys nur von den folgenden Quellanbietern: AWS CodeCommit, Bitbucket GitHub, GitHub Enterprise

Cloud und GitHub Enterprise Server. Darüber hinaus werden Amazon Simple Storage Service (Amazon S3) -Repositorys nur über GitHub Aktionen unterstützt.

- Es gibt keine automatisierte Möglichkeit, die Ergebnisse während der CI/CD-Pipeline (Continuous Integration and Continuous Deployment) auszudrucken. Stattdessen verwendet dieses Muster GitHub Aktionen als alternative Methode zur Verarbeitung und Anzeige der Ergebnisse.
- Einige AWS-Services sind nicht in allen verfügbar AWS-Regionen. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie unter AWS-Services nach Regionen. Informationen zu bestimmten Endpunkten finden Sie unter Service-Endpunkte und Kontingente. Wählen Sie dort den Link für den Service aus.

Architektur

Das folgende Diagramm zeigt die Architektur für diese Lösung.

Wie im Diagramm dargestellt, löst GitHub Actions die folgenden Schritte aus, wenn ein Entwickler eine Pull-Anfrage (PR) zur Überprüfung erstellt:

1. Annahme der IAM-Rolle — Die Pipeline verwendet die in GitHub Secrets angegebene IAM-Rolle, um Bereitstellungsaufgaben auszuführen.
2. Code-Analyse
   - CodeGuru Der Prüfer analysiert den im Amazon S3 S3-Bucket gespeicherten Code. Es identifiziert Fehler und gibt Empfehlungen für Korrekturen und Optimierungen.
   - CodeGuru Sicherheitsscans nach Richtlinienverstößen und Sicherheitslücken.
3. Überprüfung der Ergebnisse
   - Die Pipeline druckt in der Konsolenausgabe einen Link zum Ergebnis-Dashboard.
   - Wenn kritische Ergebnisse erkannt werden, schlägt die Pipeline sofort fehl.
   - Bei Befunden mit hohem, normalem oder niedrigem Schweregrad fährt die Pipeline mit dem nächsten Schritt fort.
4. PR-Genehmigung
   - Ein Prüfer muss die PR manuell genehmigen.
   - Wenn der PR verweigert wird, schlägt die Pipeline fehl und weitere Bereitstellungsschritte werden unterbrochen.
5. CDK-Bereitstellung — Nach der PR-Genehmigung beginnt der CDK-Bereitstellungsprozess. Es richtet Folgendes AWS-Services und die folgenden Ressourcen ein:

- CodeGuru Profiler
- AWS Lambda Funktion
- Amazon Simple Queue Service-Warteschlange (Amazon SQS)

6. Generierung von Profilerstellungsdaten — Um ausreichend Profilerstellungsdaten für CodeGuru Profiler zu generieren:
   - Die Pipeline ruft die Lambda-Funktion mehrfach auf, indem sie regelmäßig Nachrichten an die Amazon SQS SQS-Warteschlange sendet.

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK)ist ein Softwareentwicklungs-Framework, das Ihnen hilft, AWS Cloud Infrastruktur im Code zu definieren und bereitzustellen.
- CDK Toolkit ist ein Cloud-Entwicklungskit für die Befehlszeile, mit dem Sie mit Ihrer AWS CDK App interagieren können.
- Amazon CodeGuru Profiler sammelt Laufzeitleistungsdaten aus Ihren Live-Anwendungen und gibt Empfehlungen, die Ihnen bei der Feinabstimmung Ihrer Anwendungsleistung helfen können.
- Amazon CodeGuru Reviewer verwendet Programmanalyse und maschinelles Lernen, um potenzielle Fehler zu erkennen, die für Entwickler schwer zu finden sind. Anschließend bietet CodeGuru Profiler Vorschläge zur Verbesserung Ihres Java- und Python-Codes.
- Amazon CodeGuru Security ist ein statisches Anwendungssicherheitstool, das maschinelles Lernen verwendet, um Verstöße und Sicherheitslücken zu erkennen. Es bietet Vorschläge zur Bewältigung von Sicherheitsrisiken und generiert Metriken, mit denen Sie den Sicherheitsstatus Ihrer Anwendungen verfolgen können.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere Tools

- GitHub Actions ist eine CI/CD-Plattform (Continuous Integration and Continuous Delivery), die eng in Repositorien integriert GitHub ist. Sie können GitHub Actions verwenden, um Ihre Build-, Test- und Bereitstellungspipeline zu automatisieren.

Code-Repository

Der Code für dieses Muster ist im GitHub amazon-codeguru-suite-cdk-python-Repository verfügbar.

Bewährte Methoden

- Halten Sie sich an die Best Practices für die Entwicklung und Bereitstellung der Cloud-Infrastruktur mit dem AWS CDK.
- Beachten Sie bei der Verwendung von Workflows in GitHub Actions die bewährten Sicherheitsmethoden AWS-Services in IAM, einschließlich:
  - Speichern Sie keine Anmeldeinformationen in Ihrem Repository-Code.
  - Gehen Sie von einer IAM-Rolle aus, um temporäre Anmeldeinformationen zu erhalten, und verwenden Sie, wenn möglich, temporäre Anmeldeinformationen.
  - Gewähren Sie der IAM-Rolle, die in GitHub Actions-Workflows verwendet wird, die geringste Berechtigung. Gewähren Sie nur die Berechtigungen, die für die Ausführung der Aktionen in Ihren GitHub Aktions-Workflows erforderlich sind.
  - Überwachen Sie die Aktivität der IAM-Rolle, die in GitHub Aktions-Workflows verwendet wird.
  - Wechseln Sie regelmäßig alle langfristigen Anmeldeinformationen, die Sie verwenden.

Epen

So richten Sie Ihre Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie AWS Anmeldein formationen ein.	Führen Sie die folgenden Befehle aus, um die Variablen	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	zu exportieren, die den Stack definieren AWS-Konto und AWS-Region wo Sie ihn bereitstellen:
	`export CDK_DEFAU LT_ACCOUNT=<12-digit AWS account number>`
	`export CDK_DEFAU LT_REGION=<AWS Region>`
	Die AWS Anmeldeinformation en für AWS CDK werden über Umgebungsvariablen bereitgestellt.	

Klonen Sie das Repository	Führen Sie den folgenden Befehl aus, um das Repository auf Ihrem lokalen Computer zu klonen: `git clone https://g ithub.com/aws-samp les/amazon-codeguru- suite-cdk-python.git`	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie das CDK Toolkit.	Führen Sie den folgenden Befehl aus, um zu bestätigen, dass das CDK Toolkit installiert ist, und um die Version zu überprüfen:
	`cdk --version`
	Wenn die CDK Toolkit-Version älter als 2.27.0 ist, geben Sie den folgenden Befehl ein, um sie auf Version 2.27.0 zu aktualisieren:
	`npm install -g aws-cdk@2.27.0`
	Wenn das CDK Toolkit nicht installiert ist, führen Sie den folgenden Befehl aus, um es zu installieren:
	`npm install -g aws-cdk@2.27.0 --force`
		AWS DevOps, DevOps Ingenieur

Installieren Sie die erforderlichen Abhängigkeiten.	Führen Sie den folgenden Befehl aus, um die erforderlichen Projektabhängigkeiten zu installieren:
	`python -m pip install --upgrade pip`
	`pip install -r requirements.txt`
		AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bootstrap für die CDK-Umgebung.	Führen Sie die folgenden Befehle aus, um eine AWS-CDK-Umgebung zu booten:
	`npm install`
	`npm run cdk bootstrap "aws://${ACCOUNT_NUMBER}/${AWS_REGION}"`
	Nachdem Sie die Umgebung erfolgreich gebootet haben, sollte die folgende Ausgabe angezeigt werden:
	`# Bootstrapping environment aws://{account}/{region}...`
	`# Environment aws://{account}/{region} bootstrapped`
		AWS DevOps, DevOps Ingenieur

Stellen Sie die CDK-App bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Synthetisieren Sie die AWS CDK App.	Führen Sie den folgenden Befehl aus, um eine AWS CDK App zu synthetisieren: `cdk synth` Weitere Informationen zu diesem Befehl finden Sie in der Dokumentation unter cdk synthesize. AWS CDK	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Ressourcen bereit.	Führen Sie den folgenden Befehl aus, um die Ressourcen bereitzustellen: `cdk deploy --require-approval never` **Note** Das `--require-approval never` Kennzeichen bedeutet, dass das CDK alle Änderungen automatisch genehmigt und ausführt. Dazu gehören auch Änderungen, die das CDK normalerweise als manuell überprüfbar kennzeichnen würde (z. B. Änderungen der IAM-Richtlinien oder das Entfernen von Ressourcen). Stellen Sie sicher, dass Ihr CDK-Code und Ihre CI/CD-Pipeline gut getestet und sicher sind, bevor Sie das Flag in Produktionsumgebungen verwenden. `--`	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`require-approval never`	

Erstellen Sie GitHub Geheimnisse und persönliche Zugriffstoken

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die erforderlichen Geheimnisse in GitHub.	Um GitHub Aktionswo rkflows den sicheren Zugriff auf AWS Ressourcen zu ermöglichen, ohne vertrauli che Informationen im Code Ihres Repositorys preiszuge ben, erstellen Sie Geheimnis se. Um die Secrets in GitHub for`ROLE_TO_ASSUME` , und zu erstellen `CodeGuruR eviewArtifactBucke tName` `AWS_ACCOUNT_ID` , folgen Sie den Anweisung en unter Creating Secrets for a Repository in der GitHub Actions-Dokumentation. Im Folgenden finden Sie weitere Informationen zu den Variablen: • `AWS_ACCOUNT_ID` — Die AWS-Konto ID, unter der die Pipeline ausgeführt wird. • `CodeGuruReviewArti factBucketName` — Der Name des S3-Buckets, in	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dem CodeGuru Reviewer-Artefakte gespeicherte sind. Dieses Muster verwendet den Bucket-Namen `codeguru-reviewer-build-artifacts-<ACCOUNT_ID>-<REGION>` . • `AWS_REGION` — Der AWS-Region Ort, an dem sich die Ressourcen befinden. • `ROLE_TO_ASSUME` — Der Name der IAM-Rolle, die die Pipeline annimmt. Dieses Muster verwendet den Rollennamen `githubActionsDeployRole` .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein GitHub persönliches Zugriffstoken.	Gehen Sie wie folgt vor, um eine sichere Methode für die Authentifizierung und Interaktion mit GitHub Ihren GitHub Actions-Workflows einzurichten: 1. Um ein GitHub persönliches Zugriffstoken mit Lese- und Schreibzugriff auf Ihr Repository zu erstellen, folgen Sie den Anweisungen unter Verwaltung Ihrer persönlichen Zugriffstoken in der GitHub Dokumentation. 2. Um dieses Token als geheimen Repository-Schlüssel für GitHub Aktionen zu speichern, folgen Sie den Anweisungen unter Geheimnisse für ein Repository erstellen in der Dokumentation zu GitHub Aktionen.	AWS DevOps, DevOps Ingenieur

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen von Ressourcen.	Führen Sie den folgenden Befehl aus, um Ihre AWS CDK Python-App zu bereinigen:	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cdk destroy --all`	

Fehlerbehebung

Problem	Lösung
Link zu den Ergebnissen des Dashboards anzeigen.	Es gibt keine Möglichkeit, die Ergebnisse während der CI/CD-Pipeline auszudrucken. Stattdessen verwendet dieses Muster GitHub Aktionen als alternative Methode, um die Ergebnisse zu verarbeiten und anzuzeigen.

Zugehörige Ressourcen

AWS Ressourcen

- AWS Cloud Development Kit
- CodeGuru Amazon-Dokumentation
- Amazon S3
- AWS Identity and Access Management
- Amazon Simple Queue Service
- Was ist AWS Lambda?

GitHub Dokumentation

- Konfiguration von OpenID Connect in Amazon Web Services
- GitHub Aktionen
- Workflows wiederverwenden
- Einen Workflow auslösen

Automatisieren Sie die AWS-Ressourcenbewertung

Erstellt von Naveen Suthar (AWS), Arun Bagal (AWS), Manish Garg (AWS) und Sandeep Gawande (AWS)

Übersicht

Dieses Muster beschreibt einen automatisierten Ansatz für die Einrichtung von Funktionen zur Ressourcenbewertung mithilfe des AWS Cloud Development Kit (AWS CDK). Mithilfe dieses Musters sammeln Betriebsteams automatisiert Informationen zur Ressourcenprüfung und sehen sich die Details aller in einem AWS-Konto bereitgestellten Ressourcen auf einem einzigen Dashboard an. Dies ist in den folgenden Anwendungsfällen hilfreich:

- Identifizierung von Infrastructure-as-Code-Tools (IaC) und Isolierung von Ressourcen, die von verschiedenen IaC-Lösungen wie HashiCorp Terraform, AWS CloudFormation, AWS CDK und AWS Command Line Interface (AWS CLI) erstellt wurden
- Informationen zur Ressourcenprüfung werden abgerufen

Diese Lösung hilft dem Führungsteam auch dabei, von einem einzigen Dashboard aus Einblicke in die Ressourcen und Aktivitäten in einem AWS-Konto zu erhalten.

> **Note**
>
> Amazon QuickSight ist ein kostenpflichtiger Service. Bevor Sie es ausführen, um Daten zu analysieren und ein Dashboard zu erstellen, überprüfen Sie die QuickSight Amazon-Preise.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Rollen und Berechtigungen von AWS Identity and Access Management (IAM) mit Zugriff auf Bereitstellungsressourcen
- Ein QuickSight Amazon-Konto, das mit Zugriff auf Amazon Simple Storage Service (Amazon S3) und Amazon Athena erstellt wurde

- AWS CDK Version 2.55.1 oder höher installiert
- Python-Version 3.9 oder höher installiert

Einschränkungen

- Diese Lösung wird auf einem einzigen AWS-Konto bereitgestellt.
- Die Lösung verfolgt die Ereignisse, die vor ihrer Bereitstellung passiert sind, nicht, es sei denn, AWS CloudTrail war bereits eingerichtet und speichert Daten in einem S3-Bucket.

Produktversionen

- AWS CDK Version 2.55.1 oder höher
- Python-Version 3.9 oder höher

Architektur

Zieltechnologie-Stack

- Amazon Athena
- AWS CloudTrail
- AWS Glue
- AWS Lambda
- Amazon QuickSight
- Amazon S3

Zielarchitektur

Der AWS-CDK-Code stellt alle Ressourcen bereit, die für die Einrichtung von Funktionen zur Ressourcenbewertung in einem AWS-Konto erforderlich sind. Das folgende Diagramm zeigt den Prozess des Sendens von CloudTrail Protokollen an AWS Glue, Amazon Athena und QuickSight.

1. CloudTrail sendet Protokolle zur Speicherung an einen S3-Bucket.
2. Eine Ereignisbenachrichtigung ruft eine Lambda-Funktion auf, die die Protokolle verarbeitet und gefilterte Daten generiert.

3. Die gefilterten Daten werden in einem anderen S3-Bucket gespeichert.
4. Ein AWS Glue Glue-Crawler wird für die gefilterten Daten im S3-Bucket eingerichtet, um ein Schema in der AWS Glue Glue-Datenkatalogtabelle zu erstellen.
5. Die gefilterten Daten können jetzt von Amazon Athena abgefragt werden.
6. Auf die abgefragten Daten wird zur Visualisierung zugegriffen. QuickSight

Automatisierung und Skalierung

- Diese Lösung kann von einem AWS-Konto auf mehrere AWS-Konten skaliert werden, wenn es in AWS Organizations einen unternehmensweiten CloudTrail Trail gibt. Durch die Bereitstellung CloudTrail auf Organisationsebene können Sie diese Lösung auch verwenden, um Informationen zur Ressourcenprüfung für alle erforderlichen Ressourcen abzurufen.
- Dieses Muster verwendet serverlose AWS-Ressourcen, um die Lösung bereitzustellen.

Tools

AWS-Services

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon S3 analysieren können.
- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und AWS-Regionen hinweg zu verwalten.
- AWS CloudTrail unterstützt Sie bei der Prüfung der Unternehmensführung, der Einhaltung von Vorschriften und des Betriebsrisikos Ihres AWS-Kontos.
- AWS Glue ist ein vollständig verwalteter Service zum Extrahieren, Transformieren und Laden (ETL). Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben. Dieses Muster verwendet einen AWS Glue Glue-Crawler und eine AWS Glue Glue-Datenkatalogtabelle.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.

- Amazon QuickSight ist ein Business Intelligence (BI) -Service auf Cloud-Ebene, mit dem Sie Ihre Daten in einem einzigen Dashboard visualisieren, analysieren und melden können.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code-Repository

Der Code für dieses Muster ist im GitHub infrastructure-assessment-iac-automationRepository verfügbar.

Das Code-Repository enthält die folgenden Dateien und Ordner:

- `lib`folder — Das AWS-CDK-Konstrukt Python-Dateien, die zum Erstellen von AWS-Ressourcen verwendet werden
- `src/lambda_code`— Der Python-Code, der in der Lambda-Funktion ausgeführt wird
- `requirements.txt`— Die Liste aller Python-Abhängigkeiten, die installiert werden müssen
- `cdk.json`— Die Eingabedatei zur Bereitstellung von Werten, die zum Hochfahren von Ressourcen erforderlich sind

Bewährte Methoden

Richten Sie die Überwachung und Warnung für die Lambda-Funktion ein. Weitere Informationen finden Sie unter Überwachung und Problembehandlung von Lambda-Funktionen. Allgemeine bewährte Methoden für die Arbeit mit Lambda-Funktionen finden Sie in der AWS-Dokumentation.

Epen

So richten Sie Ihre Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repo auf Ihrem lokalen Computer.	Führen Sie zum Klonen des Repositorys den Befehl `git clone https://github.com/aws-samples/infrastructure`	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`-assessment-iac-automation.git` aus.	

Richten Sie die virtuelle Python-Umgebung ein und installieren Sie die erforderlichen Abhängigkeiten.	Führen Sie die folgenden Befehle aus, um die virtuelle Python-Umgebung einzurichten.
	`cd infrastructure-assessment-iac-automation`
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	Führen Sie den Befehl `pip install -r requirements.txt .` aus, um die erforderlichen Abhängigkeiten einzurichten
		AWS DevOps, DevOps Ingenieur

Richten Sie die AWS-CDK-Umgebung ein und synthetisieren Sie den AWS-CDK-Code.	1. Führen Sie den Befehl `cdk bootstrap aws://ACCOUNT-NUMBER/REGION` aus, um die AWS-CDK-Umgebung in Ihrem AWS-Konto einzurichten. 2. Führen Sie den Befehl `cdk synth` aus, um den Code in eine CloudFormation AWS-Stack-Konfiguration zu konvertieren.	AWS DevOps, DevOps Ingenieur

AWS-Anmeldeinformationen auf Ihrem lokalen Computer einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Exportieren Sie Variablen für das Konto und die Region, in der der Stack bereitgestellt werden soll.	Führen Sie die folgenden Befehle aus, um AWS-Anmeldeinformationen für AWS CDK mithilfe von Umgebungsvariablen bereitzustellen.
	`export CDK_DEFAULT_ACCOUNT=<12 Digit AWS Account Number>`
	`export CDK_DEFAULT_REGION=<region>`
		AWS DevOps, DevOps Ingenieur

Richten Sie das AWS-CLI-Profil ein.	Folgen Sie den Anweisungen in der AWS-Dokumentation, um das AWS-CLI-Profil für das Konto einzurichten.	AWS DevOps, DevOps Ingenieur

Konfigurieren und implementieren Sie das Tool zur Ressourcenbewertung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Ressourcen im Konto bereit.	Gehen Sie wie folgt vor, um Ressourcen im AWS-Konto mithilfe von AWS CDK bereitzustellen: 1. Geben Sie im Stammverzeichnis des geklonten Repositorys in der `cdk.json` Datei Eingaben für die folgenden Parameter ein: • `s3_context`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `ct_context` • `kms_context` • `lambda_context` • `glue_context` • `qs_context` Diese Werte definieren die Ressourcenkonfigurationen und die Nomenklatur. Standardwerte sind festgelegt und können bei Bedarf geändert werden. **Note** Um einen Fehler zu vermeiden, der besagt, dass der S3-Bucket bereits existiert, stellen Sie sicher, dass Sie `s3_context` in den `output` Abschnitten `ct` und eindeutige Namen angeben. 2. Führen Sie den Befehl aus, um Ressourcen bereitzustellen`cdk deploy`. Der `cdk deploy` Befehl erstellt eine CloudTrail Ressource zum Protokollieren von Ereignissen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und zum Speichern der Protokolldatei im S3-Eingabe-Bucket. Die Protokolldateien des Trails werden von der Lambda-Funktion verarbeitet. Die gefilterten Ergebnisse werden im S3-Ausgabe-Bucket gespeichert und können von Amazon Athena und Amazon QuickSight abgerufen werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den AWS Glue Glue-Crawler aus und erstellen Sie die Datenkata logtabelle.	Ein AWS Glue Glue-Crawler wird verwendet, um das Datenschema dynamisch zu halten. Die Lösung erstellt und aktualisiert Partitionen in der AWS Glue Data Catalog-Tabelle, indem sie den Crawler regelmäßig ausführt, wie vom AWS Glue Crawler Scheduler definiert. Nachdem die Daten im S3-Ausgabe-Bucket verfügbar sind, führen Sie die folgenden Schritte aus, um den AWS Glue Glue-Crawler auszuführen und das Data Catalog-Tabellenschema zum Testen zu erstellen: 1. Melden Sie sich bei der AWS-Managementkonsole an und navigieren Sie zur AWS Glue-Konsole. 2. Wählen Sie im Navigationsbereich unter Datenkata log die Option Crawlers aus. 3. Wählen Sie den `iac-tool-qa-resource-iac-json-crawler` Crawler aus. 4. Führen Sie den Crawler aus. 5. Nachdem der Crawler erfolgreich ausgeführt	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wurde, erstellt er eine AWS Glue Data Catalog-Tabelle. AWS verwendet QuickSight die Tabelle, um die Daten zu visualisieren. **Note** Der AWS-CDK-Code konfiguriert den AWS Glue-Crawler so, dass er zu einem bestimmten Zeitpunkt ausgeführt wird. Sie können ihn aber auch bei Bedarf ausführen.	
Stellen Sie das QuickSight Konstrukt bereit.	1. Um das QuickSight Konstrukt bereitzustellen, kommentieren Sie den Code zwischen `#QuickSight setup - start` und `#QuickSight setup – ends` in `resource_iac_tool_stack.py` . 2. Nachdem Sie den Kommentar entfernt haben, führen Sie den `cdk deploy` Befehl zum Erstellen `QuickSight DataSource` und `QuickSight DataSet` im QuickSight Konto aus.	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das QuickSight Dashboard.	Gehen Sie wie folgt vor, um das QuickSight Beispiel-Dashboard und die Analyse zu erstellen: 1. Navigieren Sie zur QuickSight Konsole und wählen Sie die AWS-Region aus, in der Ressourcen bereitgestellt werden. 2. Wählen Sie im Navigationsbereich Datensätze aus und überprüfen Sie, ob ein Datensatz mit dem Namen im QuickSight Amazon-Datensatz erstellt `ct-operations-iac-ds` wurde. Wenn Sie den Datensatz nicht sehen, stellen Sie das Konstrukt erneut bereit. QuickSight 3. Wählen Sie den `ct-operations-iac-ds` Datensatz aus und wählen Sie IN DER ANALYSE VERWENDEN. 4. Wählen Sie das Standardblatt aus. 5. Wählen Sie die entsprechenden Spalten aus der Feldliste auf der linken Seite aus.	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Nachdem Sie die erforderlichen Spalten ausgewählt haben, wählen Sie den entsprechenden visuellen Typ aus, um die Daten anzuzeigen. Weitere Informationen finden Sie unter Starten einer Analyse in Amazon QuickSight und Visuelle Typen in Amazon QuickSight.	

Bereinigen Sie alle AWS-Ressourcen in der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die AWS-Ressourcen.	1. Führen Sie den Befehl aus, um die von der Lösung bereitgestellten AWS-Ressourcen zu entfernen `cdk destroy`. 2. Löschen Sie alle Objekte aus den beiden S3-Buckets und entfernen Sie dann die Buckets. Weitere Informationen finden Sie unter Löschen eines Buckets.	AWS DevOps, DevOps Ingenieur

Richten Sie zusätzliche Funktionen zusätzlich zur Automatisierung des AWS-Tools zur Ressourcenbewertung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überwachen und bereinige n Sie manuell erstellte Ressourcen.	(Optional) Wenn Ihre Organisation Complianc e-Anforderungen für die Erstellung von Ressourcen mithilfe von IaC-Tools hat, können Sie die Einhaltung der Vorschriften erreichen , indem Sie mithilfe der Automatisierung des AWS-Tools zur Ressourcenbeurteil ung manuell bereitges tellte Ressourcen abrufen. Sie können das Tool auch verwenden, um die Ressource n in ein IaC-Tool zu importier en oder neu zu erstellen. Um manuell bereitgestellte Ressourcen zu überwache n, führen Sie die folgenden allgemeinen Aufgaben aus: 1. Stellen Sie die Automatis ierung des AWS-Tools zur Ressourcenbewertung bereit. 2. Richten Sie eine Lambda-Funktion ein, um die Athena-Tabellen täglich abzufragen, die relevanten Daten zu manuell bereitges tellten Ressourcen zu finden und sie in eine Datei	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	mit kommagetrennten Werten (CSV) zu exportier en. 3. Nachdem die Lambda-Fu nktion ausgeführt wurde, kann eine Benachrichtigung mit den erforderlichen Daten an die jeweilige n Stakeholder gesendet werden. 4. Für eine längere Aufbewahr ung kann die CSV-Datei im S3-Bucket gespeichert werden. 5. Löschen Sie anhand der Informationen in der CSV-Datei die manuell erstellten Ressourcen oder importieren Sie sie in eine bestehende IaC-Lösung.	

Fehlerbehebung

Problem	Lösung
AWS CDK gibt Fehler zurück.	Hilfe bei Problemen mit AWS CDK finden Sie unter Behebung häufiger Probleme mit AWS CDK.

Zugehörige Ressourcen

- Lambda-Funktionen mit Python erstellen
- Erste Schritte mit AWS CDK

- Arbeiten mit AWS CDK in Python
- Einen CloudTrail Log-Trail erstellen
- Erste Schritte mit Amazon QuickSight

Zusätzliche Informationen

Mehrere Konten

Verwenden Sie AWS-Profile, um die AWS-CLI-Anmeldeinformationen für mehrere Konten einzurichten. Weitere Informationen finden Sie im Abschnitt Mehrere Profile konfigurieren unter AWS-CLI einrichten.

AWS-CDK-Befehle

Beachten Sie bei der Arbeit mit AWS CDK die folgenden nützlichen Befehle:

- Listet alle Stacks in der App auf

```
cdk ls
```

- Gibt die synthetisierte AWS-Vorlage aus CloudFormation

```
cdk synth
```

- Stellt den Stack für Ihr AWS-Standardkonto und Ihre Region bereit

```
cdk deploy
```

- Vergleicht den bereitgestellten Stack mit dem aktuellen Status

```
cdk diff
```

- Öffnet die AWS CDK-Dokumentation

```
cdk docs
```

Automatische Installation von SAP-Systemen mithilfe von Open-Source-Tools

Erstellt von Guilherme Sesterheim (AWS)

Übersicht

Dieses Muster zeigt, wie die Installation von SAP-Systemen mithilfe von Open-Source-Tools automatisiert werden kann, um die folgenden Ressourcen zu erstellen:

- Eine SAP S/4HANA 1909-Datenbank
- Eine Instanz von SAP ABAP Central Services (ASCS)
- Eine Instanz des SAP Primary Application Server (PAS)

HashiCorp Terraform erstellt die Infrastruktur des SAP-Systems und Ansible konfiguriert das Betriebssystem (OS) und installiert SAP-Anwendungen. Jenkins führt die Installation aus.

Dieses Setup macht die Installation von SAP-Systemen zu einem wiederholbaren Prozess, der zur Steigerung der Effizienz und Qualität der Bereitstellung beitragen kann.

> **Note**
>
> Der in diesem Muster bereitgestellte Beispielcode funktioniert sowohl für Hochverfügbarkeitssysteme (HA) als auch für Systeme ohne Hochverfügbarkeit.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket, der all Ihre SAP-Mediendateien enthält
- Ein AWS Identity and Access Management (IAM) -Prinzipal mit einem Zugriffsschlüssel und einem geheimen Schlüssel, der über die folgenden Berechtigungen verfügt:
  - Schreibgeschützte Berechtigungen: Amazon Route 53, AWS Key Management Service (AWS KMS)

  - Lese- und Schreibberechtigungen: Amazon S3, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic File System (Amazon EFS), IAM, Amazon CloudWatch, Amazon DynamoDB
- Eine privat gehostete Route 53 53-Zone
- Ein Abonnement für Red Hat Enterprise Linux für SAP mit HA und Update Services 8.2 Amazon Machine Image (AMI) auf Amazon Marketplace
- Ein vom Kunden verwalteter AWS KMS-Schlüssel
- Ein Secure Shell (SSH) -Schlüsselpaar
- Eine EC2 Amazon-Sicherheitsgruppe, die eine SSH-Verbindung auf Port 22 von dem Hostnamen aus ermöglicht, auf dem Sie Jenkins installieren (der Hostname ist höchstwahrscheinlich localhost)
- HashiCorp Vagrant von wurde installiert und konfiguriert
- VirtualBoxvon Oracle installiert und konfiguriert
- Vertrautheit mit Git, Terraform, Ansible und Jenkins

Einschränkungen

- Nur SAP S/4HANA 1909 wurde für dieses spezielle Szenario vollständig getestet. Der Ansible-Beispielcode in diesem Muster muss geändert werden, wenn Sie eine andere Version von SAP HANA verwenden.
- Das Beispielverfahren in diesem Muster funktioniert für Mac OS- und Linux-Betriebssysteme. Einige der Befehle können nur in UNIX-basierten Terminals ausgeführt werden. Sie können jedoch ein ähnliches Ergebnis erzielen, indem Sie unterschiedliche Befehle und ein Windows-Betriebssystem verwenden.

Produktversionen

- SAP S/4HANA 1909
- Red Hat Enterprise Linux (RHEL) 8.2 oder höhere Versionen

Architektur

Das folgende Diagramm zeigt einen Beispiel-Workflow, der Open-Source-Tools verwendet, um die Installation von SAP-Systemen in einem AWS-Konto zu automatisieren:

Das Diagramm zeigt den folgenden Workflow:

1. Jenkins orchestriert die Ausführung der SAP-Systeminstallation, indem es Terraform- und Ansible-Code ausführt.
2. Terraform-Code baut die Infrastruktur des SAP-Systems auf.
3. Ansible Code konfiguriert das Betriebssystem und installiert SAP-Anwendungen.
4. Eine SAP S/4HANA 1909-Datenbank, eine ASCS-Instanz und eine PAS-Instanz, die alle definierten Voraussetzungen enthalten, sind auf einer Amazon-Instance installiert. EC2

> **Note**
>
> Das Beispiel-Setup in diesem Muster erstellt automatisch einen Amazon S3 S3-Bucket in Ihrem AWS-Konto, um die Terraform-Statusdatei zu speichern.

Technologie-Stack

- Terraform
- Ansible
- Jenkins
- Eine SAP S/4HANA 1909 Datenbank
- Eine SAP ASCS-Instanz
- Eine SAP-PAS-Instanz
- Amazon EC2

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server starten, wie Sie benötigen, und diese schnell nach oben oder unten skalieren.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Key Management Service (AWS KMS) unterstützt Sie bei der Erstellung und Kontrolle kryptografischer Schlüssel zum Schutz Ihrer Daten.

- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.

Andere Tools

- HashiCorp Terraform ist eine Befehlszeilenschnittstellenanwendung, mit der Sie mithilfe von Code Cloud-Infrastruktur und -Ressourcen bereitstellen und verwalten können.
- Ansible ist ein Open-Source-Tool zur Konfiguration als Code (CaC), mit dem Anwendungen, Konfigurationen und IT-Infrastruktur automatisiert werden können.
- Jenkins ist ein Open-Source-Automatisierungsserver, mit dem Entwickler ihre Software erstellen, testen und bereitstellen können.

Code

Der Code für dieses Muster ist im Repository -jenkins-ansible verfügbar. GitHub aws-install-sap-with

Epen

Konfigurieren Sie die Voraussetzungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Ihre SAP-Medie ndateien zu einem Amazon S3 S3-Bucket hinzu.	Erstellen Sie einen Amazon S3 S3-Bucket, der all Ihre SAP-Mediendateien enthält. **Important** Stellen Sie sicher, dass Sie der Ordnerhierarchie des AWS Launch Wizard für S/4HANA in der	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Launch Wizard-Dokumentation folgen.	
Installieren VirtualBox.	Installation und Konfiguration VirtualBoxdurch Oracle.	DevOps Ingenieur
Installieren Sie Vagrant.	Installieren und konfigurieren Sie Vagrant von. HashiCorp	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Ihr AWS-Konto.	1. Stellen Sie sicher, dass Sie über einen IAM-Prinzipal mit einem Zugriffsschlüssel und einem geheimen Schlüssel verfügen und der über die folgenden Berechtigungen verfügt: • Schreibgeschützte Berechtigungen: Amazon Route 53, AWS Key Management Service (AWS KMS) • Lese- und Schreibbe rechtigungen: Amazon S3, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic File System (Amazon EFS), IAM, Amazon CloudWatch, Amazon DynamoDB 2. Speichern Sie den Zugriffss chlüssel und den geheimen Schlüssel des IAM-Prinz ipals, damit Sie später darauf zurückgreifen können. 3. Erstellen Sie eine private gehostete Route 53 53-Zone, falls Sie noch keine haben. Speichern Sie den Zonennamen (z. B. sapteam.net), damit Sie	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	später darauf zurückgreifen können. 4. Abonnieren Sie Red Hat Enterprise Linux für SAP mit HA und Update Services 8.2 AMI auf Amazon Marketplace. Speichern Sie die AMI-ID (z. B. ami-0000000), damit Sie später darauf zurückgre ifen können. 5. Erstellen Sie einen vom Kunden verwalteten AWS KMS-Schlüssel. Speichern Sie den Amazon-Re ssourcennamen (ARN) des KMS-Schlüssels, damit Sie später darauf zurückgreifen können. **Note** Im Folgenden finden ARN ein Beispiel für einen vom Kunden verwalteten AWS-KMS-Schlüssel: arn:aws:kms:us-east- 1:1234123 41234:key/uuid 6. Erstellen Sie ein SSH-Schlü sselpaar. Speichern Sie den Namen des Schlüssel	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	paars und die PEM-Datei, um später darauf zurückgre ifen zu können. 7. Erstellen Sie eine EC2 Amazon-Sicherheitsgruppe, die eine SSH-Verbindung auf Port 22 von dem Hostnamen aus ermöglich t, auf dem Sie Jenkins installieren. Speichern Sie die Sicherheitsgruppen-ID, um später darauf zurückgre ifen zu können. **Note** Der Hostname ist höchstwahrscheinli ch localhost.	

Erstellen Sie Ihre SAP-Installation und führen Sie sie aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Code-Repo sitory von GitHub.	Klonen Sie das aws-insta ll-sap-with-jenkins-ansible- Repository auf. GitHub	DevOps Ingenieur
Starten Sie den Jenkins-S ervice.	Öffnen Sie das Linux-Ter minal. Navigieren Sie dann zu dem lokalen Ordner, der den Repository-Ordner für geklonten Code enthält, und	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	führen Sie den folgenden Befehl aus: `sudo vagrant up` **Note** Der Jenkins-Start dauert etwa 20 Minuten. Der Befehl gibt bei Erfolg die Meldung Service is up and running zurück.	
Öffnen Sie Jenkins in einem Webbrowser und melden Sie sich an.	1. Geben Sie in einem Webbrowser http://localhost:5555 ein. Jenkins wird geöffnet. 2. Melden Sie sich bei Jenkins an, indem Sie admin für den Benutzernamen und my_secret_pass_from_vault für das Passwort verwenden.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Installationsparameter Ihres SAP-Systems.	1. Wählen Sie in Jenkins Manage Jenkins aus. Wählen Sie dann Credentials verwalten aus. Eine Liste mit Variablen für Anmeldeinformationen, die Sie konfigurieren können, wird angezeigt. 2. Konfigurieren Sie alle der folgenden Anmeldeinformationsvariablen: • Geben Sie für AWS_ACCOUNT_CREDENTIALS die Zugriffsschlüssel-ID und die geheime Zugriffsschlüssel-ID Ihres IAM-Prinzipals ein. • Geben Sie für AMI_ID die AMI-ID des Red Hat Enterprise Linux for SAP with HA and Update Services 8.2 AMI ein. • Geben Sie für KMS_KEY_ARN den ARN Ihres vom Kunden verwalteten AWS KMS-Schlüssels ein. • Geben Sie für SSH_KEYPAIR_NAME den Namen Ihres SSH-Schlüsselpaars key pair, ohne den Dateityp.pem einzugeben.	AWS-Systemadministrator, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Geben Sie für SSH_KEYPAIR_FILE den vollständigen Namen der PEM-Datei Ihres Schlüsselpaars ein (z. B. mykeypair.pem). Stellen Sie sicher, dass Sie auch die PEM-Datei der Schlüsselpaare nach Jenkins hochladen. • Geben Sie für S3_ROOT_FOLDER_INSTALL_FILES den Namen des Amazon S3 S3-Buckets — und gegebenenfalls des Ordners — ein (z. B. s3:///S4H1909), der Ihre SAP-Mediendateien enthält. my-media-bucket • Geben Sie für PRIVATE_DNS_ZONE_NAME den Namen Ihrer privaten gehosteten Route 53 53-Zone ein (z. B. myprivate companyurl.net). • Geben Sie für VPC_ID die VPC-ID (z. B. vpc-12345) der Amazon-VPC ein, in der Sie die SAP-Ressourcen erstellen. • Geben Sie für SUBNET_IDS zwei öffentliche Subnetze ein, IDs wenn Sie in einer Testumgebung arbeiten (für future HA-Fähigkeiten). Wenn Sie in einer Produktio	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	nsumgebung arbeiten, empfiehlt es sich, zwei private Subnetze mit einem Bastion-Host zu verwenden. • Geben Sie für SECURITY_GROUP_ID die ID der EC2 Amazon-Sicherheitsgruppe ein, die eine SSH-Verbindung auf Port 22 von dem Hostnamen aus ermöglicht, auf dem Sie Jenkins installiert haben. **Note** Sie können die anderen nicht erforderlichen Parameter je nach Ihrem Anwendungsfall nach Bedarf konfigurieren. Sie können beispielsweise die SAP-System-ID (SID) der Instanzen, das Standardkennwort, die Namen und die Tags für Ihr SAP-System ändern. Alle erforderlichen Variablen haben (Erforderlich) am Anfang ihrer Namen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie Ihre SAP-Systeminstallation aus.	1. Wählen Sie in Jenkins Jenkins Home aus. Wählen Sie dann SAP HANA +ASCS+PAS 3 Instances. 2. Wählen Sie Spin up and install. Wählen Sie dann Main. 3. Wählen Sie Jetzt erstellen. Informationen zu den Pipeline-Schritten finden Sie im Abschnitt Grundlegendes zu den Pipeline-Schritten unter Automatisieren der SAP-Installation mit Open-Source-Tools im AWS-Blog. **Note** Wenn ein Fehler auftritt, bewegen Sie den Mauszeiger über das rote Fehlerfeld, das angezeigt wird, und wählen Sie Logs. Die Protokolle für den Pipeline-Schritt, bei dem ein Fehler aufgetreten ist, werden angezeigt. Die meisten Fehler treten aufgrund falscher Parameter einstellungen auf.	DevOps Ingenieur, AWS-Systemadministrator

Zugehörige Ressourcen

- DevOps für SAP — SAP-Installation: 2 Monate bis 2 Stunden (DevOps Enterprise Summit Video Library)

Automatisieren Sie das AWS Service Catalog-Portfolio und die Produktbereitstellung mithilfe von AWS CDK

Erstellt von Sandeep Gawande (AWS), RAJNEESH TYAGI (AWS) und Viyoma Sachdeva (AWS)

Übersicht

Mit AWS Service Catalog können Sie Kataloge von IT-Services oder Produkten, die für die Verwendung in der AWS-Umgebung Ihres Unternehmens zugelassen sind, zentral verwalten. Eine Sammlung von Produkten wird als Portfolio bezeichnet, und ein Portfolio enthält auch Konfigurationsinformationen. Mit AWS Service Catalog können Sie ein maßgeschneidertes Portfolio für jeden Benutzertyp in Ihrer Organisation erstellen und dann Zugriff auf das entsprechende Portfolio gewähren. Diese Benutzer können dann schnell jedes Produkt, das sie benötigen, aus dem Portfolio bereitstellen.

Wenn Sie über eine komplexe Netzwerkinfrastruktur verfügen, z. B. Architekturen mit mehreren Regionen und mehreren Konten, wird empfohlen, Service Catalog-Portfolios in einem einzigen, zentralen Konto zu erstellen und zu verwalten. Dieses Muster beschreibt, wie das AWS Cloud Development Kit (AWS CDK) verwendet wird, um die Erstellung von Service Catalog-Portfolios in einem zentralen Konto zu automatisieren, Endbenutzern Zugriff darauf zu gewähren und dann, optional, Produkte in einem oder mehreren AWS-Zielkonten bereitzustellen. Diese ready-to-use Lösung erstellt die Service Catalog-Portfolios im Quellkonto. Es stellt optional auch Produkte in Zielkonten mithilfe von CloudFormation AWS-Stacks bereit und hilft Ihnen bei der Konfiguration TagOptions für die Produkte:

- AWS CloudFormation StackSets — Sie können es verwenden StackSets , um Service Catalog-Produkte in mehreren AWS-Regionen und Konten auf den Markt zu bringen. In dieser Lösung haben Sie die Möglichkeit, Produkte automatisch bereitzustellen, wenn Sie diese Lösung bereitstellen. Weitere Informationen finden Sie unter Verwenden von AWS CloudFormation StackSets (Service Catalog-Dokumentation) und StackSets Konzepte (CloudFormation Dokumentation).
- TagOption Bibliothek — Mithilfe der TagOption Bibliothek können Sie Tags für bereitgestellte Produkte verwalten. A TagOptionist ein Schlüssel-Wert-Paar, das im AWS Service Catalog verwaltet wird. Es ist kein AWS-Tag, sondern dient als Vorlage für die Erstellung eines AWS-Tags auf der Grundlage von TagOption. Weitere Informationen finden Sie in der TagOption Bibliothek (Service Catalog-Dokumentation).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto, das Sie als Quellkonto für die Verwaltung von Service Catalog-Portfolios verwenden möchten.
- Wenn Sie diese Lösung verwenden, um Produkte in einem oder mehreren Zielkonten bereitzustellen, muss das Zielkonto bereits existieren und aktiv sein.
- AWS Identity and Access Management (IAM) -Berechtigungen für den Zugriff auf AWS Service Catalog CloudFormation, AWS und AWS IAM.

Produktversionen

- AWS CDK versie 2.27.0

Architektur

Zieltechnologie-Stack

- Service Catalog-Portfolios in einem zentralen AWS-Konto
- Service Catalog-Produkte, die im Zielkonto bereitgestellt werden

Zielarchitektur

1. Im Portfolio- (oder Quellkonto) aktualisieren Sie die Datei config.json mit dem AWS-Konto, der AWS-Region, der IAM-Rolle, dem Portfolio und den Produktinformationen für Ihren Anwendungsfall.
2. Sie stellen die AWS-CDK-Anwendung bereit.
3. Die AWS-CDK-Anwendung übernimmt die IAM-Rolle für die Bereitstellung und erstellt die Service Catalog-Portfolios und -Produkte, die in der Datei config.json definiert sind.

   Wenn Sie für StackSets die Bereitstellung von Produkten in einem Zielkonto konfiguriert haben, wird der Vorgang fortgesetzt. Wenn Sie nicht für StackSets die Bereitstellung von Produkten konfiguriert haben, ist der Vorgang abgeschlossen.
4. Die AWS-CDK-Anwendung übernimmt die StackSet Administratorrolle und stellt das CloudFormation AWS-Stack-Set bereit, das Sie in der Datei config.json definiert haben.

5. StackSets Übernimmt im Zielkonto die StackSet Ausführungsrolle und stellt die Produkte bereit.

Tools

AWS-Services

- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS CDK Toolkit ist ein Befehlszeilen-Cloud-Entwicklungskit, das Sie bei der Interaktion mit Ihrer AWS-CDK-App unterstützt.
- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie kontrollieren, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Mit AWS Service Catalog können Sie Kataloge von IT-Services, die für AWS zugelassen sind, zentral verwalten. Endbenutzer können schnell nur die jeweils benötigten genehmigten IT-Services bereitstellen, wobei die Einschränkungen Ihrer Organisation berücksichtigt werden.

Code-Repository

Der Code für dieses Muster ist im aws-cdk-servicecatalog-automationRepository verfügbar. GitHub Das Code-Repository enthält die folgenden Dateien und Ordner:

- cdk-sevicecatalog-app— Dieser Ordner enthält die AWS-CDK-Anwendung für diese Lösung.
- config — Dieser Ordner enthält die Datei config.json und die CloudFormation Vorlage für die Bereitstellung der Produkte im Service Catalog-Portfolio.
- config/config.json — Diese Datei enthält alle Konfigurationsinformationen. Sie aktualisieren diese Datei, um diese Lösung an Ihren Anwendungsfall anzupassen.
- config/templates — Dieser Ordner enthält die CloudFormation Vorlagen für die Service Center-Produkte.
- setup.sh — Dieses Skript stellt die Lösung bereit.
- uninstall.sh — Dieses Skript löscht den Stack und alle AWS-Ressourcen, die bei der Bereitstellung dieser Lösung erstellt wurden.

Folgen Sie den Anweisungen im Abschnitt Epics, um den Beispielcode zu verwenden.

Bewährte Methoden

- Die für die Bereitstellung dieser Lösung verwendeten IAM-Rollen sollten dem Prinzip der geringsten Rechte entsprechen (IAM-Dokumentation).
- Halten Sie sich an die Best Practices für die Entwicklung von Cloud-Anwendungen mit AWS CDK (AWS-Blogbeitrag).
- Halten Sie sich an die CloudFormation bewährten AWS-Methoden (CloudFormation Dokumentation).

Epen

So richten Sie Ihre Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie das AWS CDK Toolkit.	Stellen Sie sicher, dass Sie das AWS CDK Toolkit installiert haben. Geben Sie den folgenden Befehl ein, um zu bestätigen, ob es installiert ist, und um die Version zu überprüfen.
	`cdk --version`
	Wenn das AWS CDK Toolkit nicht installiert ist, geben Sie den folgenden Befehl ein, um es zu installieren.
	`npm install -g aws-cdk@2.27.0`
	Wenn die Version des AWS CDK Toolkit älter als 2.27.0
		AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ist, geben Sie den folgenden Befehl ein, um sie auf Version 2.27.0 zu aktualisieren. `npm install -g aws-cdk@2.27.0 --force`	

Klonen Sie das Repository	Geben Sie den folgenden Befehl ein. Unter Das Repository klonen können Sie im Abschnitt Zusätzliche Informationen den vollständigen Befehl kopieren, der die URL für das Repository enthält. Dadurch wird das aws-cdk-servicecatalog-automationRepository von GitHub geklont.
	`git clone <repository-URL>.git`
	Dadurch wird ein `cd aws-cdk-servicecatalog-automation` Ordner im Zielverzeichnis erstellt. Geben Sie den folgenden Befehl ein, um in diesen Ordner zu navigieren.
	`cd aws-cdk-servicecatalog-automation`
		AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie AWS-Anmeldeinformationen ein.	Geben Sie die folgenden Befehle ein. Diese exportieren die folgenden Variablen, die das AWS-Konto und die Region definieren, in der Sie den Stack bereitstellen.
	`export CDK_DEFAULT_ACCOUNT=<12-digit AWS account number>`
	`export CDK_DEFAULT_REGION=<AWS Region>`
	AWS-Anmeldeinformationen für AWS CDK werden über Umgebungsvariablen bereitgestellt.
		AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Berechtigungen für IAM-Rollen von Endbenutzern.	Wenn Sie IAM-Rollen verwenden möchten, um Zugriff auf das Portfolio und die darin enthaltenen Produkte zu gewähren, müssen die Rollen über Berechtigungen verfügen, damit sie vom Serviceca talog.amazonaws.com Service Principal übernommen werden können. Anweisungen zum Erteilen dieser Berechtigungen finden Sie unter Aktivieren des vertrauenswürdigen Zugriffs mit Service Catalog (Dokumentation zu AWS Organizations).	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die IAM-Rollen, die für erforderlich sind. StackSets	Wenn Sie die automatische Bereitstellung von Produkten in Zielkonten verwenden StackSets , müssen Sie die IAM-Rollen konfigurieren, mit denen das Stack-Set verwaltet und ausgeführt wird. 1. Bestätigen Sie im Quellkonto, ob das `AWSCloudFormationStackSetAdministrationRole` bereits vorhanden ist. Bestätigen Sie in den Zielkonten, ob `AWSCloudFormationStackSetExecutionRole` bereits vorhanden ist. Wenn diese Rollen bereits existieren, kannst du zum nächsten Epos springen. 2. Folgen Sie den Anweisungen unter Selbstverwaltete Berechtigungen gewähren (IAM-Dokumentation), um die Stackset-Administratorrolle im Portfoliokonto und die Ausführungsrolle in jedem Zielkonto zu erstellen.	AWS DevOps, DevOps Ingenieur

Passen Sie die Lösung an und stellen Sie sie bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die CloudFormation Vorlagen.	Erstellen Sie in dem `config/templates` Ordner CloudFormation Vorlagen für alle Produkte, die Sie in Ihre Portfolios aufnehmen möchten. Weitere Informationen finden Sie unter Arbeiten mit CloudFormation AWS-Vorlagen (CloudFormation Dokumentation).	App-Entwickler, AWS DevOps, DevOps Ingenieur
Passen Sie die Konfigurationsdatei an.	Öffnen Sie in dem `config` Ordner die Datei config.json und definieren Sie die Parameter entsprechend Ihrem Anwendungsfall. Die folgenden Parameter sind erforderlich, sofern nicht anders angegeben: Definieren Sie in `portfolios` diesem Abschnitt die folgenden Parameter, um ein oder mehrere Service Catalog-Portfolios zu erstellen: • `portfolioName` — Der Name des Portfolios. • `providerName` — Der Name der Person, des Teams oder der Organisation, die das Portfolio verwaltet.	App-Entwickler, DevOps Ingenieur, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `description` — Eine kurze Beschreibung des Portfolios. • `roles`— (Optional) Namen aller IAM-Rollen, die Zugriff auf dieses Portfolio haben sollten. Benutzer mit dieser Rolle können auf die Produkte in diesem Portfolio zugreifen. • `users`— (Optional) Namen aller IAM-Benutzer, die Zugriff auf dieses Portfolio und seine Produkte haben sollten. • `groups`— (Optional) Namen aller IAM-Benut zergruppen, die Zugriff auf dieses Portfolio und seine Produkte haben sollten. ⚠ Warning IAM-Benutzer verfügen über langfrist ige Anmeldein formationen, was ein Sicherheitsrisiko darstellt. Um dieses Risiko zu minimieren, empfehlen wir, diesen Benutzern nur die Berechtigungen zu gewähren, die sie für	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Ausführung der Aufgabe benötigen, und diese Benutzer zu entfernen, wenn sie nicht mehr benötigt werden. **Important** `rolesusers`, und `groups` sind alles optionale Parameter. Wenn Sie jedoch keinen dieser Parameter definiere n, kann niemand die Portfolioprodukte in der Service Catalog-Konsole anzeigen. Definieren Sie mindestens einen dieser Parameter . Weitere Informati onen finden Sie unter Erteilen von Berechtig ungen für Service Catalog-Endbenutze r (Service Catalog-D okumentation). • (Optional) Definieren Sie in `tagOption` diesem	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Abschnitt TagOptions für die Produkte: • `key`— Name des TagOption Schlüssels • `value`— Zulässige Zeichenkettenwerte für TagOption Weitere Informationen finden Sie in der TagOption Bibliothek (Service Catalog-Dokumentation). • Definieren Sie in **`products`**diesem Abschnitt die folgenden Parameter für die Produkte: • `portfolioName` — Der Name des Portfolios, dem Sie das Produkt hinzufüge n möchten. Sie können nur ein Portfolio angeben. • `productName` — Der Name des Produkts. • `owner`— Der Besitzer des Produkts. • `productVersionName` — Der Name der Produktversion als Zeichenkettenwert, z. `v1` B. • `templatePath` — Der Dateipfad für die	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CloudFormation Vorlage für das Produkt. • `deployWithStackSets` — (Optional) Geben Sie ein oder mehrere Konten und Regionen an, in denen Sie Produkte in den Portfolios automatisch bereitstellen möchten. StackSets Wenn Sie diese Bereitstellungsoption verwenden, sind alle folgenden Parameter in diesem Abschnitt erforderlich: • `accounts`— Die Zielkonten. • `regions`— Die Zielregionen. • `stackSetAdministrationRoleName` — Der Name der IAM-Rolle, die zur Verwaltung der StackSets Konfiguration verwendet wird. Ändern Sie diesen Wert nicht. Diese Rolle muss genau diesen Namen haben. • `stackSetExecutionRoleName` — Der	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Name der IAM-Rolle im Zielkonto, das die Stack-Instances bereitstellt. Ändern Sie diesen Wert nicht. Diese Rolle muss genau diesen Namen haben. Ein Beispiel für eine fertige Konfigurationsdatei finden Sie unter Beispielkonfigurationsdatei im Abschnitt Zusätzliche Informationen.	
Stellen Sie die Lösung bereit.	Geben Sie den folgenden Befehl ein. Dadurch wird die AWS CDK-App bereitgestellt und die Service Catalog-Portfolios und -Produkte bereitgestellt, wie in der Datei config.json angegeben. `sh +x setup.sh`	App-Entwickler, DevOps Ingenieur, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Bereitstellung.	Überprüfen Sie die erfolgreiche Bereitstellung, indem Sie wie folgt vorgehen: 1. Melden Sie sich bei der AWS-Managementkonsole mit Anmeldeinformationen an, die auf eines oder mehrere der Portfolios zugreifen können, die Sie in der Konfigurationsdatei definiert haben. 2. Öffnen Sie die Service Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/. 3. Wählen Sie im Navigationsbereich unter Provisioning die Option Produkte aus. Vergewissern Sie sich, dass eine Liste der Produkte angezeigt wird, die Sie für das Portfolio angegeben haben. 4. Folgen Sie den Anweisungen unter Produkt auf den Markt bringen (Servicekatalog-Dokumentation), um eines der verfügbaren Produkte auf den Markt zu bringen. Vergewissern Sie sich, dass die verfügbaren Produktversionen und Tags den Werten entsprech	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en, die Sie in der Konfigura tionsdatei angegeben haben. 5. Wenn Sie sich dafür entschieden haben, Produkte mithilfe von automatisch in einem oder mehreren Zielkonten bereitzustellen StackSets, gehen Sie wie folgt vor: a. Melden Sie sich mit Anmeldeinformation en an, die Ihnen die Erlaubnis geben, die bereitgestellten Produkte in einem der Zielkonten anzusehen. b. Wählen Sie in der Service Catalog-Konsole im Navigationsbereich unter Provisioning die Option Provisioned products aus. c. Vergewissern Sie sich, dass die erwarteten Produkte in der Liste angezeigt werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Aktualisieren Sie die Portfolios und Produkte.	Wenn Sie diese Lösung verwenden möchten, um die Portfolios oder Produkte zu aktualisieren oder neue Produkte bereitzustellen: 1. Nehmen Sie die erforderlichen Änderungen in der Datei config.json vor. 2. Fügen Sie dem Ordner nach Bedarf alle CloudFormation Vorlagen hinzu oder ändern Sie sie. `config/template` 3. Stellen Sie die Lösung erneut bereit. Sie können beispielsweise zusätzliche Portfolios hinzufügen oder mehr Ressourcen bereitstellen. Die AWS CDK-App implementiert nur die Änderungen. Wenn es keine Änderungen an zuvor bereitgestellten Portfolios oder Produkten gibt, hat die erneute Bereitstellung keine Auswirkungen auf sie.	App-Entwickler, DevOps Ingenieur, General AWS

Säubere die Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Entfernen Sie AWS-Ressourcen, die von dieser Lösung bereitgestellt werden.	Wenn Sie ein bereitgestelltes Produkt löschen möchten, folgen Sie den Anweisungen unter Löschen bereitgestellter Produkte (Service Catalog-Dokumentation). Wenn Sie alle mit dieser Lösung erstellten Ressourcen löschen möchten, geben Sie den folgenden Befehl ein. `sh uninstall.sh`	AWS DevOps, DevOps Ingenieur, App-Entwickler

Zugehörige Ressourcen

- AWS Service Catalog Construct-Bibliothek (AWS-API-Referenz)
- StackSets Konzepte (CloudFormation Dokumentation)
- AWS Service Catalog (AWS-Marketing)
- Verwenden von Service Catalog mit dem AWS CDK (AWS-Workshop)

Zusätzliche Informationen

Klonen Sie das Repository

Geben Sie den folgenden Befehl ein, um das Repository zu klonen GitHub.

```
git clone https://github.com/aws-samples/aws-cdk-servicecatalog-automation.git
```

Beispiel für eine Konfigurationsdatei

Im Folgenden finden Sie eine config.json-Beispieldatei mit Beispielwerten.

```
{
    "portfolios": [
        {
            "displayName": "EC2 Product Portfolio",
            "providerName": "User1",
            "description": "Test1",
            "roles": [
                "<Names of IAM roles that can access the products>"
            ],
            "users": [
                "<Names of IAM users who can access the products>"
            ],
            "groups": [
                "<Names of IAM user groups that can access the products>"
            ]
        },
        {
            "displayName": "Autoscaling Product Portfolio",
            "providerName": "User2",
            "description": "Test2",
            "roles": [
                "<Name of IAM role>"
            ]
        }
    ],
    "tagOption": [
        {
            "key": "Group",
            "value": [
                "finance",
                "engineering",
                "marketing",
                "research"
            ]
        },
        {
            "key": "CostCenter",
            "value": [
                "01",
                "02",
                "03",
                "04"
            ]
```

```
        },
        {
            "key": "Environment",
            "value": [
                "dev",
                "prod",
                "stage"
            ]
        }
    ],
    "products": [
        {
            "portfolioName": "EC2 Product Profile",
            "productName": "Ec2",
            "owner": "owner1",
            "productVersionName": "v1",
            "templatePath": "../../config/templates/template1.json"
        },
        {
            "portfolioName": "Autoscaling Product Profile",
            "productName": "autoscaling",
            "owner": "owner1",
            "productVersionName": "v1",
            "templatePath": "../../config/templates/template2.json",
            "deployWithStackSets": {
                "accounts": [
                    "012345678901",
                ],
                "regions": [
                    "us-west-2"
                ],
                "stackSetAdministrationRoleName":
 "AWSCloudFormationStackSetAdministrationRole",
                "stackSetExecutionRoleName": "AWSCloudFormationStackSetExecutionRole"
            }
        }
    ]
}
```

Automatisieren Sie ereignisgesteuerte Backups von CodeCommit zu Amazon S3 mithilfe CodeBuild von und Events CloudWatch

Erstellt von Kirankumar Chandrashekar (AWS)

Übersicht

In der Amazon Web Services (AWS) Cloud können Sie AWS verwenden, um sichere Git-basierte Repositorys CodeCommit zu hosten. CodeCommit ist ein vollständig verwalteter Service zur Quellcodeverwaltung. Wenn ein CodeCommit Repository jedoch versehentlich gelöscht wird, wird sein Inhalt ebenfalls gelöscht und kann nicht wiederhergestellt werden.

Dieses Muster beschreibt, wie ein CodeCommit Repository automatisch in einem Amazon Simple Storage Service (Amazon S3) -Bucket gesichert wird, nachdem eine Änderung am Repository vorgenommen wurde. Wenn das CodeCommit Repository später gelöscht wird, bietet Ihnen diese Backup-Strategie eine point-in-time Wiederherstellungsoption.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein vorhandenes CodeCommit Repository, dessen Benutzerzugriff gemäß Ihren Anforderungen konfiguriert ist. Weitere Informationen finden Sie CodeCommit in der CodeCommit Dokumentation unter Einrichtung für AWS.
- Ein S3-Bucket zum Hochladen der CodeCommit Backups.

Einschränkungen

- Dieses Muster sichert automatisch alle Ihre CodeCommit Repositorys. Wenn Sie einzelne CodeCommit Repositorys sichern möchten, müssen Sie die Amazon CloudWatch Events-Regel ändern.

Architektur

Das folgende Diagramm veranschaulicht den Arbeitsablauf für dieses Muster.

Der Workflow besteht aus folgenden Schritten:

1. Der Code wird in ein CodeCommit Repository übertragen.
2. Das CodeCommit Repository benachrichtigt CloudWatch Events über eine Änderung des Projektarchivs (z. B. einen `git push` Befehl).
3. CloudWatch Events ruft AWS auf CodeBuild und sendet ihm die CodeCommit Repository-Informationen.
4. CodeBuild klont das gesamte CodeCommit Repository und packt es in eine ZIP-Datei.
5. CodeBuild lädt die ZIP-Datei in einen S3-Bucket hoch.

Technologie-Stack

- CloudWatch Events
- CodeBuild
- CodeCommit
- Amazon S3

Tools

- Amazon CloudWatch Events — CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit.
- AWS CodeBuild — CodeBuild ist ein vollständig verwalteter Continuous Integration Service, der Quellcode kompiliert, Tests durchführt und Softwarepakete produziert, die sofort einsatzbereit sind.
- AWS CodeCommit — CodeCommit ist ein vollständig verwalteter Quellcodeverwaltungsservice, der sichere Git-basierte Repositorys hostet.
- AWS Identity and Access Management (IAM) — IAM ist ein Webservice, mit dem Sie den Zugriff auf AWS-Ressourcen sicher kontrollieren können.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Speicher für das Internet.

Epen

Erstelle ein Projekt CodeBuild

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CodeBuild Servicerolle.	Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole. Wählen Sie Rollen und anschließend Rolle erstellen aus. Erstellen Sie eine Servicerolle für das CodeBuild Klonen des CodeCommit Repositorys, das Hochladen von Dateien in den S3-Bucket und das Senden von Protokollen an Amazon CloudWatch. Weitere Informationen finden Sie in der CodeBuild Dokumentation unter Eine CodeBuild Servicerolle erstellen.	Cloud-Administrator
Erstellen Sie ein CodeBuild Projekt.	Wählen Sie in der CodeBuild Konsole die Option CodeBuild Projekt erstellen aus. Erstellen Sie ein CodeBuild Projekt mithilfe der `buildspec.yml` Vorlage aus dem Abschnitt Zusätzliche Informationen. Hilfe zu dieser Geschichte finden Sie in der CodeBuild Dokumentation unter Erstellen eines Build-Projekts.	Cloud-Administrator

Erstellen und konfigurieren Sie die CloudWatch Ereignisregel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle für CloudWatch Events.	Wählen Sie in der IAM-Konsole Rollen aus und erstellen Sie eine IAM-Rolle für Ereignisse. CloudWatch Weitere Informationen dazu finden Sie unter IAM-Rolle „CloudWatch Ereignisse“ in der IAM-Dokumentation. **Important** Sie müssen der IAM-Rolle für Ereignisse `codebuild:StartBuild` Berechtigungen hinzufügen. CloudWatch	Cloud-Administrator
Erstellen Sie eine CloudWatch Ereignisregel.	1. Wählen Sie auf der CloudWatch Konsole Ereignisse und dann Regeln aus. Wählen Sie Regel erstellen aus und verwenden Sie die Regel CloudWatch Ereignisse aus dem Abschnitt Zusätzliche Informationen. Dadurch wird eine Regel erstellt, die auf Änderungen an Ereignissen (z. B. `git commit` Befehle) in Ihren `git push` CodeCommit	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Repositorys wartet. Weitere Informationen finden Sie in der CodePipeline AWS-Dokumentation unter Erstellen einer CloudWatch Ereignisregel für eine CodeCommit Quelle. 2. Wählen Sie Ziele, Thema und anschließend Eingabe konfigurieren aus. Wählen Sie „Eingangstransformator“ und verwenden Sie den Eingabepfad und die Eingabevorlage aus dem Abschnitt „Zusätzliche Informationen“. Dadurch wird sichergestellt, dass Ihre CodeCommit Repository-Details analysiert und als Umgebungsvariablen an das CodeBuild Projekt gesendet werden. Weitere Informationen finden Sie im Tutorial zum Eingangstransformator in der CloudWatch Dokumentation. 3. Wählen Sie „Details konfigurieren“ und geben Sie einen Namen und eine Beschreibung für die Regel ein. Wählen Sie Regel erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Important Diese CloudWatch Ereignisregel beschreibt Änderungen in all Ihren CodeCommit Repositorys. Sie müssen die CloudWatch Ereignisregel ändern, wenn Sie einzelne CodeCommit Repositorys sichern oder separate S3-Buckets für verschiedene Repository-Backups verwenden möchten.	

Zugehörige Ressourcen

Ein CodeBuild Projekt erstellen

- Erstellen Sie eine CodeBuild Servicerolle
- Erstellen Sie ein CodeBuild Projekt
- Erforderliche Berechtigungen für Git-Client-Befehle

Eine CloudWatch Ereignisregel erstellen und konfigurieren

- Erstellen Sie eine CloudWatch Ereignisregel für eine CodeCommit Quelle
- Verwenden Sie den Eingangstransformator, um anzupassen, was an das Ereignisziel übergeben wird
- Erstellen Sie eine CloudWatch Ereignisregel, die bei einem Ereignis ausgelöst wird

- Erstellen Sie eine CloudWatch IAM-Rolle für Ereignisse

Zusätzliche Informationen

CodeBuild buildspec.yml-Vorlage

```
version: 0.2
phases:
  install:
    commands:
      - pip install git-remote-codecommit
  build:
    commands:
       - env
       - git clone -b $REFERENCE_NAME codecommit::$REPO_REGION://$REPOSITORY_NAME
       - dt=$(date '+%d-%m-%Y-%H:%M:%S');
       - echo "$dt"
       - zip -yr $dt-$REPOSITORY_NAME-backup.zip ./
       - aws s3 cp $dt-$REPOSITORY_NAME-backup.zip s3:// #substitute a valid S3 Bucket
 Name here
```

CloudWatch Regel für Ereignisse

```
{
  "source": [
    "aws.codecommit"
  ],
  "detail-type": [
    "CodeCommit Repository State Change"
  ],
  "detail": {
    "event": [
      "referenceCreated",
      "referenceUpdated"
    ]
  }
}
```

Beispiel für einen Eingangstransformator für das Regelziel „ CloudWatch Ereignisse“

Eingabepfad:

```
{"referenceType":"$.detail.referenceType","region":"$.region","repositoryName":"$.detail.reposi
```

Eingabevorlage (bitte geben Sie die entsprechenden Werte ein):

```
{
    "environmentVariablesOverride": [
        {
            "name": "REFERENCE_NAME",
            "value": ""
        },
        {
            "name": "REFERENCE_TYPE",
            "value": ""
        },
        {
            "name": "REPOSITORY_NAME",
            "value": ""
        },
        {
            "name": "REPO_REGION",
            "value": ""
        },
        {
            "name": "ACCOUNT_ID",
            "value": ""
        }
    ]
}
```

Automatisieren Sie das Löschen von AWS CloudFormation Stacks und zugehörigen Ressourcen

Erstellt von SANDEEP SINGH (AWS) und James Jacob (AWS)

Übersicht

AWS CloudFormationist ein weit verbreiteter Service zur Verwaltung der Cloud-Infrastruktur als Code (IaC). Wenn Sie ihn verwenden CloudFormation, verwalten Sie zugehörige Ressourcen als eine einzige Einheit, die als Stack bezeichnet wird. Sie können eine Sammlung von Ressourcen durch Erstellen, Aktualisieren und Löschen von Stacks erstellen und löschen.

Manchmal benötigen Sie die Ressourcen in einem CloudFormation Stapel nicht mehr. Abhängig von den Ressourcen und ihren Konfigurationen kann es kompliziert sein, einen Stapel und die zugehörigen Ressourcen zu löschen. In realen Produktionssystemen schlagen Löschungen aufgrund widersprüchlicher Bedingungen oder Einschränkungen, die nicht außer Kraft gesetzt werden können, CloudFormation manchmal fehl oder dauern lange. Es kann eine sorgfältige Planung und Ausführung erfordern, um sicherzustellen, dass alle Ressourcen ordnungsgemäß, effizient und konsistent gelöscht werden. Dieses Muster beschreibt, wie Sie ein Framework einrichten, das Sie beim Löschen von CloudFormation Stacks unterstützt, die die folgenden Komplexitäten beinhalten:

- Ressourcen mit Löschschutz — Bei einigen Ressourcen ist der Löschschutz möglicherweise aktiviert. Gängige Beispiele sind Amazon DynamoDB-Tabellen und Amazon Simple Storage Service (Amazon S3) -Buckets. Der Löschschutz verhindert automatisiertes Löschen, z. B. das Löschen durch. CloudFormation Wenn Sie diese Ressourcen löschen möchten, müssen Sie den Löschschutz manuell oder programmgesteuert außer Kraft setzen oder vorübergehend deaktivieren. Bevor Sie fortfahren, sollten Sie die Auswirkungen des Löschens dieser Ressourcen sorgfältig abwägen.
- Ressourcen mit Aufbewahrungsrichtlinien — Bestimmte Ressourcen, wie z. B. AWS Key Management Service (AWS KMS) -Schlüssel und Amazon S3 S3-Buckets, verfügen möglicherweise über Aufbewahrungsrichtlinien, die angeben, wie lange sie nach der Anforderung des Löschvorgangs aufbewahrt werden sollen. Sie sollten diese Richtlinien bei der Säuberungsstrategie berücksichtigen, um die Einhaltung der Unternehmensrichtlinien und behördlichen Anforderungen zu gewährleisten.
- Verzögertes Löschen von Lambda-Funktionen, die an eine VPC angehängt sind — Das Löschen einer AWS LambdaFunktion, die an eine Virtual Private Cloud (VPC) angehängt ist, kann 5—40 Minuten dauern, abhängig von den mehreren miteinander verbundenen Abhängigkeiten, die an

dem Prozess beteiligt sind. Wenn Sie die Funktion vor dem Löschen des Stacks von der VPC trennen, können Sie diese Verzögerung auf unter 1 Minute reduzieren.

- Ressourcen, die nicht direkt von erstellt wurden CloudFormation — In bestimmten Anwendungsdesigns können Ressourcen außerhalb des ursprünglichen CloudFormation Stacks erstellt werden, entweder von der Anwendung selbst oder durch Ressourcen, die über den Stack bereitgestellt werden. Nachfolgend finden Sie zwei Beispiele:
  - CloudFormation könnte eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance bereitstellen, die ein Benutzerdatenskript ausführt. Dann könnte dieses Skript einen AWS Systems ManagerParameter zum Speichern anwendungsbezogener Daten erstellen. Dieser Parameter wird nicht verwaltet. CloudFormation
  - CloudFormation könnte eine Lambda-Funktion bereitstellen, die automatisch eine Amazon CloudWatch Logs-Gruppe zum Speichern von Protokollen generiert. Diese Protokollgruppe wird nicht über CloudFormation verwaltet.

  Auch wenn diese Ressourcen nicht direkt von verwaltet werden CloudFormation, müssen sie häufig bereinigt werden, wenn der Stapel gelöscht wird. Wenn sie nicht verwaltet werden, können sie verwaist werden und zu unnötigem Ressourcenverbrauch führen.

Diese Leitplanken können zwar zu Komplexität führen, sind aber gewollt und von entscheidender Bedeutung. Die Möglichkeit CloudFormation , alle Beschränkungen außer Kraft zu setzen und Ressourcen wahllos zu löschen, könnte in vielen Szenarien zu nachteiligen und unvorhergesehenen Folgen führen. Als Cloud-Ingenieur, der für die Verwaltung der Umgebung verantwortlich ist, kann es jedoch vorkommen, dass diese Einschränkungen außer Kraft gesetzt werden müssen, insbesondere in Entwicklungs-, Test- DevOps oder Staging-Umgebungen.

Gezielte Geschäftsergebnisse

Durch die Implementierung dieses Frameworks können Sie die folgenden Vorteile erzielen:

- Kostenmanagement — Durch die regelmäßige und effiziente Bereinigung temporärer Umgebungen, wie end-to-end z. B. Umgebungen für Benutzerakzeptanztests, wird verhindert, dass Ressourcen länger als nötig genutzt werden. Dadurch können die Kosten erheblich gesenkt werden.
- Sicherheit — Die automatische Säuberung veralteter oder ungenutzter Ressourcen reduziert die Angriffsfläche und trägt zur Aufrechterhaltung einer sicheren AWS Umgebung bei.
- Betriebseffizienz — Regelmäßige und automatische Säuberungen können die folgenden betrieblichen Vorteile bieten:

- Automatisierte Skripts, die alte Protokollgruppen entfernen oder Amazon S3 S3-Buckets leeren, können die betriebliche Effizienz verbessern, indem sie die Umgebung sauber und überschaubar halten.
- Das schnelle Löschen und Neuerstellen von Stacks unterstützt schnelle Iterationen bei Design und Implementierung, was zu einer robusteren und robusteren Architektur führen kann.
- Das regelmäßige Löschen und Neuerstellen von Umgebungen kann Ihnen helfen, potenzielle Probleme zu identifizieren und zu beheben. Auf diese Weise können Sie sicherstellen, dass die Infrastruktur realen Szenarien standhält.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Python Version 3.6 oder höher, installiert
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert

Einschränkungen

- Eine Benennungskonvention wird verwendet, um die Ressourcen zu identifizieren, die gelöscht werden sollen. Der Beispielcode in diesem Muster verwendet ein Präfix für den Ressourcennamen, Sie können jedoch Ihre eigene Benennungskonvention definieren. Ressourcen, die diese Benennungskonvention nicht verwenden, werden nicht identifiziert oder anschließend gelöscht.

Architektur

Das folgende Diagramm zeigt, wie dieses Framework den CloudFormation Zielstapel und die damit verbundenen zusätzlichen Ressourcen identifiziert.

Das Diagramm zeigt den folgenden Workflow:

1. Ressourcen sammeln — Das Automatisierungs-Framework verwendet eine Namenskonvention, um alle relevanten CloudFormation Stacks, Amazon Elastic Container Registry (Amazon ECR) - Repositorys, DynamoDB-Tabellen und Amazon S3 S3-Buckets zurückzugeben.

> **Note**
>
> Die Funktionen für diese Phase verwenden Paginatoren, eine Funktion in Boto3, die den Prozess der Iteration über eine verkürzte API-Ergebnismenge abstrahiert. Dadurch wird sichergestellt, dass alle Ressourcen verarbeitet werden. Um die Leistung weiter zu optimieren, sollten Sie erwägen, serverseitige Filterung anzuwenden oder eine clientseitige Filterung durchzuführen. JMESPath

2. Vorverarbeitung — Das Automatisierungs-Framework identifiziert und behebt die Serviceeinschränkungen, die außer Kraft gesetzt werden müssen, damit die Ressourcen gelöscht werden können. CloudFormation Beispielsweise wird die `DeletionProtectionEnabled` Einstellung für DynamoDB-Tabellen auf geändert. `False` In der Befehlszeilenschnittstelle erhalten Sie für jede Ressource eine Eingabeaufforderung, in der Sie gefragt werden, ob Sie die Einschränkung überschreiben möchten.
3. Stapel löschen — Das Automation Framework löscht den Stapel. CloudFormation In der Befehlszeilenschnittstelle erhalten Sie eine Eingabeaufforderung mit der Frage, ob Sie den Stack löschen möchten.
4. Nachbearbeitung — Das Automatisierungs-Framework löscht alle zugehörigen Ressourcen, die nicht direkt CloudFormation als Teil des Stacks bereitgestellt wurden. Beispiele für diese Ressourcentypen sind Systems Manager Manager-Parameter und CloudWatch Protokollgruppen. Separate Funktionen sammeln diese Ressourcen, verarbeiten sie vor und löschen sie anschließend. In der Befehlszeilenschnittstelle werden Sie für jede Ressource gefragt, ob Sie die Ressource löschen möchten.

> **Note**
>
> Die Funktionen für diese Phase verwenden Paginatoren, eine Funktion in Boto3, die den Prozess der Iteration über eine verkürzte API-Ergebnismenge abstrahiert. Dadurch wird sichergestellt, dass alle Ressourcen verarbeitet werden. Um die Leistung weiter zu optimieren, sollten Sie erwägen, serverseitige Filterung anzuwenden oder eine clientseitige Filterung durchzuführen. JMESPath

Automatisierung und Skalierung

Wenn Ihr CloudFormation Stack andere Ressourcen enthält, die nicht im Beispielcode enthalten sind, oder wenn der Stack eine Einschränkung hat, die in diesem Muster nicht behoben wurde, können Sie das Automatisierungsframework an Ihren Anwendungsfall anpassen. Gehen Sie beim Sammeln von Ressourcen, der Vorverarbeitung, dem Löschen des Stacks und der anschließenden Nachverarbeitung derselben Methode nach.

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten AWS-Konten Lebenszyklus über und zu verwalten. AWS-Regionen
- CloudFormation Command Line Interface (CFN-CLI) ist ein Open-Source-Tool, mit dem Sie Erweiterungen von Drittanbietern entwickeln und testen AWS und diese dann für die Verwendung in registrieren können. CloudFormation
- AWS SDK für Python (Boto3)ist ein Softwareentwicklungskit, mit dem Sie Ihre Python-Anwendung, -Bibliothek oder Ihr Skript integrieren können AWS-Services.

Andere Tools

- Click ist ein Python-Tool, mit dem Sie Befehlszeilenschnittstellen erstellen können.
- Poetry ist ein Tool für Abhängigkeitsmanagement und Paketierung in Python.
- Pyenv ist ein Tool, mit dem Sie Python-Versionen verwalten und zwischen ihnen wechseln können.
- Python ist eine Allzweck-Computerprogrammiersprache.

Code-Repository

Der Code für dieses Muster ist im GitHub cloudformation-stack-cleanupRepository verfügbar.

Bewährte Methoden

- Kennzeichnen Sie Ressourcen zur leichteren Identifizierung — Implementieren Sie eine Tagging-Strategie, um Ressourcen zu identifizieren, die für unterschiedliche Umgebungen und Zwecke erstellt wurden. Tags können den Bereinigungsprozess vereinfachen, indem sie Ihnen helfen, Ressourcen anhand ihrer Tags zu filtern.

- Ressourcenlebenszyklen einrichten — Definieren Sie Ressourcenlebenszyklen, um Ressourcen nach einem bestimmten Zeitraum automatisch zu löschen. Auf diese Weise können Sie sicherstellen, dass temporäre Umgebungen nicht zu dauerhaften Kostenbelastungen werden.

Epen

Tools installieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	1. Erstellen Sie einen Ordner in Ihrer virtuellen Umgebung. Benennen Sie ihn mit Ihrem Projektnamen. 2. Öffnen Sie ein Terminal auf Ihrem lokalen Computer und navigieren Sie zu diesem Ordner. 3. Geben Sie den folgenden Befehl ein, um das cloudformation-stack-cleanupRepository in Ihr Projektverzeichnis zu klonen: `git clone https://github.com/aws-samples/cloudformation-stack-cleanup.git`	DevOps Ingenieur
Installieren Sie Poetry.	Folgen Sie den Anweisungen (Poesy-Dokumentation), um Poetry in der virtuellen Zielumgebung zu installieren.	DevOps Ingenieur
Installieren Sie die Abhängigkeiten.	1. Geben Sie den folgenden Befehl ein, um zum	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Projektverzeichnis zu navigieren:
	`cd cloudformation-stack-cleanup`
	2. Geben Sie den folgenden Befehl ein:
	`poetry install`
	Dadurch werden alle erforderlichen Abhängigkeiten wie Boto3, click und der Quellcode für die CloudFormation CLI installiert.	

(Optional) Installieren Sie Pyenv.	Folgen Sie den Anweisungen (GitHub), um Pyenv zu installieren.	DevOps Ingenieur

(Optional) Passen Sie das Framework an

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Funktionen, die die Zielressourcen sammeln, vorverarbeiten und löschen.	1. Geben Sie im geklonten Repository den folgenden Befehl ein, um zum Verzeichnis zu navigieren: `cli` `cd cfncli/cli` 2. Öffnen Sie die Datei cleanup_enviornment.py.	DevOps Ingenieur, Python

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Erstellen Sie eine neue Python-Funktion, die den Ressourcentyp erfasst, den Sie ändern möchten. Ein Beispiel finden Sie in der `gather_ddb_tables` Funktion in dieser Datei. 4. Erstellen Sie eine neue Python-Funktion, die die Diensteinschränkungen für die Zielressource außer Kraft setzt. Ein Beispiel finden Sie in der `remove_ddb_deletion_protection` Funktion in dieser Datei. 5. Erstellen Sie eine neue Python-Funktion, die nicht verwaltete Zielressourcen sammelt. Ein Beispiel finden Sie in der `gather_log_groups` Funktion in dieser Datei. 6. Erstellen Sie eine neue Python-Funktion, die nicht verwaltete Zielressourcen löscht. Ein Beispiel finden Sie in der `delete_log_group` Funktion in dieser Datei. 7. Speichern und schließen Sie die Datei cleanup_environment.py.	

Erstellen Sie Beispielressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen CloudFormation Stapel.	1. Navigieren Sie zum -Projektverzeichnis. 2. Geben Sie den folgenden Befehl ein, um einen CloudFormation Stack zu erstellen, der eine DynamoDB-Tabelle und eine Sicherheitsgruppe bereitstellt. Aktualisieren Sie den Wert für: `<VPCID>` `aws cloudformation create-stack \ --stack-name sampleforcleanup-Stack \ --template-body file://samples/sample-cfn-stack.yaml \ --parameters ParameterKey=VpcId,ParameterValue=<VPCID> \ --region us-east-1`	AWS DevOps
Erstellen Sie einen Systems Manager Manager-Parameter.	Geben Sie den folgenden Befehl ein, um einen Systems Manager Manager-Parameter zu erstellen, der nicht bereitgestellt wird über CloudFormation: `aws ssm put-parameter \`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--name "/samplef orcleanup/database/ password" \ --value "your_db_ password" \ --type "SecureString" \ --description "Database password for my app" \ --tier "Standard" \ --region "us-east-1"`	
Erstellen Sie einen Amazon-S3-Bucket.	Geben Sie den folgenden Befehl ein, um einen Amazon S3 S3-Bucket zu erstellen, der nicht bereitgestellt wird über CloudFormation: `aws s3api create-bucket \ --bucket samplesor cleanup-unmanagedb ucket-<UniqueIdent ifier> \ --region us-east-1 \ --create-bucket-co nfiguration LocationC onstraint=us-east-1`	AWS DevOps

Löschen Sie die Beispielressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie den CloudForm ation Stapel.	1. Geben Sie den folgenden Befehl ein, um den CloudFormation Beispiels	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	tapel, den Systems Manager Manager-P arameter und den Amazon S3 S3-Bucket zu löschen, die Sie erstellt haben: `cfncli --region us-east-1 \ dev cleanup-env \ --prefix-list sampleforcleanup` 2. Wenn Sie dazu aufgeford ert werden, geben Sie ein, Y um fortzufahren.	
Bestätigen Sie das Löschen von Ressourcen.	Vergewissern Sie sich in der Ausgabe, dass alle Beispielr essourcen gelöscht wurden. Eine Beispielausgabe finden Sie im Abschnitt Zusätzliche Ressourcen dieses Musters.	AWS DevOps

Zugehörige Ressourcen

- Einen Stack löschen (CloudFormation Dokumentation)
- Problembehandlung CloudFormation (CloudFormation Dokumentation)
- Lambda-Funktionen Zugriff auf Ressourcen in einer Amazon VPC gewähren (Lambda-Dokumentation)
- Wie lösche ich einen AWS CloudFormation Stack, der im Status DELETE_FAILED hängengeblieben ist? (Wissenszentrum)AWS

Zusätzliche Informationen

Im Folgenden finden Sie ein Beispiel für die Ausgabe des `cfncli` Befehls:

```
cfncli --region aus-east-1  dev cleanup-env --prefix-list sampleforcleanup


https://sts.us-east-1.amazonaws.com
Cleaning up: ['sampleforcleanup'] in xxxxxxxxxx:us-east-1
Do you want to proceed? [Y/n]: Y
No S3 buckets
No ECR repositories
No Lambda functions in VPC
The following DynamoDB tables will have their deletion protection removed:
sampleforcleanup-MyDynamoDBTable
Do you want to proceed with removing deletion protection from these tables? [Y/n]: Y
Deletion protection disabled for DynamoDB table 'sampleforcleanup-MyDynamoDBTable'.
The following CloudFormation stacks will be deleted:
sampleforcleanup-Stack
Do you want to proceed with deleting these CloudFormation stacks? [Y/n]: Y
Initiated deletion of CloudFormation stack: `sampleforcleanup-Stack`
Waiting for stack `sampleforcleanup-Stack` to be deleted...
CloudFormation stack `sampleforcleanup-Stack` deleted successfully.
The following ssm_params will be deleted:
/sampleforcleanup/database/password
Do you want to proceed with deleting these ssm_params? [Y/n]: Y
Deleted SSM Parameter: /sampleforcleanup/database/password
Cleaned up: ['sampleforcleanup']
```

Automatisieren Sie das dynamische Pipeline-Management für die Bereitstellung von Hotfix-Lösungen in Gitflow-Umgebungen mithilfe von und AWS Service CatalogAWS CodePipeline

Erstellt von Balaji Vedagiri (AWS), Faisal Shahdad (AWS), Shanmugam Shanker (AWS) und Vivek Thangamuthu (AWS)

Übersicht

> **Note**
>
> AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Dieses Muster bezieht sich auf ein Szenario der Verwaltung einer dynamischen Hotfix-Pipeline, die ausschließlich der sicheren Bereitstellung von Hotfix-Lösungen in einer Produktionsumgebung dient. Die Lösung wird mithilfe eines AWS Service Catalog Portfolios und Produkts implementiert und verwaltet. Eine EventBridge Amazon-Regel wird für die Automatisierung von Ereignissen verwendet. Einschränkungen werden mithilfe von Service Catalog-Portfolioeinschränkungen und AWS Identity and Access Management (IAM) -Rollen für Entwickler durchgesetzt. Nur eine AWS Lambda Funktion darf das Service Catalog-Produkt starten, ausgelöst durch die EventBridge Regel. Dieses Muster wurde für Umgebungen mit einem bestimmten Gitflow-Setup entwickelt, das unter Zusätzliche Informationen beschrieben wird.

In der Regel wird ein Hotfix bereitgestellt, um kritische Probleme oder Sicherheitsprobleme zu beheben, die in einer Live-Umgebung, z. B. in der Produktionsumgebung, gemeldet wurden. Hotfixes sollten nur direkt in Staging- und Produktionsumgebungen bereitgestellt werden. Die Staging- und Production-Pipelines werden häufig für reguläre Entwicklungsanfragen verwendet. Diese Pipelines können nicht zur Bereitstellung von Hotfixes verwendet werden, da es fortlaufende Qualitätssicherungsfunktionen gibt, die nicht auf die Produktionsumgebung übertragen werden können. Für die Veröffentlichung von Hotfixes beschreibt dieses Muster eine dynamische, kurzlebige Pipeline mit den folgenden Sicherheitsfunktionen:

- Automatische Erstellung — Eine Hotfix-Pipeline wird automatisch erstellt, wenn ein Hotfix-Branch in einem Repository erstellt wird. AWS CodeCommit

- Zugriffsbeschränkungen — Entwickler haben keinen Zugriff darauf, diese Pipeline außerhalb des Hotfix-Prozesses zu erstellen.
- Kontrollierte Phase — Die Pipeline verfügt über eine kontrollierte Phase mit einem speziellen Zugriffstoken, das sicherstellt, dass eine Pull-Anfrage (PR) nur einmal erstellt werden kann.
- Genehmigungsphasen — Genehmigungsphasen sind in der Pipeline enthalten, um die erforderlichen Genehmigungen von den relevanten Interessengruppen einzuholen.
- Automatisches Löschen — Die Hotfix-Pipeline wird automatisch gelöscht, wenn ein `hotfix` Branch im CodeCommit Repository gelöscht wird, nachdem er mit einem PR zusammengeführt wurde.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Drei aktive AWS-Konten sind wie folgt erforderlich:
  - Tools-Konto — Für die Einrichtung von Continuous Integration und Continuous Delivery (CI/CD).
  - Stage-Konto — Für Benutzerakzeptanztests.
  - Produktionskonto — Für einen geschäftlichen Endbenutzer.
  - (Optional) Fügen Sie ein Konto hinzu AWS-Konto , das als QA-Konto fungiert. Dieses Konto ist erforderlich, wenn Sie sowohl ein Haupt-Pipeline-Setup, einschließlich QA, als auch eine Hotfix-Pipeline-Lösung zum Testen benötigen.
- Ein AWS CloudFormation Stack mit einer optionalen Bedingung zur Bereitstellung im QA-Konto unter Verwendung der Hauptpipeline, falls erforderlich. Das Muster kann auch ohne die Einrichtung der Haupt-Pipeline getestet werden, indem ein `hotfix` Branch erstellt und gelöscht wird.
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket zum Speichern der CloudFormation Vorlagen, die zur Erstellung von Service Catalog-Produkten verwendet werden.
- Erstellen Sie PR-Genehmigungsregeln für das CodeCommit Repository gemäß den Compliance-Anforderungen (nachdem Sie das Repository erstellt haben).
- Schränken Sie die IAM-Berechtigungen von Entwicklern und Teamleitern ein, um die Ausführung der Lambda-Funktion prcreation-lambda zu verweigern, da sie nur von der Pipeline aus aufgerufen werden sollte.

Einschränkungen

- Der CloudFormation Anbieter wird in der Bereitstellungsphase verwendet, und die Anwendung wird mithilfe eines Änderungssatzes bereitgestellt. CloudFormation Wenn Sie eine andere Bereitstellungsoption verwenden möchten, ändern Sie den CodePipeline Stack nach Bedarf.
- Dieses Muster verwendet AWS CodeBuild und andere Konfigurationsdateien, um einen Beispiel-Microservice bereitzustellen. Wenn Sie einen anderen Workload-Typ haben (z. B. serverlose Workloads), müssen Sie alle relevanten Konfigurationen aktualisieren.
- Dieses Muster stellt die Anwendung auf einer einzigen Fläche AWS-Region (z. B. US East (N. Virginia) us-east-1) bereit. AWS-Konten Um die Bereitstellung in mehreren Regionen durchzuführen, ändern Sie die Regionsreferenz in Befehlen und Stapeln.
- Einige AWS-Services sind nicht in allen AWS-Regionen verfügbar. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie unter AWS-Services nach Regionen. Informationen zu bestimmten Endpunkten finden Sie unter Service-Endpunkte und Kontingente. Wählen Sie dort den Link für den Service aus.

Architektur

Die Diagramme in diesem Abschnitt enthalten Workflows für ein Ereignis zum Erstellen eines Lebenszyklus und für ein Ereignis zum Löschen eines Lebenszyklus.

Das obige Diagramm zur Erstellung eines Lebenszyklusereignisses zeigt Folgendes:

1. Der Entwickler erstellt einen `hotfix-*` Branch im CodeCommit Repository, um eine Hotfix-Lösung zu entwickeln.
2. Das Ereignis, bei dem ein `hotfix-*` Branch erstellt wird, wird durch die Regel erfasst. EventBridge Zu den Ereignisdetails gehören der Repository-Name und der Branch-Name.
3. Die EventBridge Regel ruft die AWS Lambda Funktion `hotfix-lambda-function` auf. Die EventBridge Regel übergibt die Ereignisinformationen als Eingabe an die Lambda-Funktion.
4. Die Lambda-Funktion verarbeitet die Eingabe, um den Repository-Namen und den Branchnamen abzurufen. Es startet das Service Catalog-Produkt mit Werten, die aus der verarbeiteten Eingabe abgerufen wurden.
5. Das Service Catalog-Produkt umfasst ein Pipeline-Setup, mit dem die Lösung in den Phasen- und Produktionsumgebungen bereitgestellt wird. Der Pipeline-Block umfasst die Phasen Sourcing, Build und Deployment. Außerdem gibt es eine manuelle Genehmigungsphase, um die Bereitstellung für die Produktionsumgebung voranzutreiben.

6. In der Quellphase wird der Code aus dem Repository und der `hotfix-*` Branch abgerufen, die im ersten Schritt erstellt wurden. Der Code wird über einen Amazon S3 S3-Bucket für Artefakte an die Build-Phase übergeben. In der Erstellungsphase wird ein Container-Image erstellt, das den Hotfix enthält, der in der `hotfix-*` Filiale entwickelt und in Amazon Elastic Container Registry (Amazon ECR) übertragen wurde.
7. In der Bereitstellungsphase für die Stage-Umgebung wird Amazon Elastic Container Service (Amazon ECS) mit dem neuesten Container-Image aktualisiert, das den Hotfix enthält. Der Hotfix wird bereitgestellt, indem ein CloudFormation Änderungssatz erstellt und ausgeführt wird.
8. Die `prcreation-lambda` Lambda-Funktion wird nach erfolgreicher Bereitstellung in der Stage-Umgebung aufgerufen. Diese Lambda-Funktion erstellt eine PR vom `hotfix-*` Zweig bis zu den `develop` `main` Zweigen des Repositorys. Die Lambda-Funktion stellt sicher, dass der in der `hotfix-*` Branche entwickelte Fix wieder zusammengeführt und in nachfolgende Bereitstellungen aufgenommen wird.
9. Eine manuelle Genehmigungsphase trägt dazu bei, dass die erforderlichen Beteiligten den Fix überprüfen und die Genehmigung für die Implementierung in der Produktionsumgebung erteilen.
10. In der Bereitstellungsphase für die Produktionsumgebung wird Amazon ECS mit dem neuesten Container-Image aktualisiert, das den Hotfix enthält. Der Hotfix wird bereitgestellt, indem ein CloudFormation Änderungssatz erstellt und ausgeführt wird.

Das vorherige Diagramm zum Löschen eines Lebenszyklusereignisses zeigt Folgendes:

1. Der Entwickler löscht den `hotfix-*` Branch nach erfolgreicher Bereitstellung des Hotfixes in der Produktionsumgebung.
2. Das Ereignis zum Löschen einer `hotfix-*` Zweigstelle wird durch eine EventBridge Regel erfasst. Zu den Ereignisdetails gehören der Repository-Name und der Branch-Name.
3. Die EventBridge Regel ruft die Lambda-Funktion auf. Die EventBridge Regel übergibt die Ereignisinformationen als Eingabe an die Lambda-Funktion.
4. Die Lambda-Funktion verarbeitet die Eingabe, um den Repository-Namen und den Branchnamen abzurufen. Die Lambda-Funktion bestimmt anhand der übergebenen Eingabe das jeweilige Service Catalog-Produkt und beendet dann das Produkt.
5. Die von Service Catalog bereitgestellte Produktbeendigung löscht die Pipeline und die entsprechenden Ressourcen, die zuvor in diesem Produkt erstellt wurden.

Automatisierung und Skalierung

- Das Muster umfasst eine EventBridge Regel und eine Lambda-Funktion, die mehrere Anfragen zur Erstellung von Hotfix-Branches parallel verarbeiten können. Die Lambda-Funktion stellt das Service Catalog-Produkt für die entsprechende Ereignisregel bereit.
- Die Pipeline-Einrichtung erfolgt mithilfe des Service Catalog-Produkts, das Funktionen zur Versionskontrolle bietet. Die Lösung skaliert außerdem automatisch, um mehrere Hotfix-Entwicklungen für dieselbe Anwendung parallel abzuwickeln.
- Die Funktion prcreation-Lambda stellt sicher, dass diese Hotfix-Änderungen durch eine automatische Pull-Request-Erstellung auch wieder in die Branches `main` und die `develop` Branches integriert werden. Dieser Ansatz ist wichtig, um die Branches `main` und die `develop` Branches mit allen Fixes auf dem neuesten Stand zu halten und mögliche Code-Regressionen zu vermeiden. Dieser Prozess trägt dazu bei, die Konsistenz zwischen den Branches aufrechtzuerhalten und Code-Regressionen zu verhindern, indem sichergestellt wird, dass alle langlebigen Branches über die neuesten Fixes verfügen.

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über und zu verwalten. AWS-Konten AWS-Regionen
- AWS CodeBuildist ein vollständig verwalteter Build-Service, der Ihnen hilft, Quellcode zu kompilieren, Komponententests durchzuführen und Artefakte zu erstellen, die sofort einsatzbereit sind.
- AWS CodeCommitist ein Versionskontrolldienst, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen. AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen findest du unter So migrierst du dein AWS CodeCommit Repository zu einem anderen Git-Anbieter.
- AWS CodePipelinehilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die zur kontinuierlichen Veröffentlichung von Softwareänderungen erforderlich sind.
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.

- Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Beenden und Verwalten von Containern in einem Cluster vereinfacht.
- AWS Key Management Service (AWS KMS) hilft Ihnen dabei, kryptografische Schlüssel zu erstellen und zu kontrollieren, um Ihre Daten zu schützen.
- AWS Service Catalogunterstützt Sie bei der zentralen Verwaltung von Katalogen mit IT-Services, für die eine Genehmigung erteilt wurde. AWS Endbenutzer können schnell nur die jeweils benötigten genehmigten IT-Services bereitstellen, wobei die Einschränkungen Ihrer Organisation berücksichtigt werden.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere Tools

- AWS CloudFormation Linter (cfn-lint) ist ein Linter, der CloudFormation YAML- oder JSON-Vorlagen anhand der Ressourcenspezifikation überprüft. CloudFormation Es führt auch andere Prüfungen durch, z. B. die Überprüfung auf gültige Werte für Ressourceneigenschaften und die Einhaltung von Best Practices.
- cfn-nag ist ein Open-Source-Tool, das potenzielle Sicherheitsprobleme in CloudFormation Vorlagen identifiziert, indem es nach Mustern sucht.
- Docker ist eine Reihe von Platform-as-a-Service (PaaS) -Produkten, die Virtualisierung auf Betriebssystemebene nutzen, um Software in Containern bereitzustellen. Dieses Muster verwendet Docker, um Container-Images lokal zu erstellen und zu testen.
- Git ist ein verteiltes Open-Source-Versionskontrollsystem.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub dynamic_hotfix_codepipeline verfügbar.

Bewährte Methoden

Überprüfen und passen Sie die IAM-Rollen und Service Control Policies (SCP) in Ihrer Umgebung an, um sicherzustellen, dass sie den Zugriff angemessen einschränken. Dies ist wichtig, um Aktionen zu verhindern, die die in diesem Muster enthaltenen Sicherheitsmaßnahmen außer Kraft setzen könnten. Folgen Sie dem Prinzip der geringsten Rechte und gewähren Sie die für die Ausführung

einer Aufgabe erforderlichen Mindestberechtigungen. Weitere Informationen finden Sie in der IAM-Dokumentation unter Gewährung der geringsten Rechte und bewährte Methoden zur Sicherheit.

Epen

Richten Sie die Arbeitsumgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Führen Sie den folgenden Befehl aus, um das Beispiel-Repository in ein neues Verzeichnis an Ihrem Arbeitsplatz zu klonen: `git clone git@github.com:aws-samples/dynamic_hotfix_codepipeline.git`	AWS DevOps
Exportieren Sie Umgebungsvariablen für die CloudFormation Stack-Bereitstellung.	Definieren Sie die folgenden Umgebungsvariablen, die später in diesem Muster als Eingabe für die CloudFormation Stacks verwendet werden. • `ApplicationName` — Diese Variable wird verwendet, um Ressourcen zu benennen, die für eine Anwendung erstellt wurden, sodass sie leichter nachverfolgt werden können. Verwenden Sie den folgenden Befehl und `Applicationname` ersetzen Sie ihn durch Ihren	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	tatsächlichen Anwendungsnamen:
	
	`export ApplicationName=<Applicationname>`
	
	• `BucketStartName` — Diese Variable dient zur Benennung eines Amazon S3 S3-Buckets. S3-Bucket-Namen müssen global für alle eindeutig sein AWS-Konten. Verwenden Sie den folgenden Befehl und `BucketName` ersetzen Sie ihn durch einen eindeutigen Namen für Ihren S3-Bucket:
	
	`export BucketStartName=<BucketName>`
	
	• Kontonummern und Regionen — Diese Variablen speichern AWS-Konto Zahlen für verschiedene Umgebungen und die Bereitstellungsregion. Verwenden Sie die folgenden Befehle und ersetzen Sie die Platzhalter (wie `prodaccountnumber` und`region`) durch Ihre tatsächlichen AWS-Konto Zahlen und	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	die AWS-Region , die Sie verwenden.
	
	Note
	`QAAccount` ist optional. Wenn Sie es verwenden möchten`QAAccount` , richten Sie es mithilfe der Parameter für den Haupt-Pipeline-Stack ein.
	
	`export ProdAccount=<prodaccountnumber>`
	`export StageAccount=<stage/preprodaccountnumber>`
	`export QAAccount=<qaccountnumber>`
	`export ToolsAccount=<toolsaccountnumber>`
	`export DepRegion=<region>`	

Richten Sie die erforderlichen Voraussetzungen ein in AWS-Konten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die für CI/CD erforderlichen Ressourcen im Tools-Konto.	Verwenden Sie die folgenden Befehle, um den CloudFormation Stack im Tools-Konto bereitzustellen. (Entfernen Sie den `QAAccount` Parameter, wenn Sie das QA-Konto nicht für die Einrichtung verwenden .)
	`#InToolsAccount`
	`aws cloudformation deploy \`
	`--template-file pre-requisites/pre-reqs.yaml \`
	`--stack-name prereqs \`
	`--parameter-overrides BucketStartName=${BucketStartName} \`
	`ApplicationName=${ApplicationName} ProdAccount=${ProdAccount} \`
	`StageAccount=${StageAccount} ToolsAccount=${ToolsAccount} \`
	`QAAccount=${QAAccount} \`
	`--capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM --region ${DepRegion}`
	Notieren Sie sich die Ressourcen, die das
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CodeCommit Repository und Amazon ECR aus dem vorherigen Stack erstellt haben. Diese Parameter sind erforderlich, um den `main` Zweig der Pipeline in den nächsten Schritten einzurich ten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die für CI/CD erforderlichen Ressourcen in den Workload-Konten.	1. Verwenden Sie die folgenden Befehle, um die CloudFormation Vorlage in jedes Workload-Konto (Phase, Produktion und optionale Qualitätssicherung) zu packen. Ersetzen Sie im folgenden Befehl `S3bucketpackage` durch den Namen des Amazon S3 S3-Buckets, den Sie für die Paketierung verwenden möchten.
	
	`#InStageAccount`
	`aws cloudformation package \`
	`--template-file pre-requisites/infrastack.yaml \`
	`--s3-bucket <S3bucketpackage> \`
	`--s3-prefix infraStack \`
	`--region ${DepRegion} \`
	`--output-template-file pre-requisites/infrastructure_stage.template`
	
	`#InProdAccount`
	`aws cloudformation package \`
	`--template-file pre-requisites/infrastack.yaml \`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>--s3-bucket
	<S3bucketpackage> \
	--s3-prefix
	infraStack \
	--region ${DepRegi
	on} \
	--output-
	template-file
	pre-requisites/inf
	rastructure_prod.t
	emplate</pre>
	2. Verwenden Sie die folgenden Befehle, um die CloudFormation Vorlage in jedem Workload-Konto bereitzustellen:
	<pre>#InStageAccount
	aws cloudformation
	deploy --stack-name
	inframainstack \
	--parameter-over
	rides Applicati
	onName=${Applicati
	onName} ToolsAcco
	unt=${ToolsAccount
	} DepRegion=${DepReg
	ion} \
	--template-file
	pre-requisites/inf
	rastructure_stage.
	template --region
	${DepRegion}
	--capabilities
	CAPABILITY_NAMED_I
	AM
	
	#InProdAccount</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws cloudformation deploy --stack-name inframainstack \ --parameter-overrides ApplicationName=${ApplicationName} ToolsAccount=${ToolsAccount} DepRegion=${DepRegion} \ --template-file pre-requisites/infrastructure_prod.template --region ${DepRegion} --capabilities CAPABILITY_NAMED_IAM`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisieren Sie die Richtlinie für S3-Artefakt-Buckets, um den Zugriff für Workload-Konten zu ermöglichen.	Um die CloudFormation Stack-Voraussetzungen im Tools-Konto zu aktualisieren, verwenden Sie die folgenden Befehle, um alle erforderlichen Berechtigungen für die Workload-Konten Stage und Production hinzuzufügen. (Entfernen Sie den `QAAccount` Parameter, wenn Sie ihn nicht für die Einrichtung verwenden.)
	`#InToolsAccount`
	`aws cloudformation deploy \`
	`--template-file pre-requisites/pre-reqs.yaml \`
	`--stack-name prereqs \`
	`--parameter-overrides BucketStartName=${BucketStartName} \`
	`ApplicationName=${ApplicationName} ProdAccount=${ProdAccount} \`
	`StageAccount=${StageAccount} ToolsAccount=${ToolsAccount} \`
	`QAAccount=${QAAccount} PutPolicy=true \`
	`--capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM --region ${DepRegion}`
		AWS DevOps

Lambda-Funktion und Service Catalog-Ressourcen im Tools-Konto einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie das Service Catalog-Portfolio und die Produkte ein.	Gehen Sie wie folgt vor, um das Service Catalog-Portfolio und die Produkte einzurichten:
	
	1. Laden Sie die Vorlagen pipeline-main.yaml und pipeline-hotfix.yaml aus dem Repository im CodePipeline Verzeichnis in einen vorhandenen Amazon S3 S3-Bucket (`Bucketname`) in der Region hoch, in der Sie die Bereitstellung durchführen möchten (`DepRegion`).
	
	`#InToolsAccount`
	`aws s3 cp ./codepipeline/pipeline-main.yaml s3://<Bucketname>/pipeline-main.yaml`
	`aws s3 cp ./codepipeline/pipeline-hotfix.yaml s3://<Bucketname>/pipeline-hotfix.yaml`
	
	2. Richten Sie das Servicekatalog-Portfolio und das Produkt ein, das die Pipeline für die `hotfix` Filialen `main` und verwaltet. Notieren Sie sich die Details aus dem `Outputs`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Abschnitt für `MainProductId` und `MainProductArtifactId` aus dem folgenden Stapel. Die Informationen werden in späteren Schritten während der Pipeline-Einrichtung für die `main` Filiale benötigt. `#InToolsAccount aws cloudformation deploy \ --template-file pre-requisites/servicecatalogsetup.yaml \ --stack-name servicecatalogsetup \ --parameter-overrides TemplateBucket=<Bucketname> \ --capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM --region ${DepRegion}` 3. Stellen Sie Zugriff für eine IAM-Rolle bereit, die Ressourcen im Tools-Konto für das Haupt-Pipeline-Portfolio des Service Catalog-Portfolios bereitstellt. Verwenden Sie dieses Portfolio, um die Anwendung mithilfe der `main` Filiale bereitzus	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	tellen. Weitere Informationen zur Bereitstellung von Zugriff finden Sie unter Benutzern Zugriff gewähren in der Servicekatalog-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Lambda-Funktionen ein.	Diese Lösung verwendet die folgenden Lambda-Funktionen zur Verwaltung von Hotfix-Workflows: • `hotfix-lambda-function` kümmert sich um die Bereitstellung von Service Catalog-Produkten, wenn eine `hotfix` Filiale erstellt wird. • `hotfix-cleanup-lambda-function` verwaltet die Kündigung eines Produkts, wenn eine `hotfix` Filiale gelöscht wird. • `prcreation-lambda` erstellt Pull-Requests vom `hotfix` Branch zu den `main` Branches `develop` und. Gehen Sie wie folgt vor, damit die Lambda-Funktionen Service Catalog-Produkte bereitstellen und beenden können, wenn `hotfix` Zweige mithilfe der zugehörigen EventBridge Regel erstellt oder gelöscht werden: 1. Verwenden Sie den folgenden Befehl, um die	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	IAM-Rollen und -Berechtigungen für die Lambda-Funktionen zu erstellen, um einen CloudFormation Stack bereitzustellen: `#InToolsAccount aws cloudformation deploy \ --template-file pre-requisites/lambdasetup.yaml \ --stack-name prsclambdasetup \ --capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM --region ${DepRegion}` 2. Gewähren Sie nach der Stack-Bereitstellung den `hotfix-lambda-execution-role` Zugriff auf das Hotfix-Pipeline-Portfolio des Service Catalog-Portfolios mithilfe von. AWS Management Console Dieser Zugriff ermöglicht es der Lambda-Funktion, das Service Catalog-Produkt für Hotfix-Branches zu starten oder zu beenden.	

Erstellen Sie eine Pipeline für den Hauptzweig und stellen Sie die Anwendung in Workload-Konten bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie die Pipeline für die `main` Filiale ein.	Um die Pipeline für den Hauptzweig einzurichten, führen Sie den folgenden Befehl im Tools-Konto aus. Ersetzen Sie die Parameter für `MainProductId` und `MainProductArtifactId` durch Werte aus den `servicecatalogsetup` Stack-Ausgaben.
	`#InToolsAccount`
	`aws servicecatalog provision-product \`
	`--product-id <MainProductId> \`
	`--provisioning-artifact-id <MainProductArtifactId> \`
	`--provisioned-product-name "${ApplicationName}-main-pipeline" \`
	`--provisioning-parameters Key=CodeCommitRepoName,Value="${ApplicationName}-repository" Key=ECRRepository,Value="${ApplicationName}-app" \`
	`--region=${DepRegion}`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung mithilfe der `main` Filiale bereit.	1. Verwenden Sie den Befehl, um das CodeCommit Repository zu klonen, das in den Voraussetzungen erstellt wurde. `git clone` Weitere Informationen finden Sie unter Connect zum CodeCommit Repository herstellen, indem Sie das Repository klonen, wie in der CodeCommit Dokumentation beschrieben. 2. Kopieren Sie alle Anwendungsdateien aus dem im Repository verfügbaren `repotemplates` Verzeichnis in Ihr lokales Repository clone (`${ApplicationName}-repository`). Ändern Sie die folgenden Dateien, um die `ToolsAccount` ID zu aktualisieren. Suchen Sie in jeder Datei den `RegistryAccountid` Parameter und setzen Sie seinen Wert auf Ihre `ToolsAccount` ID. Übernehmen Sie die Änderungen im CodeCommit Repository und übertragen Sie die	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dateien sowohl in die Branches als auch in die `main` `develop` Branches. • ecs-configuration-prod.yaml • ecs-configuration-qa.yaml • ecs-configuration-stage.yaml 3. Um die Anwendung sbereitstellung zu überprüfen, überwachen Sie die CodePipeline Ausführung mithilfe von. AWS Management Console Greifen Sie nach Abschluss der Bereitstellung mithilfe des Application Load Balancer Balancer-FQDN in der Stage-Umgebung auf die Anwendung zu. Vergewissern Sie sich, dass die Anwendung wie erwartet funktioniert. 4. Um die Bereitstellung für die Produktion zu genehmigen, suchen Sie in der CodePipeline Konsole nach der Pipeline für Ihre Anwendung. Finden Sie die `ApprovalToStart` Bühne. Prüfen Sie die Änderungen und geben Sie, falls Sie zufrieden sind, die Genehmigung manuell	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ein, um mit der Produktio nsbereitstellung fortzufah ren.	

Erstellen Sie die Pipeline für einen Hotfix-*-Zweig und stellen Sie den Hotfix bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen `hotfix-*` Branch und übernehmen Sie die Änderungen.	Gehen Sie wie folgt vor, um eine Pipeline für den `hotfix-*` Branch zu erstellen und den Hotfix für die Workload-Konten bereitzustellen: 1. Erstellen Sie einen Branch mit einem Namen, der mit dem Schlüsselwort `hotfix` beginnt. Dieses Muster verwendet beispiels weise den `hotfix-check1` Branch im CodeCommit Anwendung s-Repository (`${Applica tionName}-reposito ry`). Ausführlichere Schritte finden Sie in der CodeCommit Dokumenta tion unter Connect einem AWS CodeCommit Repository herstellen und Grundlegende Git-Befehle. 2. Stellen Sie sicher, dass das Service Catalog-P rodukt `Hotfix CICD`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`Pipeline` erfolgreich dynamisch für die `hotfix-check1` Filiale bereitgestellt wurde. Der Name des bereitgestellten Produkts ist nach diesem Hotfix-Branchnamen und dem Repository-Namen der CodeCommit Anwendung benannt. 3. Übernehmen Sie einige kleinere Änderungen in der Datei index.html und übertragen Sie sie in das CodeCommit Repository. 4. Stellen Sie sicher, dass die CodePipeline Ausführung in der Stage-Umgebung erfolgreich ist. Für die Bereitstellung in der Produktionsumgebung müssen Sie die manuelle Genehmigung in vornehmen CodePipeline. 5. Vergewissern Sie sich, dass die Änderungen auf der Anwendungsstartseite sichtbar sind, indem Sie den vollqualifizierten Domänennamen (FQDN) des Application Load Balancer verwenden. Der FQDN ist im Abschnitt	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	von verfügbar. `Outputs infraMainStack-ALB Stack-*`	
Löschen Sie den `hotfix-check1` Zweig.	Gehen Sie wie folgt vor, um den zuvor erstellten `hotfix-check1` Zweig zu löschen: 1. Löschen Sie den `hotfix-check1` Branch, der sich im CodeCommit Anwendungs-Repository befindet. 2. Stellen Sie sicher, dass das Service Catalog-Produkt, das für die `hotfix-check1` Filiale bereitgestellt wurde, erfolgreich beendet wurde.	AWS DevOps

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen Sie die eingesetzten Ressourcen.	Gehen Sie wie folgt vor, um die Ressourcen zu bereinigen, die zuvor bereitgestellt wurden: 1. Verwenden Sie den folgenden Befehl, um den Amazon ECS-Service auf null Replikate in den Workload-Konten herunterzuskalieren:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>aws ecs update-service --cluster ${ApplicationName}-Cluster --service ${ApplicationName}-Service-stage --desired-count 0 --region ${DepRegion}
	aws ecs update-service --cluster ${ApplicationName}-Cluster --service ${ApplicationName}-Service-prod --desired-count 0 --region ${DepRegion}</pre>
	2. Beenden Sie das Service Catalog-Produkt, das für die `main` Filiale bereitgestellt wurde.
	3. Bereinigen Sie Objekte, die in den Amazon S3 S3-Buckets im Tools-Konto erstellt wurden. Löschen Sie alle Docker-Images in Amazon ECR, bevor Sie die Registrierung selbst löschen.
	4. Entfernen Sie IAM-Rollen im Abschnitt „Zugriff gewährt“ der Servicekatalog-Portfolios, bevor Sie das Servicekatalog-Portfolio löschen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	5. Löschen Sie die CloudFormation Stacks, die im Tools-Konto und in den Workload-Konten bereitgestellt wurden.
	
	`##In Tools Account##`
	`aws cloudformation delete-stack --stack-name servicecatalogsetup --region ${DepRegion}`
	`aws cloudformation delete-stack --stack-name prlambdasetup --region ${DepRegion}`
	`aws cloudformation delete-stack --stack-name prereqs --region ${DepRegion}`
	
	`##In Workload Accounts##`
	`aws cloudformation delete-stack --stack-name inframainstack --region ${DepRegion}`
	
	Weitere Informationen finden Sie in der Service Catalog-Dokumentation unter Löschen bereitgestellter Produkte.	

Fehlerbehebung

Problem	Lösung
Änderungen, die Sie für das CodeCommit Repository übernommen haben, werden nicht bereitgestellt.	Überprüfen Sie die CodeBuild Protokolle auf Fehler bei der Docker-Build-Aktion. Weitere Informationen finden Sie in der CodeBuild -Dokumentation.
Das Service Catalog-Produkt wird nicht bereitgestellt.	Überprüfen Sie die zugehörigen CloudFormation Stacks auf fehlgeschlagene Ereignisse. Weitere Informationen finden Sie in der CloudFormation -Dokumentation.

Zugehörige Ressourcen

- Grundlegende Git-Befehle
- Konfigurieren Sie eine IAM-Richtlinie, um Pushs und Merges auf einen Branch zu beschränken
- Stellen Sie eine Connect zu einem AWS CodeCommit Repository her
- Benutzern Zugriff gewähren
- Ein Docker-Image in ein privates Amazon ECR-Repository übertragen
- Fehlersuche AWS CodeBuild
- Was ist? AWS CodePipeline

Zusätzliche Informationen

Dieses Muster wurde für Umgebungen mit einem Gitflow-Setup entwickelt, das für den Entwicklungsworkflow übernommen wurde. Das CI/CD process. The pipelines follow the deployment cycle that starts from development and moves through quality assurance (QA), stage, and production environments. The CI/CD Setup umfasst zwei Git-Branches mit Werbebereitstellungen in Umgebungen wie folgt:

- Der `develop` Branch wird in der Entwicklungsumgebung bereitgestellt.
- Die `main` Filiale wird in der QA-, Stage- und Produktionsumgebung eingesetzt.

Bei dieser Konfiguration ist es eine Herausforderung, einen Hotfix oder Sicherheitspatch schneller als im üblichen Bereitstellungszyklus zu installieren, während die aktive Entwicklung neuer Funktionen andauert. Für die Bearbeitung von Hotfix- oder Sicherheitsanfragen ist ein spezieller Prozess erforderlich, um sicherzustellen, dass Live-Umgebungen weiterhin ordnungsgemäß funktionieren und sicher sind.

In den folgenden Fällen können Sie jedoch auch andere verfügbare Optionen verwenden, ohne dass ein spezieller Bereitstellungsprozess erforderlich ist:

- Der CI/CD process is well-equipped with automated testing, such as functional and end-to-end tests, which eliminate the need for manual testing and prevent delays in deployments to production. However, if automated testing isn't well integrated into the CI/CD Prozess, bei dem ein kleiner Fix in die Produktionsumgebung übertragen wird, kann für Entwickler komplex und umständlich werden. Dies liegt daran, dass in der QA-Umgebung möglicherweise neue Funktionen auf ihre Genehmigung und Genehmigung warten. Ein Hotfix oder Sicherheitsupdate kann nicht auf einfache Weise gleichzeitig in die Produktionsumgebung eingeführt werden.
- Entwicklungsteams implementieren kontinuierlich neue Funktionen in der Produktionsumgebung und integrieren Hotfixes oder Sicherheitspatches in die geplante Bereitstellung jeder neuen Funktion. Mit anderen Worten, das nächste Funktionsupdate für die Produktionsumgebung besteht aus zwei Komponenten: der Hinzufügung einer neuen Funktion und der Aufnahme des Hotfixes oder Sicherheitspatches. Wenn der Bereitstellungszyklus jedoch nicht kontinuierlich ist, können mehrere neue Funktionen bereits auf die Genehmigung in der QA-Umgebung warten. Die Verwaltung verschiedener Versionen und die Sicherstellung, dass die richtigen Änderungen erneut angewendet werden, können dann komplex und fehleranfällig werden.

> **Note**
>
> Wenn Sie Version 2 von AWS CodePipeline verwenden und die richtigen Auslöser in der `hotfix` Filiale eingerichtet haben, benötigen Sie dennoch einen speziellen Prozess, um ungeplante Anfragen zu bearbeiten. In Version 2 können Sie Trigger entweder für Push- oder Pull-Anfragen einrichten. Die Ausführung wird entweder in die Warteschlange gestellt oder sofort ausgeführt, abhängig vom vorherigen Status der Pipeline. Bei einer dedizierten Pipeline werden die Fixes jedoch sofort auf die Produktionsumgebung angewendet, wodurch sichergestellt wird, dass dringende Probleme unverzüglich behoben werden.

Automatisieren Sie die Erfassung und Visualisierung von benutzerdefinierten Amazon MWAA-Metriken auf Amazon Managed Grafana mithilfe von Terraform

Erstellt von Faisal Abdullah (AWS) und Satya Vajrapu (AWS)

Übersicht

In diesem Muster wird beschrieben, wie Amazon Managed Grafana verwendet wird, um benutzerdefinierte Metriken zu erstellen und zu überwachen, die von Amazon Managed Workflows for Apache Airflow (Amazon MWAA) aufgenommen werden. Amazon MWAA dient als Orchestrator für Workflows und verwendet Directed Acyclic Graphs (DAGs), die in Python geschrieben sind. Im Mittelpunkt dieses Musters steht die Überwachung benutzerdefinierter Metriken, einschließlich der Gesamtzahl der in der letzten Stunde DAGs ausgeführten und fehlgeschlagenen Vorgänge DAGs pro Stunde sowie der durchschnittlichen Dauer dieser Prozesse. Diese Analyse zeigt, wie Amazon Managed Grafana in Amazon MWAA integriert wird, um eine umfassende Überwachung und Einblicke in die Orchestrierung von Workflows in dieser Umgebung zu ermöglichen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver Benutzer AWS-Konto mit den erforderlichen Benutzerberechtigungen, um Folgendes zu erstellen und zu verwalten: AWS-Services
  - AWS Identity and Access Management (IAM) Rollen und Richtlinien
  - AWS Lambda
  - Amazon Managed Grafana
  - Amazon Managed Workflows für Apache Airflow (Amazon MWAA)
  - Amazon Simple Storage Service (Amazon-S3)
  - Amazon Timestream
- Zugriff auf eine Shell-Umgebung, die ein Terminal auf Ihrem lokalen Computer sein kann oder AWS CloudShell.
- Eine Shell-Umgebung, in der Git installiert und die neueste Version von AWS Command Line Interface (AWS CLI) installiert und konfiguriert ist. Weitere Informationen finden Sie AWS CLI in der AWS CLI Dokumentation unter Installation oder Aktualisierung auf die neueste Version von.

- Die folgende Terraform-Version ist installiert: `required_version = ">= 1.6.1, < 2.0.0"` Sie können tfswitch verwenden, um zwischen verschiedenen Versionen von Terraform zu wechseln.
- Konfigurierte Identitätsquelle für Ihren. AWS IAM Identity Center AWS-Konto Weitere Informationen finden Sie unter Bestätigen Sie Ihre Identitätsquellen in IAM Identity Center in der IAM Identity Center-Dokumentation. Sie können zwischen dem Standard IAM-Identity-Center-Verzeichnis, Active Directory oder einem externen Identitätsanbieter (IdP) wie Okta wählen. Weitere Informationen finden Sie unter Verwandte Ressourcen.

Einschränkungen

- Einige AWS-Services sind nicht in allen verfügbar AWS-Regionen. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie unter Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Produktversionen

- Terraform `required_version = ">= 1.6.1, < 2.0.0"`
- Amazon Managed Grafana Version 9.4 oder höher. Dieses Muster wurde auf Version 9.4 getestet.

Architektur

Das folgende Architekturdiagramm hebt die in der Lösung AWS-Services verwendeten Komponenten hervor.

In der obigen Abbildung wird der folgende Arbeitsablauf schrittweise beschrieben:

1. Benutzerdefinierte Metriken in Amazon MWAA stammen von DAGs denen, die innerhalb der Umgebung ausgeführt werden. Die Metriken werden in einem CSV-Dateiformat in den Amazon S3 S3-Bucket hochgeladen. Im Folgenden werden die Datenbankabfragefunktionen von Amazon MWAA DAGs verwendet:
   - `run-example-dag`— Diese DAG enthält Python-Beispielcode, der eine oder mehrere Aufgaben definiert. Sie läuft alle 7 Minuten und druckt das Datum. Nach dem Drucken des Datums enthält die DAG eine Aufgabe, die Ausführung für eine bestimmte Dauer in den Standbymodus zu versetzen oder anzuhalten.

- `other-sample-dag`— Diese DAG wird alle 10 Minuten ausgeführt und druckt das Datum. Nach dem Drucken des Datums enthält die DAG eine Aufgabe, die Ausführung für eine bestimmte Dauer in den Ruhezustand versetzt oder unterbricht.
- `data-extract`— Diese DAG wird stündlich ausgeführt und fragt die Amazon MWAA-Datenbank ab und sammelt Metriken. Nachdem die Metriken erfasst wurden, schreibt diese DAG sie zur weiteren Verarbeitung und Analyse in einen Amazon S3 S3-Bucket.

2. Um die Datenverarbeitung zu optimieren, werden Lambda-Funktionen ausgeführt, wenn sie durch Amazon S3 S3-Ereignisse ausgelöst werden, was das Laden von Metriken in Timestream erleichtert.
3. Timestream ist als Datenquelle in Amazon Managed Grafana integriert, wo alle benutzerdefinierten Metriken von Amazon MWAA gespeichert werden.
4. Benutzer können die Daten abfragen und benutzerdefinierte Dashboards erstellen, um wichtige Leistungsindikatoren zu visualisieren und Einblicke in die Orchestrierung von Workflows innerhalb von Amazon MWAA zu gewinnen.

Tools

AWS-Services

- AWS IAM Identity Centerhilft Ihnen dabei, den Single Sign-On (SSO) -Zugriff auf all Ihre Anwendungen und Cloud-Anwendungen zentral zu verwalten. AWS-Konten
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen. In diesem Muster AWS Lambda wird der Python-Code als Reaktion auf Amazon S3 S3-Ereignisse ausgeführt und die Rechenressourcen automatisch verwaltet.
- Amazon Managed Grafana ist ein vollständig verwalteter Datenvisualisierungsservice, mit dem Sie Ihre Metriken, Logs und Traces abfragen, korrelieren und visualisieren und Warnmeldungen dazu erhalten können. Dieses Muster verwendet Amazon Managed Grafana, um ein Dashboard für die Visualisierung von Kennzahlen und Benachrichtigungen zu erstellen.
- Amazon Managed Workflows for Apache Airflow (Amazon MWAA) ist ein verwalteter Orchestrierungsservice für Apache Airflow, mit dem Sie Daten-Pipelines in der Cloud in großem Umfang einrichten und betreiben können. Apache Airflow ist ein Open-Source-Tool, mit dem Sie Abläufe und Aufgaben, sogenannte Workflows, programmgesteuert erstellen, planen und

überwachen können. In diesem Muster werden ein Beispiel DAGs und ein Metrik-Extraktor-DAG in Amazon MWAA bereitgestellt.

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt. In diesem Muster wird Amazon S3 zum Speichern von DAGs Skripten und benutzerdefinierten Metriken im CSV-Format verwendet.
- Amazon Timestream for LiveAnalytics is ist eine schnelle, skalierbare, vollständig verwaltete, speziell entwickelte Zeitreihendatenbank, die es einfach macht, Billionen von Zeitreihendatenpunkten pro Tag zu speichern und zu analysieren. Timestream for lässt sich LiveAnalytics auch in häufig verwendete Dienste für Datenerfassung, Visualisierung und maschinelles Lernen integrieren. In diesem Muster wird es verwendet, um die generierten benutzerdefinierten Amazon MWAA-Metriken aufzunehmen.

Andere Tools

- HashiCorp Terraform ist ein Infrastructure-as-Code-Tool (IaC), mit dem Sie mithilfe von Code Cloud-Infrastruktur und -Ressourcen bereitstellen und verwalten können. Dieses Muster verwendet ein Terraform-Modul, um die Bereitstellung der Infrastruktur in zu automatisieren. AWS

Code-Repository

Der Code für dieses Muster ist GitHub im Repository visualize-amazon-mwaa-custom-metrics-grafana verfügbar. Der Ordner enthält Folgendes`stacks/Infra`:

- Terraform-Konfigurationsdateien für alle Ressourcen AWS
- Grafana-Dashboard-.json-Datei im Ordner `grafana`
- Amazon Managed Workflows für Apache Airflow DAGs im Ordner `mwaa/dags`
- Lambda-Code zum Analysieren der CSV-Datei und zum Speichern von Metriken in der Timestream-Datenbank im Ordner `src`
- .json-Dateien für IAM-Richtlinien im Ordner `templates`

Bewährte Methoden

Terraform muss den Status Ihrer verwalteten Infrastruktur und Konfiguration speichern, damit es Ihrer Konfiguration reale Ressourcen zuordnen kann. Standardmäßig speichert Terraform den Status lokal

in einer Datei mit dem Namen. `terraform.tfstate` Es ist wichtig, die Sicherheit und Integrität Ihrer Terraform-Statusdatei zu gewährleisten, da sie den aktuellen Status Ihrer Infrastruktur beibehält. Weitere Informationen finden Sie unter Remote State in der Terraform-Dokumentation.

Epen

Stellen Sie die Infrastruktur mit Terraform bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Infrastruktur bereit.	Gehen Sie wie folgt vor, um die Lösungsinfrastruktur bereitzustellen: 1. Öffnen Sie ein Terminal oder eine Befehlszeile auf Ihrem lokalen Computer oder mithilfe von AWS CloudShell. 2. Navigieren Sie zu dem Verzeichnis, in das Sie das Repository klonen möchten. 3. Führen Sie den folgenden Befehl aus, um das Repository zu klonen: `git clone https://github.com/aws-samples/visualize-amazon-mwaa-custom-metrics-grafana` 4. Führen Sie nach Abschluss des Klonvorgangs den folgenden Befehl aus, um in das geklonte Repository-Verzeichnis zu navigieren:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`cd visualize-amazon-mwaa-custom-metrics-grafana/stacks/infra`
	5. Führen Sie den folgenden Befehl aus, um die erforderlichen Anbieter herunterzuladen und zu initialisieren:
	`terraform init`
	6. Führen Sie den folgenden Befehl aus, um einen umfassenden Überblick über alle Ressourcen zu erhalten, die Terraform erstellen wird:
	`terraform plan`
	Terraform stellt die folgenden Ressourcen bereit:
	• Amazon Virtual Private Cloud (Amazon VPC) und zugehörige Netzwerkkomponenten
	• Amazon-S3-Ressourcen
	• AWS Lambda Funktionen
	• Amazon Managed Grafana-Ressourcen (Arbeitsbereich, Dashboards, Datenquelle)	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	• Unterstützung von IAM-Ressourcen (Rollen und Richtlinien)
	7. Führen Sie den folgenden Befehl aus, um die AWS Ressourcen aus der Planausgabe zu erstellen:
	`terraform apply -auto-approve`
	Die Bereitstellung der Infrastruktur ist in etwa 20 Minuten abgeschlossen.
	8. Führen Sie den folgenden Befehl aus, um die angegebenen AWS Ressourcen gemäß der in Ihren Terraform-Dateien definierten Konfiguration zu erstellen:
	`terraform apply`	

Validieren Sie die bereitgestellten Infrastrukturressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Amazon MWAA-Umgebung.	Gehen Sie wie folgt vor, um die Amazon MWAA-Umgebung zu validieren: 1. Melden Sie sich bei der an AWS Management	AWS DevOps, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Console, navigieren Sie zur Amazon MWAA-Dashboard-Konsole und wählen Sie Airflow UI öffnen aus. 2. Im Status Aktiv sollten Sie die folgenden drei DAGs sehen: • Datenextraktion • run-example-dag • other-sample-dag 3. Wenn eine DAG nicht aktiv ist, können Sie sie aktivieren, indem Sie den Kippschalter neben dem DAG-Namen aktivieren.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die DAG-Zeitpläne.	Um die einzelnen DAG-Zeitpläne einzusehen, wechseln Sie in der Airflow-Benutzeroberfläche zur Registerkarte Zeitplan. Jede der folgenden Optionen DAGs hat einen vorkonfigurierten Zeitplan, der in der Amazon MWAA-Umgebung ausgeführt wird und benutzerdefinierte Metriken generiert: • run-example-dag- Läuft alle 7 Minuten • other-sample-dag- Läuft alle 10 Minuten • Datenextrakt - Läuft jede Stunde Sie können auch die erfolgreichen Ausführungen der einzelnen DAG in der Spalte Runs sehen.	Dateningenieur, AWS DevOps

Konfigurieren Sie die Amazon Managed Grafana-Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Zugriff auf den Amazon Managed Grafana-Arbeitsbereich.	Die Terraform-Skripte haben den erforderlichen Amazon Managed Grafana-Arbeitsbereich, die Dashboards und die Metrikseite erstellt. Gehen Sie	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wie folgt vor, um den Zugriff so zu konfigurieren, dass Sie sie anzeigen können: 1. Öffnen Sie die Amazon Managed Grafana-Konsole. 2. Wählen Sie unter Workspaces den Workspace `grafana-ws-dev` aus und navigieren Sie im unteren Bereich zur Registerkarte Authentifizierung. 3. Wählen Sie die Schaltfläche „Neuen Benutzer oder Gruppe zuweisen“. 4. Fügen Sie entweder Ihre Gruppe auf der Registerkarte Gruppen oder einen Benutzer auf der Registerkarte Benutzer hinzu und wählen Sie dann die Schaltfläche Benutzer und Gruppen zuweisen. 5. Nachdem der Benutzer (oder die Gruppe) hinzugefügt wurde, ernennen Sie diesen Benutzer (oder diese Gruppe) zum Administrator. Wählen Sie den Benutzer unter Zugewiesene Benutzer oder Gruppe auf der Registerkarte Zugewiesene Benutzerg	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ruppe aus und wählen Sie im Dropdownmenü die Option Zum Administrator ernennen aus. Weitere Informationen finden Sie unter Verwendung AWS IAM Identity Center mit Ihrem Amazon Managed Grafana-Workspace in der Amazon Managed Grafana-Dokumentation. 6. Navigieren Sie zu Workspaces und wählen Sie dann die Grafana-W orkspace-URL aus. Um sich als Administrator bei Amazon Managed Grafana anzumelden, wählen Sie Anmelden mit AWS IAM Identity Center.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie das Amazon Timestream Timestream-Plugin.	Benutzerdefinierte Amazon MWAA-Metriken werden in die Timestream-Datenba nk geladen. Sie verwenden das Timestream-Plugin, um die Metriken mit Amazon Managed Grafana-D ashboards zu visualisieren. Gehen Sie wie folgt vor, um das Timestream-Plugin zu installieren: 1. Erweitern Sie in der Amazon Managed Grafana-Konsole das Menü im linken Navigationsbereich und gehen Sie zu Administr ation, Plugins. 2. Suchen Sie nach der neuesten Version des Amazon Timestream Timestream-Plug-ins und installieren Sie sie. 3. Gehen Sie nach der Installation des Plug-ins zu Administration, Datenquel len, um die Timestream-Datenquelle zu sehen. Wenn die Datenquelle nicht aufgeführt ist, aktualisieren Sie die Seite.	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter Erweitern Sie Ihren Workspace mit Plugins in der Amazon Managed Grafana-Dokumentation.	

Visualisieren Sie die benutzerdefinierten Metriken im Amazon Managed Grafana-Dashboard

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich das Amazon Managed Grafana-Dashboard an.	Gehen Sie wie folgt vor, um die Metriken anzuzeigen, die in den Amazon Managed Grafana-Workspace aufgenommen wurden: 1. Wählen Sie in der Amazon Managed Grafana-Konsole im linken Navigationsbereich Dashboards aus. 2. Um die Metriken anzuzeigen, wählen Sie MWAA events dashboards und dann mwaa_metrics aus. Auf der Seite mit den Dashboard-Kennzahlen werden die folgenden Informationen angezeigt: • Gesamtzahl der DAG-Läufe in der letzten Stunde • Gesamtzahl der erfolgreichen, fehlgeschlagenen und	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ausgeführten DAG-Läufe in der letzten Stunde • Durchschnittliche Dauer für alle erfolgreichen und fehlgeschlagenen DAG-Läufe	
Passen Sie das Amazon Managed Grafana-Dashboard an.	Gehen Sie wie folgt vor, um die Dashboards für weitere future Verbesserungen anzupassen: 1. Wählen Sie auf der Amazon Managed `mwaa_metrics` Grafana-Dashboard-Seite das Symbol Dashboard-Einstellungen aus. 2. Um die Datenstruktur anzuzeigen, die das Dashboard definiert, wählen Sie JSON-Modell. Sie können das Dashboard anpassen, indem Sie dieses JSON-Modell direkt in der Konsole bearbeiten. Alternativ ist der Quellcode für dieses Dashboard in der `dashboard.json` Datei im `stacks/infra/grafana` Ordner im GitHub Repository verfügbar.	AWS DevOps

AWS Ressourcen bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Unterbrechen Sie die Ausführung der Amazon MWAA-DAG.	Gehen Sie wie folgt vor, um die DAG-Ausführung anzuhalten: 1. Navigieren Sie in der Amazon MWAA-Konsole zu Airflow-Umgebungen und wählen Sie Open Airflow UI. 2. Um die DAG anzuhalten, verwenden Sie den Kippschalter neben jeder DAG. 3. Aktualisieren Sie die Airflow-UI-Seite, auf der DAGs im Abschnitt „Angehalten“ drei angezeigt werden sollten.	AWS DevOps, Dateningenieur
Löschen Sie die Objekte in den Amazon S3 S3-Buckets.	Um die Amazon S3 S3-Buckets mwaa-events-bucket-* und mwaa-metrics-bucket-* zu löschen, folgen Sie den Anweisungen zur Verwendung der Amazon S3 S3-Konsole unter Löschen eines Buckets in der Amazon S3 S3-Dokumentation.	AWS DevOps
Zerstöre die von Terraform erstellten Ressourcen.	Gehen Sie wie folgt vor, um die von Terraform erstellten Ressourcen und die zugehörige lokale Terraform-Statusdatei zu löschen:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. (Optional) Bevor Sie die Ressourcen löschen, können Sie sich eine Vorschau der Änderungen ansehen, die Terraform vornehmen wird. Führen Sie den folgenden Befehl aus, um einen Plan zu generieren: `terraform plan -destroy` Die Befehlsausgabe zeigt, dass der `destroy` Befehl alle AWS Ressourcen löscht, die zuvor erstellt wurden. 2. `terraform destroy -auto-approve` Dieser Befehl benötigt ungefähr 20 Minuten, um die Infrastruktur zu zerstören. **Note** Führen Sie den folgenden Befehl aus, um alle von Terraform verwalteten Ressourcen zu löschen. : Das `-auto-approve`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Tag wartet nicht auf die Bestätigung des Benutzers, um mit der Zerstörung der Ressourcen zu beginnen.
	3. Führen Sie die folgenden Befehle aus, um die lokale Terraform-Statusdatei zu löschen:
	`rm .terraform.lock.hcl`
	`rm -rf .terraform`
	`rm terraform.tfstate*`	

Fehlerbehebung

Problem	Lösung
`null_resource.plugin_mgmt (local-exec): aws: error: argument operation: Invalid choice, valid choices are:`	Führen Sie ein Upgrade AWS CLI auf die neueste Version durch.
Fehler beim Laden der Datenquellen - `Fetch error: 404 Not Found Instantiating…`	Der Fehler tritt sporadisch auf. Warten Sie einige Minuten, und aktualisieren Sie dann Ihre Datenquellen, um die aufgelistete Timestream-Datenquelle anzuzeigen.

Zugehörige Ressourcen

AWS Dokumentation

- Amazon Managed Grafana für Dashboarding und Visualisierung
- Amazon Managed Grafana für die Verwendung von Okta konfigurieren
- AWS IAM Identity Center Mit Ihrem Amazon Managed Grafana-Workspace verwenden
- Arbeiten mit DAGs auf Amazon MWAA

AWS Videos

- Konfigurieren Sie IAM Identity Center mit Amazon Managed Grafana für die Authentifizierung, wie im folgenden Video gezeigt.

https://www.youtube-nocookie.com/embed/XX2Xcz-Ps9U? Steuerungen=0

- Wenn IAM Identity Center nicht verfügbar ist, können Sie die Amazon Managed Grafana-Authentifizierung auch mithilfe eines externen Identitätsanbieters (IdP) wie Okta integrieren, wie im folgenden Video gezeigt.

https://www.youtube-nocookie.com/embed/JHxl2xpZ4 Og? Steuerungen=0

Zusätzliche Informationen

Sie können eine umfassende Überwachungs- und Warnlösung für Ihre Amazon MWAA-Umgebung erstellen, die ein proaktives Management und eine schnelle Reaktion auf potenzielle Probleme oder Anomalien ermöglicht. Amazon Managed Grafana umfasst die folgenden Funktionen:

Warnung — Sie können Benachrichtigungen in Amazon Managed Grafana auf der Grundlage vordefinierter Schwellenwerte oder Bedingungen konfigurieren. Richten Sie E-Mail-Benachrichtigungen ein, um relevante Stakeholder zu benachrichtigen, wenn bestimmte Kennzahlen bestimmte Schwellenwerte über- oder unterschreiten. Weitere Informationen finden Sie unter Grafana-Benachrichtigungen in der Amazon Managed Grafana-Dokumentation.

Integration — Sie können Amazon Managed Grafana in verschiedene Tools von Drittanbietern wie OpsGenie, oder Slack integrieren PagerDuty, um erweiterte Benachrichtigungsfunktionen zu erhalten. Sie können beispielsweise Webhooks einrichten oder integrieren, APIs um Vorfälle und Benachrichtigungen auf diesen Plattformen auszulösen, die auf in Amazon Managed Grafana

generierten Warnungen basieren. Darüber hinaus bietet dieses Muster ein GitHub Repository zum Erstellen AWS von Ressourcen. Sie können diesen Code weiter in Ihre Workflows zur Infrastrukturbereitstellung integrieren.

Optimieren Sie die Entwicklung und Bereitstellung von Amazon Lex Lex-Bot mithilfe eines automatisierten Workflows

Erstellt von Balaji Panneerselvam (AWS), Anand Jumnani (AWS), Attila Dancso (AWS), James O'Hara (AWS) und Pavan Dusanapudi (AWS)

Übersicht

Die Entwicklung und Bereitstellung von Amazon Lex Conversational Bots kann eine Herausforderung sein, wenn Sie versuchen, mehrere Funktionen, Entwickler und Umgebungen zu verwalten. Ein automatisierter Arbeitsablauf, der die Prinzipien von Infrastructure as Code (IaC) verwendet, kann dazu beitragen, den Prozess zu rationalisieren. Dieses Muster kann dazu beitragen, die Produktivität der Amazon Lex-Entwickler zu verbessern und ein effizientes Bot-Lebenszyklusmanagement auf folgende Weise zu ermöglichen:

- Ermöglichen Sie die gleichzeitige Entwicklung mehrerer Funktionen — Mit einem automatisierten Workflow können Entwickler in separaten Zweigen parallel an verschiedenen Funktionen arbeiten. Änderungen können dann zusammengeführt und bereitgestellt werden, ohne dass andere Arbeiten blockiert werden.
- Verwenden Sie die Benutzeroberfläche der Amazon Lex-Konsole — Entwickler können die benutzerfreundliche Amazon Lex-Konsole verwenden, um Bots zu erstellen und zu testen. Die Bots werden dann im Infrastrukturcode für die Bereitstellung beschrieben.
- Werbung für Bots in allen Umgebungen — Der Workflow automatisiert das Bewerben von Bot-Versionen aus niedrigeren Umgebungen wie Entwicklung und Test bis hin zur Produktion. Dieser Ansatz reduziert das Risiko und den Aufwand manueller Werbeaktionen.
- Behalten Sie die Versionskontrolle bei — Die Verwaltung von Bot-Definitionen in Git statt ausschließlich über den Amazon Lex Lex-Service bietet Ihnen Versionskontrolle und einen Audit-Trail. Änderungen werden bis zu den einzelnen Entwicklern zurückverfolgt, anders als wenn nur die AWS Management Console oder APIs zur Änderung der darin gespeicherten Bots verwendet werden AWS.

Durch die Automatisierung des Amazon Lex Lex-Bot-Release-Prozesses können Teams Funktionen schneller und mit geringerem Risiko und geringerem Aufwand bereitstellen. Bots unterliegen weiterhin der Versionskontrolle und sind nicht isoliert in der Amazon Lex Lex-Konsole.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Der Workflow umfasst mehrere AWS-Konten für verschiedene Umgebungen (Entwicklung, Produktion und DevOps), was Kontoverwaltung und kontenübergreifende Zugriffskonfigurationen erfordert.
- Python 3.9 ist in Ihrer Bereitstellungsumgebung oder Pipeline verfügbar.
- Git wurde auf einer lokalen Workstation für die Quellcodeverwaltung installiert und konfiguriert.
- AWS Command Line Interface (AWS CLI) installiert und konfiguriert, um sich über die Befehlszeile oder Python zu authentifizieren.

Einschränkungen

- Zugriff auf das Repository — Der Workflow geht davon aus, dass die CI/CD-Pipeline (Continuous Integration and Continuous Delivery) über die erforderlichen Berechtigungen verfügt, um Änderungen an das Quellcode-Repository zu übertragen.
- Erste Bot-Version — Das Tooling erfordert, dass eine erste Version des Bots mithilfe von Vorlagen bereitgestellt wird. AWS CloudFormation Sie müssen die erste Iteration des Bots erstellen und sie in das Repository übernehmen, bevor der automatisierte Workflow die Kontrolle übernehmen kann.
- Zusammenführungskonflikte — Obwohl der Workflow darauf abzielt, die gleichzeitige Entwicklung zu ermöglichen, besteht immer noch die Möglichkeit von Zusammenführungskonflikten, wenn Änderungen aus verschiedenen Branchen integriert werden. Die Lösung von Konflikten in Bot-Konfigurationen erfordert möglicherweise manuelles Eingreifen.

Produktversionen

- Python 3.9 oder höher
- AWS CDK v2 2.124.0 oder höher
- AWS SDK für Python (Boto3)1.28 oder höher

Architektur

Das folgende Diagramm zeigt die allgemeine Architektur und die wichtigsten Komponenten der Lösung.

Zu den wichtigsten Komponenten gehören:

- Lex-Bot-Repo — Ein Git-Repository, das die IaC-Definitionen für die Amazon Lex-Bots speichert.
- DevOps— Ein, das sich der Unterbringung der CI/CD-Pipelines und der zugehörigen Ressourcen für den Entwicklungs- und Bereitstellungsprozess AWS-Konto widmet.
- Pipelines — Die AWS CodePipeline Instanzen, die verschiedene Phasen des Bot-Entwicklungs- und Bereitstellungszyklus automatisieren, z. B. das Erstellen eines neuen Bots, das Exportieren einer Bot-Definition, das Importieren einer Bot-Definition und das Löschen eines Bots.
- Ticket-Bots und Haupt-Bot — Die Amazon Lex Lex-Bot-Ressourcen, wobei es sich bei den Ticket-Bots um funktionsspezifische Bots handelt, die von einzelnen Teams oder Entwicklern entwickelt wurden, und der Haupt-Bot der Basis-Bot ist, der alle Funktionen integriert.

Das Architekturdiagramm veranschaulicht den folgenden Arbeitsablauf:

1. Baseline-Haupt-Bot — Der Ausgangspunkt des Workflows besteht darin, den Haupt-Bot in der Entwicklungsumgebung (Dev) als Basis zu betrachten. Der Haupt-Bot dient als Grundlage für future Entwicklungen und Funktionserweiterungen.
2. Ticket-Bot erstellen — Wenn eine neue Funktion oder Änderung erforderlich ist, wird ein Ticket-Bot erstellt. Der Ticket-Bot ist im Grunde eine Kopie oder ein Zweig des Haupt-Bots, an dem Entwickler arbeiten können, ohne die Hauptversion zu beeinträchtigen.
3. Ticket-Bot exportieren — Nachdem die Arbeit am Ticket-Bot abgeschlossen ist, wird er aus dem Amazon Lex Lex-Service exportiert. Dann wird der Zweig, der den Ticket-Bot enthält, vom Hauptzweig aus umbenannt. Dieser Schritt stellt sicher, dass alle Änderungen, die während der Entwicklung des Ticket-Bot am Haupt-Bot vorgenommen wurden, übernommen werden, wodurch potenzielle Konflikte reduziert werden.
4. Bot für rebased Ticket importieren und validieren — Der Bot für rebased Tickets wird zurück in die Entwicklungsumgebung importiert und validiert, um sicherzustellen, dass er mit den neuesten Änderungen aus dem Hauptzweig korrekt funktioniert. Wenn die Validierung erfolgreich ist, wird eine Pull-Anfrage (PR) erstellt, um die Ticket-Bot-Änderungen mit dem Hauptzweig zusammenzuführen.
5. Ticket-Bot löschen — Nachdem die Änderungen erfolgreich mit dem Hauptzweig zusammengeführt wurden, wird der Ticket-Bot nicht mehr benötigt. Der Ticket-Bot kann gelöscht werden, um die Umgebung sauber und überschaubar zu halten.
6. Den Haupt-Bot in der Entwicklungsumgebung bereitstellen und testen — Der aktualisierte Haupt-Bot, der jetzt die neuen Funktionen oder Änderungen enthält, wird in der Entwicklungsumgebung

bereitgestellt. Hier wird er gründlichen Tests unterzogen, um sicherzustellen, dass alle Funktionen wie erwartet funktionieren.

7. Stellen Sie den Haupt-Bot in der Produktionsumgebung bereit — Nachdem die Tests in der Entwicklungsumgebung abgeschlossen und erfolgreich abgeschlossen sind, wird der Haupt-Bot in der Produktionsumgebung bereitgestellt. Dieser Schritt ist die letzte Phase des Workflows, in der die neuen Funktionen den Endbenutzern zur Verfügung stehen.

Automatisierung und Skalierung

Der automatisierte Workflow ermöglicht es Entwicklern, parallel an verschiedenen Funktionen zu arbeiten, jeweils in separaten Zweigen. Dies erleichtert die gleichzeitige Entwicklung, sodass Teams effektiv zusammenarbeiten und Funktionen schneller bereitstellen können. Da die Filialen voneinander isoliert sind, können Änderungen zusammengeführt und bereitgestellt werden, ohne dass andere laufende Arbeiten blockiert oder beeinträchtigt werden.

Der Workflow automatisiert die Bereitstellung und Vermarktung von Bot-Versionen in verschiedenen Umgebungen, z. B. in der Entwicklung, beim Testen und bei der Produktion.

Das Speichern von Bot-Definitionen in einem Versionskontrollsystem wie Git bietet einen umfassenden Prüfpfad und ermöglicht eine effiziente Zusammenarbeit. Änderungen werden bis zu den einzelnen Entwicklern nachverfolgt, wodurch Transparenz und Rechenschaftspflicht während des gesamten Entwicklungszyklus gewährleistet sind. Dieser Ansatz erleichtert auch Code-Reviews, sodass Teams Probleme erkennen und beheben können, bevor sie in der Produktion eingesetzt werden.

Durch die Verwendung AWS CodePipeline und andere Funktionen kann der automatisierte Workflow skaliert werden AWS-Services, um der steigenden Arbeitsbelastung und Teamgröße gerecht zu werden.

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK)ist ein Open-Source-Framework für die Softwareentwicklung zur Definition von AWS Cloud Infrastruktur im Code unter Verwendung vertrauter Programmiersprachen und deren Bereitstellung. AWS CloudFormation Die Beispielimplementierung in diesem Muster verwendet Python.
- AWS CDK Befehlszeilenschnittstelle (AWS CDK CLI) — Das AWS CDK Toolkit ist das wichtigste Tool für die Interaktion mit Ihrer AWS CDK App. Es führt Ihre App aus, fragt das von

Ihnen definierte Anwendungsmodell ab und erstellt und stellt die vom CDK generierten AWS CloudFormation Vorlagen bereit.

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über und zu verwalten. AWS-Konten AWS-Regionen Dieses Muster wird CloudFormation für die Bereitstellung der Amazon Lex Lex-Bot-Konfigurationen und verwandter Ressourcen unter Verwendung von Infrastruktur als Code verwendet.
- AWS CodeBuildist ein vollständig verwalteter Build-Service, der Ihnen hilft, Quellcode zu kompilieren, Komponententests durchzuführen und Artefakte zu erstellen, die sofort einsatzbereit sind. Dieses Muster wird CodeBuild zum Erstellen und Verpacken der Bereitstellungsartefakte verwendet.
- AWS CodePipelinehilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind. Dieses Muster dient CodePipeline zur Orchestrierung der Continuous Delivery-Pipeline.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie AWS-Services über Befehle in Ihrer Befehlszeilen-Shell interagieren können.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem es kontrolliert, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Lex V2 dient AWS-Service zum Erstellen von Konversationsschnittstellen (Bots) für Anwendungen, die Sprache und Text verwenden.
- AWS SDK für Python (Boto3)ist ein Softwareentwicklungskit, mit dem Sie Ihre Python-Anwendung, -Bibliothek oder Ihr Skript integrieren können AWS-Services.

Andere Tools

- Git ist ein verteiltes Open-Source-Versionskontrollsystem.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub management-framework-sample-for-amazon-lex verfügbar. Das Code-Repository enthält die folgenden Ordner und Dateien:

- `prerequisite`Ordner — Enthält CloudFormation Stack-Definitionen (unter Verwendung von AWS CDK) für die Einrichtung der erforderlichen Ressourcen und Umgebungen.
- `prerequisite/lexmgmtworkflow`folder — Hauptverzeichnis für das Lex Management Workflow-Projekt, einschließlich Stack-Definitionen und Python-Code.
- `prerequisite/tests`— Enthält Komponententests.
- `src`folder — Quellcode-Verzeichnis, einschließlich des Amazon Lex-Bot-Management-Wrappers und der Dienstprogramme.
- `src/dialogue_lambda`— Quellcodeverzeichnis der Dialog-Hook-Lambda-Funktion, die Benutzereingaben während einer Konversation mit einem Amazon Lex Lex-Bot abfängt und verarbeitet.

Bewährte Methoden

- Trennung der Anliegen
  - Achten Sie auf eine klare Trennung der Zuständigkeiten zwischen DevOps Entwicklungs- und Produktionsumgebung.
  - Verwenden Sie separate AWS-Konten Optionen für jede Umgebung, um angemessene Isolations- und Sicherheitsgrenzen durchzusetzen.
  - Verwenden Sie kontenübergreifende Rollen und Prinzipien für den Zugriff mit den geringsten Rechten, um einen kontrollierten Zugriff zwischen Umgebungen sicherzustellen.
- Infrastruktur als Code
  - Überprüfen und aktualisieren Sie den Infrastrukturcode regelmäßig, um ihn an bewährte Verfahren und sich ändernde Anforderungen anzupassen.
  - Etablieren Sie eine klare Strategie zur Verzweigung und Zusammenführung des Quellcode-Repositorys
- Testen und Validieren
  - Implementieren Sie automatisierte Tests in verschiedenen Phasen der Pipeline, catch Probleme schon früh im Entwicklungszyklus zu erkennen.
  - Verwenden Sie die Amazon Lex Lex-Konsole oder automatisierte Test-Frameworks, um Bot-Konfigurationen und -Funktionen zu validieren, bevor Sie auf höhere Umgebungen umsteigen.

    - Erwägen Sie die Implementierung manueller Genehmigungsschranken für Bereitstellungen in Produktionsumgebungen oder kritischen Umgebungen.
- Überwachung und Protokollierung
    - Richten Sie Überwachungs- und Protokollierungsmechanismen für die Pipelines, Bereitstellungen und Bot-Interaktionen ein.
    - Überwachen Sie Pipeline-Ereignisse, Bereitstellungsstatus und Bot-Leistungskennzahlen, um Probleme umgehend zu identifizieren und zu beheben.
    - Verwenden Sie AWS-Services wie Amazon CloudWatch und AWS X-Ray für die zentrale Protokollierung und Überwachung. AWS CloudTrail
    - Überprüfen und analysieren Sie regelmäßig die Leistung, Effizienz und Effektivität des automatisierten Workflows.
- Sicherheit und Einhaltung von Vorschriften
    - Implementieren Sie sichere Programmierpraktiken und befolgen Sie bewährte AWS Sicherheitsmethoden für die Entwicklung und Bereitstellung von Amazon Lex Lex-Bot.
    - Überprüfen und aktualisieren Sie regelmäßig die IAM-Rollen, -Richtlinien und -Berechtigungen, damit sie dem Prinzip der geringsten Rechte entsprechen.
    - Erwägen Sie, Sicherheitsscans und Konformitätsprüfungen in die Pipelines zu integrieren.

Epen

IaC für Amazon Lex-Bot-Management einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die lokale CDK-Umgebung ein.	1. Führen Sie den folgenden Befehl aus, um das Repo dieses Musters zu klonen und zum `prerequisite` Verzeichnis zu navigieren: `git clone https://github.com/aws-samples/management-framework-sample-for-amazon-lex.git`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`cd management-framework-sample-for-amazon-lex`
	2. Um die virtuelle Python-Umgebung zu installieren und zu aktivieren, führen Sie den folgenden Befehl aus, der die Abhängigkeiten des CDK lokal im Projektordner statt global installiert:
	`pip install virtualenv`
	`python<version> -m venv .venv`
	`source .venv/bin/activate`
	`python -m pip install -r requirements.txt`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine kontoüber greifende Rolle in der `devops` Umgebung.	Das `devops` Konto ist für das Hosten und Verwalten der CI/CD pipelines. To enable the CI/CD Pipelines für die Interaktion mit den `prod` Umgebungen `dev` und verantwortlich. Führen Sie die folgenden Befehle aus, um eine kontoübergreifende Rolle in dem Konto zu erstellen. `devops`
	
	`cdk bootstrap --profile =devops`
	
	`cdk deploy LexMgmtDe vopsRoleStack -c dev-account-id=222 2222222222 -c prod- account-id=33333333333 3 --profile=devops`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine kontoüber greifende Rolle in der `dev` Umgebung.	Erstellen Sie im `dev` Konto eine IAM-Rolle mit den erforderlichen Berechtigungen, damit das `devops` Konto diese Rolle übernehmen kann. Die CI/CD-Pipeline verwendet diese Rolle, um Aktionen im `dev` Konto auszuführen, z. B. die Bereitstellung und Verwaltung von Amazon Lex Lex-Bot-Ressourcen.
	
	Führen Sie die folgenden Befehle aus, um die IAM-Rolle zu erstellen:
	
	`cdk bootstrap --profile =dev`
	
	`cdk deploy LexMgmtCr ossaccountRoleStac k -c devops-account- id=1111111111111 -- profile=dev`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine kontoüber greifende Rolle in der `prod` Umgebung.	Erstellen Sie im `prod` Konto eine IAM-Rolle mit den erforderlichen Berechtigungen, damit das `devops` Konto diese Rolle übernehmen kann. Die CI/CD-Pipeline verwendet diese Rolle, um Aktionen im `prod` Konto auszuführen, z. B. die Bereitstellung und Verwaltung von Amazon Lex Lex-Bot-Ressourcen.
	`cdk bootstrap --profile =prod`
	
	`cdk deploy LexMgmtCr ossaccountRoleStac k -c devops-account- id=1111111111111 -- profile=prod`
		AWS DevOps

Erstellen Sie Pipelines in der `devops` Umgebung.	Um den Entwicklungsworkfl ow für Amazon Lex-Bots zu verwalten, führen Sie den folgenden Befehl aus, um Pipelines in der `devops` Umgebung einzurichten. `cdk deploy LexMgmtWo rkflowStack -c devops- account-id=111111111 1111 -c dev-account- id=2222222222222 -c prod-account-id=33 3333333333 --profile =devops`	AWS DevOps

Legen Sie die Grundlage für den Haupt-Bot fest

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definiere die erste Version des Haupt-Bots.	Um die erste Version des Haupt-Bots zu definieren, lösen Sie die `BaselineBotPipeline` Pipeline aus. Die Pipeline stellt die grundlegende Bot-Definition bereit, die in der CloudFormation Vorlage definiert ist, exportiert die Haupt-Bot-Definition als.json-Dateien und speichert den Haupt-Bot-Code in einem Versionskontrollsystem.	AWS DevOps

Implementieren Sie den Workflow zur Feature-Entwicklung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Ticket-Bot, um eine Funktion zu entwickeln und zu testen.	`TicketBot` ist eine neue Bot-Instanz, die aus der vorhandenen Haupt-Bot-Definition im Feature-Branch importiert wurde. Dieser Ansatz stellt sicher, dass der neue Bot über alle aktuellen Funktionen und Konfigurationen des Haupt-Bot verfügt. Um die erste Version des Ticketbots zu definieren, lösen Sie die `CreateTic`	Lex Bot Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`ketBotPipeline` Pipeline aus. Die Pipeline erstellt einen neuen Funktionszweig im Versionskontrollsystem und erstellt eine neue Ticket-Bot-Instanz, die auf dem Haupt-Bot basiert.	
Entwickeln und testen Sie die Ticket-Bot-Funktion.	Um die Funktion zu entwickeln und zu testen, melden Sie sich bei der Amazon Lex Lex-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/lex/. Weitere Informationen finden Sie in der Amazon Lex Lex-Dokumentation unter Einen Bot mithilfe der Konsole testen. Mit der `TicketBot` Instance können Sie jetzt die Funktionalität des Bots hinzufügen, ändern oder erweitern, um die neue Funktion zu implementieren. Sie können beispielsweise Absichten, Äußerungen, Slots und Dialogabläufe erstellen oder ändern. Weitere Informationen finden Sie unter Hinzufügen von Absichten in der Amazon Lex Lex-Dokumentation.	Lex Bot Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Exportieren Sie die Ticket-Bot-Definition.	Die exportierte Bot-Definition ist im Wesentlichen eine Darstellung der Konfiguration und Funktionalität des Bots in einem JSON-Format. Um die Ticket-Bot-Definition zu exportieren, lösen Sie die `ExportTicketBotPipeline` Pipeline aus. Die Pipeline exportiert die Ticket-Bot-Definition als.json-Dateien und speichert den Ticket-Bot-Code in einem Feature-Branch im Versionskontrollsystem.	Lex Bot Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Der Feature-Branch wird vom letzten Hauptzweig aus neu erstellt.	Während der Entwicklung einer neuen Funktion hat der Hauptzweig möglicher weise weitere Änderungen von anderen Entwicklern oder Teams erhalten. Um diese Änderungen in den Feature-Branch zu integrieren, führen Sie eine `rebase` Git-Operation aus. Bei dieser Operation werden im Wesentlichen die Commits aus dem Feature-Branch zusätzlich zu den letzten Commits aus dem Haupt-Branch wiederholt, sodass sichergestellt wird, dass der Feature-Branch alle aktuellen Änderungen enthält	Lex Bot Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Importieren und validieren Sie den neu erstellten Ticket-Bot.	Nachdem Sie den Feature-Branch neu erstellt haben, müssen Sie ihn in die Ticket-Bot-Instanz importieren. Durch diesen Import wird der bestehende Ticket-Bot mit den neuesten Änderungen aus dem neu basierten Branch aktualisiert. Um den umbasierten Ticket-Bot zu importieren, lösen Sie die `ImportTicketBotPipeline` Pipeline aus. Die Pipeline importiert die .json-Dateien mit der Ticket-Bot-Definition im Feature-Branch des Versionskontrollsystems in die `TicketBot` Instanz.	Lex Bot Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die neu erstellte Bot-Definition.	Nachdem Sie die Definitio n des neu erstellten Bots importiert haben, ist es wichtig, ihre Funktionalität zu überprüfen. Sie möchten sicherstellen, dass die neue Funktion wie erwartet funktioniert und nicht mit der vorhandenen Funktionalität kollidiert. Diese Validierung umfasst in der Regel das Testen des Bots anhand verschied ener Eingabeszenarien, das Überprüfen der Antworten und das Überprüfen, ob sich der Bot wie beabsichtigt verhält. Sie können die Validierung auf eine der folgenden Arten durchführen: • Testen Sie den Bot manuell mithilfe der Amazon Lex Lex-Konsole. • Verwenden Sie einen automatisierten Ansatz, indem Sie Test-Frameworks und Tools verwenden , mit denen Benutzeri nteraktionen simuliert und die erwarteten Antworten bestätigt werden können.	Lex Bot Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den Feature-Zweig mit dem Hauptzweig zusammen.	Nachdem Sie die neue Funktion in der isolierten `TicketBot` Instanz entwickelt und getestet haben, gehen Sie wie folgt vor: 1. Übernehmen Sie die Änderungen in den entsprechenden Funktionszweig im Versionskontrollsystem. 2. Um den Feature-Branch mit dem Haupt-Branch zusammenzuführen, erstellen Sie einen Pull-Request (PR). Diese PR dient als Aufforderung, die Änderungen zu überprüfen und in die Haupt-Codebasis aufzunehmen.	Lex Bot Entwickler, Repository-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie den Feature-Branch und den Ticket-Bot.	Nachdem ein Feature-Branch erfolgreich mit dem Haupt-Branch zusammengeführt wurde, löschen Sie den Feature-Branch und den Ticket-Bot aus dem Quellcode-Repository. Um den Feature Branch und den Ticket-Bot zu löschen, lösen Sie die `DeleteTicketBotPipeline` Pipeline aus. Die Pipeline entfernt temporäre Bot-Ressourcen, die während des Entwicklungsprozesses erstellt wurden (z. B. der Ticket-Bot). Diese Aktion trägt dazu bei, ein sauberes Repo aufrechtzuerhalten und Verwirrung oder Konflikte mit future Feature-Branches zu vermeiden.	Lex Bot Entwickler

Pflegen Sie den Haupt-Bot

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Importieren Sie die neueste Haupt-Bot-Definition in die `dev` Umgebung.	Um die neueste Haupt-Bot-Definition im Hauptzweig in die `dev` Umgebung zu importieren, lösen Sie die `DeployBotDevPipeline` Pipeline aus.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Die Pipeline erstellt bei der Genehmigung auch ein Git-Tag.	
Importieren Sie die neueste Haupt-Bot-Definition in die `prod` Umgebung.	Um die neueste Bot-Definition im Hauptzweig in die `prod` Umgebung zu importieren, geben Sie die Tag-Referenz aus der vorherigen Aufgabe als Parameter an und lösen Sie die `DeployBotProdPipeline` Pipeline aus. Die Pipeline importiert die neueste Bot-Definition aus einem bestimmten Tag in die `prod` Umgebung.	AWS DevOps

Fehlerbehebung

Problem	Lösung
Wenn Sie Amazon Lex-Bots auf verschiedenen Konten bereitstellen AWS-Konten, müssen die Tooling-Services über die erforderlichen Berechtigungen für den Zugriff auf Ressourcen in diesen Konten verfügen.	Verwenden Sie IAM-Rollen und -Richtlinien, um kontoübergreifenden Zugriff zu gewähren. Erstellen Sie IAM-Rollen in den Zielkonten und fügen Sie den Rollen Richtlinien hinzu, die die erforderlichen Berechtigungen gewähren. Nehmen Sie dann diese Rollen von dem Konto aus an, in dem der Amazon Lex Lex-Bot bereitgestellt wird. Weitere Informationen finden Sie in der Amazon Lex Lex-Dokumentation unter Für den Import erforderliche IAM-Berechtigungen und

Problem	Lösung
	für den Export von Bots in Lex V2 erforderliche IAM-Berechtigungen.

Zugehörige Ressourcen

- Bots in Amazon Lex V2 importieren
- Starten Sie eine Pipeline in CodePipeline
- Arbeiten mit Amazon Lex V2-Bots

Automatisieren Sie die Stackset-Bereitstellung mithilfe von AWS CodePipeline und AWS CodeBuild

Erstellt von Thiyagarajan Mani (AWS), Mihir Borkar (AWS) und Raghu Gowda (AWS)

Übersicht

Hinweis: ist für Neukunden nicht mehr verfügbar. AWS CodeCommit Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

In Ihrer CI/CD) processes, you might want to deploy applications automatically into all your existing AWS accounts and into new accounts that you add to your organization in AWS Organizations. When you architect a CI/CD Lösung für Continuous Integration and Continuous Delivery (Continuous Integration and Continuous Delivery) für diese Anforderung CloudFormation ist die delegierte Stack-Set-Administratorfunktion von AWS nützlich, da sie eine Sicherheitsebene ermöglicht, indem der Zugriff auf das Verwaltungskonto eingeschränkt wird. AWS CodePipeline verwendet jedoch das vom Service verwaltete Berechtigungsmodell, um Anwendungen in mehreren Konten und Regionen bereitzustellen. Sie müssen das Verwaltungskonto von AWS Organizations für die Bereitstellung mit Stack-Sets verwenden, da AWS die Funktion zum delegierten Stack-Set-Administrator CodePipeline nicht unterstützt.

Dieses Muster beschreibt, wie Sie diese Einschränkung umgehen können. Das Muster verwendet AWS CodeBuild und ein benutzerdefiniertes Skript, um die Stackset-Bereitstellung mit AWS zu automatisieren CodePipeline. Es automatisiert diese Aktivitäten zur Anwendungsbereitstellung:

- Stellen Sie eine Anwendung als Stack-Sets in vorhandenen Organisationseinheiten bereit () OUs
- Erweitern Sie die Bereitstellung einer Anwendung auf weitere OUs Regionen
- Entfernen Sie eine bereitgestellte Anwendung aus allen OUs oder bestimmten Regionen

Voraussetzungen und Einschränkungen

Voraussetzungen

Bevor Sie die Schritte in diesem Muster ausführen:

- Erstellen Sie Organisationen in Ihrem AWS-Verwaltungskonto für Organisationen. Anweisungen finden Sie in der Dokumentation zu AWS Organizations.

- Ermöglichen Sie vertrauenswürdigen Zugriff zwischen AWS Organizations und verwenden CloudFormation Sie vom Service verwaltete Berechtigungen. Anweisungen finden Sie in der CloudFormation Dokumentation unter Aktivieren des vertrauenswürdigen Zugriffs mit AWS Organizations.

Einschränkungen

Der Code, der mit diesem Muster geliefert wird, hat die folgenden Einschränkungen:

- Sie können nur eine einzige CloudFormation Vorlage für eine Anwendung bereitstellen. Die Bereitstellung mehrerer Vorlagen wird derzeit nicht unterstützt.
- Die Anpassung der aktuellen Implementierung erfordert DevOps Fachwissen.
- Dieses Muster verwendet keine AWS Key Management System (AWS KMS) -Schlüssel. Sie können diese Funktionalität jedoch aktivieren, indem Sie die in diesem Muster enthaltene CloudFormation Vorlage neu konfigurieren.

Architektur

Diese Architektur für die CI/CD-Bereitstellungspipeline behandelt Folgendes:

- Schränkt den direkten Zugriff auf das Verwaltungskonto ein, indem die Verantwortung für die Stackset-Bereitstellung an ein spezielles CI/CD-Konto als Stackset-Administrator für Anwendungsbereitstellungen delegiert wird.
- Verwendet das vom Dienst verwaltete Berechtigungsmodell, um die Anwendung automatisch bereitzustellen, wenn ein neues Konto erstellt und einer Organisationseinheit zugeordnet wird.
- Stellt die Konsistenz der Anwendungsversionen für alle Konten auf Umgebungsebene sicher.
- Nutzt mehrere Genehmigungsphasen auf Repository- und Pipeline-Ebene, um zusätzliche Sicherheits- und Governance-Ebenen für die bereitgestellte Anwendung bereitzustellen.
- Überwindet die derzeitige Einschränkung, Stack-Sets und Stack-Instances CodePipeline mithilfe eines benutzerdefinierten Bereitstellungsskripts automatisch bereitzustellen oder CodeBuild zu entfernen. Eine Veranschaulichung der Ablaufsteuerung und der Hierarchie der API-Aufrufe, die durch das benutzerdefinierte Skript implementiert werden, finden Sie im Abschnitt Zusätzliche Informationen.
- Erstellt individuelle Stacksets für die Entwicklungs-, Test- und Produktionsumgebung. Darüber hinaus können Sie Stack-Sets erstellen, die in jeder Phase mehrere OUs Regionen kombinieren.

Sie können beispielsweise Sandbox und Entwicklung OUs innerhalb einer Entwicklungsphase kombinieren.

- Unterstützt die Anwendungsbereitstellung für oder den Ausschluss aus einer Teilmenge von Konten oder einer Liste von. OUs

Automatisierung und Skalierung

Sie können den mit diesem Muster bereitgestellten Code verwenden, um ein CodeCommit AWS-Repository und eine Code-Pipeline für Ihre Anwendung zu erstellen. Sie können diese dann als Stack-Sets für mehrere Konten auf OU-Ebene bereitstellen. Der Code automatisiert auch Komponenten wie Amazon Simple Notification Service (Amazon SNS) -Themen zur Benachrichtigung von Genehmigern, die erforderlichen AWS Identity and Access Management (IAM) -Rollen und die Service Control Policy (SCP), die für das Verwaltungskonto gelten soll.

Tools

AWS-Services

- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.
- AWS CodeBuild ist ein vollständig verwalteter Build-Service, der Sie beim Kompilieren von Quellcode, beim Ausführen von Komponententests und beim Erstellen von Artefakten unterstützt, die sofort einsatzbereit sind.
- AWS CodeCommit ist ein Versionskontrollservice, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodeDeploy automatisiert Bereitstellungen auf Amazon Elastic Compute Cloud (Amazon EC2) oder lokalen Instances, AWS Lambda Lambda-Funktionen oder Amazon Elastic Container Service (Amazon ECS) -Services.
- AWS CodePipeline hilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.
- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten.

- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub automated-code-pipeline-stackset-deployment verfügbar. Die Ordnerstruktur und weitere Details finden Sie in der Readme-Datei für das Repository.

Bewährte Methoden

Dieses Muster schränkt den direkten Zugriff auf das Verwaltungskonto bei der Bereitstellung der Anwendung auf OU-Ebene ein. Das Hinzufügen mehrerer Genehmigungsphasen zum Pipeline- und Repository-Prozess trägt dazu bei, zusätzliche Sicherheit und Steuerung für die Anwendungen und Komponenten zu gewährleisten, die Sie mit diesem Ansatz bereitstellen.

Epen

Konten in AWS Organizations konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie alle Funktionen im Verwaltungskonto.	Aktivieren Sie alle Funktionen im Verwaltungskonto für Ihre Organisation, indem Sie den Anweisungen in der Dokumentation zu AWS Organizations folgen.	AWS-Administrator, Plattformadministrator
Erstellen Sie ein CI/CD-Konto.	Erstellen Sie in AWS Organizations in Ihrer Organisation ein spezielles CI/CD-Konto und weisen Sie einem Team zu, das für das Konto verantwortlich ist und den Zugriff darauf kontrolliert.	AWS-Administrator
Fügen Sie einen delegierten Administrator hinzu.	Registrieren Sie im Verwaltungskonto das CI/CD-Konto,	AWS-Administrator, Plattformadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	das Sie im vorherigen Schritt erstellt haben, als delegiert en Stackset-Administrator. Anweisungen finden Sie in der CloudFormation AWS-Dokum entation.	

Erstellen Sie ein Anwendungs-Repository und eine CI/CD-Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Code-Repo sitory.	1. Klonen Sie das Code-Repository, das mit diesem Muster bereitgestellt wurde, auf Ihren Computer: `git clone https://g ithub.com/aws-samp les/automated-code -pipeline-stackset- deployment.git` 2. Lesen Sie die Readme-Datei, um die Verzeichn isstruktur und andere Details zu verstehen.	AWS DevOps
Erstellen Sie SNS-Themen.	Sie können die im GitHub Repository bereitgestellte `sns-template.yaml` Vorlage verwenden, um SNS-Themen zu erstellen und Abonnements für Genehmigu ngsanfragen zu konfigurieren.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Melden Sie sich auf der AWS-Konsole beim CI/CD-Konto an. 2. Öffnen Sie die CloudFormation Konsole unter / cloudformation. https://console.aws.amazon.com 3. Erstellen Sie einen neuen Stack mit neuen Ressourcen (Standardoption). 4. Wählen Sie für Vorlage angeben die Option Eine Vorlagendatei hochladen, Datei auswählen und wählen Sie dann die `sns-template.yaml` Datei aus dem `templates` Ordner des geklonten GitHub Repositorys aus. Wählen Sie Weiter aus. 5. Geben Sie einen aussagekräftigen Namen für den Anwendungsstapel ein. 6. Geben Sie ein Präfix für Ressourcen an. 7. Wählen Sie „Weiter“, „Weiter“ und „Absenden“. 8. Wenn der Stack erfolgreich erstellt wurde, wählen Sie den Tab Outputs und notieren Sie sich die Amazon-Ressourcennamen (ARNs) der SNS-Theme	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	n für Pull-Requests, die Testumgebung und die Produktionsumgebung. Sie werden diese Informati onen in den nachfolgenden Schritten verwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie IAM-Rollen für CI/CD-Komponenten.	Sie können die im GitHub Repository bereitgestellte `cicd-role-template.yaml` Vorlage verwenden, um IAM-Rollen und -Richtlinien zu erstellen, die für CI/CD-Komponenten erforderlich sind. 1. Melden Sie sich auf der AWS-Konsole beim CI/CD-Konto an. 2. Öffnen Sie die CloudFormation Konsole unter / cloudformation. https://console.aws.amazon.com 3. Erstellen Sie einen neuen Stack mit neuen Ressourcen (Standardoption). 4. Wählen Sie für Vorlage angeben die Option Eine Vorlagendatei hochladen, Datei auswählen und wählen Sie dann die `cicd-role-template.yaml` Datei aus dem `templates` Ordner des geklonten GitHub Repositorys aus. Wählen Sie Weiter aus. 5. Geben Sie einen aussagekräftigen Namen für den Anwendungsstapel ein. 6. Geben Sie Werte für die folgenden Parameter ein:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Der ARN für die Permission Boundary Policy. Sie können diesen ARN in der IAM-Konsole im Abschnitt „Richtliniendetails“ Ihrer Richtlinie zur Begrenzung der Zugriffsrechte abrufen. • Die ARN für das Thema SNS-Produktionsgenehmigung, das Sie zuvor notiert haben. • Der ARN für das Thema SNS-Testgenehmigung, das Sie zuvor notiert haben. • Ein Präfix für Ressourcen, die mit der Vorlage erstellt wurden. 7. Wählen Sie „Weiter“, „Weiter“ und „Absenden“. 8. Wenn der Stack erfolgreich erstellt wurde, wählen Sie die Registerkarte Outputs und notieren Sie sich die ARNs IAM-Rollen, die erstellt wurden. Sie werden diese Informationen in den nachfolgenden Schritten verwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein CodeCommit Repository und eine CodePipeline für Ihre Anwendung.	Sie können die im Repository bereitgestellte `cicd-pipeline-template.yaml` Vorlage verwenden, um ein GitHub CodeCommit Repository und eine CodePipeline für Ihre Anwendung zu erstellen. 1. Melden Sie sich auf der AWS-Konsole beim CI/CD-Konto an. 2. Öffnen Sie die CloudFormation Konsole unter / cloudformation. https://console.aws.amazon.com 3. Erstellen Sie einen neuen Stack mit neuen Ressourcen (Standardoption). 4. Wählen Sie für Vorlage angeben die Option Eine Vorlagendatei hochladen, Datei auswählen und wählen Sie dann die `cicd-pipeline-template.yaml` Datei aus dem `templates` Ordner des geklonten GitHub Repositorys aus. Wählen Sie Weiter aus. 5. Geben Sie einen aussagekräftigen Namen für den Anwendungsstapel ein.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Geben Sie Werte für die folgenden Parameter ein: • AppRepositoryName— Der Name des CodeCommit Repositorys, das für die Anwendung erstellt wird. • AppRepositoryDescription— Eine kurze Beschreibung des CodeCommit Repositorys, das für die Anwendung erstellt wird. • ApplicationName— Der Name Ihrer Anwendung. Diese Zeichenfolge wird als Name des CodeCommit Repositorys und als Präfix der CI/CD-Pipeline verwendet. • CloudWatchEventRoleARN — Der ARN der CloudWatch Ereignisrolle aus der vorherigen Aufgabe. • CodeBuildProjectRoleARN — Der ARN der CodeBuild Projektrolle aus der vorherigen Aufgabe. • CodePipelineRoleARN — Der ARN der CodePipeline Rolle aus der vorherigen Aufgabe.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• DeploymentConfigBucket— Der Name des Amazon Simple Storage Service (Amazon S3) -Buckets, in dem die Einrichtungskonfigurationsdateien und die ZIP-Skriptdatei gespeichert werden. • DeploymentConfigKey— Der Pfad und der ZIP-Dateiname (Amazon S3 S3-Schlüssel). • PRApprovalSNSARN — Der ARN für das SNS-Thema für Pull-Request-Benachrichtigungen. • ProdApprovalSNSARN — Der ARN für das SNS-Thema für Produktionsgenehmigungen. • TESTApprovalSNSARN — Der ARN für das SNS-Thema für Testgenehmigungen. • TemplateBucket— Der Name des S3-Buckets in der Vorlage zur CI/CD account where the CI/CD Pipeline-Erstellung wird gespeichert. 7. Wählen Sie Weiter, Weiter und Senden aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Wenn der Stack erfolgrei ch abgeschlossen wurde, erstellt er ein CodeCommi t Repository mit dem angegebenen Namen und einer Standardv erzeichnisstruktur, Einrichtu ngskonfigurationsdateien, Skripten und einer Code-Pipeline für das Repository.	

Stellen Sie ein Stack-Set bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Anwendungs-Repository.	Die CI/CD-Pipeline-Vorlage, die Sie zuvor verwendet haben, erstellt ein Beispiela nwendungs-Repository und eine Code-Pipeline. So klonen und verifizieren Sie das Repository: 1. Melden Sie sich beim CI/CD-Konto an. 2. Suchen Sie das Anwendungs-Repository und die CI/CD-Pipeline, die Sie im vorherigen Epic erstellt haben. 3. Kopieren Sie die URL für das Repository und verwenden Sie den Befehl git clone, um das Repositor	App-Entwickler, Dateninge nieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	y auf Ihrem lokalen Computer zu klonen.
	4. Stellen Sie sicher, dass die Verzeichnisstruktur und die Dateien den folgenden Kriterien entsprechen:
	`root`
	` |- deploy_configs`
	` |  |- deployment_config.json`
	` |- parameters`
	` |  |- template-parameter-dev.json`
	` |  |- template-parameter-test.json`
	` |  |- template-parameter-prod.json`
	` |- templates`
	` |  |- template.yml`
	` |- buildspec.yml`
	wobei der `deploy_configs` Ordner die Einrichtungskonfigurationsdatei und die `parameters` Ordner `templates` und Standarddateien enthalten, die Sie durch Ihre eigenen CloudFormation Vorlagen- und Parameterdateien ersetzen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Important Passen Sie die Ordnerstruktur nicht an. 5. Erstellen Sie einen Feature-Branch.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Anwendung sartefakte hinzu.	Aktualisieren Sie das Anwendungs-Repository mithilfe einer CloudFormation Vorlage. **Note** Diese Lösung unterstützt die Bereitstellung nur einer einzigen CloudFormation Vorlage. 1. Erstellen Sie Ihre CloudFormation Vorlage für die Bereitstellung der Änderungen am Anwendungscode und geben Sie ihr einen Namen<application-name>.yaml . 2. Ersetzen Sie die `template.yml` Datei im `templates` Ordner des Anwendungs-Repositorys durch die CloudFormation Vorlage, die Sie in Schritt 1 erstellt haben. 3. Bereiten Sie Parameter dateien für jede Umgebung (Entwicklung, Test und Produktion) vor.	App-Entwickler, Dateninge nieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Benennen Sie die Parameterdateien mithilfe des Formats `<cloudformation-template-name>-parameter-<environment-name>.json` . 5. Ersetzen Sie die Standardparameterdateien im `parameters` Ordner durch Ihre Dateien aus Schritt 4.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Einrichtungskonfigurationsdatei.	Aktualisieren Sie die `deployment_config.json` Datei: 1. Navigieren Sie im Anwendungs-Repository zu dem `deploy_configs` Ordner. 2. Öffnen Sie die Dateideploymen `t_config.json` : `{ "deployment_action": "<deploy/delete>", "stack_set_name": "<stack set name>", "stack_set_desciption": "<stack set description>", "deployment_targets": { "dev": { "org_units": ["list of OUs"], "regions": ["list of regions"], "filter_accounts": ["list of accounts"],`	App-Entwickler, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"filter_type": "<DIFFERENCE/INTERSECTION/UNION>"
	},
	"test": {
	"org_units": ["list of OUs"],
	"regions": ["list of regions"],
	"filter_accounts": ["list of accounts"],
	"filter_type": "<DIFFERENCE/INTERSECTION/UNION>"
	},
	"prod": {
	"org_units": ["list of OUs"],
	"regions": ["list of regions"],</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"filter_accounts": ["list of accounts"], "filter_type": "<DIFFERENCE/INTERSECTION/UNION>" } }, "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"], "auto_deployement": "<True/False>", "retain_stacks_on_account_removal": "<True/False>", "region_deployment_concurrency": "<SEQUENTIAL/PARALLEL>" }</pre> 3. Aktualisieren Sie die Werte für die Bereitstellungsaktion, den Namen des Stack-Sets, die Beschreibung des Stack-Sets und die Bereitstellungsziele. Sie können beispielsweise festlegen, `deployment_action` dass `delete`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	das gesamte Stack-Set und die zugehörigen Stack-Ins tances gelöscht werden. Wird verwendet, `deploy` um ein neues Stack-Set zu erstellen, ein vorhanden es Stack-Set zu aktualisi eren oder um Stack-Ins tances für zusätzliche OUs oder Regionen hinzuzufü gen oder zu entfernen. Weitere Beispiele finden Sie im Abschnitt Zusätzliche Informationen. Dieses Muster erstellt individuelle Stack-Sets für jede Umgebung, indem der Umgebungsname zu dem Stack-Set-Namen hinzugefügt wird, den Sie in der Einrichtu ngskonfigurationsdatei angeben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Übernehmen Sie die Änderungen und stellen Sie das Stack-Set bereit.	Übernehmen Sie die Änderungen, die Sie in Ihrer Anwendungsvorlage angegeben haben, und führen Sie das Stack-Set Schritt für Schritt zusammen und stellen Sie es in mehreren Umgebungen bereit: 1. Speichern Sie alle Ihre Dateien und übertrage n Sie die Änderungen in den Feature-Branch Ihres lokalen Anwendungs-Repositorys. 2. Schieben Sie den Feature-Branch in das Remote-Re pository. 3. Erstellen Sie einen Pull-Request, um die Änderunge n mit dem Haupt-Branch zusammenzuführen. Wenn der Pull-Request genehmigt wurde und die Änderungen mit dem Hauptzweig zusammeng eführt wurden, wird die CI/ CD-Pipeline initiiert. 4. Wenn die Dev-Deplo yment-Phase erfolgrei ch abgeschlossen wurde, überprüfen Sie die CloudFormation	App-Entwickler, Dateninge nieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Konsole auf der Registerkarte Service-Managed. StackSets Sie werden ein neues Stack-Set mit dem Suffix sehen. `dev` 5. Suchen Sie in den CodeBuild Protokollen für die Dev-Deployment-Phase nach Problemen. 6. Stellen Sie das Stack-Set in den Test- und Produktionsumgebungen bereit, indem Sie Ihre Genehmigungsberechtigten bitten, die Bereitstellungen für diese Phasen zu genehmigen, und die Schritte 5 und 6 wiederholen. Die Stacksets für die Test- und Produktionsumgebungen haben die `test` Suffixe und. `prod`	

Fehlerbehebung

Problem	Lösung
Die Bereitstellung schlägt mit der folgenden Ausnahme fehl: Ändern Sie den Namen der Vorlagenparameterdatei in -parameter- .json mit,	Die CloudFormation Vorlagenparameterdateien müssen der angegebenen Namenskonvention entsprechen. Aktualisieren Sie die Namen der Parameterdateien und versuchen Sie es erneut.

Problem	Lösung
Standardnamen sind nicht zulässig <application name><evn>	
Die Bereitstellung schlägt mit der folgenden Ausnahme fehl: Ändern Sie den Namen der CloudFormation Vorlage in .yml. Die Standardwerte template.yml oder template.yaml sind nicht zulässig <application name>	Der CloudFormation Vorlagenname muss der angegebenen Benennungskonvention entsprechen. Aktualisieren Sie den Dateinamen und versuchen Sie es erneut.
Die Bereitstellung schlägt mit der folgenden Ausnahme fehl: Für die Umgebung {Umgebungsname} wurden keine gültige CloudFormation Vorlage und die zugehörige Parameterdatei gefunden	Überprüfen Sie die Dateibenennungskonventionen für die CloudFormation Vorlage und ihre Parameterdatei für die angegebene Umgebung.
Die Bereitstellung schlägt mit der folgenden Ausnahme fehl: In der Einrichtungskonfigurationsdatei wurde eine ungültige Bereitstellungsaktion angegeben. Gültige Optionen sind „Bereitstellen“ und „Löschen“.	Sie haben einen ungültigen Wert für den `deployment_action` Parameter in der Einrichtungskonfigurationsdatei angegeben. Der Parameter hat zwei gültige Werte: `deploy` und`delete`. Wird verwendet`deploy`, um die Stack-Sets und die zugehörigen Stack-Instances zu erstellen und zu aktualisieren. `delete`Nur verwenden, wenn Sie das gesamte Stack-Set und die zugehörigen Stack-Instances entfernen möchten.

Zugehörige Ressourcen

- GitHub automated-code-pipeline-stackset-Bereitstellungs-Repository
- Aktivierung aller Funktionen in Ihrer Organisation (Dokumentation zu AWS Organizations)
- Registrieren Sie einen delegierten Administrator (CloudFormation AWS-Dokumentation)
- Ziele auf Kontoebene für servicemanaged Stack Sets (CloudFormation AWS-Dokumentation)

Zusätzliche Informationen

Flussdiagramm

Das folgende Flussdiagramm zeigt die Ablaufsteuerung und die Hierarchie der API-Aufrufe, die durch das benutzerdefinierte Skript implementiert werden, um die Bereitstellung von Stacksets zu automatisieren.

Beispiele für Konfigurationsdateien für die Bereitstellung

Ein neues Stack-Set erstellen

Die folgende Einrichtungskonfigurationsdatei erstellt ein neues Stack-Set, das `sample-stack-set` in der AWS-Region `us-east-1` in Three aufgerufen wird OUs.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                           },
     "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
     "auto_deployement": "True",
     "retain_stacks_on_account_removal": "True",
```

```
     "region_deployment_concurrency": "PARALLEL"
 }
```

Bereitstellung eines vorhandenen Stack-Sets in einer anderen Organisationseinheit

Wenn Sie die im vorherigen Beispiel gezeigte Konfiguration bereitstellen und das Stack-Set in einer zusätzlichen Organisationseinheit bereitstellen möchten, die `dev-org-unit-2` in der Entwicklungsumgebung aufgerufen wird, könnte die Einrichtungskonfigurationsdatei wie folgt aussehen.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1", "dev-org-
unit-2"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                          },
     "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
     "auto_deployement": "True",
     "retain_stacks_on_account_removal": "True",
     "region_deployment_concurrency": "PARALLEL"
 }
```

Bereitstellung eines vorhandenen Stack-Sets in einer anderen AWS-Region

Wenn Sie die im vorherigen Beispiel gezeigte Konfiguration bereitstellen und das Stack-Set in einer zusätzlichen AWS-Region (`us-east-2`) in der Entwicklungsumgebung für zwei OUs (`dev-org-unit-1`und`dev-org-unit-2`) bereitstellen möchten, könnte die Einrichtungskonfigurationsdatei wie folgt aussehen.

> **Note**
>
> Die Ressourcen in der CloudFormation Vorlage müssen gültig und regionsspezifisch sein.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                              "dev": {
                                        "org_units": ["dev-org-unit-1", "dev-org-
unit-2"],
                                        "regions": ["us-east-1", "us-east-2"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                              "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                              "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                            },
     "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
     "auto_deployement": "True",
     "retain_stacks_on_account_removal": "True",
     "region_deployment_concurrency": "PARALLEL"
 }
```

Entfernen einer Stack-Instance aus einer OU- oder AWS-Region

Nehmen wir an, dass die im vorherigen Beispiel gezeigte Bereitstellungskonfiguration bereitgestellt wurde. Die folgende Konfigurationsdatei entfernt die Stack-Instances aus beiden Regionen der OU`dev-org-unit-2`.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1"],
                                        "regions": ["us-east-1", "us-east-2"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                          },
     "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
     "auto_deployement": "True",
     "retain_stacks_on_account_removal": "True",
     "region_deployment_concurrency": "PARALLEL"
 }
```

Die folgende Konfigurationsdatei entfernt die Stack-Instance aus der AWS-Region `us-east-1` für beide OUs in der Entwicklungsumgebung.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
```

```
    "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1", "dev-org-
unit-2"],
                                        "regions": ["us-east-2"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                           },
     "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
     "auto_deployement": "True",
     "retain_stacks_on_account_removal": "True",
     "region_deployment_concurrency": "PARALLEL"
 }
```

Das gesamte Stack-Set wird gelöscht

Die folgende Einrichtungskonfigurationsdatei löscht das gesamte Stack-Set und alle zugehörigen Stack-Instances.

```
{
     "deployment_action": “delete”,
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1", "dev-org-
unit-2"],
                                        "regions": ["us-east-2"],
                                        "filter_accounts": [],
                                        "filter_type": ""
```

```
                                },
                            "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                },
                            "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                }
                        },
    "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
    "auto_deployement": "True",
    "retain_stacks_on_account_removal": "True",
    "region_deployment_concurrency": "PARALLEL"
}
```

Ein Konto von der Bereitstellung ausschließen

Die folgende Einrichtungskonfigurationsdatei schließt das Konto`111122223333`, das Teil der Organisationseinheit ist`dev-org-unit-1`, von der Bereitstellung aus.

```
{
    "deployment_action": "deploy",
    "stack_set_name": "sample-stack-set",
    "stack_set_desciption": "this is a sample stack set",
   "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": ["111122223333"],
                                        "filter_type": "DIFFERENCE"
                                },
                            "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                },
                            "prod": {
```

```
                                    "org_units": ["prod-org-unit-1"],
                                    "regions": ["us-east-1"],
                                    "filter_accounts": [],
                                    "filter_type": ""
                                }
                            },
    "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
    "auto_deployement": "True",
    "retain_stacks_on_account_removal": "True",
    "region_deployment_concurrency": "PARALLEL"
}
```

Bereitstellung der Anwendung für eine Teilmenge von Konten in einer Organisationseinheit

Mit der folgenden Einrichtungskonfigurationsdatei wird die Anwendung nur für drei Konten (111122223333, 444455556666, und777788889999) in der Organisationseinheit bereitgestellt. `dev-org-unit-1`

```
{
    "deployment_action": "deploy",
    "stack_set_name": "sample-stack-set",
    "stack_set_desciption": "this is a sample stack set",
   "deployment_targets": {
                            "dev": {
                                    "org_units": ["dev-org-unit-1"],
                                    "regions": ["us-east-1"],
                                    "filter_accounts": ["111122223333",
"444455556666", "777788889999"],
                                    "filter_type": "INTERSECTION"
                                },
                            "test": {
                                    "org_units": ["test-org-unit-1"],
                                    "regions": ["us-east-1"],
                                    "filter_accounts": [],
                                    "filter_type": ""
                                },
                            "prod": {
                                    "org_units": ["prod-org-unit-1"],
                                    "regions": ["us-east-1"],
                                    "filter_accounts": [],
                                    "filter_type": ""
                                }
                            },
```

```
    "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
    "auto_deployement": "True",
    "retain_stacks_on_account_removal": "True",
    "region_deployment_concurrency": "PARALLEL"
}
```

Automatisches Hinzufügen einer von AWS verwalteten Richtlinie für Systems Manager zu EC2 Instanzprofilen mithilfe von Cloud Custodian und AWS CDK

Erstellt von Ali Asfour (AWS) und Aaron Lennon (AWS)

Übersicht

Sie können Amazon Elastic Compute Cloud (Amazon EC2) -Instances in AWS Systems Manager integrieren, um betriebliche Aufgaben zu automatisieren und für mehr Transparenz und Kontrolle zu sorgen. Für die Integration mit Systems Manager müssen für EC2 Instances ein installierter AWS Systems Manager Agent (SSM Agent) und eine `AmazonSSMManagedInstanceCore` AWS Identity and Access Management (IAM) -Richtlinie an ihre Instance-Profile angehängt sein.

Wenn Sie jedoch sicherstellen möchten, dass allen EC2 Instance-Profilen die `AmazonSSMManagedInstanceCore` Richtlinie angehängt ist, kann es schwierig werden, neue EC2 Instances zu aktualisieren, die keine Instance-Profile haben, oder EC2 Instances, die ein Instance-Profil haben, aber nicht über die `AmazonSSMManagedInstanceCore` Richtlinie verfügen. Es kann auch schwierig sein, diese Richtlinie für mehrere Amazon Web Services (AWS) -Konten und AWS-Regionen hinzuzufügen.

Dieses Muster hilft bei der Lösung dieser Herausforderungen, indem es drei Cloud Custodian-Richtlinien in Ihren AWS-Konten bereitstellt:

- Die erste Cloud Custodian-Richtlinie sucht nach vorhandenen EC2 Instances, die über ein Instanzprofil, aber nicht über die `AmazonSSMManagedInstanceCore` Richtlinie verfügen. Die `AmazonSSMManagedInstanceCore` Richtlinie wird dann angehängt.
- Die zweite Cloud Custodian-Richtlinie sucht nach vorhandenen EC2 Instanzen ohne Instanzprofil und fügt ein Standard-Instanzprofil hinzu, dem die `AmazonSSMManagedInstanceCore` Richtlinie angehängt ist.
- Die dritte Cloud Custodian-Richtlinie erstellt AWS Lambda Lambda-Funktionen in Ihren Konten, um die Erstellung von EC2 Instanzen und Instanzprofilen zu überwachen. Dadurch wird sichergestellt, dass die `AmazonSSMManagedInstanceCore` Richtlinie automatisch angehängt wird, wenn eine EC2 Instanz erstellt wird.

Dieses Muster verwendet DevOpsAWS-Tools, um eine kontinuierliche, maßstabsgetreue Bereitstellung der Cloud Custodian-Richtlinien in einer Umgebung mit mehreren Konten zu erreichen, ohne eine separate Rechenumgebung bereitzustellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zwei oder mehr aktive AWS-Konten. Ein Konto ist das Sicherheitskonto und die anderen sind Mitgliedskonten.
- Berechtigungen zur Bereitstellung von AWS-Ressourcen im Sicherheitskonto. Dieses Muster verwendet Administratorberechtigungen, Sie sollten jedoch Berechtigungen entsprechend den Anforderungen und Richtlinien Ihrer Organisation gewähren.
- Möglichkeit, vom Sicherheitskonto aus eine IAM-Rolle für Mitgliedskonten zu übernehmen und die erforderlichen IAM-Rollen zu erstellen. Weitere Informationen dazu finden Sie unter Delegieren des Zugriffs auf AWS-Konten mithilfe von IAM-Rollen in der IAM-Dokumentation.
-

> **Important**
>
> AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert. Zu Testzwecken können Sie die AWS-CLI konfigurieren, indem Sie den `aws configure` Befehl verwenden oder Umgebungsvariablen festlegen. : Dies wird für Produktionsumgebungen nicht empfohlen und wir empfehlen, diesem Konto nur Zugriff mit den geringsten Rechten zu gewähren. Weitere Informationen dazu finden Sie in der IAM-Dokumentation unter Gewährung der geringsten Rechte.

- Die `devops-cdk-cloudcustodian.zip` Datei (angehängt), die auf Ihren lokalen Computer heruntergeladen wurde.
- Vertrautheit mit Python.
- Die erforderlichen Tools (Node.js, AWS Cloud Development Kit (AWS CDK) und Git) wurden installiert und konfiguriert. Sie können die `install-prerequisites.sh` Datei in der `devops-cdk-cloudcustodian.zip` Datei verwenden, um diese Tools zu installieren. Stellen Sie sicher, dass Sie diese Datei mit Root-Rechten ausführen.

Einschränkungen

- Dieses Muster kann zwar in einer Produktionsumgebung verwendet werden, stellen Sie jedoch sicher, dass alle IAM-Rollen und -Richtlinien den Anforderungen und Richtlinien Ihres Unternehmens entsprechen.

Paketversionen

- Cloud Custodian Version 0.9 oder höher
- TypeScript Version 3.9.7 oder höher
- Node.js Version 14.15.4 oder höher
- npmVersion 7.6.1 oder höher
- AWS CDK Version 1.96.0 oder höher

Architektur

Das Diagramm zeigt den folgenden Workflow:

1. Cloud Custodian-Richtlinien werden in ein CodeCommit AWS-Repository im Sicherheitskonto übertragen. Eine Amazon CloudWatch Events-Regel initiiert automatisch die CodePipeline AWS-Pipeline.
2. Die Pipeline ruft den neuesten Code von CodeCommit und sendet ihn an den Continuous-Integration-Teil der von AWS verwalteten CI/CD-Pipeline (Continuous Integration and Continuous Delivery). CodeBuild
3. CodeBuild führt die vollständigen DevSecOps Aktionen aus, einschließlich der Überprüfung der Richtliniensyntax für die Cloud Custodian-Richtlinien, und führt diese Richtlinien im `--dryrun` Modus aus, um zu überprüfen, welche Ressourcen identifiziert wurden.
4. Wenn keine Fehler vorliegen, fordert die nächste Aufgabe einen Administrator auf, die Änderungen zu überprüfen und die Bereitstellung in den Mitgliedskonten zu genehmigen.

Technologie-Stack

- AWS-CDK
- CodeBuild
- CodeCommit

- CodePipeline
- IAM
- Cloud Custodian

Automatisierung und Skalierung

Das AWS-Modul CDK-Pipelines stellt eine CI/CD-Pipeline bereit, CodePipeline mit der neben der Bereitstellung von AWS-Ressourcen mit CodeBuild AWS-Stacks auch die Erstellung und das Testen von Quellcode orchestriert werden. CloudFormation Sie können dieses Muster für alle Mitgliedskonten und Regionen in Ihrer Organisation verwenden. Sie können den `Roles creation` Stack auch erweitern, um andere IAM-Rollen in Ihren Mitgliedskonten bereitzustellen.

Tools

- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungsframework zur Definition der Cloud-Infrastruktur im Code und deren Bereitstellung über AWS. CloudFormation
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS CodeBuild ist ein vollständig verwalteter Build-Service in der Cloud.
- AWS CodeCommit ist ein Versionskontrollservice, mit dem Sie Assets privat speichern und verwalten können.
- AWS CodePipeline ist ein Continuous Delivery Service, mit dem Sie die zur Veröffentlichung Ihrer Software erforderlichen Schritte modellieren, visualisieren und automatisieren können.
- AWS Identity and Access Management ist ein Webservice, mit dem Sie den Zugriff auf AWS-Ressourcen sicher kontrollieren können.
- Cloud Custodian ist ein Tool, das Dutzende von Tools und Skripten, die die meisten Unternehmen für die Verwaltung ihrer Public-Cloud-Konten verwenden, in einem Open-Source-Tool vereint.
- Node.js ist eine JavaScript Runtime, die auf der V8-Engine von Google Chrome basiert. JavaScript

Code

Eine detaillierte Liste der Module, Kontofunktionen, Dateien und Bereitstellungsbefehle, die in diesem Muster verwendet werden, finden Sie in der `README` Datei in der `devops-cdk-cloudcustodian.zip` Datei (angehängt).

Epen

Die Pipeline mit AWS CDK einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie das CodeCommit Repository ein.	1. Entpacken Sie die `devops-cdk-cloudcustodian.zip` Datei (angehängt) im Arbeitsverzeichnis auf Ihrem lokalen Computer. 2. Melden Sie sich bei der AWS-Managementkonsole für Ihr Sicherheitskonto an, öffnen Sie die CodeCommit Konsole und erstellen Sie dann ein neues `devops-cdk-cloudcustodian` Repository. 3. Wechseln Sie in das Projektverzeichnis und richten Sie das CodeCommit Repository als Ursprung ein, übernehmen Sie die Änderungen und übertragen Sie sie dann in den Ursprungszweig, indem Sie die folgenden Befehle ausführen: • `cd devops-cdk-cloudcustodian` • `git init --initial-branch=main`	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `git add . git commit -m 'initial commit'` • `git remote add origin https://git-codecommit.us-east-1.amazonaws.com/v1/devops-cdk-cloudcustodian` • `git push origin main` Weitere Informationen dazu finden Sie in der CodeCommit AWS-Dokumentation unter Erstellen eines CodeCommit Repositorys.	
Installieren Sie die erforderlichen Tools.	Verwenden Sie die `install-prerequisites.sh` Datei, um alle erforderlichen Tools auf Amazon Linux zu installieren. Dies beinhaltet nicht die AWS-CLI, da sie vorinstalliert ist. Weitere Informationen dazu finden Sie im Abschnitt Voraussetzungen unter Erste Schritte mit dem AWS-CDK in der AWS-CDK-Dokumentation.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die erforderlichen AWS CDK-Pakete.	1. Richten Sie Ihre virtuelle Umgebung ein, indem Sie den folgenden Befehl in der AWS-CLI ausführen: `$ python3 -m venv .env` 2. Aktivieren Sie Ihre virtuelle Umgebung, indem Sie den folgenden Befehl ausführen: `$ source .env/bin/activate` 3. Nachdem die virtuelle Umgebung aktiviert wurde, installieren Sie die erforderlichen Abhängigkeiten, indem Sie den folgenden Befehl ausführen: `$ pip install -r requirements.txt` 4. Um zusätzliche Abhängigkeiten hinzuzufügen (z. B. andere AWS-CDK-Bibliotheken), fügen Sie sie der `requirements.txt` Datei hinzu und führen Sie dann den folgenden Befehl aus: `pip install -r requirements.txt` Die folgenden Pakete werden von AWS CDK benötigt und sind in der `requirements.txt` Datei enthalten:	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `aws-cdk.aws-cloudwatch` • `aws-cdk.aws-codebuild` • `aws-cdk.aws-codecommit` • `aws-cdk.aws-codedeploy` • `aws-cdk.aws-codepipeline` • `aws-cdk.aws-codepipeline-actions` • `aws-cdk.aws-events` • `aws-cdk.aws-events-targets` • `aws-cdk.aws-iam` • `aws-cdk.aws-logs` • `aws-cdk.aws-s3` • `aws-cdk.aws-sns` • `aws-cdk.aws-sns-subscriptions` • `aws-cdk.aws-sqs` • `aws-cdk.core`	

Konfigurieren Sie Ihre Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die erforderlichen Variablen.	Öffnen Sie die `vars.py` Datei im Stammordner Ihres CodeCommit Repositorys und	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	aktualisieren Sie die folgenden Variablen: • Geben Sie `var_deploy_region = 'us-east-1'` bei der Aktualisierung die AWS-Region an, in der die Pipeline bereitgestellt werden soll. • Aktualisieren Sie `var_codecommit_repo_name = "cdk-cloudcustodian"` mit dem Namen Ihres CodeCommit Repositorys. • Aktualisieren Sie `var_codecommit_branch_name = "main"` mit dem Namen der CodeCommit Filiale. • Geben Sie `var_adminEmail=notifyadmin@email.com'` die E-Mail-Adresse des Administrators an, der die Änderungen genehmigt. • Aktualisiere `var_slackWebHookUrl = https://hooks.slack.com/services/T000000000/B00000000/XXXXXXXXXXXXXXXXXXXXXXXX` 'mit dem Slack-Webhook, der verwendet	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wird, um Cloud Custodian -Benachrichtigungen zu senden, wenn Änderungen vorgenommen werden. • Aktualisiere `var_orgId = 'o-yyyyyyyyyy'` mit deiner Organisations-ID. • Aktualisieren Sie `security_account = '123456789011'` mit der AWS-Konto-ID für das Konto, auf dem die Pipeline bereitgestellt wird. • Aktualisieren Sie `member_accounts = ['111111111111','111111111112','111111111113']` mit den Mitgliedskonten, für die Sie den AWS-CDK-Stack booten und die erforderlichen IAM-Rollen bereitstellen möchten. • Stellen Sie diese Option ein`cdk_bootstrap_member_accounts = True` , `True` wenn Sie möchten, dass die Pipeline das AWS-CDK automatisch auf Ihre Mitgliedskonten bootet. Wenn `True` diese Option aktiviert ist, ist auch der Name einer vorhandenen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	IAM-Rolle in den Mitglieds konten erforderlich, die vom Sicherheitskonto übernommen werden kann. Diese IAM-Rolle muss auch über die erforderlichen Berechtigungen verfügen, um das AWS-CDK zu booten. • **Note** Aktualisieren Sie `cdk_boots trap_role = 'AWSContr olTowerEx ecution'` mit der vorhandenen IAM-Rolle in den Mitgliedskonten, die vom Sicherhei tskonto übernomme n werden kann. Diese Rolle muss auch berechtigt sein, das AWS-CDK zu booten. : Dies gilt nur, wenn auf gesetzt `cdk_boots trap_memb er_accounts` ist. `True`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisieren Sie die Datei account.yml mit den Informationen zum Mitgliedskonto.	Um das c7n-org Cloud Custodian-Tool für mehrere Konten auszuführen, müssen Sie die `accounts.yml` Konfigurationsdatei im Stammverzeichnis des Repositorys ablegen. Im Folgenden finden Sie ein Beispiel für eine Cloud Custodian-Konfigurationsdatei für AWS:
	`accounts:`
	`- account_id: '123123123123'`
	`  name: account-1`
	`  regions:`
	`  - us-east-1`
	`  - us-west-2`
	`  role: arn:aws:iam::123123123123:role/CloudCustodian`
	`  vars:`
	`  charge_code: xyz`
	`  tags:`
	`  - type:prod`
	`  - division:some division`
	`  - partition:us`
	`  - scope:pci`
		Developer

Bootstrap der AWS-Konten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Boostrap das Sicherheitskonto.	Führen Sie den Bootstrap `deploy_account` mit der `cloudcustodian_stack` Anwendung aus, indem Sie den folgenden Befehl ausführen: `cdk bootstrap -a 'python3 cloudcustodian/cloudcustodian_stack.py`	Developer
Option 1 — Automatisches Bootstrapping der Mitgliedskonten.	Wenn die `cdk_bootstrap_member_accounts` Variable `True` in der `vars.py` Datei auf gesetzt ist, werden die in der `member_accounts` Variablen angegebenen Konten automatisch von der Pipeline gestartet. Bei Bedarf können Sie `*cdk_bootstrap_role*` mit einer IAM-Rolle aktualisieren, die Sie vom Sicherheitskonto aus übernehmen können und die über die erforderlichen Berechtigungen für das Bootstrapping des AWS-CDK verfügt. Neue Konten, die der `member_accounts`	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Variablen hinzugefügt werden, werden automatisch von der Pipeline gestartet, sodass die erforderlichen Rollen bereitgestellt werden können.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Option 2 — Manuelles Bootstrapping der Mitglieds konten.	Wir empfehlen zwar nicht, diesen Ansatz zu verwenden , Sie können jedoch den Wert `cdk_bootstrap_memb er_accounts` auf festlegen `False` und diesen Schritt manuell ausführen , indem Sie den folgenden Befehl ausführen:
	
	`$ cdk bootstrap -a 'python3 cloudcust odian/member_accou nt_roles_stack.py' \`
	
	`--trust {security _account_id} \`
	
	`--context assume-ro le-credentials:wri teIamRoleName={rol e_name} \`
	
	`--context assume-ro le-credentials:rea dIamRoleName={role _name} \`
	
	`--mode=ForWriting \`
	
	`--context bootstrap =true \`
	
	`--cloudformation- execution-policies arn:aws:iam::aws:p olicy/Administrato rAccess`
		Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Important Stellen Sie sicher, dass Sie die `{role_name}` Werte `{security_account_id}` und mit dem Namen einer IAM-Rolle aktualisieren, die Sie vom Sicherheitskonto aus übernehmen können und die über die erforderlichen Berechtigungen für das Bootstrapping des AWS-CDK verfügt. Sie können auch andere Methoden verwenden, um die Mitgliedskonten zu booten, z. B. mit AWS CloudFormation. Weitere Informationen dazu finden Sie unter Bootstrapping in der AWS CDK-Dokumentation.	

Stellen Sie die AWS CDK-Stacks bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Rollen in den Mitgliedskonten.	Führen Sie den folgenden Befehl aus, um den	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`member_account_roles_stack` Stack bereitzustellen und die IAM-Rollen in den Mitgliedskonten zu erstellen: `cdk deploy --all -a 'python3 cloudcustodian/member_account_roles_stack.py' --require-approval never`	
Stellen Sie den Cloud Custodian-Pipeline-Stack bereit.	Führen Sie den folgenden Befehl aus, um die Cloud `cloudcustodian_stack.py` Custodian-Pipeline zu erstellen, die im Sicherheitskonto bereitgestellt wird: `cdk deploy -a 'python3 cloudcustodian/cloudcustodian_stack.py'`	Developer

Zugehörige Ressourcen

- Erste Schritte mit dem AWS CDK

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Automatisches Erstellen von CI/CD-Pipelines und Amazon ECS-Clustern für Microservices mithilfe von AWS CDK

Erstellt von Varsha Raju (AWS)

Übersicht

Dieses Muster beschreibt, wie Sie automatisch die CI/CD) pipelines and underlying infrastructure for building and deploying microservices on Amazon Elastic Container Service (Amazon ECS). You can use this approach if you want to set up proof-of-concept CI/CD pipelines to show your organization the benefits of CI/CD, microservices, and DevOps. You can also use this approach to create initial CI/CD Pipelines für kontinuierliche Integration und kontinuierliche Bereitstellung (Continuous Delivery) erstellen, die Sie dann an die Anforderungen Ihres Unternehmens anpassen oder ändern können.

Der Ansatz des Musters schafft eine Produktionsumgebung und eine Nicht-Produktionsumgebung, die jeweils über eine Virtual Private Cloud (VPC) und einen Amazon ECS-Cluster verfügen, die für die Ausführung in zwei Availability Zones konfiguriert sind. Diese Umgebungen werden von all Ihren Microservices gemeinsam genutzt. Anschließend erstellen Sie eine CI/CD pipeline for each microservice. These CI/CD Pipeline, rufen Änderungen aus einem Quell-Repository in AWS ab CodeCommit, erstellen die Änderungen automatisch und stellen sie dann in Ihren Produktions- und Nichtproduktionsumgebungen bereit. Wenn eine Pipeline alle Phasen erfolgreich abgeschlossen hat, können Sie URLs damit in der Produktions- und Nichtproduktionsumgebung auf den Microservice zugreifen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS) -Konto.
- Ein vorhandener Amazon Simple Storage Service (Amazon S3) -Bucket, der die `starter-code.zip` Datei (angehängt) enthält.
- AWS Cloud Development Kit (AWS CDK), in Ihrem Konto installiert und konfiguriert. Weitere Informationen dazu finden Sie unter Erste Schritte mit dem AWS-CDK in der AWS-CDK-Dokumentation.
- Python 3 und`pip`, installiert und konfiguriert. Weitere Informationen dazu finden Sie in der Python-Dokumentation.
- Vertrautheit mit AWS CDK, AWS CodePipeline, AWS CodeBuild CodeCommit, Amazon Elastic Container Registry (Amazon ECR), Amazon ECS und AWS Fargate.

- Vertrautheit mit Docker.
- Ein Verständnis von CI/CD und. DevOps

Einschränkungen

- Es gelten allgemeine AWS-Kontobeschränkungen. Weitere Informationen dazu finden Sie unter AWS-Servicekontingente in der Dokumentation AWS General Reference.

Produktversionen

- Der Code wurde mit Node.js Version 16.13.0 und AWS CDK Version 1.132.0 getestet.

Architektur

Das Diagramm zeigt den folgenden Workflow:

1. Ein Anwendungsentwickler überträgt den Code in ein Repository. CodeCommit
2. Eine Pipeline wird initiiert.
3. CodeBuild erstellt das Docker-Image und überträgt es in ein Amazon ECR-Repository
4. CodePipeline stellt ein neues Image für einen vorhandenen Fargate-Service in einem nicht produktiven Amazon ECS-Cluster bereit.
5. Amazon ECS ruft das Bild aus dem Amazon ECR-Repository in einen Fargate-Dienst ab, der nicht zur Produktion verwendet wird.
6. Die Tests werden unter Verwendung einer URL durchgeführt, die nicht für die Produktion verwendet wird.
7. Der Release-Manager genehmigt die Produktionsbereitstellung.
8. CodePipeline stellt das neue Image für einen vorhandenen Fargate-Service in einem Amazon ECS-Produktionscluster bereit
9. Amazon ECS ruft das Bild aus dem Amazon ECR-Repository in den Fargate-Produktionsservice ab.
10. Produktionsbenutzer greifen über eine Produktions-URL auf Ihre Funktion zu.

Technologie-Stack

- AWS-CDK
- CodeBuild
- CodeCommit
- CodePipeline
- Amazon ECR
- Amazon ECS
- Amazon VPC

Automatisierung und Skalierung

Sie können den Ansatz dieses Musters verwenden, um Pipelines für Microservices zu erstellen, die in einem gemeinsamen CloudFormation AWS-Stack bereitgestellt werden. Die Automatisierung kann mehr als einen Amazon ECS-Cluster in jeder VPC erstellen und auch Pipelines für Microservices erstellen, die in einem gemeinsamen Amazon ECS-Cluster bereitgestellt werden. Dies erfordert jedoch, dass Sie neue Ressourceninformationen als Eingaben für den Pipeline-Stack angeben.

Tools

- AWS CDK — Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungsframework zur Definition der Cloud-Infrastruktur im Code und deren Bereitstellung über AWS. CloudFormation
- AWS CodeBuild — AWS CodeBuild ist ein vollständig verwalteter Build-Service in der Cloud. CodeBuild kompiliert Ihren Quellcode, führt Komponententests durch und produziert Artefakte, die sofort einsatzbereit sind.
- AWS CodeCommit — AWS CodeCommit ist ein Versionskontrollservice, mit dem Sie Git-Repositorys privat in der AWS-Cloud speichern und verwalten können. CodeCommit macht es für Sie überflüssig, Ihr eigenes Quellcodeverwaltungssystem zu verwalten oder sich Gedanken über die Skalierung der Infrastruktur zu machen.
- AWS CodePipeline — AWS CodePipeline ist ein Continuous Delivery Service, mit dem Sie die zur Veröffentlichung Ihrer Software erforderlichen Schritte modellieren, visualisieren und automatisieren können. Sie können die verschiedenen Phasen eines Softwareveröffentlichungsprozesses schnell modellieren und konfigurieren. CodePipeline automatisiert die Schritte, die zur kontinuierlichen Veröffentlichung Ihrer Softwareänderungen erforderlich sind.

- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der zum Ausführen, Stoppen und Verwalten von Containern in einem Cluster verwendet wird. Sie können Ihre Aufgaben und Services auf einer serverlosen Infrastruktur ausführen, die von AWS Fargate verwaltet wird. Für mehr Kontrolle über Ihre Infrastruktur können Sie Ihre Aufgaben und Dienste alternativ auf einem Cluster von Amazon Elastic Compute Cloud (Amazon EC2) -Instances ausführen, die Sie verwalten.
- Docker — Docker hilft Entwicklern dabei, jede Anwendung als leichten, portablen und autarken Container zu packen, zu versenden und auszuführen.

Code

Der Code für dieses Muster ist in den `starter-code.zip` Dateien `cicdstarter.zip` und (im Anhang) verfügbar.

Epen

So richten Sie Ihre Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie das Arbeitsverzeichnis für AWS CDK ein.	1. Erstellen Sie ein Verzeichnis mit dem Namen `cicdproject` auf Ihrem lokalen Computer. 2. Laden Sie die `cicdstarter.zip` Datei (angehängt) in das `cicdproject` Verzeichnis herunter und entpacken Sie sie. Dadurch wird ein Ordner mit dem Namen `cicdstarter` erstellt. 3. Führen Sie den Befehl `cd <user-home>/cicdproject/cicdstarter` aus.	AWS DevOps, Cloud-Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Richten Sie die virtuelle Python-Umgebung ein, indem `python3 -m venv .venv` Sie den Befehl ausführen. 5. Führen Sie den Befehl `source ./.venv/bin/activate` aus. 6. Konfigurieren Sie Ihre AWS-Umgebung, indem `aws configure` Sie den Befehl ausführen oder die folgenden Umgebungsvariablen verwenden: • `AWS_ACCESS_KEY_ID` • `AWS_SECRET_ACCESS_KEY` • `AWS_DEFAULT_REGION`	

Erstellen Sie die gemeinsame Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die gemeinsame Infrastruktur.	1. Führen Sie in Ihrem Arbeitsverzeichnis den `cd cicdvpcecs` Befehl aus. 2. Führen Sie den `pip3 install -r requirements.txt` Befehl aus, um alle erforderlichen Python-Abhängigkeiten zu installieren	AWS DevOps, Cloud-Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Führen Sie den aus`cdk bootstrap command`, um die AWS-Umgebung für das AWS-CDK festzulegen. 4. Führen Sie den Befehl `cdk synth --context aws_account=<aws_account_ID> --context aws_region=<aws-region>` aus. 5. Führen Sie den Befehl `cdk deploy --context aws_account=<aws_account_ID> --context aws_region=<aws-region>` aus. 6. Der CloudFormation AWS-Stack erstellt die folgende Infrastruktur: • Eine Nicht-Produktions-VPC mit dem Namen `cicd-vpc-ecs/cicd-vpc-nonprod` • Eine Produktions-VPC mit dem Namen `cicd-vpc-ecs/cicd-vpc-prod` • Ein nicht produktiver Amazon ECS-Cluster mit dem Namen `cicd-ecs-nonprod` • Ein Amazon ECS-Produktionscluster mit dem	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Namen `cicd-ecs-prod`	
Überwachen Sie den CloudFormation AWS-Stack.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die CloudFormation AWS-Konsole und wählen Sie dann den `cicd-vpc-ecs` Stack aus der Liste aus. 2. Wählen Sie im Bereich mit den Stack-Details die Registerkarte Ereignisse und überwachen Sie den Fortschritt Ihrer Stack-Erstellung.	AWS DevOps, Cloud-Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie den CloudFormation AWS-Stack.	1. Nachdem der `cicd-vpc-ecs` CloudFormation AWS-Stack erstellt wurde, stellen Sie sicher, dass `cicd-vpc-ecs/cicd-vpc-prod` VPCs die `cicd-vpc-ecs/cicd-vpc-nonprod` und erstellt wurden. 2. Stellen Sie sicher, dass die `cicd-ecs-nonprod` und `cicd-ecs-prod` Amazon ECS-Cluster erstellt wurden. **Important** Stellen Sie sicher, dass Sie die Sicherheitsgruppe IDs für die beiden VPCs und die Sicherheitsgruppe IDs für die Standardsicherheitsgruppen in beiden Gruppen aufzeichnen VPCs.	AWS DevOps, Cloud-Infrastruktur

Erstellen Sie eine CI/CD-Pipeline für einen Microservice

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Infrastruktur für den Microservice.	1. Benennen Sie Ihren Microservice. In diesem	AWS DevOps, Cloud-Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Muster wird beispielsweise der Name des Microservices verwendet `myservice1`. 2. Führen Sie in Ihrem Arbeitsverzeichnis den `cd <working-directory>/cdkpipeline` Befehl aus. 3. Führen Sie den Befehl `pip3 install -r requirements.txt` aus. 4. Führen Sie den vollständigen `cdk synth` Befehl aus, der im Abschnitt Zusätzliche Informationen dieses Musters verfügbar ist. 5. Führen Sie den vollständigen `cdk deploy` Befehl aus, der im Abschnitt Zusätzliche Informationen dieses Musters verfügbar ist. **Note** Sie können die Werte für beide Befehle auch mithilfe der `cdk.json` Datei im Verzeichnis angeben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überwachen Sie den CloudFormation AWS-Stack.	Öffnen Sie die CloudFormation AWS-Konsole und überwachen Sie den Fortschritt des `myservice1-cicd-stack` Stacks. Schließlich ändert sich der Status zu `CREATE_COMPLETE` .	AWS DevOps, Cloud-Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie den CloudFormation AWS-Stack.	1. Stellen Sie auf der CodeCommit AWS-Konsole sicher, dass ein Repository mit dem Namen `myservice1` existiert und den Startercode enthält. 2. Stellen Sie auf der CodeBuild AWS-Konsole sicher, dass ein Build-Projekt mit dem Namen `myservice1` existiert. 3. Stellen Sie auf der Amazon ECR-Konsole sicher, dass ein Amazon ECR-Repository mit dem Namen `myservice1` existiert. 4. Stellen Sie auf der Amazon ECS-Konsole sicher, dass ein Fargate-Service mit dem Namen sowohl in einem Amazon ECS-Cluster als auch in einem Produktionscluster `myservice1` vorhanden ist. 5. Stellen Sie auf der Amazon Elastic Compute Cloud (Amazon EC2) -Konsole sicher, dass die Application Load Balancer für die Produktion und für die Produktion erstellt wurden. Notieren Sie sich die DNS-Namen der. ALBs	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Stellen Sie auf der CodePipeline AWS-Konsole sicher, dass eine Pipeline mit dem Namen `myservice 1` existiert. Sie muss `Deploy-Prod` Stufen `SourceBuild`,`Deploy-NonProd` , und haben. Die Pipeline sollte auch einen `in progress` Status haben. 7. Überwachen Sie die Pipeline, bis alle Phasen abgeschlossen sind. 8. Genehmigen Sie es manuell für die Produktion. 9. Geben Sie in einem Browserfenster die DNS-Namen von ein ALBs. 10. Die Anwendung sollte `Hello World` in den Bereichen Nichtproduktion und Produktion URLs angezeigt werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie die Pipeline.	1. Öffnen Sie das CodeCommit Repository, das Sie zuvor erstellt haben, und öffnen Sie die `index.js` Datei. 2. Ersetzen Sie `Hello World` durch `Hello CI/CD`. 3. Speichern Sie die Änderungen und übernehmen Sie sie im Hauptzweig. 4. Stellen Sie sicher, dass die Pipeline initiiert wird und ob die Änderung die `Deploy-Prod` Phasen `BuildDeploy-NonProd` , und durchläuft. 5. Genehmigen Sie die Produktion manuell. 6. Sowohl Produktion als auch Nichtproduktion URLs sollten jetzt angezeigt *`Hello CICD`* werden.	AWS DevOps, Cloud-Infrastruktur
Wiederhole dieses Epos für jeden Microservice.	Wiederholen Sie die Aufgaben in diesem Epos, um eine CI/CD-Pipeline für jeden Ihrer Microservices zu erstellen.	AWS DevOps, Cloud-Infrastruktur

Zugehörige Ressourcen

- Python mit AWS CDK verwenden
- AWS CDK Python-Referenz

- Einen AWS Fargate-Service mithilfe des AWS CDK erstellen

Zusätzliche Informationen

cdk synth -Befehl

```
cdk synth --context aws_account=<aws_account_number> --context
 aws_region=<aws_region> --context vpc_nonprod_id=<id_of_non_production
 VPC> --context vpc_prod_id=<id_of_production_VPC> --context
 ecssg_nonprod_id=< default_security_group_id_of_non-production_VPC>
 --context ecssg_prod_id=<default_security_group_id_of_production_VPC>
 --context code_commit_s3_bucket_for_code=<S3 bucket name> --context
 code_commit_s3_object_key_for_code=<Object_key_of_starter_code> --context
 microservice_name=<name_of_microservice>
```

cdk deploy command

```
cdk deploy --context aws_account=<aws_account_number> --context
 aws_region=<aws_region> --context vpc_nonprod_id=<id_of_non_production_VPC>
 --context vpc_prod_id=<id_of_production_VPC> --context ecssg_nonprod_id=<
 default_security_group_id_of_non-production_VPC> --context
 ecssg_prod_id=<default_security_group_id_of_production_VPC> --
context code_commit_s3_bucket_for_code=<S3 bucket name> --context
 code_commit_s3_object_key_for_code=<Object_key_of_starter_code> --context
 microservice_name=<name_of_microservice>
```

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Erstellen Sie eine lose gekoppelte Architektur mit Microservices mithilfe von DevOps Praktiken und AWS Cloud9

Erstellt von Alexandre Nardi (AWS)

Übersicht

Hinweis: AWS Cloud9 ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS Cloud9 können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Hinweis: AWS CodeCommit steht Neukunden nicht mehr zur Verfügung. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Dieses Muster zeigt, wie eine typische Webanwendung in einer serverlosen Architektur für Entwickler und Entwicklungsleiter entwickelt wird, die damit beginnen, DevOps Praktiken auf Amazon Web Services (AWS) zu testen. Es erstellt eine Beispielanwendung, die eine Storefront und ein Backend für das Durchsuchen und Kaufen von Büchern erstellt und einen Microservice bereitstellt, der unabhängig entwickelt werden kann. Das Muster verwendet AWS Cloud9 als Entwicklungsumgebung, eine Amazon DynamoDB DynamoDB-Datenbank als Datenspeicher und AWS-Services wie AWS und AWS CodeBuild für Continuous Integration CodePipeline and Continuous Deployment (CI/CD) -Funktionalität.

Das Muster führt Sie durch die folgenden Entwicklungsaktivitäten:

- Erstellen einer standardmäßigen AWS Cloud9 Cloud9-Entwicklungsumgebung
- Verwenden von CloudFormation AWS-Vorlagen zur Erstellung einer Webanwendung und eines Microservices für Bücher
- Verwenden von AWS Cloud9, um das Front-End zu modifizieren, Änderungen zu übernehmen und Änderungen zu testen
- Erstellen und Testen einer CI/CD-Pipeline zum Microservice
- Automatisierung von Komponententests

Der Code für dieses Muster befindet sich im GitHub AWS DevOps End-to-End Workshop-Repository.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Dateien aus dem DevOps End-to-End AWS-Workshop wurden auf Ihren Computer heruntergeladen

> **Important**
>
> Wenn Sie diese Demo-Anwendung in Ihrem AWS-Konto erstellen, werden AWS-Ressourcen erstellt und verbraucht. Sie sind für die Kosten der AWS-Services und Ressourcen verantwortlich, die für die Erstellung und Ausführung der Anwendung verwendet werden. Stellen Sie sicher, dass Sie nach Abschluss Ihrer Arbeit alle Ressourcen entfernen, um laufende Gebühren zu vermeiden. Anweisungen zur Bereinigung finden Sie im Abschnitt Epics.

Einschränkungen

Diese exemplarische Vorgehensweise dient nur zu Demonstrations- und Entwicklungszwecken. Informationen zur Verwendung in einer Produktionsumgebung finden Sie unter Bewährte Sicherheitsmethoden in der Dokumentation zu AWS Identity and Access Management (IAM) und nehmen Sie die erforderlichen Änderungen an den IAM-Rollen, Amazon DynamoDB und anderen verwendeten Services vor. Die Webanwendung ist von der AWS Bookstore Demo App abgeleitet. Weitere Überlegungen finden Sie im Abschnitt Bekannte Einschränkungen der README-Datei.

Architektur

Die Architektur der Bookstore-Anwendung wird im Abschnitt Architektur der README-Datei für die AWS-Bookstore-Demo-App veranschaulicht.

Aus Sicht der Bereitstellung verwendet die Bookstore-Demo-App eine einzige CloudFormation Vorlage, um alle Dienste und Objekte in einem Stack bereitzustellen. Dieses Muster enthält einige Änderungen, um zu demonstrieren, wie ein bestimmter Entwickler oder ein bestimmtes Team an einem bestimmten Produkt (Bücher) arbeiten und es unabhängig vom Rest der Anwendung aktualisieren könnte. Aus diesem Grund teilt der Code für dieses Muster die AWS Lambda Lambda-Funktionen und zugehörigen Objekte für den Microservice Books in eine zweite CloudFormation Vorlage auf, die einen Books-Stack erstellt. Auf diese Weise können Sie sehen, wie der Microservice mithilfe von CI/CD-Praktiken aktualisiert wird. In der folgenden Abbildung kennzeichnet der gestrichelte Rand den Microservice Books.

Tools

Tools

- Jest-Framework zum Testen JavaScript
- Python 3.9

Code

Der Quellcode und die Vorlagen für dieses Muster sind im AWS DevOps End-to-End Workshop-Repository verfügbar. GitHub Bevor Sie den Schritten im Abschnitt Epics folgen, laden Sie alle Dateien aus dem Repository auf Ihren Computer herunter.

> **Note**
>
> Der Abschnitt Epics enthält die allgemeinen Schritte für diese exemplarische Vorgehensweise, um Ihnen allgemeine Informationen über den Vorgang zu geben. Um jeden Schritt abzuschließen, finden Sie in der README-Datei im AWS DevOps End-to-End Workshop-Repository detaillierte Anweisungen.

Das AWS DevOps End-to-End Workshop-Repository erweitert das AWS Bookstore Demo App-Repository und verwendet eine modifizierte Version des AWS Cloud9-Bootstrapping-Codes, um die AWS Cloud9 Cloud9-IDE zu erstellen.

Bewährte Methoden

Die Verwendung der Bookstore-Anwendung ist unkompliziert. Hier sind einige empfohlene bewährte Methoden:

- Bei der Installation der Anwendung können Sie einen Projektnamen Ihrer Wahl oder der Einfachheit halber den Standardnamen (`demobookstore`) verwenden.
- Nachdem Sie die Anwendung betriebsbereit haben, empfiehlt es sich, die Amazon Neptune Neptune-Datenbank herunterzufahren, wenn Sie den Test für einen weiteren Tag fortsetzen möchten, da die Datenbank-Instance zusätzliche Kosten verursachen kann. Beachten Sie jedoch, dass die Datenbank nach sieben Tagen automatisch gestartet wird.
- Einzelheiten zum Code finden Sie in der Dokumentation zum AWS Bookstore Demo App-Repository. Sie beschreibt jeden Microservice und jede Tabelle.

- Weitere bewährte Methoden finden Sie unter Einige Herausforderungen, wenn Sie Zeit haben... Abschnitt der README-Datei im AWS DevOps End-to-End Workshop-Repository. Wir empfehlen Ihnen, die Informationen zu lesen, um sich eingehend mit zusätzlichen Sicherheitsfunktionen vertraut zu machen und Entkopplungsdienste zu üben.

Epen

Laden Sie den Quellcode herunter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Quellcode von herunter GitHub.	Der Quellcode und die Vorlagen für dieses Muster sind im GitHub AWS DevOps End-to-End Workshop-Repository verfügbar. Bevor Sie die nächsten Schritte im Abschnitt Epics ausführen , laden Sie alle Dateien aus dem Repository auf Ihren Computer herunter. **Note** Der Abschnitt Epics enthält die allgemein en Schritte für diese exemplarische Vorgehensweise, um Ihnen allgemein e Informationen über den Vorgang zu geben. Um jeden Schritt abzuschli eßen, finden Sie in der README-Datei im AWS DevOps End-	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	to-End Workshop-Repository detaillierte Anweisungen. Das AWS DevOps End-to-End Workshop-Repository erweitert das AWS Bookstore Demo App-Repository und verwendet eine modifizierte Version des AWS Cloud9-Bootstrapping-Codes, um die AWS Cloud9 Cloud9-IDE zu erstellen.	

Erstellen Sie die Bookstore-Webanwendung und den Books-Microservice

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Front-End- und Lambda-Funktionen für die Bookstore-App.	1. Melden Sie sich bei der CloudFormation Konsole an und stellen Sie die `DemoBookstoreMainTemplate.yml` Vorlage bereit, um den Stack zu erstellen . DemoBookStoreStack Dadurch werden die Front-End- und Lambda-Funktionen erstellt, die sich außerhalb des Microservices Books befinden. 2. Notieren Sie sich auf der Registerkarte Ausgaben	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	des Stacks die URL der Website unter dem Label. WebApplication	
Erstellen Sie den Microservice Books.	Stellen Sie auf der CloudFormation Konsole die `DemoBookstoreBooksServiceTemplate.yml` Vorlage bereit, um den DemoBooks ServiceStack Stack zu erstellen.	Developer
Testen Sie Ihre Anwendung.	Verwenden Sie die Website-URL aus dem DemoBookStoreStack Stack, um auf die Bookstore-Anwendung zuzugreifen.	Developer

Verwenden Sie die Cloud9-Umgebung, um Ihre Anwendung zu verwalten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS Cloud9 Cloud9-IDE.	Stellen Sie auf der CloudFormation Konsole die `C9EnvironmentTemplate.yml` Vorlage bereit, um eine AWS Cloud9 Cloud9-Umgebung zu erstellen.	Entwickler, Leiter des Entwicklers
Erstellen Sie CodeCommit Repositorys.	1. Melden Sie sich bei der CodeCommit AWS-Konsole an und vergewissern Sie sich, dass Sie über ein `demobookstore-WebAssets` Repository	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	verfügen, das den Code für die Front-End-Anwendung enthält. 2. Erstellen Sie ein Repository für den Microservice Books namens. `demobookstore-BooksService` 3. Klonen Sie die beiden Repositorys in AWS Cloud9 (`demobookstore-WebAssets` und `demobookstore-BooksService`) mithilfe des `git clone` Befehls.	
Ändern Sie den Code im Frontend und überprüfen Sie die Pipeline.	1. Verwenden Sie AWS Cloud9, um einige Codeänderungen auf einer Webseite vorzunehmen. Dadurch wird das `demobookstore-WebAssets` Repository aktualisiert. 2. Stellen Sie auf der CodePipeline AWS-Konsole sicher, dass DemoBookStore-Assets-Pipeline läuft. 3. Testen Sie Ihre Webanwendung, indem Sie sie über den Browser aktualisieren (Strg+F5 in Firefox).	Developer

Implementieren Sie eine CI/CD-Pipeline für den Microservice Books

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die YAML-Dateien für das Build- und Service-Update hinzu.	1. Laden Sie in AWS Cloud9 die `DemoBookstoreBooksServiceUpdateTemplate.yml` Dateien `buildspec.yml` und hoch. • `buildspec.yml` enthält Bauanweisungen und enthält auch Testanweisungen für automatisierte Tests. Sie werden an dieser Stelle kommentiert und werden später verwendet. • `DemoBookstoreBooksServiceUpdateTemplate.yml` ist eine aktualisierte Version von`DemoBookstoreBooksServiceTemplate.yml`, die in der Bereitstellungsphase der Pipeline verwendet werden soll. 2. Übergeben Sie die Dateien und übertragen Sie sie.	Developer
Erstellen Sie einen S3-Bucket für die Build-Pipeline.	Folgen Sie den Anweisungen in der Amazon S3-Dokume	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ntation, um einen S3-Bucket zu erstellen. • Der Bucket-Name muss global eindeutig sein, zum Beispiel `demobookstore-books-service-pipeline-bucket-<YYYYMMDDHHMM>` . • Deaktivieren Sie das Kontrollkästchen Allen öffentlichen Zugriff blockieren und aktivieren Sie das Kontrollkästchen Ich bestätige...	
Verwenden Sie IAM, um eine Rolle für die CloudFormation Bereitstellung zu erstellen.	Erstellen Sie eine `demobookstore-CloudFormation-role` Rolle und hängen Sie die `AdministratorAccess` Richtlinie an. Im nächsten Epic kannst du diese Rolle für Mindestberechtigungen neu konfigurieren.	Developer
Erstellen Sie eine neue Pipeline, um die Erstellung und Bereitstellung des Microservices Books zu automatisieren.	Erstellen Sie eine Pipeline (z. B. demobookstore- BooksService -Pipeline) mit den Phasen Commit, Build und Deploy, wie in der README-Datei beschrieben.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie Ihren Microservice in AWS Cloud9.	Nehmen Sie eine Änderung an der ListBooksFunktion vor und sehen Sie, wie die Pipeline funktioniert.	Developer
Automatisieren Sie den Komponententest für die ListBooks Lambda-Funktion.	Aktivieren Sie in der AWS Cloud9 Cloud9-IDE den Build, um Komponententests auszuführen, und überprüfe n Sie die Testergebnisse. Anweisungen finden Sie in der README-Datei.	Developer

(Optional) Implementieren Sie zusätzliche Funktionen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Machen Sie Ihre Lösung sicher.	Stellen Sie `demobooks tore-CloudFormatio n-role` die Konfiguration so ein, dass Sie über Mindestbe rechtigungen verfügen, und überprüfen Sie auch andere verwendete Rollen.	Developer
Beseitigen Sie Abhängigk eiten in den CloudFormation Vorlagen.	Die Methode für den Informati onsaustausch zwischen der `DemoBookstoreMainT emplate.yml` Vorlage und der `DemoBookstoreBooks ServiceTemplate.yml` Vorlage basiert auf Ausgaben und Importen. Durch die Übergabe von Werten	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zwischen diesen beiden Vorlagen werden Abhängigkeiten hinzugefügt. Um die Abhängigkeiten zu beseitigen, sollten Sie die Verwendung von AWS Systems Manager Parameter Store in Betracht ziehen.	
Erstellen Sie einen Cart-Microservice.	Verwenden Sie den Microservice Books als Beispiel, um Funktionen im Zusammenhang mit Einkaufswagen aus der `DemoBookstoreMainTemplate.yml` Vorlage zu übernehmen und einen Warenkorb-Microservice zu erstellen.	Developer

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die S3-Buckets.	Löschen Sie auf der Amazon S3 S3-Konsole die folgenden Buckets, die mit der Beispiel-Webanwendung verknüpft sind: • Zwei Buckets, die für die AWS Bookstore Demo App erstellt wurden. Die Buckets-Namen beginnen mit dem Stack-Namen, den Sie für AWS angegeben	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	haben CloudFormation , als Sie das Frontend erstellt haben; zum Beispiel. DemoBookStoreStack • <YYYYMMDDHHMM>Ein Bucket für die Build-Pipeline, zum Beispiel demobookstore-books-service-pipeline-bucket -.	
Lösche die Stapel.	Löschen Sie auf der CloudFormation Konsole die Stacks, die der Beispiel-Webanwendung zugeordnet sind: • DemoBooksServiceStack • DemoBookStoreStack Das Entfernen kann mehr als 90 Minuten dauern. Wenn das Entfernen fehlschlägt, löschen Sie sie erneut und löschen Sie auch alle manuellen Ressourcen (z. B. die VPC oder Netzwerkschnittstellen), die auf Benachrichtigungen basieren.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die IAM-Rollen.	Löschen Sie auf der IAM-Konsole die folgenden Rollen: • `demobookstore-Cloudformation-role` • `demobookstore-BooksService-BuildProject-service-role` step-by-stepAnweisungen finden Sie in der IAM-Dokumentation.	Developer

Zugehörige Ressourcen

- AWS-Bookstore-Demo-App
- Beispiel für AWS Cloud9 Bootstrapping
- Einen Stack auf der CloudFormation AWS-Konsole erstellen (CloudFormation AWS-Dokumentation)
- Einen Bucket erstellen (Amazon S3 S3-Dokumentation)

Zusätzliche Informationen

Eine ausführliche step-by-step Anleitung finden Sie in der README-Datei im AWS DevOps End-to-End GitHub Workshop-Repository.

Über das Update vom Mai 2023: Dieses Muster wurde aktualisiert, um neuere Versionen von Node und Python zu verwenden. Wir haben viele Pakete im Quellcode aktualisiert und Glyphicon entfernt, da es nicht mehr kostenlos ist. Wir haben auch alle Abhängigkeiten vom AWS Bookstore Demo App-Repository entfernt, sodass sich die beiden Repositorys nun unabhängig voneinander weiterentwickeln können.

Erstellen und übertragen Sie Docker-Images mithilfe von GitHub Actions und Terraform auf Amazon ECR

Erstellt von Ruchika Modi (AWS)

Übersicht

Dieses Muster erklärt, wie Sie wiederverwendbare GitHub Workflows erstellen können, um Ihr Dockerfile zu erstellen und das resultierende Image an Amazon Elastic Container Registry (Amazon ECR) zu übertragen. Das Muster automatisiert den Erstellungsprozess Ihrer Dockerfiles mithilfe von Terraform und Aktionen. GitHub Dies minimiert die Möglichkeit menschlicher Fehler und reduziert die Bereitstellungszeit erheblich.

Eine GitHub Push-Aktion zum Hauptzweig Ihres GitHub Repositorys leitet die Bereitstellung von Ressourcen ein. Der Workflow erstellt ein eindeutiges Amazon ECR-Repository, das auf der Kombination aus GitHub Organisation und Repository-Name basiert. Anschließend wird das Dockerfile-Image in das Amazon ECR-Repository übertragen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein aktives GitHub Konto.
- Ein GitHub Repositorium.
- Terraform Version 1 oder höher wurde installiert und konfiguriert.
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket für das Terraform-Backend.
- Eine Amazon DynamoDB-Tabelle für Terraform-Statussperrung und Konsistenz. Die Tabelle muss einen Partitionsschlüssel haben, der den Typ `LockID` hat. `String` Wenn dies nicht konfiguriert ist, wird die Statussperre deaktiviert.
- Eine AWS Identity and Access Management (IAM) -Rolle, die über Berechtigungen zum Einrichten des Amazon S3 S3-Backends für Terraform verfügt. Anweisungen zur Konfiguration finden Sie in der Terraform-Dokumentation.

Einschränkungen

Dieser wiederverwendbare Code wurde nur mit GitHub Aktionen getestet.

Architektur

Zieltechnologie-Stack

- Amazon ECR-Repository
- GitHub Aktionen
- Terraform

Zielarchitektur

Das Diagramm veranschaulicht folgende Vorgänge:

1. Ein Benutzer fügt dem Repository ein Dockerfile und Terraform-Vorlagen hinzu. GitHub

2. Diese Ergänzungen initiieren einen Aktions-Workflow. GitHub

3. Der Workflow prüft, ob ein Amazon ECR-Repository vorhanden ist. Wenn nicht, erstellt er das Repository auf der Grundlage der GitHub Organisation und des Repository-Namens.

4. Der Workflow erstellt das Dockerfile und überträgt das Image in das Amazon ECR-Repository.

Tools

Amazon-Dienste

- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Registry-Service, der sicher, skalierbar und zuverlässig ist.

Andere Tools

- GitHub Actions ist in die GitHub Plattform integriert und hilft Ihnen beim Erstellen, Teilen und Ausführen von Workflows in Ihren GitHub Repositorys. Mithilfe von GitHub Aktionen können Sie Aufgaben wie das Erstellen, Testen und Bereitstellen Ihres Codes automatisieren.
- Terraform ist ein IaC-Tool (Infrastructure as Code) HashiCorp , mit dem Sie Cloud- und lokale Infrastrukturen erstellen und verwalten können.

Code-Repository

Der Code für dieses Muster ist im GitHub Docker ECR Actions Workflow-Repository verfügbar.

- Wenn Sie GitHub Aktionen erstellen, werden Docker-Workflow-Dateien im `/.github/workflows/` Ordner dieses Repositorys gespeichert. Der Workflow für diese Lösung befindet sich in der Datei workflow.yaml.
- Der `e2e-test` Ordner enthält ein Dockerfile-Beispiel zum Nachschlagen und Testen.

Bewährte Methoden

- Bewährte Methoden zum Schreiben von Dockerfiles finden Sie in der Docker-Dokumentation.
- Verwenden Sie einen VPC-Endpunkt für Amazon ECR. VPC-Endpunkte werden von AWS unterstützt PrivateLink, einer Technologie, mit der Sie privat über private IP-Adressen auf Amazon ECR APIs zugreifen können. Bei Amazon ECS-Aufgaben, die den Starttyp Fargate verwenden, ermöglicht der VPC-Endpunkt der Aufgabe, private Images aus Amazon ECR abzurufen, ohne der Aufgabe eine öffentliche IP-Adresse zuzuweisen.

Epen

Richten Sie den OIDC-Anbieter und das Repository ein GitHub

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie OpenID Connect.	Erstellen Sie einen OpenID Connect (OIDC) -Anbieter. Sie verwenden den Anbieter in der Vertrauensrichtlinie für die in dieser Aktion verwendete IAM-Rolle. Anweisungen finden Sie in der GitHub Dokumentation unter Konfiguration von OpenID Connect in Amazon Web Services.	AWS-Administrator, AWS DevOps, Allgemeines AWS
Klonen Sie das GitHub Repository.	Klonen Sie das GitHub Docker ECR Actions Workflow-Repository in Ihren lokalen Ordner:	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`$git clone https://github.com/aws-samples/docker-ecr-actions-workflow`	

Passen Sie den GitHub wiederverwendbaren Workflow an und stellen Sie das Docker-Image bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie das Ereignis an, das den Docker-Workflow initiiert.	Der Workflow für diese Lösung befindet sich in workflow.yaml. Dieses Skript ist derzeit so konfiguriert, dass es Ressourcen bereitstellt, wenn es das Ereignis empfängt. `workflow_dispatch` Sie können diese Konfiguration anpassen, indem Sie das Ereignis in einen anderen übergeordneten Workflow ändern `workflow_call` und den Workflow von dort aufrufen.	DevOps Ingenieur
Passen Sie den Arbeitsablauf an.	Die Datei workflow.yaml ist so konfiguriert, dass sie einen dynamischen, wiederver wendbaren Workflow erstellt. GitHub Sie können diese Datei bearbeiten, um die Standardk onfiguration anzupassen, oder Sie können die Eingabewe rte aus der GitHub Aktionsko nsole übergeben, wenn Sie	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	das `workflow_dispatch` Ereignis verwenden, um die Bereitstellung manuell einzuleiten.
	• Stellen Sie sicher, dass Sie die richtige AWS-Konto-ID und Zielregion angeben.
	• Erstellen Sie eine Amazon ECR-Lebenszyklusrichtlinie (siehe Beispielrichtlinie) und aktualisieren Sie den Standardpfad (`e2e-test/policy.json`) entsprechend.
	• Für die Workflow-Datei sind zwei IAM-Rollen als Eingabe erforderlich:
	  • Eine IAM-Rolle, die über Berechtigungen zum Einrichten des Amazon S3 S3-Backends für Terraform verfügt (siehe Abschnitt Voraussetzungen). Sie können den Standard-Rollennamen in der aktualisieren. `workload-assumable-role` `yaml`Datei entsprechend.
	  • Eine IAM-Rolle mit Zugriffsberechtigungen. GitHub Diese Rolle wird auch in der Amazon ECR-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Richtlinie verwendet, um Amazon ECR-Operationen einzuschränken. Weitere Informationen finden Sie in der Datei data.tf.	
Stellen Sie die Terraform-Vorlagen bereit.	Der Workflow stellt automatisch die Terraform-Vorlagen bereit, die das Amazon ECR-Repository erstellen, basierend auf dem von Ihnen konfigurierten GitHub Ereignis. Diese Vorlagen sind als `.tf` Dateien im Stammverzeichnis des Github-Repositorys verfügbar.	AWS DevOps, DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Probleme oder Fehler bei der Konfiguration von Amazon S3 und DynamoDB als Terraform-Remote-Backend.	Folgen Sie den Anweisungen in der Terraform-Dokumentation, um die erforderlichen Berechtigungen für die Amazon S3- und DynamoDB-Ressourcen für die Remote-Backend-Konfiguration einzurichten.
Der Workflow mit dem Ereignis konnte nicht ausgeführt oder gestartet werden. `workflow_dispatch`	Der Workflow, der für die Bereitstellung über das `workflow_dispatch` Ereignis konfiguriert ist, funktioniert nur, wenn der Workflow auch für den Hauptzweig konfiguriert ist.

Zugehörige Ressourcen

- Workflows wiederverwenden (GitHub Dokumentation)
- Einen Workflow auslösen (Dokumentation) GitHub

Erstellen und testen Sie iOS-Apps mit AWS CodeCommit CodePipeline, AWS und AWS Device Farm

Erstellt von Abdullahi Olaoye (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Dieses Muster beschreibt die Schritte zur Erstellung einer CI/CD-Pipeline (Continuous Integration and Continuous Delivery), die AWS verwendet, CodePipeline um iOS-Anwendungen auf echten Geräten auf AWS zu erstellen und zu testen. Das Muster verwendet AWS CodeCommit zum Speichern des Anwendungscodes, das Jenkins-Open-Source-Tool zum Erstellen der iOS-Anwendung und AWS Device Farm, um die erstellte Anwendung auf realen Geräten zu testen. Diese drei Phasen werden mithilfe von AWS CodePipeline zusammen in einer Pipeline orchestriert.

Dieses Muster basiert auf dem Beitrag Erstellen und Testen von iOS- und iPadOS-Apps mit AWS DevOps und mobilen Diensten im DevOps AWS-Blog. Eine ausführliche Anleitung finden Sie im Blogbeitrag.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Apple-Entwicklerkonto
- Server erstellen (macOS)
- Xcode Version 11.3 (auf dem Build-Server installiert und eingerichtet)
- Auf der Workstation installierte und konfigurierte AWS-Befehlszeilenschnittstelle (AWS CLI)
- Grundkenntnisse in Git

Einschränkungen

- Auf dem Anwendungs-Build-Server muss macOS ausgeführt werden.
- Der Build-Server muss über eine öffentliche IP-Adresse verfügen, sodass er sich remote mit ihm verbinden CodePipeline kann, um Builds zu initiieren.

Architektur

Quelltechnologie-Stack

- Ein Prozess zur Erstellung von iOS-Anwendungen vor Ort, bei dem ein Simulator oder ein manueller Test auf physischen Geräten verwendet wird

Zieltechnologie-Stack

- Ein CodeCommit AWS-Repository zum Speichern von Anwendungsquellcode
- Ein Jenkins-Server für Anwendungsbuilds mit Xcode
- Ein AWS Device Farm Farm-Gerätepool zum Testen von Anwendungen auf realen Geräten

Zielarchitektur

Wenn ein Benutzer Änderungen am Quell-Repository festschreibt, ruft die Pipeline (AWS CodePipeline) den Code aus dem Quell-Repository ab, initiiert einen Jenkins-Build und übergibt den Anwendungscode an Jenkins. Nach dem Build ruft die Pipeline das Build-Artefakt ab und startet einen AWS Device Farm Farm-Job, um die Anwendung anhand eines Gerätepools zu testen.

Tools

- AWS CodePipeline ist ein vollständig verwalteter Continuous Delivery Service, der Sie bei der Automatisierung Ihrer Release-Pipelines für schnelle und zuverlässige Anwendungs- und Infrastrukturupdates unterstützt. CodePipeline automatisiert die Erstellungs-, Test- und Bereitstellungsphasen Ihres Release-Prozesses bei jeder Codeänderung auf der Grundlage des von Ihnen definierten Release-Modells.
- AWS CodeCommit ist ein vollständig verwalteter Quellcodeverwaltungsservice, der sichere Git-basierte Repositorys hostet. Es erleichtert Teams die Zusammenarbeit an Code in einem sicheren und hoch skalierbaren Ökosystem. CodeCommit macht es überflüssig, Ihr eigenes Quellcodeverwaltungssystem zu betreiben oder sich Gedanken über die Skalierung der Infrastruktur zu machen.
- AWS Device Farm ist ein Service zum Testen von Anwendungen, mit dem Sie die Qualität Ihrer Web- und mobilen Apps verbessern können, indem Sie sie mit einer Vielzahl von Desktop-Browsern und echten Mobilgeräten testen, ohne eine Testinfrastruktur bereitstellen und verwalten zu müssen.

- Jenkins ist ein Open-Source-Automatisierungsserver, der es Entwicklern ermöglicht, ihre Software zu erstellen, zu testen und bereitzustellen.

Epen

Richten Sie die Build-Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Jenkins auf dem Build-Server, auf dem macOS ausgeführt wird.	Jenkins wird für die Erstellung der Anwendung verwendet, daher müssen Sie sie zuerst auf dem Build-Server installieren. Detaillierte Anweisungen für diese und nachfolgende Aufgaben finden Sie im AWS-Blogbeitrag Erstellen und Testen von iOS- und iPadOS-Apps mit AWS DevOps und mobilen Services und anderen Ressourcen im Abschnitt Verwandte Ressourcen am Ende dieses Musters.	DevOps
Konfigurieren Sie Jenkins.	Folgen Sie den Anweisungen auf dem Bildschirm, um Jenkins zu konfigurieren.	DevOps
Installieren Sie das CodePipeline AWS-Plugin für Jenkins.	Dieses Plugin muss auf dem Jenkins-Server installiert sein, damit Jenkins mit dem AWS-Service interagieren kann. CodePipeline	DevOps
Erstellen Sie ein Jenkins-Freestyle-Projekt.	Erstellen Sie in Jenkins ein Freestyle-Projekt. Konfigurieren Sie das Projekt, um Trigger und andere Build-Kon	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	figurationsoptionen anzugeben .	

AWS-Gerätefarm konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Device Farm Farm-Projekt.	Öffnen Sie die AWS Device Farm Farm-Konsole. Erstellen Sie ein Projekt und einen Gerätepool zum Testen. Anweisungen finden Sie im Blogbeitrag.	Developer

Konfigurieren Sie das Quell-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein CodeCommit Repository.	Erstellen Sie ein Repository, in dem der Quellcode gespeiche rt wird.	DevOps
Übergeben Sie Ihren Anwendungscode in das Repository.	Connect zu dem CodeCommi t Repository her, das Sie erstellt haben. Übertragen Sie den Code von Ihrem lokalen Computer in das Repository.	DevOps

Konfigurieren Sie die Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Pipeline in AWS CodePipeline.	Öffnen Sie die CodePipeline AWS-Konsole und erstellen Sie eine Pipeline. Die Pipeline orchestriert alle Phasen des CI/CD-Prozesses. Anweisungen finden Sie im AWS-Blogbeitrag Erstellen und Testen von iOS- und iPadOS-Apps mit AWS DevOps und mobilen Services.	DevOps
Fügen Sie der Pipeline eine Testphase hinzu.	Um eine Testphase hinzuzufügen und sie in AWS Device Farm zu integrieren, bearbeiten Sie die Pipeline.	DevOps
Initiieren Sie die Pipeline.	Um die Pipeline und den CI/CD-Prozess zu starten, wählen Sie Release change.	DevOps

Testergebnisse der Anwendung anzeigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Testergebnisse.	Wählen Sie in der AWS Device Farm Farm-Konsole das von Ihnen erstellte Projekt aus und überprüfen Sie die Ergebnisse der Tests. In der Konsole werden die Details der einzelnen Tests angezeigt.	Developer

Zugehörige Ressourcen

Step-by-step Anweisungen für dieses Muster

- iOS- und iPadOS-Apps mit AWS und mobilen Services erstellen DevOps und testen (DevOps AWS-Blogbeitrag)

AWS-Gerätefarm konfigurieren

- AWS Device Farm Farm-Konsole

Konfigurieren Sie das Quell-Repository

- Ein CodeCommit AWS-Repository erstellen
- Stellen Sie eine Connect zu einem CodeCommit AWS-Repository her

Konfigurieren Sie die Pipeline

- CodePipeline AWS-Konsole

Weitere Ressourcen

- CodePipeline AWS-Dokumentation
- CodeCommit AWS-Dokumentation
- Dokumentation zu AWS Device Farm
- Jenkins-Dokumentation
- Jenkins-Installation auf macOS
- CodePipeline AWS-Plugin für Jenkins
- Xcode-Installation
- Installation und Konfiguration von AWS CLI
- Git-Dokumentation

Suchen Sie in den AWS-CDK-Anwendungen oder CloudFormation - Vorlagen nach bewährten Methoden mithilfe von cdk-nag-Regelpaketen

Erstellt von Arun Donti

Übersicht

Dieses Muster erklärt, wie Sie mithilfe des Dienstprogramms cdk-nag mithilfe einer Kombination von Regelpaketen die Anwendungen des AWS Cloud Development Kit (AWS CDK) auf bewährte Methoden überprüfen können. cdk-nag ist ein Open-Source-Projekt, das von cfn_nag inspiriert wurde. Es implementiert Regeln in Evaluierungspaketen wie der AWS Solutions Library, dem Health Insurance Portability and Accountability Act (HIPAA) und dem National Institute of Standards and Technology (NIST) 800-53 mithilfe von AWS CDK Aspects. Sie können Ihre AWS CDK-Anwendungen anhand der Regeln in diesen Paketen auf bewährte Methoden überprüfen, Code anhand von Best Practices erkennen und korrigieren und die Regeln unterdrücken, die Sie in Ihren Evaluierungen nicht verwenden möchten.

Sie können auch cdk-nag verwenden, um Ihre CloudFormation AWS-Vorlagen mithilfe des cloudformation-include-Moduls zu überprüfen.

Informationen zu allen verfügbaren Paketen finden Sie im Abschnitt Regeln des cdk-nag-Repositorys. Evaluierungspakete sind verfügbar für:

- AWS-Lösungsbibliothek
- HIPAA-Sicherheit
- NIST 800-53, Rev. 4
- NIST 800-53 Rev. 5
- Datensicherheitsstandard der Zahlungskartenindustrie (PCI DSS) 3.2.1

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Anwendung, die das AWS-CDK verwendet

Tools

- AWS CDK — Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungsframework zur Definition der Cloud-Infrastruktur im Code und deren Bereitstellung über AWS. CloudFormation
- AWS CloudFormation — AWS CloudFormation hilft Ihnen dabei, Ihre AWS-Ressourcen zu modellieren und einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus zu verwalten. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben, und Sie können sie zusammen als Stack starten und konfigurieren, anstatt Ressourcen einzeln zu verwalten. Sie können Stacks für mehrere AWS-Konten und AWS-Regionen verwalten und bereitstellen.

Epen

Integrieren Sie cdk-nag in Ihre AWS-CDK-Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erfahren Sie mehr über cdk-nag.	Navigiere zum GitHub cdk-nag-Repository und lies dir die Dokumentation durch.	App-Developer
Installieren Sie das cdk-nag-Paket in Ihrer AWS-CDK-Anwendung.	Um cdk-nag in Ihrer AWS CDK-Anwendung verwenden zu können, müssen Sie es zuerst installieren. cdk-nag kann von PyPI, npm und Apache Maven heruntergeladen werden. NuGet Die neuesten Informationen zu verfügbaren Versionen und Download-Speicherorten finden Sie in der Readme-Datei im Repository.	App-Developer
Wählen Sie Ihre NagPacks.	cdk-nag hat verschiedene Regelpakete aufgerufen. NagPacks Jede NagPack	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	enthält Regeln, die einem bestimmten Standard entsprechen. Die AWS-Lösungen NagPack enthalten beispielsweise allgemeine Best Practices, und NIST 800-53 Rev. 5 NagPack kann bei der Einhaltung von Vorschriften helfen. Sie können mehrere Pakete NagPacks auf Ihre Anwendung anwenden und bei Bedarf Pakete hinzufüge n und entfernen. Eine Liste der verfügbaren Pakete finden Sie in der Readme-Datei im GitHub Repository. Informati onen zu den einzelnen Regeln in den einzelnen Paketen finden Sie im Abschnitt Regeln des GitHub Repositorys.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Integrieren Sie cdk-nag in Ihre AWS-CDK-Anwendung.	Sie können cdk-nag auf anwendungsweiter Ebene in Ihre Anwendung integrieren oder es in einzelne Stufen oder Stacks Ihrer Anwendung integrieren. Um beispielsweise die AWS-Lösungen und die HIPAA-Sicherheit auf anwendungsweiter Ebene NagPacks in eine AWS CDK TypeScript v2-Anwendung zu integrieren, können Sie den folgenden Code verwenden:
	
	`import { App, Aspects } from 'aws-cdk-lib';`
	`import { CdkTestStack } from '../lib/cdk-test-stack';`
	`import { AwsSolutionsChecks, HIPAASecurityChecks } from 'cdk-nag';`
	
	`const app = new App();`
	`new CdkTestStack(app, 'CdkNagDemo');`
	`// Simple rule informational messages`
	`Aspects.of(app).add(new AwsSolutionsChecks());`
	`// Additional explanations on the purpose of triggered rules`
	`Aspects.of(app).add(new HIPAASecurityChecks({ verbose: true }));`
		App-Developer

Zugehörige Ressourcen

- cdk-nag-Code-Repository
- cdk-nag im Construct Hub

Konfigurieren Sie die gegenseitige TLS-Authentifizierung für Anwendungen, die auf Amazon EKS ausgeführt werden

Erstellt von Mahendra Siddappa (AWS)

Übersicht

Zertifikatsbasierte Mutual Transport Layer Security (TLS) ist eine optionale TLS-Komponente, die eine bidirektionale Peer-Authentifizierung zwischen Servern und Clients ermöglicht. Bei Mutual TLS müssen Clients während der Sitzungsaushandlung ein X.509-Zertifikat bereitstellen. Der Server verwendet dieses Zertifikat, um den Client zu identifizieren und zu authentifizieren.

Mutual TLS ist eine häufige Anforderung für Internet of Things (IoT) -Anwendungen und kann für business-to-business Anwendungen oder Standards wie Open Banking verwendet werden.

Dieses Muster beschreibt, wie Mutual TLS für Anwendungen, die auf einem Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster ausgeführt werden, mithilfe eines NGINX-Ingress-Controllers konfiguriert wird. Sie können integrierte Mutual TLS-Funktionen für den NGINX-Ingress-Controller aktivieren, indem Sie die Ingress-Ressource mit Anmerkungen versehen. Weitere Informationen zu gegenseitigen TLS-Anmerkungen auf NGINX-Controllern finden Sie in der Kubernetes-Dokumentation unter Authentifizierung mit Client-Zertifikaten.

> **Important**
>
> Dieses Muster verwendet selbstsignierte Zertifikate. Es wird empfohlen, dieses Muster nur mit Testclustern und nicht in Produktionsumgebungen zu verwenden. Wenn Sie dieses Muster in einer Produktionsumgebung verwenden möchten, können Sie AWS Private Certificate Authority (AWS Private CA) oder Ihren bestehenden Public Key Infrastructure (PKI) -Standard verwenden, um private Zertifikate auszustellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS) -Konto.
- Ein vorhandener Amazon-EKS-Cluster.
- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 1.7 oder höher, installiert und konfiguriert auf macOS, Linux oder Windows.

- Das kubectl-Befehlszeilenprogramm, das für den Zugriff auf den Amazon EKS-Cluster installiert und konfiguriert wurde. Weitere Informationen dazu finden Sie unter Installation von kubectl in der Amazon EKS-Dokumentation.
- Ein vorhandener DNS-Name (Domain Name System) zum Testen der Anwendung.

Einschränkungen

- Dieses Muster verwendet selbstsignierte Zertifikate. Es wird empfohlen, dieses Muster nur mit Testclustern und nicht in Produktionsumgebungen zu verwenden.

Architektur

Technologie-Stack

- Amazon EKS
- Amazon Route 53
- Kubectl

Tools

- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen dabei, Kubernetes auf AWS auszuführen, ohne Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten zu müssen.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.
- Kubectl ist ein Befehlszeilenprogramm, das Sie für die Interaktion mit einem Amazon EKS-Cluster verwenden.

Epen

Generieren Sie die selbstsignierten Zertifikate

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie den CA-Schlüssel und das Zertifikat.	Generieren Sie den Schlüssel und das Zertifikat der Zertifizi	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	erungsstelle (CA), indem Sie den folgenden Befehl ausführen. `openssl req -x509 -sha256 -newkey rsa:4096 -keyout ca.key -out ca.crt -days 356 -nodes -subj '/CN=Test Cert Authority'`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie den Serversch lüssel und das Zertifikat und signieren Sie mit dem CA-Zertifikat.	Generieren Sie den Serversch lüssel und das Zertifikat und signieren Sie mit dem CA-Zertifikat, indem Sie den folgenden Befehl ausführen. `openssl req -new -newkey rsa:4096 -keyout server.key -out server.csr -nodes -subj '/CN= <your_domain_name> ' && openssl x509 -req -sha256 -days 365 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out server.crt` **Important** Stellen Sie sicher, dass Sie es `<your_domain_name>` durch Ihren vorhanden en Domainnamen ersetzen.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie den Client-Schlüssel und das Zertifikat und signieren Sie mit dem CA-Zertifikat.	Generieren Sie den Client-Schlüssel und das Zertifikat und signieren Sie mit dem CA-Zertifikat, indem Sie den folgenden Befehl ausführen. `openssl req -new -newkey rsa:4096 -keyout client.key -out client.csr -nodes -subj '/CN=Test' && openssl x509 -req -sha256 -days 365 -in client.csr -CA ca.crt -CAkey ca.key -set_serial 02 -out client.crt`	DevOps Ingenieur

Stellen Sie den NGINX-Ingress-Controller bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den NGINX-Ingress-Controller in Ihrem Amazon EKS-Cluster bereit.	Stellen Sie den NGINX-Ingress-Controller mithilfe des folgenden Befehls bereit. `kubectl apply -f https://raw.githubusercontent.com/kubernetes/ingress-nginx/controller-v1.7.0/deploy/static/provider/aws/deploy.yaml`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass der NGINX-Ingress-Controller-Dienst ausgeführt wird.	Stellen Sie mithilfe des folgenden Befehls sicher, dass der NGINX-Ingress-Controller-Dienst ausgeführt wird. `kubectl get svc -n ingress-nginx` **Important** Stellen Sie sicher, dass das Adressfeld den Domänennamen des Network Load Balancers enthält.	DevOps Ingenieur

Erstellen Sie einen Namespace im Amazon EKS-Cluster, um gegenseitiges TLS zu testen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Namespace im Amazon EKS-Cluster.	Erstellen Sie einen Namespace, `mtls` der in Ihrem Amazon EKS-Cluster aufgerufen wird, indem Sie den folgenden Befehl ausführen. `kubectl create ns mtls` Dadurch wird die Beispielanwendung zum Testen von Mutual TLS bereitgestellt.	DevOps Ingenieur

Erstellen Sie die Bereitstellung und den Service für die Beispielanwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Kubernetes-Bereitstellung und den Dienst im mtls-Namespace.	Erstellen Sie eine Datei namens `mtls.yaml` . Fügen Sie folgenden Code in die Datei ein.
	
	`kind: Deployment`
	`apiVersion: apps/v1`
	`metadata:`
	`  name: mtls-app`
	`  labels:`
	`  app: mtls`
	`spec:`
	`  replicas: 1`
	`  selector:`
	`  matchLabels:`
	`  app: mtls`
	`  template:`
	`  metadata:`
	`  labels:`
	`  app: mtls`
	`  spec:`
	`  containers:`
	`  - name: mtls-app`
	`  image: hashicorp/http-echo`
	`  args:`
	`  - "-text=mTLS is working"`
	
	`---`
	
	`kind: Service`
	`apiVersion: v1`
	`metadata:`
	`  name: mtls-service`
	`spec:`
	`  selector:`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>app: mtls
	ports:
	- port: 5678 #
	Default port for image</pre>
	Erstellen Sie die Kubernetes-Bereitstellung und den Kubernetes-Dienst im `mtls` Namespace, indem Sie den folgenden Befehl ausführen.
	<pre>kubectl create -f
	mtls.yaml -n mtls</pre>	

Stellen Sie sicher, dass die Kubernetes-Bereitstellung erstellt wurde.	Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die Bereitstellung erstellt wurde und einen Pod im Status „Verfügbar“ hat.
	<pre>kubectl get deploy -n
	mtls</pre>
		DevOps Ingenieur

Stellen Sie sicher, dass der Kubernetes-Dienst erstellt wurde.	Stellen Sie sicher, dass der Kubernetes-Dienst erstellt wurde, indem Sie den folgenden Befehl ausführen.
	<pre>kubectl get service -n
	mtls</pre>
		DevOps Ingenieur

Erstellen Sie ein Geheimnis im MTLS-Namespace

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Geheimnis für die Eingangsressource.	Führen Sie den folgenden Befehl aus, um mithilfe der zuvor erstellten Zertifikate ein Geheimnis für den NGINX-Ingress-Controller zu erstellen. `kubectl create secret generic mtls-certs --from-file=tls.crt=server.crt --from-file=tls.key=server.key --from-file=ca.crt=ca.crt -n mtls` Ihr Secret umfasst ein Serverzertifikat für den Client zur Identifizierung des Servers und ein CA-Zertifikat für den Server zur Überprüfung der Client-Zertifikate.	DevOps Ingenieur

Erstellen Sie die Ingress-Ressource im MTLS-Namespace

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Ingress-Ressource im mtls-Namespace.	Erstellen Sie eine Datei namens `ingress.yaml` . Fügen Sie den folgenden Code in die Datei ein (`<your_domain_name>` ersetzen Sie ihn durch Ihren vorhandenen Domainnamen).	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>apiVersion: networkin
	g.k8s.io/v1
	kind: Ingress
	metadata:
	  annotations:
	    nginx.ingress.kube
	rnetes.io/auth-tls-
	verify-client: "on"
	    nginx.ingress.kube
	rnetes.io/auth-tls-
	secret: mtls/mtls-certs
	  name: mtls-ingress
	spec:
	  ingressClassName:
	 nginx
	  rules:
	  - host: "*.<your_
	domain_name>"
	    http:
	      paths:
	      - path: /
	        pathType: Prefix
	        backend:
	          service:
	            name: mtls-
	service
	            port:
	              number:
	 5678
	  tls:
	  - hosts:
	    - "*.<your_
	domain_name>"
	    secretName: mtls-
	certs</pre>
	Erstellen Sie die Ingress-Ressource im `mtls` Namespace, indem Sie den folgenden Befehl ausführen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`kubectl create -f ingress.yaml -n mtls` Das bedeutet, dass der NGINX-Ingress-Controller den Datenverkehr an Ihre Beispielanwendung weiterlei ten kann.	
Stellen Sie sicher, dass die Eingangsressource erstellt wurde.	Stellen Sie sicher, dass die Eingangsressource erstellt wurde, indem Sie den folgenden Befehl ausführen. `kubectl get ing -n mtls` **Important** Stellen Sie sicher, dass die Adresse der Eingangsressource den Load Balancer anzeigt, der für den NGINX-Ingress-Cont roller erstellt wurde.	DevOps Ingenieur

Konfigurieren Sie DNS so, dass der Hostname auf den Load Balancer verweist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen CNAME-Eintrag, der auf den Load Balancer für den NGINX-Ing ress-Controller verweist.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon Route 53 53-Konsole und erstellen	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie einen Canonical Name (CNAME) -Eintrag, der auf den Load Balancer für `mtls.<your_domain_name>` den NGINX-Ingress-Controller verweist. Weitere Informationen finden Sie unter Erstellen von Datensätzen mithilfe der Route 53 53-Konsole in der Route 53 53-Dokumentation.	

Testen der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie das gegenseitige TLS-Setup ohne Zertifikate.	Führen Sie den folgenden Befehl aus. `curl -k https://mtls.<your_domain_name>` Sie sollten die Fehlermeldung „400 Kein erforderliches SSL-Zertifikat wurde gesendet“ erhalten.	DevOps Ingenieur
Testen Sie das gegenseitige TLS-Setup mit Zertifikaten.	Führen Sie den folgenden Befehl aus. `curl -k https://mtls.<your_domain_n`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`ame> --cert client.crt --key client.key` Sie sollten die Antwort „mTLS funktioniert“ erhalten.	

Zugehörige Ressourcen

- Erstellen von Datensätzen mithilfe der Amazon Route 53 53-Konsole
- Verwenden eines Network Load Balancer mit dem NGINX-Ingress-Controller auf Amazon EKS
- Authentifizierung des Client-Zertifikats

Automatisieren Sie die Erstellung von AppStream 2.0-Ressourcen mit AWS CloudFormation

Erstellt von Ram Kandaswamy (AWS)

Übersicht

Dieses Muster enthält Codebeispiele und Schritte zur Automatisierung der Erstellung von Amazon AppStream 2.0-Ressourcen in der Amazon Web Services (AWS) -Cloud mithilfe einer CloudFormation AWS-Vorlage. Das Muster zeigt Ihnen, wie Sie einen CloudFormation AWS-Stack verwenden, um die Erstellung Ihrer AppStream 2.0-Anwendungsressourcen zu automatisieren, einschließlich eines Image Builders, eines Images, einer Flotteninstanz und eines Stacks. Sie können Ihre AppStream 2.0-Anwendung in einem HTML5 -kompatiblen Browser an Endbenutzer streamen, indem Sie entweder den Desktop- oder den Anwendungsbereitstellungsmodus verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Annahme der Allgemeinen Geschäftsbedingungen von AppStream 2.0
- Grundkenntnisse in Bezug auf AppStream Ressourcen wie Stacks, Flotten und Image Builder

Einschränkungen

- Sie können die AWS Identity and Access Management (IAM) -Rolle, die einer AppStream 2.0-Instance zugeordnet ist, nicht ändern, nachdem diese Instance erstellt wurde.
- Sie können keine Eigenschaften (wie das Subnetz oder die Sicherheitsgruppe) auf der AppStream 2.0-Image Builder-Instance ändern, nachdem diese Image Builder-Instance erstellt wurde.

Architektur

Das folgende Diagramm zeigt Ihnen, wie Sie die Erstellung von AppStream 2.0-Ressourcen mithilfe einer CloudFormation AWS-Vorlage automatisieren können.

Das Diagramm zeigt den folgenden Workflow:

1. Sie erstellen eine CloudFormation AWS-Vorlage auf der Grundlage des YAML-Codes im Abschnitt Zusätzliche Informationen dieses Musters.
2. Die CloudFormation AWS-Vorlage erstellt einen CloudFormation AWS-Teststack.
   a. (Optional) Sie erstellen eine Image Builder-Instanz mithilfe von AppStream 2.0.
   b. (Optional) Sie erstellen ein Windows-Abbild mithilfe Ihrer benutzerdefinierten Software.
3. Der CloudFormation AWS-Stack erstellt eine AppStream 2.0-Flotteninstanz und einen Stack.
4. Sie stellen Ihre AppStream 2.0-Ressourcen für Endbenutzer in einem HTML5 -kompatiblen Browser bereit.

Technologie-Stack

- Amazon AppStream 2.0
- AWS CloudFormation

Tools

- Amazon AppStream 2.0 ist ein vollständig verwalteter Anwendungs-Streaming-Service, mit dem Sie von überall aus sofort auf Ihre Desktop-Anwendungen zugreifen können. AppStream 2.0 verwaltet die AWS-Ressourcen, die zum Hosten und Ausführen Ihrer Anwendungen erforderlich sind, skaliert automatisch und bietet Ihren Benutzern bei Bedarf Zugriff.
- AWS CloudFormation hilft Ihnen dabei, Ihre AWS-Ressourcen zu modellieren und einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus zu verwalten. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben und sie zusammen als Stapel zu starten und zu konfigurieren, anstatt Ressourcen einzeln zu verwalten. Sie können Stacks für mehrere AWS-Konten und AWS-Regionen verwalten und bereitstellen.

Epen

(Optional) Erstellen Sie ein AppStream 2.0-Image

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie benutzerdefinierte Software und erstellen Sie ein Image.	1. Installieren Sie die AppStream 2.0-Anwendung, die Sie Ihren Benutzern bereitstellen möchten. 2. Verwenden Sie den Photon Create Image Agent oder ein PowerShell Skript, um ein neues Windows-Image für Ihre benutzerdefinierte Software zu erstellen. **Note** Erwägen Sie, die AppLocker Windows-Funktion zu verwenden, um das Bild weiter zu sperren.	AWS DevOps, Cloud-Architekt

Stellen Sie die CloudFormation AWS-Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die CloudFormation AWS-Vorlage.	1. Speichern Sie den Code im Abschnitt Zusätzliche Informationen dieses Musters als YAML-Datei.	AWS-Systemadministrator, Cloud-Administrator, Cloud-Architekt, Allgemeines AWS, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Aktualisieren Sie die YAML-Datei mit den erforderlichen Werten für die Parameter in Ihrer Umgebung.	
Erstellen Sie mithilfe der Vorlage einen CloudFormation AWS-Stack.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudFormation AWS-Konsole. 2. Wählen Sie im Navigationsbereich Stacks aus. 3. Wählen Sie Stack erstellen und dann Mit neuen Ressourcen (Standard) aus. 4. Wählen Sie im Abschnitt Voraussetzung — Vorlage vorbereiten die Option Vorlage ist bereit aus. 5. Wählen Sie im Abschnitt Vorlage angeben die Option Vorlagendatei hochladen aus. 6. Wählen Sie Datei auswählen und wählen Sie dann Ihre aktualisierte CloudFormation AWS-Vorlage aus. 7. Führen Sie die restlichen Schritte im Assistenten aus, um Ihren Stack zu erstellen.	App-Besitzer, AWS-Systemadministrator, Windows-Ingenieur

Zugehörige Ressourcen

Referenzen

- Erste Schritte mit Amazon AppStream 2.0: Einrichtung mit Beispielanwendungen
- Erstellen Sie eine AppStream 2.0-Flotte und einen Stack

Anleitungen und Videos

- Amazon AppStream 2.0-Benutzerworkflow
- So migrieren Sie eine ältere Windows Forms-App zu Amazon AppStream 2.0
- AWS re:Invent 2018: Sichere Bereitstellung von Desktop-Anwendungen mit Amazon AppStream 2.0 (01) BAP2

Zusätzliche Informationen

Der folgende Code ist ein Beispiel für eine CloudFormation AWS-Vorlage, mit der Sie automatisch AppStream 2.0-Ressourcen erstellen können.

```
AWSTemplateFormatVersion: 2010-09-09
Parameters:
  SubnetIds:
    Type: 'List<AWS::EC2::Subnet::Id>'
  testSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup::Id'
  ImageName:
    Type: String
Resources:

  AppStreamFleet:
    Type: 'AWS::AppStream::Fleet'
    Properties:
      ComputeCapacity:
        DesiredInstances: 5
      InstanceType: stream.standard.medium
      Name: appstream-test-fleet
      DisconnectTimeoutInSeconds: 1200
      FleetType: ON_DEMAND
      IdleDisconnectTimeoutInSeconds: 1200
      ImageName: !Ref ImageName
```

```
      MaxUserDurationInSeconds: 345600
      VpcConfig:
        SecurityGroupIds:
          - !Ref testSecurityGroup
        SubnetIds: !Ref SubnetIds
  AppStreamStack:
    Type: 'AWS::AppStream::Stack'
    Properties:
      Description: AppStream stack for test
      DisplayName: AppStream test Stack
      Name: appstream-test-stack
      StorageConnectors:
        - ConnectorType: HOMEFOLDERS
      UserSettings:
        - Action: CLIPBOARD_COPY_FROM_LOCAL_DEVICE
          Permission: ENABLED
        - Action: CLIPBOARD_COPY_TO_LOCAL_DEVICE
          Permission: ENABLED
        - Action: FILE_DOWNLOAD
          Permission: ENABLED
        - Action: PRINTING_TO_LOCAL_DEVICE
          Permission: ENABLED
  AppStreamFleetAssociation:
    Type: 'AWS::AppStream::StackFleetAssociation'
    Properties:
      FleetName: appstream-test-fleet
      StackName: appstream-test-stack
    DependsOn:
      - AppStreamFleet
      - AppStreamStack
```

Erstellen Sie einen benutzerdefinierten Protokollparser für Amazon ECS mithilfe eines Firelens-Protokollrouters

Erstellt von Varun Sharma (AWS)

Übersicht

Firelens ist ein Protokollrouter für Amazon Elastic Container Service (Amazon ECS) und AWS Fargate. Sie können Firelens verwenden, um Container-Logs von Amazon ECS an Amazon CloudWatch und andere Ziele (z. B. Splunk oder Sumo Logic) weiterzuleiten. Firelens arbeitet mit Fluentd oder Fluent Bit als Protokollierungsagent, was bedeutet, dass Sie Amazon ECS-Aufgabendefinitionsparameter verwenden können, um Protokolle weiterzuleiten.

Wenn Sie sich dafür entscheiden, Protokolle auf Quellenebene zu analysieren, können Sie Ihre Protokolldaten analysieren und Abfragen durchführen, um effizienter und effektiver auf betriebliche Probleme zu reagieren. Da verschiedene Anwendungen unterschiedliche Protokollierungsmuster haben, müssen Sie einen benutzerdefinierten Parser verwenden, der die Protokolle strukturiert und die Suche am Zielort erleichtert.

Dieses Muster verwendet einen Firelens-Protokollrouter mit einem benutzerdefinierten Parser, um Protokolle CloudWatch von einer Spring Boot-Beispielanwendung, die auf Amazon ECS ausgeführt wird, zu übertragen. Anschließend können Sie Amazon CloudWatch Logs Insights verwenden, um die Protokolle auf der Grundlage benutzerdefinierter Felder zu filtern, die vom benutzerdefinierten Parser generiert werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS) -Konto.
- AWS-Befehlszeilenschnittstelle (AWS CLI), auf Ihrem lokalen Computer installiert und konfiguriert.
- Docker, auf Ihrem lokalen Computer installiert und konfiguriert.
- Eine bestehende Spring Boot-basierte containerisierte Anwendung in Amazon Elastic Container Registry (Amazon ECR).

Architektur

Technologie-Stack

- CloudWatch
- Amazon ECR
- Amazon ECS
- Fargate
- Docker
- Fluent Bit

Tools

- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) ist ein von AWS verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Stoppen und Verwalten von Containern in einem Cluster vereinfacht.
- AWS Identity and Access Management (IAM) — IAM ist ein Webservice zur sicheren Steuerung des Zugriffs auf AWS-Services.
- AWS CLI — AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Docker — Docker ist eine offene Plattform für die Entwicklung, den Versand und den Betrieb von Anwendungen.

Code

Die folgenden Dateien sind an dieses Muster angehängt:

- `customFluentBit.zip`— Enthält die Dateien zum Hinzufügen der benutzerdefinierten Analyse und Konfigurationen.
- `firelens_policy.json`— Enthält das Richtliniendokument zur Erstellung einer IAM-Richtlinie.
- `Task.json`— Enthält eine Beispielaufgabendefinition für Amazon ECS.

Epen

Erstellen Sie ein benutzerdefiniertes Fluent Bit-Bild

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon-ECR-Repository.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon ECR-Konsole und erstellen Sie ein Repository namens `fluentbit_custom` . Weitere Informationen dazu finden Sie unter Erstellen eines Repositorys in der Amazon ECR-Dokumentation.	Systemadministrator, Entwickler
Entpacken Sie das customFluentBit ZIP-Paket.	1. Laden Sie das `customFluentBit.zip` Paket (angehängt) auf Ihren lokalen Computer herunter. 2. Entpacken Sie das Paket in das `customFluentBit` Verzeichnis, indem Sie den folgenden Befehl ausführen: `unzip -d customFluentBit.zip` 3. Das Verzeichnis enthält die folgenden Dateien, die für das Hinzufügen der benutzerdefinierten Analyse und Konfigurationen erforderlich sind:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `parsers/springboot_parser.conf` — Enthält die Parser-Direktive und definiert das reguläre Ausdrucksmuster (Regex) für den benutzerdefinierten Parser. Sie können das Regex-Muster für Ihren spezifischen Parser hinzufügen. • `conf/parse_springboot.conf` — Enthält den Filter und die Service-Direktive. • Das Dockerfile	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das benutzerd efinierte Docker-Image.	1. Ändern Sie das Verzeichnis in `customFluentBit .` 2. Öffnen Sie die Amazon ECR-Konsole, wählen Sie das `fluentbit_custom` Repository aus und wählen Sie dann Push-Befehle anzeigen. 3. Laden Sie Ihr Projekt hoch. 4. Nachdem der Upload abgeschlossen ist, kopieren Sie die URL des Builds. Diese URL ist erforderlich, wenn Sie einen Container in Amazon ECS erstellen Weitere Informationen dazu finden Sie unter Pushing a Docker-Image in der Amazon ECR-Dokumentation.	Systemadministrator, Entwickler

Den Amazon ECS-Cluster einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon-ECS-Cluster.	Erstellen Sie einen Amazon ECS-Cluster, indem Sie den Anweisungen im Abschnitt Nur Netzwerkvorlage unter Cluster erstellen in der Amazon ECS-Dokumentation folgen.	Systemadministrator, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Stellen Sie sicher, dass Sie Create VPC wählen, um eine neue Virtual Private Cloud (VPC) für Ihren Amazon ECS-Cluster zu erstellen.	

Die Amazon ECS-Aufgabe einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die IAM-Rolle für die Amazon ECS-Aufgabenausführung ein.	Erstellen Sie mithilfe der `AmazonECSTaskExecutionRolePolicy` verwalteten Richtlinie eine Amazon ECS-IAM-Rolle für die Ausführung von Aufgaben. Weitere Informationen dazu finden Sie in der Amazon ECS-Dokumentation unter IAM-Rolle für die Ausführung von Aufgaben in Amazon ECS. **Note** Stellen Sie sicher, dass Sie den Amazon-Ressourcennamen	Systemadministrator, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(ARN) der IAM-Rolle aufzeichnen.	
Fügen Sie die IAM-Richtlinie der IAM-Rolle für die Amazon ECS-Aufgabenausführung hinzu.	1. Erstellen Sie mithilfe des `firelens_policy.json` (angehängten) Richtliniendokuments eine IAM-Richtlinie. Weitere Informationen dazu finden Sie in der IAM-Dokumentation unter Richtlinien auf der Registerkarte JSON erstellen. 2. Fügen Sie diese Richtlinie der IAM-Rolle für die Amazon ECS-Aufgabenausführung hinzu, die Sie zuvor erstellt haben. Weitere Informationen dazu finden Sie unter Hinzufügen von IAM-Richtlinien (AWS CLI) in der IAM-Dokumentation.	Systemadministrator, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Amazon ECS-Aufgabendefinition ein.	1. Aktualisieren Sie die folgenden Abschnitte in der `Task.json` Beispielaufgabendefinition (im Anhang): • Aktualisieren Sie das `executionRoleArn` und `taskRoleArn` mit dem ARN der IAM-Rolle zur Aufgabenausführung • Aktualisieren Sie das Image `containerDefinitions` mit dem benutzerdefinierten Fluent Bit Docker-Image, das Sie zuvor erstellt haben • Aktualisieren Sie das Image `containerDefinitions` mit dem Namen Ihres Anwendungs-Images 2. Öffnen Sie die Amazon ECS-Konsole, wählen Sie Aufgabendefinitionen, wählen Sie Neue Aufgabendefinition erstellen und wählen Sie dann Fargate auf der Seite Kompatibilitäten auswählen aus. 3. Wählen Sie Configure via Json, fügen Sie die aktualisi	Systemadministrator, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	erte **`Task.json`** Datei in den Textbereich ein und wählen Sie dann Speichern. 4. Erstellen Sie die Aufgabend efinition. Weitere Informationen dazu finden Sie unter Erstellen einer Aufgabendefinition in der Amazon ECS-Dokumentation.	

Führen Sie die Amazon ECS-Aufgabe aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Amazon ECS-Aufgabe aus.	Wählen Sie in der Amazon ECS-Konsole Clusters, wählen Sie den Cluster aus, den Sie zuvor erstellt haben, und führen Sie dann die eigenstän dige Aufgabe aus. Weitere Informationen dazu finden Sie unter Ausführen einer eigenständigen Aufgabe in der Amazon ECS-Dokum entation.	Systemadministrator, Entwickler

Überprüfen Sie die CloudWatch Protokolle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Protokolle.	1. Öffnen Sie die CloudWatc h Konsole, wählen	Systemadministrator, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie Protokollgruppen und dann`/aws/ecs/containerinsights/{{cluster_ARN}}/firelens/application` . 2. Überprüfen Sie die Protokolle, insbesondere die benutzerdefinierten Felder, die vom benutzerdefinierten Parser hinzugefügt wurden. 3. Wird verwendet CloudWatch , um Protokolle auf der Grundlage der benutzerdefinierten Felder zu filtern.	

Zugehörige Ressourcen

- Docker-Grundlagen für Amazon ECS
- Amazon ECS auf AWS Fargate
- Konfiguration grundlegender Serviceparameter

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Erstellen Sie eine Pipeline und ein AMI mit CodePipeline und HashiCorp Packer

Erstellt von Akash Kumar (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Dieses Muster enthält Codebeispiele und Schritte zum Erstellen sowohl einer Pipeline in der Amazon Web Services (AWS) -Cloud mithilfe von AWS CodePipeline als auch eines Amazon Machine Image (AMI) mithilfe von HashiCorp Packer. Das Muster basiert auf der Praxis der kontinuierlichen Integration, die das Erstellen und Testen von Code mit einem Git-basierten Versionskontrollsystem automatisiert. In diesem Muster erstellen und klonen Sie mithilfe von AWS ein Code-Repository CodeCommit. Erstellen Sie anschließend ein Projekt und konfigurieren Sie Ihren Quellcode mithilfe von AWS CodeBuild. Erstellen Sie abschließend ein AMI, das in Ihr Repository übernommen wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Amazon Linux AMI zum Starten von Amazon Elastic Compute Cloud (Amazon EC2) -Instances
- HashiCorp Packer 0.12.3 oder höher
- CloudWatch Amazon-Veranstaltungen (optional)
- CloudWatch Amazon-Protokolle (optional)

Architektur

Das folgende Diagramm zeigt ein Beispiel für Anwendungscode, der die Erstellung eines AMI mithilfe der Architektur dieses Musters automatisiert.

Das Diagramm zeigt den folgenden Workflow:

1. Der Entwickler überträgt Codeänderungen in ein privates CodeCommit Git-Repository. Wird dann CodePipeline verwendet, CodeBuild um den Build zu initiieren und dem Amazon Simple Storage Service (Amazon S3) -Bucket neue Artefakte hinzuzufügen, die für die Bereitstellung bereit sind.

2. CodeBuild verwendet Packer, um das AMI auf der Grundlage einer JSON-Vorlage zu bündeln und zu verpacken. Wenn diese Option aktiviert ist, können CloudWatch Events die Pipeline automatisch starten, wenn eine Änderung im Quellcode auftritt.

Technologie-Stack

- CodeBuild
- CodeCommit
- CodePipeline
- CloudWatch Ereignisse (optional)

Tools

- AWS CodeBuild — AWS CodeBuild ist ein vollständig verwalteter Build-Service in der Cloud. CodeBuild kompiliert Ihren Quellcode, führt Komponententests durch und produziert Artefakte, die sofort einsatzbereit sind.
- AWS CodeCommit — AWS CodeCommit ist ein Versionskontrollservice, mit dem Sie Git-Repositorys privat in der AWS-Cloud speichern und verwalten können. CodeCommit macht es für Sie überflüssig, Ihr eigenes Quellcodeverwaltungssystem zu verwalten oder sich Gedanken über die Skalierung der Infrastruktur zu machen.
- AWS CodePipeline — AWS CodePipeline ist ein Continuous Delivery Service, mit dem Sie die zur Veröffentlichung Ihrer Software erforderlichen Schritte modellieren, visualisieren und automatisieren können.
- HashiCorp Packer — HashiCorp Packer ist ein Open-Source-Tool zur Automatisierung der Erstellung identischer Maschinenabbilder aus einer einzigen Quellkonfiguration. Packer ist leichtgewichtig, läuft auf allen gängigen Betriebssystemen und erstellt Maschinenabbilder für mehrere Plattformen parallel.

Code

Dieses Muster umfasst die folgenden Anlagen:

- `buildspec.yml`— Diese Datei wird verwendet CodeBuild , um ein Artefakt für die Bereitstellung zu erstellen und zu erstellen.

- `amazon-linux_packer-template.json`— Diese Datei verwendet Packer, um ein Amazon Linux AMI zu erstellen.

Epen

Richten Sie das Code-Repository ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Repository.	Erstellen Sie ein CodeCommit Repository.	AWS-Systemadministrator
Klonen Sie das Repository	Connect zum CodeCommit Repository her, indem Sie das Repository klonen.	App-Developer
Übertragen Sie den Quellcode in das Remote-Repository.	1. Erstellen Sie einen Commit, um die `amazon-linux_packer-template.json` Dateien `buildspec.yml` und zu Ihrem lokalen Repository hinzuzufügen. 2. Übertragen Sie den Commit von Ihrem lokalen Repository in das CodeCommit Remote-Repository.	App-Developer

Erstellen Sie ein CodeBuild Projekt für die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Build-Projekt.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die CodeBuild AWS-Konso	App-Entwickler, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	le und wählen Sie dann Create build project aus. 2. Geben Sie unter Projektname den Namen Ihres Projekts ein. 3. Wählen Sie als Quellanbieter AWS aus CodeCommit. 4. Wählen Sie für Repository das Repository aus, in dem Sie die Code-Pipeline erstellen möchten. 5. Wählen Sie für Umgebungs-Image die Option Verwaltetes Image oder Benutzerdefiniertes Image aus. 6. Wählen Sie für Operating system (Betriebssystem) die Option Ubuntu aus. 7. Wählen Sie für RunTime(s) die Option Standard. 8. Wählen Sie für Bild: 4.0aws/codebuild/standard. 9. Wählen Sie für Image-Version die Option Immer das neueste Image für diese Runtime-Version verwenden aus. 10. Wählen Sie für Umgebung die Option Linux aus. 11 Aktivieren Sie das Kontrollkästchen Privilegiert.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	12. Wählen Sie für Servicerolle die Option Neue Servicerolle oder Bestehende Servicerolle aus. 13. Wählen Sie für Buildspezifikationen die Option Buildspec-Datei verwenden oder Build-Befehle einfügen aus. 14. (Optional) Wählen Sie im Abschnitt Artefakte für Typ die Option Keine Artefakte aus. 15. (Empfohlen) Um Build-Output-Logs in Logs hochzuladen, wählen Sie CloudWatch Logs aus. CloudWatch 16. (Optional) Um Build-Ausgabeprotokolle auf Amazon S3 hochzuladen, aktivieren Sie das Kontrollkästchen S3-Protokolle. 17. Wählen Sie Create build project (Build-Projekt erstellen) aus.	

Richten Sie die Pipeline ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Pipeline-Name	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die	App-Entwickler, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CodePipeline AWS-Konsole und wählen Sie dann Create Pipeline aus. 2. Geben Sie unter Pipeline-Name einen Namen für die Pipeline ein. 3. Wählen Sie für Servicerolle die Option Neue Servicerolle oder Bestehende Servicerolle aus. 4. Geben Sie unter Role name (Rollenname) einen Namen für Ihre Rolle ein. 5. Wählen Sie im Abschnitt Erweiterte Einstellungen für Artifact Store die Option Standardstandort aus, wenn Amazon S3 einen Bucket erstellen und die Artefakte im Bucket speichern soll. Um einen vorhandenen S3-Bucket zu verwenden, wählen Sie Benutzerdefinierter Speicherort. Wählen Sie Weiter aus. 6. Wählen Sie als Quellanbieter AWS aus CodeCommit. 7. Wählen Sie als Repository-Name das Repository aus, das Sie zuvor geklont haben. Wählen Sie als Branch-Name Ihren Quellcode-Branch aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Wählen Sie für Optionen zur Änderungserkennung Amazon CloudWatch Events (empfohlen), um die Pipeline zu starten, oder AWS CodePipeline, um regelmäßig nach Änderungen zu suchen. Wählen Sie Weiter aus. 9. Wählen Sie als Build-Anbieter AWS aus CodeBuild. 10. Wählen Sie als Projektname das Build-Projekt aus, das Sie im Epic Ein CodeBuild Projekt für die Anwendung erstellen erstellt haben. 11. Wählen Sie Ihre Build-Optionen aus und klicken Sie dann auf Weiter. 12. Wählen Sie „Bereitstellungsphase überspringen“. 13. Wählen Sie Create pipeline (Pipeline erstellen) aus.	

Zugehörige Ressourcen

- Arbeiten mit Repositorys in AWS CodeCommit
- Arbeit mit Build-Projekten
- Arbeiten mit Pipelines in CodePipeline

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Erstellen Sie eine Pipeline und stellen Sie Artefaktaktualisierungen für lokale Instanzen EC2 bereit mit CodePipeline

Erstellt von Akash Kumar (AWS) und Sandeep Reddy Jogammagari (AWS)

Übersicht

Dieses Muster enthält Codebeispiele und Schritte zum Erstellen einer Pipeline in der Amazon Web Services (AWS) -Cloud und zum Bereitstellen aktualisierter Artefakte für lokale Amazon Elastic Compute Cloud (Amazon EC2) -Instances in AWS CodePipeline. Das Muster basiert auf der Praxis der kontinuierlichen Integration. Diese Vorgehensweise automatisiert das Erstellen und Testen von Code mit einem Git-basierten Versionskontrollsystem. In diesem Muster erstellen und klonen Sie mithilfe von AWS ein Code-Repository CodeCommit. Anschließend erstellen Sie ein Projekt und konfigurieren Ihren Quellcode mithilfe von AWS CodeBuild. Schließlich erstellen Sie Ihre Anwendung und konfigurieren ihre Zielumgebung für lokale EC2 Instances mithilfe von AWS CodeDeploy.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Benutzerdefinierte Tags zur Identifizierung von EC2 Instanzen während der Bereitstellung
- CodeDeploy Agent, auf EC2 Instanzen installiert
- Ihre erforderliche Runtime-Software, auf EC2 Instanzen installiert
- Amazon Corretto 8 für das Java Development Kit
- Apache Tomcat-Webserver, installiert
- CloudWatch Amazon-Veranstaltungen (optional)
- Ein key pair für die Anmeldung am Webserver (optional)
- Ein Apache Maven-Anwendungsprojekt für eine Webanwendung

Architektur

Das folgende Diagramm zeigt ein Beispiel für eine Java-Webanwendung, die mithilfe der Architektur dieses Musters auf lokalen EC2 Instanzen bereitgestellt wird.

Das Diagramm zeigt den folgenden Workflow:

1. Der Entwickler überträgt Codeänderungen in ein privates CodeCommit Git-Repository.
2. CodePipeline verwendet CodeBuild , um den Build zu initiieren und neue Artefakte hinzuzufügen, die für die Bereitstellung im Amazon Simple Storage Service (Amazon S3) -Bucket bereit sind.
3. CodePipeline verwendet den CodeDeploy Agenten, um alle Abhängigkeiten vorzuinstallieren, die für die Änderungen am Bereitstellungsartefakt erforderlich sind.
4. CodePipeline verwendet den CodeDeploy Agenten, um die Artefakte aus dem S3-Bucket auf EC2 Zielinstanzen bereitzustellen. Wenn diese Option aktiviert ist, können CloudWatch Events die Pipeline automatisch starten, wenn eine Änderung im Quellcode auftritt.

Technologie-Stack

- CodeBuild
- CodeCommit
- CodeDeploy
- CodePipeline
- CloudWatch Ereignisse (optional)

Tools

- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Komponententests ausführen und bereitstellungsbereite Artefakte erstellen können. CodeBuild kompiliert Ihren Quellcode, führt Komponententests durch und erzeugt Artefakte, die sofort einsatzbereit sind.
- AWS CodeCommit ist ein Versionskontrollservice, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodeDeploy automatisiert Bereitstellungen auf Amazon Elastic Compute Cloud (Amazon EC2) oder lokalen Instances, AWS Lambda Lambda-Funktionen oder Amazon Elastic Container Service (Amazon ECS) -Services.
- AWS CodePipeline hilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.

Code

Dieses Muster umfasst die folgenden Anlagen:

- `buildspec.yml`— Diese Datei spezifiziert die Aktionen, die CodeBuild erforderlich sind, um ein Artefakt für die Bereitstellung zu erstellen und zu erstellen.
- `appspec.yml`— Diese Datei spezifiziert die Aktionen, die CodeDeploy erforderlich sind, um eine Anwendung zu erstellen und eine Zielumgebung für lokale EC2 Instanzen zu konfigurieren.
- `install_dependencies.sh`— Diese Datei installiert Abhängigkeiten für den Apache Tomcat-Webserver.
- `start_server.sh`— Diese Datei startet den Apache Tomcat-Webserver.
- `stop_server.sh`— Diese Datei stoppt den Apache Tomcat-Webserver.

Epen

Richten Sie das Code-Repository ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Repository.	Erstellen Sie ein CodeCommit Repository.	AWS-Systemadministrator
Klonen Sie das Repository	Connect zum CodeCommit Repository her, indem Sie das Repository klonen.	App-Developer
Übertragen Sie den Quellcode in das Remote-Repository.	1. Erstellen Sie einen Commit, um die `appspec.yml` Dateien `buildspec.yml` und zu Ihrem lokalen Repository hinzuzufügen. 2. Übertragen Sie den Commit von Ihrem lokalen Repository in das CodeCommit Remote-Repository.	App-Developer

Erstellen Sie ein CodeBuild Projekt für die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Build-Projekt.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die CodeBuild AWS-Konsole und wählen Sie dann Create build project aus. 2. Geben Sie unter Projektname den Namen Ihres Projekts ein. 3. Wählen Sie als Quellanbieter AWS aus CodeCommit. 4. Wählen Sie für Repository das Repository aus, in dem Sie die Code-Pipeline erstellen möchten. 5. Wählen Sie für Umgebungs-Image die Option Verwaltetes Image oder Benutzerdefiniertes Image aus. 6. Wählen Sie für Operating system (Betriebssystem) die Option Amazon Linux 2 aus. **Note** Amazon Linux 2 nähert sich dem Ende des Supports. Weitere Informationen finden Sie	AWS-Administrator, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	unter Amazon Linux FAQs 2. 7. Wählen Sie für RunTime(s) Standard. 8. Wählen Sie für Image die Option aws/codebuild/amazonlinux2-aarch64-standard:2.0 aus. 9. Wählen Sie für Image-Version die Option Immer das neueste Image für diese Runtime-Version verwenden aus. 10. Wählen Sie für Servicerolle die Option Neue Servicerolle oder Bestehende Servicerolle aus. 11. Wählen Sie für Buildspezifikationen die Option Buildspec-Datei verwenden oder Build-Befehle einfügen aus. 12. (Optional) Wählen Sie Artefakt hinzufügen, um Artefakte zu konfigurieren. 13. (Optional) Um Build-Output-Logs auf Amazon hochzuladen CloudWatch, wählen Sie CloudWatch Logs.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	14. Wählen Sie Create build project (Build-Projekt erstellen) aus.	

Konfigurieren Sie die Bereitstellung von Artefakten für lokale Instanzen EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Anwendung.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die CodeDeploy AWS-Konsole und wählen Sie dann Anwendung erstellen. 2. Geben Sie unter Anwendungsname einen Namen für Ihre Anwendung ein. 3. Wählen Sie für Compute-Plattform EC2 /On-premises aus. 4. Wählen Sie Anwendung erstellen und dann Bereitstellungsgruppe erstellen aus. 5. Geben Sie unter Name der Bereitstellungsgruppe einen Namen ein. 6. **Note** Erstellen Sie eine Servicerolle für CodeDeploy. : Die Servicerolle muss	AWS-Systemadministrator, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	über Berechtig ungen verfügen, um CodeDeploy Zugriff auf Ihre Zielumgeb ung zu gewähren. 7. Wählen Sie unter Servicero lle die Servicerolle aus, die Sie in Schritt 6 erstellt haben. 8. Wählen Sie je nach Ihren Geschäftsanforderungen als Bereitstellungstyp entweder Direkt vor Ort oder Blau/Grün aus. 9. Wählen Sie für die Umgebungskonfiguration die Optionen aus, die Ihren Geschäftsanforderungen entsprechen. 10. (Optional) Erstellen Sie eine separate Zielgruppe für Ihren Load Balancer in der EC2 Amazon-Konsole und kehren Sie dann zur Seite „Bereitstellungsgruppe erstellen“ der CodeDeploy AWS-Konsole zurück, um Ihren Load Balancer und Ihre Zielgruppe auszuwähl en. 11. Wählen Si Create deployment group (Bereitst ellungsgruppe erstellen).	

Richten Sie die Pipeline ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Pipeline.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die CodePipeline AWS-Konsole und wählen Sie dann Create Pipeline aus. 2. Geben Sie unter Pipeline-Name einen Namen für die Pipeline ein. 3. Wählen Sie für Servicerolle die Option Neue Servicerolle oder Bestehende Servicerolle aus. 4. Geben Sie unter Role name (Rollenname) einen Namen für Ihre Rolle ein. 5. Wählen Sie im Abschnitt Erweiterte Einstellungen für Artifact Store die Option Standardstandort aus, wenn Amazon S3 einen Bucket erstellen und die Artefakte im Bucket speichern soll. Um einen vorhandenen S3-Bucket zu verwenden, wählen Sie Benutzerdefinierter Speicherort. Wählen Sie Weiter aus. 6. Wählen Sie als Quellanbieter AWS aus CodeCommit.	AWS-Systemadministrator, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Wählen Sie als Repository-Name das Repository aus, das Sie zuvor geklont haben. Wählen Sie als Branch-Name Ihren Quellcode-Branch aus. 8. Wählen Sie für Optionen zur Änderungserkennung Amazon CloudWatch Events (empfohlen) oder AWS CodePipeline. Wählen Sie Weiter aus. 9. Wählen Sie als Build-Anbieter AWS aus CodeBuild. 10. Wählen Sie als Projektname das Build-Projekt aus, das Sie im Abschnitt CodeBuild Projekt für die Anwendung erstellen dieses Musters erstellt haben. 11. Wählen Sie Ihre Build-Optionen und dann Weiter. 12. Wählen Sie für Deploy Provider die Option AWS aus CodeDeploy. 13. Wählen Sie einen Anwendungsnamen und eine Bereitstellungsgruppe aus und klicken Sie dann auf Weiter. 14. Wählen Sie Create pipeline (Pipeline erstellen) aus.	

Zugehörige Ressourcen

- Arbeiten mit Repositorys in AWS CodeCommit
- Arbeit mit Build-Projekten
- Arbeiten mit Anwendungen in CodeDeploy
- Arbeiten mit Pipelines in CodePipeline

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Automatisches Erstellen dynamischer CI-Pipelines für Java- und Python-Projekte

Erstellt von Aromal Raj Jayarajan (AWS), Amarnath Reddy (AWS), MAHESH RAGHUNANDANAN (AWS) und Vijesh Vijayakumaran Nair (AWS)

Übersicht

AWS CodeCommit Hinweis: ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Dieses Muster zeigt, wie dynamische CI-Pipelines (Continuous Integration) für Java- und Python-Projekte mithilfe der AWS-Entwicklertools automatisch erstellt werden.

Mit der Diversifizierung der Technologie-Stacks und der Zunahme der Entwicklungsaktivitäten kann es schwierig werden, CI-Pipelines zu erstellen und aufrechtzuerhalten, die unternehmensweit einheitlich sind. Durch die Automatisierung des Prozesses in AWS Step Functions können Sie sicherstellen, dass Ihre CI-Pipelines in ihrer Verwendung und Herangehensweise konsistent sind.

Um die Erstellung dynamischer CI-Pipelines zu automatisieren, verwendet dieses Muster die folgenden Variableneingaben:

- Programmiersprache (nur Java oder Python)
- Pipeline-Name
- Erforderliche Pipeline-Stufen

> **Note**
>
> Step Functions orchestriert die Pipeline-Erstellung mithilfe mehrerer AWS-Services. Weitere Informationen zu den in dieser Lösung verwendeten AWS-Services finden Sie im Abschnitt Tools dieses Musters.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

- Ein Amazon S3 S3-Bucket in derselben AWS-Region, in der diese Lösung bereitgestellt wird
- Ein AWS Identity and Access Management (IAM) -Prinzipal, der über die CloudFormation AWS-Berechtigungen verfügt, die zum Erstellen der für diese Lösung benötigten Ressourcen erforderlich sind

Einschränkungen

- Dieses Muster unterstützt nur Java- und Python-Projekte.
- Die in diesem Muster bereitgestellten IAM-Rollen folgen dem Prinzip der geringsten Rechte. Die Berechtigungen der IAM-Rollen müssen auf der Grundlage der spezifischen Ressourcen aktualisiert werden, die Ihre CI-Pipeline erstellen muss.

Architektur

Zieltechnologie-Stack

- AWS CloudFormation
- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- IAM
- Amazon Simple Storage Service (Amazon-S3)
- AWS Systems Manager
- AWS Step Functions
- AWS Lambda
- Amazon-DynamoDB

Zielarchitektur

Das folgende Diagramm zeigt einen Beispiel-Workflow für die automatische Erstellung dynamischer CI-Pipelines für Java- und Python-Projekte mithilfe von AWS-Entwicklertools.

Das Diagramm zeigt den folgenden Workflow:

1. Ein AWS-Benutzer stellt die Eingabeparameter für die CI-Pipeline-Erstellung im JSON-Format bereit. Diese Eingabe startet einen Step Functions Functions-Workflow (State Machine), der mithilfe von AWS-Entwicklertools eine CI-Pipeline erstellt.
2. Eine Lambda-Funktion liest einen Ordner mit dem Namen input-reference, der in einem Amazon S3 S3-Bucket gespeichert ist, und generiert dann eine buildspec.yml-Datei. Diese generierte Datei definiert die CI-Pipeline-Stufen und wird wieder in demselben Amazon S3 S3-Bucket gespeichert, in dem die Parameterreferenzen gespeichert sind.
3. Step Functions überprüft die Abhängigkeiten des Workflows zur Erstellung der CI-Pipeline auf Änderungen und aktualisiert den Abhängigkeitsstapel nach Bedarf.
4. Step Functions erstellt die CI-Pipeline-Ressourcen in einem CloudFormation Stack, einschließlich eines CodeCommit Repositorys, eines CodeBuild Projekts und einer CodePipeline Pipeline.
5. Der CloudFormation Stack kopiert den Beispielquellcode für den ausgewählten Technologie-Stack (Java oder Python) und die Datei buildspec.yml in das Repository. CodeCommit
6. Die Laufzeitdetails der CI-Pipeline werden in einer DynamoDB-Tabelle gespeichert.

Automatisierung und Skalierung

- Dieses Muster ist nur für die Verwendung in einer einzigen Entwicklungsumgebung vorgesehen. Für die Verwendung in mehreren Entwicklungsumgebungen sind Konfigurationsänderungen erforderlich.
- Um Unterstützung für mehr als einen CloudFormation Stack hinzuzufügen, können Sie zusätzliche CloudFormation Vorlagen erstellen. Weitere Informationen finden Sie CloudFormation in der CloudFormation Dokumentation unter Erste Schritte mit AWS.

Tools

Tools

- AWS Step Functions ist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.

- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Komponententests ausführen und bereitstellungsbereite Artefakte erstellen können.
- AWS CodeCommit ist ein Versionskontrollservice, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodePipeline hilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Key Management Service (AWS KMS) unterstützt Sie bei der Erstellung und Kontrolle kryptografischer Schlüssel, um Ihre Daten zu schützen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- AWS Systems Manager Parameter Store bietet sicheren, hierarchischen Speicher für die Verwaltung von Konfigurationsdaten und Geheimnissen.

Code

Der Code für dieses Muster ist im GitHub automated-ci-pipeline-creationRepository verfügbar. Das Repository enthält die CloudFormation Vorlagen, die zur Erstellung der in diesem Muster beschriebenen Zielarchitektur erforderlich sind.

Bewährte Methoden

- Geben Sie Anmeldeinformationen (Geheimnisse) wie Token oder Passwörter nicht direkt in CloudFormation Vorlagen oder Aktionskonfigurationen von Step Functions ein. Wenn Sie dies tun, werden die Informationen in den DynamoDB-Protokollen angezeigt. Verwenden Sie stattdessen AWS Secrets Manager, um Secrets einzurichten und zu speichern. Verweisen Sie dann nach Bedarf in den Aktionskonfigurationen der CloudFormation Vorlagen und Step Functions auf die

im Secrets Manager gespeicherten Geheimnisse. Weitere Informationen finden Sie unter Was ist AWS Secrets Manager in der Secrets Manager-Dokumentation.

- Konfigurieren Sie die serverseitige Verschlüsselung für in Amazon S3 gespeicherte CodePipeline Artefakte. Weitere Informationen finden Sie in der CodePipeline Dokumentation unter Serverseitige Verschlüsselung für in Amazon S3 gespeicherte Artefakte konfigurieren. CodePipeline
- Wenden Sie bei der Konfiguration von IAM-Rollen Berechtigungen mit den geringsten Rechten an. Weitere Informationen finden Sie unter Geringste Berechtigungen anwenden in der IAM-Dokumentation.
- Stellen Sie sicher, dass Ihr Amazon S3 S3-Bucket nicht öffentlich zugänglich ist. Weitere Informationen finden Sie unter Konfiguration der Einstellung zum Blockieren des öffentlichen Zugriffs für Ihre S3-Buckets in der Amazon S3 S3-Dokumentation.
- Stellen Sie sicher, dass Sie die Versionierung für Ihren Amazon S3 S3-Bucket aktivieren. Weitere Informationen finden Sie unter Verwenden der Versionierung in S3-Buckets in der Amazon S3 S3-Dokumentation.
- Verwenden Sie IAM Access Analyzer bei der Konfiguration von IAM-Richtlinien. Das Tool bietet umsetzbare Empfehlungen, die Sie bei der Erstellung sicherer und funktionaler IAM-Richtlinien unterstützen. Weitere Informationen finden Sie unter Verwenden von AWS Identity and Access Management Access Analyzer in der IAM-Dokumentation.
- Definieren Sie nach Möglichkeit spezifische Zugriffsbedingungen bei der Konfiguration von IAM-Richtlinien.
- Aktivieren Sie die CloudWatch Amazon-Protokollierung für Überwachungs- und Prüfungszwecke. Weitere Informationen finden Sie unter Was ist Amazon CloudWatch Logs? in der CloudWatch Dokumentation.

Epen

Konfigurieren Sie die Voraussetzungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon-S3-Bucket.	Erstellen Sie einen Amazon S3 S3-Bucket (oder verwenden Sie einen vorhandenen Bucket), um die erforderlichen CloudFormation	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Vorlagen, den Quellcode und die Eingabedateien für die Lösung zu speichern. Weitere Informationen finden Sie unter Schritt 1: Erstellen Sie Ihren ersten S3-Bucket in der Amazon S3 S3-Dokumentation. **Note** Der Amazon S3 S3-Bucket muss sich in derselben AWS-Region befinden, in der Sie die Lösung bereitstellen.	
Klonen Sie das GitHub Repository.	Klonen Sie das GitHub automated-ci-pipeline-creationRepository, indem Sie den folgenden Befehl in einem Terminalfenster ausführen: `git clone https://github.com/aws-samples/automated-ci-pipeline-creation.git` Weitere Informationen finden Sie in der GitHub Dokumentation unter Ein Repository klonen.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Ordner Solution Templates aus dem geklonten GitHub Repository in Ihren Amazon S3 S3-Bucket hoch.	Kopieren Sie den Inhalt aus dem geklonten Solution-Templates-Ordner und laden Sie ihn in den Amazon S3 S3-Bucket hoch, den Sie erstellt haben. Weitere Informationen finden Sie unter Hochladen von Objekten in der Amazon S3 S3-Dokumentation. **Note** Stellen Sie sicher, dass Sie nur den Inhalt des Ordners Solution-Templates hochladen. Sie können die Dateien nur auf der Stammebene des Amazon S3 S3-Bucket s hochladen.	AWS DevOps

Stellen Sie die Lösung bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen CloudFormation Stack, um die Lösung mithilfe der Datei template.yml im geklonten Repository bereitzustellen. GitHub	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die CloudFormation AWS-Konsole.	AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie Stack erstellen aus. Eine Dropdownliste wird angezeigt. 3. Wählen Sie in der Dropdownliste die Option Mit neuen Ressourcen (Standard) aus. Die Seite Stack erstellen wird geöffnet. 4. Aktivieren Sie im Abschnitt „Vorlage angeben“ das Kontrollkästchen neben „Eine Vorlagendatei hochladen“. 5. Wählen Sie Datei auswählen aus. Navigieren Sie dann zum Stammordner des geklonten GitHub Repositorys und wählen Sie die Datei template.yml aus. Wählen Sie dann Open (Öffnen) aus. 6. Wählen Sie Weiter aus. Die Seite „Stack-Details angeben“ wird geöffnet. 7. Geben Sie im Abschnitt Parameter die folgenden Parameter an: • Geben Sie für S3 TemplateBucketName den Namen des Amazon S3 S3-Buckets ein, den Sie zuvor erstellt haben und der den Quellcode	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und die Referenzen für diese Lösung enthält. Stellen Sie sicher, dass der Parameter für den Bucket-Namen in Kleinbuchstaben geschrieben ist. • Geben Sie für DynamoDBTable einen Namen für die DynamoDB-Tabelle ein, die der CloudFormation Stapel erstellt. • Geben Sie für StateMachineNameeinen Namen für die Step Functions Functions-Zustandsmaschine ein, die der CloudFormation Stack erstellt. 8. Wählen Sie Weiter aus. Die Seite „Stack-Optionen konfigurieren“ wird geöffnet. 9. Wählen Sie auf der Seite Configure stack options (Stack-Optionen konfigurieren) Next (Weiter) aus. Ändern Sie keinen der Standardwerte. Die Seite „Überprüfen“ wird geöffnet. 10. Überprüfen Sie die Einstellungen für die Stack-Erstellung. Wählen Sie dann	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Stack erstellen, um Ihren Stack zu starten. **Note** Während Ihr Stack erstellt wird, wird er auf der Seite Stacks mit dem Status CREATE_IN _PROGRESS aufgeführt. Stellen Sie sicher, dass Sie warten, bis sich der Status des Stacks auf CREATE_COMPLETE ändert, bevor Sie die verbleibenden Schritte in diesem Muster abschließen.	

Testen der Einrichtung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Schrittfunktion aus, die Sie erstellt haben.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die Step Functions Functions-Konsole. 2. Öffnen Sie die Step-Funk tion, die Sie erstellt haben.	AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie Start execution (Ausführung starten) aus. Geben Sie dann Ihre Eingabewerte für den Workflow im JSON-Form at ein (siehe die folgenden Beispieleingaben). 4. Wählen Sie Start execution (Ausführung starten) aus. JSON-Formatierung `{ "details": { "tech_stack": "Name of the Tech Stack (python/java)", "project_name": "Name of the Project that you want to create with", "pre_build": "Choose the step if it required in the buildspec.yml file i.e., yes/no", "build": "Choose the step if it required in the buildspec.yml file i.e., yes/no", "post_build": "Choose the step if it required in the buildspec.yml file i.e., yes/no", "reports": "Choose the step if it required in the buildspec.yml file i.e., yes/no",`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
  }
}
```

Beispiel für eine Java-JSON-Eingabe

```
{
  "details": {
    "tech_stack":
 "java",
    "project_name":
 "pipeline-java-pjt",
    "pre_build": "yes",
    "build": "yes",
    "post_build":
 "yes",
    "reports": "yes"
  }
}
```

Beispiel für Python-JSON-Eingabe

```
{
  "details": {
    "tech_stack":
 "python",
    "project_name":
 "pipeline-python-p
jt",
    "pre_build": "yes",
    "build": "yes",
    "post_build":
 "yes",
    "reports": "yes"
  }
}
```

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vergewissern Sie sich, dass das CodeCommit Repository für die CI-Pipeline erstellt wurde.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die CodeCommit Konsole. 2. Vergewissern Sie sich auf der Seite Repositorys, dass der Name des CodeCommit Repositorys, das Sie erstellt haben, in der Liste der Repositorys erscheint. An den Namen des Repositorys wird Folgendes angehängt: -Repo pipeline-java-pjt 3. Öffnen Sie das CodeCommit Repository und überprüfen Sie, ob der Beispielquellcode zusammen mit den buildspec.yml-Dateien in den Hauptzweig übertragen wurde.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die CodeBuild Projektressourcen.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die CodeBuild Konsole. 2. Vergewissern Sie sich auf der Seite Projekte erstellen, dass der Name des CodeBuild Projekts, das Sie erstellt haben, in der Projektliste angezeigt wird. An den Namen des Projekts wird Folgendes angehängt: pipeline-java-pjt -Build 3. Wählen Sie den Namen Ihres CodeBuild Projekts aus, um das Projekt zu öffnen. Überprüfen und validieren Sie anschließend die folgenden Konfigura tionen: • Konfiguration des Projekts • Quelle • Umgebung • Buildspec • Batch-Konfiguration • Artefakte	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die CodePipeline Stufen.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die CodePipeline Konsole. 2. Stellen Sie auf der Seite Pipelines sicher, dass der Name der Pipeline, die Sie erstellt haben, in der Liste der Pipelines erscheint. An den Namen der Pipeline wird Folgendes angehängt: -Pipeline pipeline-java-pjt 3. Wählen Sie den Namen Ihrer Pipeline aus, um die Pipeline zu öffnen. Überprüfen und validieren Sie anschließend jede Phase der Pipeline, einschließlich Commit und Deploy.	AWS DevOps
Vergewissern Sie sich, dass die CI-Pipeline erfolgreich ausgeführt wurde.	1. Wählen Sie in der CodePipeline Konsole auf der Seite Pipelines den Namen Ihrer Pipeline aus, um den Status der Pipeline anzuzeigen. 2. Stellen Sie sicher, dass jede Phase der Pipeline den Status Erfolgreich hat.	AWS DevOps

Bereinigen Ihrer Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie den Ressource nstapel CloudFormation.	Löschen Sie den Ressource nstapel der CI-Pipeline CloudFormation. Weitere Informationen finden Sie in der CloudForm ation Dokumentation unter Löschen eines Stacks auf der CloudFormation AWS-Konso le. **Note** Stellen Sie sicher, dass Sie den Stack mit dem Namen -stack <project_name>lösc hen.	AWS DevOps
Löschen Sie die Abhängigk eiten der CI-Pipeline in Amazon S3 und CloudForm ation.	1. Leeren Sie den Amazon S3 S3-Bucket mit dem Namen DeploymentArtifactBucket. Weitere Informationen finden Sie in der Amazon S3 S3-Dokumentation unter Einen Bucket leeren. 2. Löschen Sie den Abhängigk eitsstapel der CI-Pipeli ne in. CloudFormation Weitere Informationen finden Sie in der CloudForm ation Dokumentation unter Löschen eines Stacks auf	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der CloudFormation AWS-Konsole. **Note** Stellen Sie sicher, dass Sie den genannten Stack löschen pipeline-creation-dependencies-stack.	
Löschen Sie den Amazon S3 S3-Vorlagen-Bucket.	Löschen Sie den Amazon S3-Bucket, den Sie im Abschnitt Voraussetzungen konfigurieren dieses Musters erstellt haben, in dem die Vorlagen für diese Lösung gespeichert sind. Weitere Informationen finden Sie unter Löschen eines Buckets in der Amazon S3 S3-Dokumentation.	AWS DevOps

Zugehörige Ressourcen

- Erstellen einer Step Functions Functions-Zustandsmaschine, die Lambda verwendet (AWS Step Functions Functions-Dokumentation)
- AWS Step Functions WorkFlow Studio (Dokumentation zu AWS Step Functions)
- DevOps und AWS
- Wie CloudFormation funktioniert AWS? (CloudFormation AWS-Dokumentation)

- Vollständiges CI/CD mit AWS CodeCommit, AWS CodeBuild, AWS und AWS CodeDeploy CodePipeline (AWS-Blogbeitrag)
- IAM- und AWS-STS-Kontingente, Namensanforderungen und Zeichenbeschränkungen (IAM-Dokumentation)

Stellen Sie CloudWatch Synthetics Canaries mithilfe von Terraform bereit

Erstellt von Dhrubajyoti Mukherjee (AWS) und Jean-Francois Landreau (AWS)

Übersicht

Es ist wichtig, den Zustand eines Systems aus Kundensicht zu überprüfen und sicherzustellen, dass Kunden eine Verbindung herstellen können. Dies ist schwieriger, wenn die Kunden den Endpunkt nicht ständig anrufen. Amazon CloudWatch Synthetics unterstützt die Erstellung von Canaries, mit denen sowohl öffentliche als auch private Endgeräte getestet werden können. Durch die Verwendung von Canaries können Sie den Status eines Systems ermitteln, auch wenn es nicht verwendet wird. Diese Kanarien sind entweder Node.js Puppeteer-Skripte oder Python Selenium-Skripte.

Dieses Muster beschreibt, wie HashiCorp Terraform verwendet wird, um Canaries bereitzustellen, die private Endpunkte testen. Es bettet ein Puppeteer-Skript ein, das testet, ob eine URL zurückkehrt. `200-OK` Das Terraform-Skript kann dann in das Skript integriert werden, das den privaten Endpunkt bereitstellt. Sie können die Lösung auch ändern, um öffentliche Endpunkte zu überwachen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS) -Konto mit einer Virtual Private Cloud (VPC) und privaten Subnetzen
- Die URL des Endpunkts, der von den privaten Subnetzen aus erreicht werden kann
- Terraform ist in der Bereitstellungsumgebung installiert

Einschränkungen

Die aktuelle Lösung funktioniert für die folgenden CloudWatch Synthetics-Laufzeitversionen:

- syn-nodejs-puppeteer-3.4
- syn-nodejs-puppeteer-3,5
- syn-nodejs-puppeteer-3,6
- syn-nodejs-puppeteer-3,7

Wenn neue Runtime-Versionen veröffentlicht werden, müssen Sie möglicherweise die aktuelle Lösung aktualisieren. Sie müssen die Lösung auch ändern, um mit den Sicherheitsupdates Schritt zu halten.

Produktversionen

- Terraform 1.3.0

Architektur

Amazon CloudWatch Synthetics basiert auf CloudWatch Lambda und Amazon Simple Storage Service (Amazon S3). Amazon CloudWatch bietet einen Assistenten zum Erstellen der Canaries und ein Dashboard, das den Status der Canaries Runs anzeigt. Die Lambda-Funktion führt das Skript aus. Amazon S3 speichert die Protokolle und Screenshots der Canary Runs.

Dieses Muster simuliert einen privaten Endpunkt über eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance, die in den Zielsubnetzen bereitgestellt wird. Die Lambda-Funktion erfordert elastische Netzwerkschnittstellen in der VPC, in der der private Endpunkt bereitgestellt wird.

Das Diagramm zeigt Folgendes:

1. Der Synthetics Canary initiiert die kanarische Lambda-Funktion.
2. Die kanarische Lambda-Funktion stellt eine Verbindung zur elastic network interface her.
3. Die Canary-Lambda-Funktion überwacht den Status des Endpunkts.
4. Der Synthetics Canary überträgt Laufdaten und CloudWatch Metriken in den S3-Bucket.
5. Auf der Grundlage der Metriken wird ein CloudWatch Alarm ausgelöst.
6. Der CloudWatch Alarm leitet das Thema Amazon Simple Notification Service (Amazon SNS) ein.

Tools

AWS-Services

- Amazon CloudWatch hilft Ihnen dabei, die Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie auf AWS ausführen, in Echtzeit zu überwachen.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.

- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS. Dieses Muster verwendet VPC-Endpunkte und elastische Netzwerkschnittstellen.

Andere Dienste

- HashiCorp Terraform ist ein Open-Source-Tool für Infrastruktur als Code (IaC), mit dem Sie mithilfe von Code Cloud-Infrastruktur und -Ressourcen bereitstellen und verwalten können. Dieses Muster verwendet Terraform, um die Infrastruktur bereitzustellen.
- Puppeteer ist eine Node.js Bibliothek. Die CloudWatch Synthetics-Laufzeit verwendet das Puppeteer-Framework.

Code

Die Lösung ist im Cloud-Repository verfügbar. GitHub watch-synthetics-canary-terraform Weitere Informationen finden Sie im Abschnitt Zusätzliche Informationen.

Epen

Implementieren Sie die Lösung für die Überwachung einer privaten URL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie die Anforderungen für die Überwachung der privaten URL.	Erfassen Sie die vollständige URL-Definition: Domäne, Parameter und Header. Verwenden Sie VPC-Endpunkte CloudWatch, um privat mit Amazon S3 und Amazon zu kommunizieren. Beachten	Cloud-Architekt, Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie, wie der Endpunkt auf die VPC und die Subnetze zugreifen kann. Beachten Sie die Häufigkeit von Canary Runs.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die bestehende Lösung, um die private URL zu überwachen.	Ändern Sie die `terraform .tfvars` Datei: • `name`— Der Name deines Kanarienvogels. • `runtime_version` — Die Runtime-Version des Canary. Wir empfehlen die Verwendung von syn-nodej s-puppeteer -3.7. • `take_screenshot` — Ob ein Screenshot aufgenomm en werden soll. • `api_hostname` — Der Hostname des überwachten Endpunkts. • `api_path`— Der Pfad des überwachten Endpunkts. • `vpc_id`— Die VPC-ID, die von der Canary-Lambda-Funktion verwendet wird. • `subnet_ids` — Das Subnetz IDs , das von der Canary-Lambda-Funktion verwendet wird. • `frequency` — Die Lauffrequenz des Canary in Minuten. • `alert_sns_topic` — Das SNS-Thema, an das die CloudWatch Alarmbena chrichtigung gesendet wird.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die Lösung bereit und betreiben Sie sie.	Gehen Sie wie folgt vor, um die Lösung bereitzustellen:
	1. Initialisieren Sie Terraform aus dem `cloudwatch-synthetics-canary-terraform` Verzeichnis in Ihrer Entwicklungsumgebung.
	`terraform init`
	2. Planen und überprüfen Sie die Änderungen.
	`terraform plan`
	3. Stellen Sie die Lösung bereit.
	`terraform apply`
		Cloud-Architekt, DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Das Löschen der bereitgestellten Ressourcen bleibt hängen.	Löschen Sie die Canary-Lambda-Funktion, die entsprechende elastic network interface und die Sicherheitsgruppe manuell in dieser Reihenfolge.

Zugehörige Ressourcen

- Synthetische Überwachung verwenden

- Überwachen Sie API Gateway Gateway-Endpunkte mit Amazon CloudWatch Synthetics (Blogbeitrag)

Zusätzliche Informationen

Artefakte aus dem Repository

Die Repository-Artefakte haben die folgende Struktur.

```
.
### README.md
### main.tf
### modules
#   ### canary
#   ### canary-infra
### terraform.tfvars
### tf.plan
### variable.tf
```

Die `main.tf` Datei enthält das Kernmodul und stellt zwei Untermodule bereit:

- `canary-infra`stellt die für die Kanaren benötigte Infrastruktur bereit.
- `canary`setzt die Kanarischen Inseln ein.

Die Eingabeparameter für die Lösung befinden sich in der `terraform.tfvars` Datei. Sie können das folgende Codebeispiel verwenden, um einen Canary zu erstellen.

```
module "canary" {
    source = "./modules/canary"
    name   = var.name
    runtime_version = var.runtime_version
    take_screenshot = var.take_screenshot
    api_hostname = var.api_hostname
    api_path = var.api_path
    reports-bucket = module.canary_infra.reports-bucket
    role = module.canary_infra.role
    security_group_id = module.canary_infra.security_group_id
    subnet_ids = var.subnet_ids
    frequency = var.frequency
    alert_sns_topic = var.alert_sns_topic
```

```
}
```

Es folgt die entsprechende .var-Datei.

```
name   = "my-canary"
runtime_version = "syn-nodejs-puppeteer-3.7"
take_screenshot = false
api_hostname = "mydomain.internal"
api_path = "/path?param=value"
vpc_id = "vpc_id"
subnet_ids = ["subnet_id1"]
frequency = 5
alert_sns_topic = "arn:aws:sns:eu-central-1:111111111111:yyyyy"
```

Die Lösung aufräumen

Wenn Sie dies in einer Entwicklungsumgebung testen, können Sie die Lösung bereinigen, um Kosten zu vermeiden.

1. Navigieren Sie in der AWS-Managementkonsole zur Amazon S3 S3-Konsole. Leeren Sie den Amazon S3 S3-Bucket, den die Lösung erstellt hat. Stellen Sie sicher, dass Sie bei Bedarf eine Sicherungskopie der Daten erstellen.
2. Führen Sie in Ihrer Entwicklungsumgebung den `destroy` Befehl aus dem `cloudwatch-synthetics-canary-terraform` Verzeichnis aus.

   ```
   terraform destroy
   ```

Stellen Sie eine CI/CD-Pipeline für Java-Microservices auf Amazon ECS bereit

Erstellt von Vijay Thompson (AWS) und Sankar Sangubotla (AWS)

Übersicht

Dieses Muster führt Sie durch die Schritte zur Implementierung einer kontinuierlichen Integration und kontinuierlichen Bereitstellung (die CI/CD) pipeline for Java microservices on an existing Amazon Elastic Container Service (Amazon ECS) cluster by using AWS CodeBuild. When the developer commits the changes, the CI/CD Pipeline wird initiiert und der Build-Prozess beginnt in. CodeBuild Wenn der Build abgeschlossen ist, wird das Artefakt an Amazon Elastic Container Registry (Amazon ECR) übertragen und der neueste Build von Amazon ECR wird abgerufen und an den Amazon ECS-Service übertragen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine bestehende Java-Microservices-Anwendung, die auf Amazon ECS läuft
- Vertrautheit mit AWS CodeBuild und AWS CodePipeline

Architektur

Quelltechnologie-Stack

- Java-Microservices, die auf Amazon ECS ausgeführt werden
- Code-Repository in Amazon ECR
- AWS Fargate

Quellarchitektur

Zieltechnologie-Stack

- Amazon ECR
- Amazon ECS
- AWS Fargate

- AWS CodePipeline
- AWS CodeBuild

Zielarchitektur

Automatisierung und Skalierung

CodeBuild `buildspec.yml`-Datei:

```
version: 0.2

phases:
  pre_build:
    commands:
      - echo Logging in to Amazon ECR...
      - aws --version
      - $(aws ecr get-login --region $AWS_DEFAULT_REGION --no-include-email)
      - REPOSITORY_URI=$AWS_ACCOUNT_ID.dkr.ecr.$AWS_DEFAULT_REGION.amazonaws.com/
$IMAGE_REPO
      - COMMIT_HASH=$(echo $CODEBUILD_RESOLVED_SOURCE_VERSION | cut -c 1-7)
      - IMAGE_TAG=build-$(echo $CODEBUILD_BUILD_ID | awk -F":" '{print $2}')
  build:
    commands:
      - echo Build started on `date`
      - echo building the Jar file
      - mvn clean install
      - echo Building the Docker image...
      - docker build -t $REPOSITORY_URI:$BUILD_TAG .
      - docker tag $REPOSITORY_URI:$BUILD_TAG $REPOSITORY_URI:$IMAGE_TAG
  post_build:
    commands:
      - echo Build completed on `date`
      - echo Pushing the Docker images...
      - docker push $REPOSITORY_URI:$BUILD_TAG
      - docker push $REPOSITORY_URI:$IMAGE_TAG
      - echo Writing image definitions file...
      - printf '[{"name":"%s","imageUri":"%s"}]' $DOCKER_CONTAINER_NAME
 $REPOSITORY_URI:$IMAGE_TAG > imagedefinitions.json
      - cat imagedefinitions.json
artifacts:
    files:
```

```
    - imagedefinitions.json
    - target/DockerDemo.jar
```

Tools

AWS-Services

- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Komponententests ausführen und bereitstellungsbereite Artefakte erstellen können. AWS CodeBuild skaliert kontinuierlich und verarbeitet mehrere Builds gleichzeitig, sodass Ihre Builds nicht in der Warteschlange verbleiben.
- AWS CodePipeline hilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind. Sie können AWS CodePipeline in Dienste von Drittanbietern wie GitHub Amazon ECR integrieren oder einen AWS-Service wie Amazon ECR verwenden.
- Amazon Elastic Container Registry (Amazon ECR) ist eine vollständig verwaltete Registry, die es Entwicklern erleichtert, Docker-Container-Images zu speichern, zu verwalten und bereitzustellen. Amazon ECR ist in Amazon ECS integriert, um Ihren development-to-production Arbeitsablauf zu vereinfachen. Amazon ECR hostet Ihre Images in einer hochverfügbaren und skalierbaren Architektur, sodass Sie Container für Ihre Anwendungen zuverlässig bereitstellen können. Die Integration mit AWS Identity and Access Management (IAM) ermöglicht die Kontrolle jedes Repositorys auf Ressourcenebene.
- Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, leistungsstarker Container-Orchestrierungsservice, der Docker-Container unterstützt und es Ihnen ermöglicht, containerisierte Anwendungen auf AWS einfach auszuführen und zu skalieren. Mit Amazon ECS müssen Sie keine eigene Container-Orchestrierungssoftware installieren und betreiben, einen Cluster von virtuellen Maschinen verwalten und skalieren oder Container auf diesen virtuellen Maschinen planen.
- AWS Fargate ist eine Rechen-Engine für Amazon ECS, mit der Sie Container ausführen können, ohne Server oder Cluster verwalten zu müssen. Mit AWS Fargate müssen Sie keine Cluster von virtuellen Maschinen mehr bereitstellen, konfigurieren und skalieren, um Container auszuführen. Auf diese Weise müssen keine Servertypen mehr ausgewählt werden, es muss nicht entschieden werden, wann die Cluster skaliert werden oder das Cluster-Packing optimiert werden.

Andere Tools

- Docker ist eine Plattform, mit der Sie Anwendungen in Paketen, sogenannten Containern, erstellen, testen und bereitstellen können.
- Git ist ein verteiltes Versionskontrollsystem zur Nachverfolgung von Änderungen im Quellcode während der Softwareentwicklung. Es wurde für die Koordinierung der Arbeit zwischen Programmierern entwickelt, kann jedoch verwendet werden, um Änderungen an beliebigen Dateien zu verfolgen. Zu seinen Zielen gehören Geschwindigkeit, Datenintegrität und Unterstützung verteilter, nichtlinearer Workflows.

Epen

Richten Sie das Build-Projekt in AWS ein CodeBuild

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein CodeBuild Build-Projekt.	Erstellen Sie in der CodeBuild AWS-Konsole ein Build-Projekt und geben Sie dessen Namen an.	App-Entwickler, AWS-Systemadministrator
Wählen Sie die Quelle aus.	Dieses Muster verwendet Git für das Code-Repository. Wählen Sie also GitHub aus der Liste der verfügbaren Optionen. Wähle ein öffentliches Repository oder aus deinem GitHub Konto.	App-Entwickler, AWS-Systemadministrator
Wählen Sie ein Repository aus.	Wählen Sie das Repository aus, aus dem Sie den Code erstellen möchten.	App-Entwickler, AWS-Systemadministrator
Wählen Sie die Umgebung aus.	Sie können aus einer Liste verwalteter Images auswählen oder sich mit Docker für ein benutzerdefiniertes Image entscheiden. Dieses Muster	App-Entwickler, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	verwendet das folgende verwaltete Image: • **Note** Amazon Linux 2 (: Amazon Linux 2 nähert sich dem Ende der Unterstützung. Weitere Informationen finden Sie unter Amazon Linux FAQs 2.) • Laufzeit: Standard • Bildversion 1.0	
Wählen Sie eine Servicerolle.	Sie können eine Servicerolle erstellen oder aus einer Liste vorhandener Rollen auswählen.	App-Entwickler, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Hinzufügen von Umgebungsvariablen	Konfigurieren Sie im Abschnitt Zusätzliche Konfiguration die folgenden Umgebungsvariablen: • AWS_DEFAULT_REGION für die AWS-Standardregion • AWS_ACCOUNT_ID für die Benutzerkontonummer • IMAGE_REPO für das private Amazon ECR-Repository • BUILD_TAG für die Version des Builds (der neueste Build ist der Wert für diese Variable) • DOCKER_CONTAINER_NAME für den Namen des Containers in der Aufgabe Diese Variablen sind Platzhalter in der `buildspec.yml` Datei und werden durch ihre jeweiligen Werte ersetzt.	App-Entwickler, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Buildspec-Datei.	Sie können eine `buildspec.yml` Datei am selben Speicherort wie die in diesem Muster bereitgestellte Konfiguration erstellen `pom.xml` und hinzufügen, oder Sie können den Online-Buildspec-Editor verwenden und die Konfiguration hinzufügen. Konfigurieren Sie die Umgebungsvariablen mit den entsprechenden Werten, indem Sie die angegebenen Schritte ausführen.	App-Entwickler, AWS-Systemadministrator
Konfigurieren Sie das Projekt für Artefakte.	(Optional) Konfigurieren Sie das Build-Projekt für Artefakte, falls erforderlich.	App-Entwickler, AWS-Systemadministrator
Konfigurieren Sie Amazon CloudWatch Logs.	(Optional) Konfigurieren Sie Amazon CloudWatch Logs für das Build-Projekt, falls erforderlich. Dieser Schritt ist optional, wird aber empfohlen.	App-Entwickler, AWS-Systemadministrator
Konfigurieren Sie Amazon S3 S3-Protokolle.	(Optional) Konfigurieren Sie Amazon Simple Storage Service (Amazon S3) - Protokolle für das Build-Projekt, wenn Sie die Protokolle speichern möchten.	App-Entwickler, AWS-Systemadministrator

Konfigurieren Sie die Pipeline in AWS CodePipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Pipeline.	Erstellen Sie auf der CodePipeline AWS-Konsole eine Pipeline und geben Sie ihren Namen an. Weitere Informationen zum Erstellen einer Pipeline finden Sie in der CodePipeline AWS-Dokumentation.	App-Entwickler, AWS-Systemadministrator
Wählen Sie eine Servicerolle aus.	Erstellen Sie eine Servicerolle oder wählen Sie eine aus der Liste der vorhandenen Servicerollen aus. Wenn Sie eine Servicerolle erstellen, geben Sie einen Namen für die Rolle ein und wählen Sie die Option CodePipeline zum Erstellen der Rolle aus.	App-Entwickler, AWS-Systemadministrator
Wählen Sie einen Artefaktspeicher.	Wenn Sie möchten, dass Amazon S3 in den erweiterten Einstellungen einen Bucket erstellt und die Artefakte darin speichert, verwenden Sie den Standardspeicherort für den Artefaktspeicher. Oder wählen Sie einen benutzerdefinierten Speicherort und geben Sie einen vorhandenen Bucket an. Sie können das Artefakt auch mithilfe eines Verschlüsselungsschlüssels verschlüsseln.	App-Entwickler, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den Quellanbieter an.	Wählen Sie als Quellanbieter GitHub (Version 2) aus.	App-Entwickler, AWS-Systemadministrator
Wählen Sie das Repository und den Zweig des Codes aus.	Wenn Sie nicht angemeldet sind, geben Sie die Verbindungsdetails ein, zu denen Sie eine Verbindung herstellen möchten GitHub, und wählen Sie dann den Namen des Repositorys und den Namen der Filiale aus.	App-Entwickler, AWS-Systemadministrator
Erkennungsoptionen ändern.	Wählen Sie Bei Änderung des Quellcodes die Pipeline starten und fahren Sie mit der nächsten Seite fort.	App-Entwickler, AWS-Systemadministrator
Wählen Sie einen Build-Anbieter aus.	Wählen Sie als Build-Anbieter AWS CodeBuild aus und geben Sie dann die AWS-Region und den Projektnamen für das Build-Projekt an. Wählen Sie als Build-Typ die Option Single Build aus.	App-Entwickler, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie einen Bereitstellungsanbieter.	Wählen Sie als Bereitstellungsanbieter Amazon ECS aus. Wählen Sie den Clusternamen, den Servicenamen, die Image-Definitionsdatei, falls vorhanden, und einen Wert für das Bereitstellungs-Timeout, falls erforderlich. Wählen Sie Create pipeline (Pipeline erstellen) aus.	App-Entwickler, AWS-Systemadministrator

Zugehörige Ressourcen

- AWS ECS-Dokumentation
- AWS-ECR-Dokumentation
- CodeBuild AWS-Dokumentation
- CodePipeline AWS-Dokumentation
- Erstellen Sie eine Continuous Delivery-Pipeline für Ihre Container-Images mit Amazon ECR als Quelle (Blogbeitrag)

Stellen Sie eine ChatOps Lösung zur Verwaltung von SAST-Scanergebnissen bereit, indem Sie Amazon Q Developer in Chat-Anwendungen verwenden, benutzerdefinierte Aktionen und AWS CloudFormation

Erstellt von Anand Bukkapatnam Tirumala (AWS)

Übersicht

Dieses Muster stellt eine umfassende Lösung dar, die Amazon Q Developer in Chat-Anwendungen verwendet, um die Verwaltung von SAST-Scanfehlern (Static Application Security Testing) zu optimieren, die gemeldet wurden. SonarQube Dieser innovative Ansatz integriert benutzerdefinierte Aktionen und Benachrichtigungen in eine Konversationsoberfläche und ermöglicht so effiziente Zusammenarbeit und Entscheidungsprozesse innerhalb der Entwicklungsteams.

In der heutigen schnelllebigen Softwareentwicklungsumgebung ist die effiziente Verwaltung der SAST-Scanergebnisse entscheidend für die Aufrechterhaltung der Codequalität und -sicherheit. Viele Unternehmen stehen jedoch vor den folgenden großen Herausforderungen:

- Verspätete Erkennung kritischer Sicherheitslücken aufgrund ineffizienter Meldesysteme
- Langsame Entscheidungsprozesse aufgrund unzusammenhängender Genehmigungsabläufe
- Mangel an sofortigen, umsetzbaren Reaktionen auf SAST-Scanfehler
- Fragmentierte Kommunikation und Zusammenarbeit im Zusammenhang mit Sicherheitsergebnissen
- Zeitaufwändige und fehleranfällige manuelle Einrichtung der Infrastruktur für Sicherheitstools

Diese Probleme führen häufig zu erhöhten Sicherheitsrisiken, verzögerten Releases und verminderter Teamproduktivität. Um diesen Herausforderungen effektiv zu begegnen, ist eine Lösung erforderlich, die das SAST-Ergebnismanagement rationalisiert, die Teamzusammenarbeit verbessert und die Bereitstellung der Infrastruktur automatisiert.

Zu den wichtigsten Funktionen der Lösung gehören:

- Maßgeschneiderte Benachrichtigungen — Warnmeldungen und Benachrichtigungen in Echtzeit werden direkt an die Chat-Kanäle des Teams gesendet, sodass Sicherheitslücken oder Fehler beim SAST-Scan umgehend erkannt und entsprechende Maßnahmen ergriffen werden können.

- Genehmigungen per Konversation — Beteiligte können Genehmigungsworkflows für SAST-Scanergebnisse nahtlos über die Chat-Oberfläche initiieren und abschließen, wodurch die Entscheidungsprozesse beschleunigt werden.
- Benutzerdefinierte Aktionen — Teams können auf der Grundlage von SAST-Scanergebnissen benutzerdefinierte Aktionen definieren und ausführen, z. B. das automatische Auslösen von E-Mail-Nachrichten bei Quality-Gate-Ausfällen, wodurch die Reaktionsfähigkeit bei Sicherheitsproblemen verbessert wird.
- Zentralisierte Zusammenarbeit — Alle Diskussionen, Entscheidungen und Aktionen im Zusammenhang mit SAST-Scans werden in einer einheitlichen Chat-Umgebung abgehalten, wodurch die Zusammenarbeit und der Wissensaustausch zwischen den Teammitgliedern verbessert werden.
- Infrastructure as Code (IaC) — Die gesamte Lösung ist mit AWS CloudFormation Vorlagen ausgestattet, die eine schnellere und zuverlässigere Bereitstellung der Infrastruktur ermöglichen und gleichzeitig Fehler bei der manuellen Einrichtung reduzieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver. AWS-Konto
- Eine AWS Identity and Access Management (IAM-) Rolle mit Berechtigungen zum Erstellen und Verwalten von Ressourcen, die mit den unter Tools AWS-Services aufgelisteten Ressourcen verknüpft sind.
- Ein Slack-Workspace.
- Amazon Q Developer in Chat-Anwendungen wurde dem erforderlichen Slack-Workspace als Plugin hinzugefügt. Weitere Informationen findest du unter Apps zu deinem Slack-Workspace hinzufügen in der Slack-Dokumentation. Notiere dir die Workspace-ID von Slack, wie sie auf der AWS Management Console nach erfolgreicher Registrierung angegeben ist.
- Ein konfigurierter Client für Amazon Q Developer in Chat-Anwendungen, bei dem die Workspace-ID sofort zur Eingabe in der AWS CloudFormation Konsole verfügbar ist. Anweisungen finden Sie unter Konfiguration eines Slack-Clients im Administratorhandbuch für Amazon Q Developer in Chat-Anwendungen.
- Ein Quell-E-Mail-Konto, das in Amazon Simple Email Service (Amazon SES) erstellt und verifiziert wurde, um Genehmigungs-E-Mail-Nachrichten zu versenden. Anweisungen zur Einrichtung finden

Sie unter E-Mail-Identitäten erstellen und verifizieren im Amazon Simple Email Service Developer Guide.

- Eine Ziel-E-Mail-Adresse für den Empfang von Genehmigungsbenachrichtigungen. Diese Adresse kann ein gemeinsam genutzter Posteingang oder eine bestimmte Team-Verteilerliste sein.
- Eine betriebsbereite SonarQube Instanz, auf die von Ihrem aus zugegriffen werden kann AWS-Konto. Weitere Informationen finden Sie in den SonarQube Installationsanweisungen.
- Ein SonarQube Benutzertoken mit Berechtigungen zum Auslösen und Erstellen von Projekten über die Pipeline.

Einschränkungen

- Die Erstellung von benutzerdefinierten Aktionsschaltflächen ist in dieser Lösung ein manueller Prozess.
- Einige AWS-Services sind nicht in allen verfügbar AWS-Regionen. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie unter Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Architektur

Das folgende Diagramm zeigt den Workflow und die Architekturkomponenten für dieses Muster.

Das Diagramm zeigt den automatisierten Arbeitsablauf zur Sicherung der Codequalität:

1. Codevorbereitung und Upload:
   - Der Entwickler komprimiert die Codebasis in eine ZIP-Datei.
   - Der Entwickler lädt die ZIP-Datei manuell in einen dafür vorgesehenen Amazon Simple Storage Service (Amazon S3) -Bucket hoch.
2. Auslösung und AWS Step Functions Orchestrierung von Amazon S3 S3-Ereignissen:
   - Das Amazon S3 S3-Upload-Ereignis löst einen Step Functions Functions-Workflow aus.
   - Step Functions orchestriert einen SAST-Scan mit. SonarQube
   - Der Workflow überwacht den AWS CodeBuild Auftragsstatus, um die nächsten Aktionen festzulegen. Wenn der CodeBuild Vorgang erfolgreich ist (Quality Gate bestanden), wird der Workflow beendet. CodeBuild Schlägt dies fehl, wird eine AWS Lambda Funktion zur Diagnose

aufgerufen. Weitere Einzelheiten finden Sie weiter unten in diesem Abschnitt unter AWS Step Functions Logik.

3. AWS CodeBuild Ausführung:
   - Der CodeBuild Job führt einen SonarQube Scan der hochgeladenen Codebasis aus.
   - Scan-Artefakte werden zur Prüfung und Analyse in einem separaten Amazon S3 S3-Bucket gespeichert.
4. Fehleranalyse (Lambda-Funktion):
   - CodeBuild Bei einem Fehler wird die `CheckBuildStatus` Lambda-Funktion ausgelöst.
   - Bei CodeBuild Erfolg wird der Prozess beendet und es sind keine weiteren Maßnahmen erforderlich.
5. Die Lambda-Funktion analysiert die Fehlerursache (Quality-Gate-Ausfall oder andere Probleme)
   - Die `CheckBuildStatus` Funktion erstellt eine benutzerdefinierte Nutzlast mit detaillierten Fehlerinformationen.
   - Die `CheckBuildStatus` Funktion veröffentlicht die benutzerdefinierte Nutzlast in einem Amazon Simple Notification Service (Amazon SNS) -Thema.
6. Benachrichtigungssystem:
   - Amazon SNS leitet die Nutzdaten in Chat-Anwendungen für die Slack-Integration an Amazon Q Developer weiter.
7. Slack-Integration:
   - Amazon Q Developer in Chat-Anwendungen veröffentlicht eine Benachrichtigung im dafür vorgesehenen Slack-Kanal.
8. Genehmigungsprozess:
   - Genehmigende Personen überprüfen die Fehlerdetails in der Slack-Benachrichtigung.
   - Genehmiger können die Genehmigung über die Schaltfläche Genehmigen in Slack einleiten.
9. Genehmigungshandler:
   - Eine Approval Lambda-Funktion verarbeitet die Genehmigungsaktion von Slack.
   - Die Genehmigungsfunktion veröffentlicht die benutzerdefinierte Nachricht an Amazon SES.
10. Generierte Nachricht:
   - Die Genehmigungsfunktion generiert eine benutzerdefinierte Nachricht für die Benachrichtigung des Entwicklers.
11. Benachrichtigung für Entwickler:

- Amazon SES sendet eine E-Mail-Nachricht mit den nächsten Schritten oder erforderlichen Aktionen an den Entwickler.

Dieser Workflow kombiniert manuelles Hochladen von Code mit automatisierten Qualitätsprüfungen, bietet sofortiges Feedback über Slack und ermöglicht bei Bedarf menschliches Eingreifen, wodurch ein robuster und flexibler Codeüberprüfungsprozess gewährleistet wird.

AWS Step Functions Logik

Wie im vorherigen Architekturdiagramm gezeigt, geht der Workflow zur `CheckBuildStatus` Lambda-Funktion über, wenn der Quality Gate-Passon SonarQube fehlschlägt. Die `CheckBuildStatus` Funktion löst eine Benachrichtigung im Slack-Channel aus. Jede Benachrichtigung enthält Informationen mit Vorschlägen für die nächsten Schritte. Im Folgenden sind die Arten von Benachrichtigungen aufgeführt:

- Die Anwendung ist beim Code-Sicherheitsscan fehlgeschlagen — Der Benutzer erhält diese Benachrichtigung, wenn der hochgeladene Code den SonarQube Sicherheitsscan nicht bestanden hat. Der Benutzer kann APPROVE wählen, um den Build zu akzeptieren. In der Benachrichtigung wird der Benutzer jedoch darauf hingewiesen, sich vor potenziell schlechter Codequalität und Sicherheitsrisiken zu hüten. Die Benachrichtigung enthält die folgenden Einzelheiten:
  - Nächste Schritte: Fehler: Quality Gate-Status: FEHLGESCHLAGEN — Details finden Sie unter der angegebenen URL.
  - Untersuchen Sie die Sicherheitslücken, wie sie im Dokument unter der angegebenen URL erwähnt werden.
  - CodeBuild Einzelheiten sind an der Stelle unter der angegebenen URL verfügbar.
- Die Pipeline für Anwendungsscans ist aus einem anderen Grund ausgefallen — Der Benutzer erhält diese Benachrichtigung, wenn die Pipeline aus einem anderen Grund als dem fehlgeschlagenen Code-Sicherheitsscan ausgefallen ist. Die Benachrichtigung enthält die folgenden Details:
  - Die nächsten Schritte finden Sie unter dem angegebenen Link zur weiteren Fehlerbehebung.

Um Screenshots der Benachrichtigungen zu sehen, wie sie in einem Slack-Channel erscheinen, gehe zum Assets-Ordner im GitHub chatops-Slack-Repository.

Das folgende Diagramm zeigt ein Beispiel für den Schrittstatus von Step Functions, nachdem der Quality-Gate-Pass fehlgeschlagen ist.

Tools

AWS-Services

- Mit Amazon Q Developer in Chat-Anwendungen können Sie die Chat-Kanäle Amazon Chime, Microsoft Teams und Slack verwenden, um betriebliche Ereignisse in Ihren AWS Anwendungen zu überwachen und darauf zu reagieren. Hinweis zum Ende des Supports: Am 20. Februar 2026 AWS wird der Support für den Amazon Chime Chime-Service eingestellt. Nach dem 20. Februar 2026 können Sie nicht mehr auf die Amazon Chime-Konsole oder die Amazon Chime Chime-Anwendungsressourcen zugreifen. Weitere Informationen finden Sie im Blogbeitrag. Dies hat keine Auswirkungen auf die Verfügbarkeit des Amazon Chime SDK-Dienstes.
- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und AWS-Regionen zu verwalten.
- AWS CodeBuildist ein vollständig verwalteter Build-Service, der Ihnen hilft, Quellcode zu kompilieren, Komponententests durchzuführen und Artefakte zu erstellen, die sofort einsatzbereit sind.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Key Management Service (AWS KMS) hilft Ihnen dabei, kryptografische Schlüssel zu erstellen und zu kontrollieren, um Ihre Daten zu schützen.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Mit AWS Secrets Manager können Sie fest codierte Anmeldeinformationen im Code (einschließlich Passwörter) durch einen API-Aufruf an Secrets Manager ersetzen und das Geheimnis programmgesteuert abrufen.
- Amazon Simple Email Service (Amazon SES) unterstützt Sie beim Senden und Empfangen von E-Mail-Nachrichten mithilfe Ihrer eigenen E-Mail-Adressen und Domains.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Step Functionsist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Funktionen und andere Funktionen kombinieren können, um geschäftskritische Anwendungen AWS-Services zu erstellen.

Andere Tools

- Slack, ein Salesforce-Angebot, ist eine KI-gestützte Konversationsplattform, die Chat- und Videozusammenarbeit ermöglicht, Prozesse ohne Code automatisiert und den Informationsaustausch unterstützt.
- SonarQubeist ein lokales Analysetool, das entwickelt wurde, um Codierungsprobleme in über 30 Sprachen, Frameworks und IaC-Plattformen zu erkennen.

Code-Repository

Der Code für dieses Muster ist im GitHub Chatops-Slack-Repository verfügbar.

Bewährte Methoden

- CloudFormation Stack-Management — Wenn Sie bei der CloudFormation Stack-Ausführung auf Fehler stoßen, empfehlen wir Ihnen, den ausgefallenen Stack zu löschen. Erstellen Sie ihn anschließend mit den richtigen Parameterwerten neu. Dieser Ansatz unterstützt eine saubere Bereitstellung und hilft, potenzielle Konflikte oder teilweise Implementierungen zu vermeiden.
- E-Mail-Konfiguration für gemeinsam genutzten Posteingang — Verwenden Sie bei der Konfiguration des `SharedInboxEmail` Parameters eine gemeinsame Verteilerliste, auf die alle relevanten Entwickler zugreifen können. Dieser Ansatz fördert die Transparenz und trägt dazu bei, dass wichtige Benachrichtigungen die zuständigen Teammitglieder erreichen.
- Workflow für Produktionsgenehmigungen — Beschränken Sie für Produktionsumgebungen den Zugriff auf den Slack-Channel, der für Build-Genehmigungen verwendet wird. Nur designierte Genehmiger sollten Mitglieder dieses Channels sein. Diese Vorgehensweise gewährleistet eine klare Verantwortungskette und erhöht die Sicherheit, indem begrenzt wird, wer kritische Änderungen genehmigen kann.
- IAM-Berechtigungen — Folgen Sie dem Prinzip der geringsten Rechte und gewähren Sie nur die für die Ausführung einer Aufgabe erforderlichen Mindestberechtigungen. Weitere Informationen

finden Sie in der IAM-Dokumentation unter Gewährung der geringsten Rechte und bewährte Methoden zur Sicherheit.

Epen

Führen Sie die Ersteinrichtung durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Verwenden Sie den folgenden Befehl, um das Chatops-Slack-Repository für dieses Muster zu klonen. `git clone “git@github.com:aws-samples/chatops-slack.git“`	AWS DevOps, Build-Leiter, DevOps Ingenieur, Cloud-Administrator

Erstellen Sie die ZIP-Dateien, die Lambda-Code enthalten.	Erstellen Sie die .zip-Dateien für den AWS Lambda Funktionscode für die `CheckBuildStatus` und -Funktionalität. `ApprovalEmail` Verwenden Sie die folgenden Befehle`approval.zip` , um `notification.zip` und zu erstellen.
	`cd chatops-slack/src`
	`chmod -R 775 *`
	`zip -r approval.zip approval`
		AWS DevOps, Build-Leiter, DevOps Ingenieur, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`zip -r notification.zip notification`	

Stellen Sie die Stack-Datei prerequisite.yml bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die `pre-requisite.yml` Stack-Datei aus.	Die `pre-requisite.yml` CloudFormation Stack-Datei stellt die anfänglichen Ressourcen bereit, die benötigt werden, bevor Sie die `app-security.yml` Stack-Datei ausführen. Gehen Sie wie folgt vor, um die `pre-requisite.yml` Datei auszuführen: 1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS CloudFormationKonsole. Wählen Sie Stack erstellen und dann in der Dropdownliste die Option Mit neuen Ressourcen (Standard) aus. 2. Wählen Sie auf der Seite Stack erstellen die Optionen Vorhandene Vorlage auswählen und Vorlagendatei hochladen aus. Wählen Sie dann Datei auswählen und anschließend pre-requi	AWS-Administrator, AWS DevOps, Build-Leiter, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	site.yml aus. Wählen Sie Weiter aus. 3. Geben Sie auf der Seite „Stack-Details angeben“ Werte für die Parameter ein, wie unter Zusätzliche Informationen beschrieben. Wählen Sie anschließend Weiter. 4. Wählen Sie auf der Seite „Stack-Optionen konfigurieren“ die IAM-Rolle für die Erstellung der Ressourcen aus, wie unter Voraussetzungen beschrieben. Wählen Sie anschließend Weiter. 5. Wählen Sie auf der Seite Überprüfen und erstellen die Option Senden aus. 6. Wählen Sie auf der Detailseite für den Stack die Registerkarten Ressourcen und Ausgaben aus. Notieren Sie sich die Werte für die `CKMSKeyId` Parameter `S3LambdaCKMSKeyArn`, und, die in den folgenden Schritten verwendet werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die ZIP-Dateien in den Amazon S3 S3-Bucket hoch.	Laden Sie die `approval.zip` Dateien `notification.zip` und, die Sie zuvor erstellt haben, in den Amazon S3 S3-Bucket mit dem Namen hoch`S3LambdaBucket` . Die `app-security.yml` CloudFormation Stack-Datei wird `S3LambdaBucket` zur Bereitstellung der Lambda-Funktion verwendet.	AWS DevOps, Build-Leiter, DevOps Ingenieur, AWS-Systemadministrator

Führen Sie die Stack-Datei app-security.yml aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die `app-security.yml` Stack-Datei aus.	Die `app-security.yml` Stack-Dateien stellen die verbleibende Infrastruktur für das Benachrichtigungs- und Genehmigungssystem bereit. Gehen Sie wie folgt vor, um die `app-security.yml` Datei auszuführen: 1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS CloudFormationKonsole. Wählen Sie Stack erstellen und dann in der Dropdownliste die Option Mit neuen Ressourcen (Standard) aus.	AWS DevOps, AWS-Systemadministrator, DevOps Ingenieur, Build-Leiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie auf der Seite Stack erstellen die Optionen Vorhandene Vorlage auswählen und Vorlagendatei hochladen aus. Wählen Sie dann Datei auswählen und anschließend app-security.yml aus. Wählen Sie Weiter aus. 3. Geben Sie auf der Seite „Stack-Details angeben“ Werte für die Parameter ein, wie unter Zusätzliche Informationen beschrieben. Wählen Sie anschließend Weiter. 4. Wählen Sie auf der Seite „Stack-Optionen konfigurieren“ die IAM-Rolle für die Erstellung der Ressourcen aus, wie unter Voraussetzungen beschrieben. Wählen Sie anschließend Weiter. 5. Wählen Sie auf der Seite Überprüfen und erstellen die Option Senden aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie das Benachrichtigungs-Setup.	Gehen Sie wie folgt vor, um das Benachrichtigungs-Setup zu testen: 1. Öffnen Sie die Amazon-SNS-Konsole. Wählen Sie im linken Navigationsbereich Topics (Themen). 2. Wählen Sie den Themennamen, der mit LambdaToAWSSlackChatbot endet. 3. Wählen Sie auf der Detailseite des Themas die Option Nachricht veröffentlichen aus. 4. Geben Sie auf der Seite Nachricht im Thema veröffentlichen für Nachrichtentext, der an den Endpunkt gesendet werden soll, Folgendes ein: `{ "version": "1.0", "source": "custom", "content": { "description": ":warning: This is a test notification" } }`	AWS DevOps, AWS-Systemadministrator, DevOps Ingenieur, Build-Leiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Wählen Sie Publish message (Nachricht veröffentlichen) aus. Nachdem die Testnachricht erfolgreich zugestellt wurde, solltest du im Slack-Kanal eine Benachrichtigung sehen. Weitere Informationen findest du unter Testbenachrichtigungen von AWS-Services zu Slack im Administratorhandbuch für Amazon Q Developer in Chat-Anwendungen.	

Richten Sie den Genehmigungsablauf ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie eine benutzerdefinierte Lambda-Aktion.	Gehen Sie wie folgt vor, um die benutzerdefinierte AWS Lambda Aktion einzurichten: 1. Wähle die Schaltfläche mit den vertikalen Auslassungspunkten unten in der Lieferbenachrichtigung in deinem Slack-Kanal. 2. Wähle unter Aktionen verwalten die Option Erstellen aus. 3. Geben Sie einen benutzerdefinierten Aktionsnamen ein, zum Beispiel	AWS-Administrator, AWS DevOps, Build-Leiter, DevOps Ingenieur, Slack-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Genehmigen. Dieser Name ist ein eindeutig er Bezeichner für Ihre benutzerdefinierte Aktion. 4. Geben Sie einen Namen für Ihre benutzerdefinierte Aktionsschaltfläche ein, z. B. Genehmigen. Dieser Name wird auf einer Schaltfläche in Ihrer Benachrichtigung angezeigt . Dieser Name sollte 20 Zeichen oder weniger lang sein und kann Emojis enthalten. 5. Wählen Sie für Benutzerd efinierter Aktionstyp die Option Lambda-Aktion aus. 6. Wählen Sie Weiter aus. 7. Wählen Sie die Aktion AWS-Konto und den AWS-Region Ort aus, an dem Sie diese Aktion bereitstellen möchten. 8. Wählen Sie Load Lambdas aus. 9. Wählen Sie unter Lambda-Funktion definieren eine Lambda-Funktion aus, die mit endet. ApprovalE mailLambdaWählen Sie anschließend Weiter.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	10. Um die Schaltfläche „Genehmigen“ zu erstellen , wählen Sie auf der Seite mit den Anzeigekriterien die Option Speichern.	
Bestätigen Sie den Genehmigungsablauf.	Um zu überprüfen, ob der Genehmigungsablauf wie erwartet funktioniert, wähle in Slack die Schaltfläche Genehmigen. Slackbot sollte im Nachricht en-Thread eine Benachric htigung mit der Bestätigu ngszeichenfolge Approval Email successfully sent successfully sendeten.	AWS-Administrator, AWS DevOps, DevOps Ingenieur, Slack-Administrator

Fehlerbehebung

Problem	Lösung
Fehlkonfigurationen bei Slack	Informationen zur Behebung von Problemen im Zusammenhang mit Fehlkonfigurationen von Slack finden Sie unter Troubleshooting Amazon Q Developer im Administratorhandbuch für Amazon Q Developer in Chat-Anwendungen.
Der Scan ist aus einem anderen Grund fehlgeschlagen	Dieser Fehler bedeutet, dass die Aufgabe zur Codeerstellung fehlgeschlagen ist. Um das Problem zu beheben, rufen Sie den Link in der Nachricht auf. Der Fehler bei der Codeerste llungsaufgabe kann folgende Ursachen haben:

Problem	Lösung
	• Die Anwendung ist nicht richtig gepackt. Der `sonar-scanner` Befehl kann die `sonar.project.env.properties` Datei nicht finden. • Die Werte für die `SonarToken` Parameter `SonarFileName` `SonarFileDirectory` , oder sind falsch. Überprüfen Sie die Werte und führen Sie dann die Stack-Dateien erneut aus. • Der Sonar-Host ist nicht erreichbar. • Andere Probleme, die Sie anhand der Protokolle beheben können.

Zugehörige Ressourcen

AWS Dokumentation

- Konfiguriere einen Slack-Client
- Eine benutzerdefinierte Aktion erstellen
- Ein Verfahren zur Identifizierung von E-Mail-Adressen erstellen
- Tutorial: Erste Schritte mit Slack

Sonstige Ressourcen

- Füge Apps zu deinem Slack-Workspace hinzu (Slack-Dokumentation)
- Generierung und Verwendung von Tokens (Dokumentation) SonarQube
- Einführung in die Serverinstallation (SonarQube Dokumentation)

Zusätzliche Informationen

Diese Lösung konzentriert sich auf benutzerdefinierte Aktionen von Amazon Q Developer in Chat-Anwendungen für das Release-Management. Sie können die Lösung jedoch wiederverwenden, indem Sie den Lambda-Code für Ihren speziellen Anwendungsfall ändern und darauf aufbauen.

Parameter von CloudFormation Stack-Dateien

Die folgende Tabelle zeigt die Parameter und ihre Beschreibungen für die CloudFormation Stack-Dateipre-requisite.yml.

Key (Schlüssel)	Beschreibung
StackName	Der Name des CloudFormation Stacks.
S3LambdaBucket	Der Name des Amazon S3 S3-Buckets, in den Sie den Lambda-Code hochladen. Der Name muss global eindeutig sein.
SonarToken	Das SonarQube Benutzertoken, wie unter Voraussetzungen beschrieben.

Die folgende Tabelle zeigt die Parameter und ihre Beschreibungen für die CloudFormation Stack-Dateiapp-security.yml.

Key (Schlüssel)	Beschreibung
CKMSKeyArn	Der AWS KMS key Amazon-Ressourcenn ame (ARN), der in IAM-Rollen und Lambda-Fu nktionen verwendet wird, die in diesem Stack erstellt wurden.
CKMSKeyId	Die AWS KMS key ID, die im Amazon SNS SNS-Thema verwendet wird, das in diesem Stack erstellt wurde.
EnvironmentType	Der Name der Client-Umgebung für die Bereitstellung der Application-Scan-Pipeline. Wählen Sie den Umgebungsnamen aus der Dropdownliste der zulässigen Werte aus.
S3LambdaBucket	Der Name des Amazon S3 S3-Buckets, der die approval.zip notification.zip UND-Dateien enthält.

`SESEmail`	Der Name der registrierten E-Mail-Identität in Amazon SES, wie unter Voraussetzungen beschrieben. Diese Identität ist die Quell-E-Mail-Adresse.
`SharedInboxMail`	Die Ziel-E-Mail-Adresse, an die die Scan-Benachrichtigungen gesendet werden.
`SlackChannelId`	Die Kanal-ID des Slack-Channels, an den die Benachrichtigungen gesendet werden sollen. Um die Kanal-ID zu finden, klicke in der Slack-App in den Kanaldetails mit der rechten Maustaste auf den Kanalnamen. Die Kanal-ID befindet sich unten.
`SlackWorkspaceId`	Die Workspace-ID von Slack, wie unter Voraussetzungen beschrieben. Um die Workspace-ID von Slack zu finden, melden Sie sich bei der an AWS Management Console, öffnen Sie die Amazon Q Developer in Chat-Anwendungskonsole und wählen Sie Konfigurierte Clients, Slack, WorkspaceID aus.
`StackName`	Der Name des Stacks. CloudFormation
`SonarFileDirectory`	Das Verzeichnis, das die `sonar.project.<env>.properties` Datei enthält.
`SonarFileName`	Der Name der `sonar.project.<env>properties` Datei.
`SourceCodeZip`	Der Name der ZIP-Datei, die die `sonar.project.<env>properties` Datei und den Quellcode enthält.

Stellen Sie eine Firewall mit AWS Network Firewall und AWS Transit Gateway bereit

Erstellt von Shrikant Patil (AWS)

Übersicht

Dieses Muster zeigt Ihnen, wie Sie eine Firewall mithilfe von AWS Network Firewall und AWS Transit Gateway bereitstellen. Die Netzwerk-Firewall-Ressourcen werden mithilfe einer CloudFormation AWS-Vorlage bereitgestellt. Die Network Firewall passt sich automatisch Ihrem Netzwerkverkehr an und kann Hunderttausende von Verbindungen unterstützen, sodass Sie sich keine Gedanken über den Aufbau und die Wartung Ihrer eigenen Netzwerksicherheitsinfrastruktur machen müssen. Ein Transit-Gateway ist ein Netzwerk-Transit-Hub, über den Sie Ihre virtuellen privaten Clouds (VPCs) und lokalen Netzwerke miteinander verbinden können.

In diesem Muster lernen Sie auch, eine Inspektions-VPC in Ihre Netzwerkarchitektur einzubeziehen. Schließlich wird in diesem Muster erklärt, wie Sie Amazon verwenden CloudWatch , um die Aktivitäten Ihrer Firewall in Echtzeit zu überwachen.

> **Tip**
>
> Es hat sich bewährt, die Verwendung eines Netzwerk-Firewall-Subnetzes zur Bereitstellung anderer AWS-Services zu vermeiden. Dies liegt daran, dass die Network Firewall den Datenverkehr von Quellen oder Zielen innerhalb des Subnetzes einer Firewall nicht untersuchen kann.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Rollen- und Richtlinienberechtigungen für AWS Identity and Access Management (IAM)
- CloudFormation Vorlagenberechtigungen

Einschränkungen

Möglicherweise haben Sie Probleme mit der Domainfilterung und es könnte eine andere Konfiguration erforderlich sein. Weitere Informationen finden Sie unter Stateful Domain List Rule Groups in AWS Network Firewall in der Dokumentation zur Network Firewall.

Architektur

Technologie-Stack

- CloudWatch Amazon-Protokolle
- Amazon VPC
- AWS Network Firewall
- AWS Transit Gateway

Zielarchitektur

Das folgende Diagramm zeigt, wie Sie Network Firewall und Transit Gateway verwenden, um Ihren Datenverkehr zu überprüfen:

Die Architektur umfasst die folgenden Komponenten:

- Ihre Anwendung wird in den beiden Speichen gehostet VPCs. Sie VPCs werden von der Network Firewall überwacht.
- Die Ausgangs-VPC hat direkten Zugriff auf das Internet-Gateway, ist jedoch nicht durch die Network Firewall geschützt.
- Die Inspektions-VPC ist der Ort, an dem die Network Firewall bereitgestellt wird.

Automatisierung und Skalierung

Sie können dieses Muster mithilfe von Infrastruktur als Code erstellen. CloudFormation

Tools

AWS-Services

- Amazon CloudWatch Logs hilft Ihnen dabei, die Protokolle all Ihrer Systeme, Anwendungen und AWS-Services zu zentralisieren, sodass Sie sie überwachen und sicher archivieren können.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen

Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.

- Die AWS Network Firewall ist ein zustandsbehafteter, verwalteter Netzwerk-Firewall sowie Service zur Erkennung und Verhinderung von Eindringlingen VPCs in der AWS-Cloud.
- AWS Transit Gateway ist ein zentraler Knotenpunkt, der lokale Netzwerke verbindet VPCs .

Code

Der Code für dieses Muster ist in der GitHub AWS-Netzwerk-Firewall-Bereitstellung mit dem Transit Gateway Gateway-Repository verfügbar. Sie können die CloudFormation Vorlage aus diesem Repository verwenden, um eine einzelne Inspektions-VPC bereitzustellen, die die Network Firewall verwendet.

Epen

Erstellen Sie die Spoke-VPC und die Inspektion-VPC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die CloudFormation Vorlage vor und stellen Sie sie bereit.	1. Laden Sie die `cloudformation/aws_nw_fw.yml` Vorlage aus dem GitHub Repository herunter. 2. Aktualisieren Sie die Vorlage mit Ihren Werten. 3. Stellen Sie die Vorlage bereit.	AWS DevOps

Erstellen Sie das Transit-Gateway und die Routen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Transit-Gateway.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon VPC-Konsole.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie im Navigation sbereich Transit Gateways aus. 3. Wählen Sie Create Transit Gateway (Transit Gateway erstellen) aus. 4. Geben Sie unter Namenstag einen Namen für das Transit-Gateway ein. 5. Geben Sie unter Beschreibung eine Beschreibung für das Transit-Gateway ein. 6. Behalten Sie für die Amazon-seitige Autonome Systemnummer (ASN) den ASN-Standardwert bei. 7. Wählen Sie die DNS-Supportoption aus. 8. Wählen Sie die Option VPN ECMP-Unterstützung aus. 9. Wählen Sie die Option Standardroutentabellenzuordnung aus. Diese Option ordnet die Transit-Gateway-Anlagen automatisch der Standardroutentabelle für das Transit-Gateway zu. 10. Wählen Sie die Option Standardweiterleitung für Routing-Tabellen aus. Mit dieser Option werden	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Transit-Gateway-An lagen automatisch an die Standardroutentabelle für das Transit-Gateway weitergegeben. 11. Wählen Sie Create Transit Gateway (Transit Gateway erstellen) aus.	
Erstellen Sie Transit-Gateway-Anhänge.	Erstellen Sie einen Transit-Gateway-Anhang für Folgendes: • Ein Inspektionsanhang im Inspektions-VPC- und Transit Gateway Gateway-Subnetz • Ein SpokeVPCA-Anhang im Spoke-VPCA und im privaten Subnetz • Ein SpokeVPCB-Anhang in der Spoke-VPCB und im privaten Subnetz • Ein EgressVPC-Anhang in der Ausgangs-VPC und im privaten Subnetz	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Routentabelle für das Transit-Gateway.	1. Erstellen Sie eine Transit-Gateway-Routentabelle für die Spoke-VPC. Diese Routing-Tabelle muss allen VPCs anderen VPCs als der Inspektions-VPC zugeordnet sein. 2. Erstellen Sie eine Transit-Gateway-Routentabelle für die Firewall. Diese Routentabelle darf nur der Inspektions-VPC zugeordnet werden. 3. Fügen Sie der Transit-Gateway-Routentabelle für die Firewall eine Route hinzu: • Verwenden Sie für `0.0.0/0` den EgressVPC-Anhang. • Verwenden Sie für den SpokeVPCA CIDR-Block den Spoke-Anhang. VPC1 • Verwenden Sie für den SpokeVPCB CIDR-Block den Spoke-Anhang. VPC2 4. Fügen Sie der Transit-Gateway-Routentabelle für die Spoke-VPC eine Route hinzu. Verwenden Sie	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`0.0.0/0` dazu den VPC-Anhang von Inspection.	

Erstellen Sie die Firewall und die Routen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Firewall in der Inspektions-VPC.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon VPC-Konsole. 2. Wählen Sie im Navigationsbereich unter Network Firewall die Option Firewalls aus. 3. Wählen Sie Firewall erstellen aus. 4. Geben Sie unter Name den Namen ein, mit dem Sie diese Firewall identifizieren möchten. Sie können den Namen einer Firewall nicht mehr ändern, nachdem Sie sie erstellt haben. 5. Wählen Sie für VPC Ihre Inspektions-VPC aus. 6. Wählen Sie für Availability Zone und Subnet die Zone und das Firewall-Subnetz aus, die Sie identifiziert haben. 7. Wählen Sie im Abschnitt Zugeordnete Firewall-	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Richtlinie die Option Einer vorhandenen Firewall-Richtlinie zuordnen aus, und wählen Sie dann die Firewall-Richtlinie aus, die Sie zuvor erstellt haben. 8. Wählen Sie „Firewall erstellen“.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Firewall-Richtlinie.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon VPC-Konsole. 2. Wählen Sie im Navigationsbereich unter Network Firewall die Option Firewall-Richtlinien aus. 3. Wählen Sie auf der Seite „Firewall-Richtlinie beschreiben“ die Option Firewall-Richtlinie erstellen aus. 4. Geben Sie unter Name den Namen ein, den Sie für die Firewall-Richtlinie verwenden möchten. Sie verwenden den Namen, um die Richtlinie zu identifizieren, wenn Sie die Richtlinie später in diesem Muster Ihrer Firewall zuordnen. Sie können den Namen einer Firewall-Richtlinie nicht mehr ändern, nachdem Sie sie erstellt haben. 5. Wählen Sie Weiter aus. 6. Wählen Sie auf der Seite Regelgruppen hinzufügen im Abschnitt Stateless Rule Group die Option Stateless Rule Groups hinzufügen aus.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Aktivieren Sie im Dialogfeld Aus vorhandenen Regelgruppen hinzufügen das Kontrollkästchen für die statuslose Regelgruppe, die Sie zuvor erstellt haben. Wählen Sie Regelgruppen hinzufügen aus. Hinweis: Unten auf der Seite zeigt der Kapazitätszähler der Firewall-Richtlinie neben der maximal zulässigen Kapazität für eine Firewall-Richtlinie die Kapazität an, die durch das Hinzufügen dieser Regelgruppe verbraucht wurde. 8. Stellen Sie die Standardaktion „Statuslos“ auf „An statusbehaftete Regeln weiterleiten“ ein. 9. Wählen Sie im Abschnitt Stateful-Regelgruppe die Option Stateful-Regelgruppen hinzufügen aus und aktivieren Sie dann das Kontrollkästchen für die statusbehaftete Regelgruppe, die Sie zuvor erstellt haben. Wählen Sie Regelgruppen hinzufügen aus. 10. Wählen Sie Weiter, um den Rest des Einrichtungsassist	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	enten durchzugehen, und wählen Sie dann Firewall-Richtlinie erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie Ihre VPC-Routentabellen.	VPC-Routentabellen für Inspektionen 1. Fügen Sie in der ANF Subnetz-Routentabelle (`Inspection-ANFRT`) die Transit-Gateway-ID hinzu`0.0.0/0`. 2. Fügen Sie in der Transit Gateway Gateway-Subnetz-Routentabelle (`Inspection-TGWRT`) die Datei `0.0.0/0` zur EgressVPC hinzu. SpokeVPCA-Routentabelle Fügen Sie in der Tabelle für private Routen `0.0.0.0/0` die Transit Gateway Gateway-ID hinzu. Spoke VPCB-Routentabelle Fügen Sie in der Tabelle für private Routen `0.0.0.0/0` die Transit Gateway Gateway-ID hinzu. Ausgangs-VPC-Routing-Tabellen Fügen Sie in der Tabelle für öffentliche Ausgangsrouten den SpokeVPCA- und Spoke VPCB CIDR-Block zur Transit	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Gateway Gateway-ID hinzu. Wiederholen Sie den gleichen Schritt für das private Subnetz.	

Für die Durchführung CloudWatch von Netzwerkinspektionen in Echtzeit eingerichtet

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Logging-Konfiguration der Firewall.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon VPC-Konsole. 2. Wählen Sie im Navigationsbereich unter Network Firewall die Option Firewalls aus. 3. Wählen Sie auf der Seite Firewalls den Namen der Firewall aus, die Sie bearbeiten möchten. 4. Wählen Sie die Registerkarte Firewall-Details. Wählen Sie im Abschnitt Protokollierung die Option Bearbeiten aus. 5. Passen Sie die Auswahl des Protokolltyps nach Bedarf an. Sie können die Protokollierung für Alert- und Flow-Logs konfigurieren. • Warnung — Sendet Protokolle für Datenverk	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ehr, der einer Statusreg el entspricht, bei der die Aktion auf Alert oder Drop gesetzt ist. Weitere Informationen zu statusbehafteten Regeln und Regelgruppen finden Sie unter Regelgruppen in der AWS-Netzwerk-Firewall. • Flow — Sendet Protokoll e für den gesamten Netzwerkverkehr, den die Stateless Engine an die Stateful-Regel-Engine weiterleitet. 6. Wählen Sie für jeden ausgewählten Protokolltyp den Zieltyp aus, und geben Sie dann die Informationen für das Protokollierungszi el ein. Weitere Informati onen finden Sie unter AWS Network Firewall-Protokollierungsziele in der Dokumentation zur Network Firewall. 7. Wählen Sie Speichern.	

Überprüfen Sie das Setup

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie eine EC2 Instanz, um das Setup zu testen.	Starten Sie zwei Amazon Elastic Compute Cloud (Amazon EC2) -Instances in der Spoke-VPC: eine für Jumpbox und eine für Testkonnektivität.	AWS DevOps
Überprüfen Sie die Metriken.	Die Metriken werden zuerst nach dem Service-Namespace und dann nach den verschiedenen Dimensionskombinationen innerhalb der einzelnen Namespaces gruppiert. Der CloudWatch Namespace für die Network Firewall ist `AWS/NetworkFirewall` . 1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudWatch -Konsole. 2. Wählen Sie im Navigationsbereich Metriken aus. 3. Wählen Sie auf der Registerkarte Alle Metriken die Region und dann NetworkFirewallAWS/ aus.	AWS DevOps

Zugehörige Ressourcen

- Einfache Einzelzonenarchitektur mit einem Internet-Gateway
- Mehrzonenarchitektur mit einem Internet-Gateway

- Architektur mit einem Internet-Gateway und einem NAT-Gateway

Stellen Sie einen AWS Glue Glue-Job mit einer AWS CodePipeline CI/CD-Pipeline bereit

Erstellt von Bruno Klein (AWS) und Luis Henrique Massao Yamada (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Dieses Muster zeigt, wie Sie AWS CodeCommit und AWS CodePipeline mit AWS Glue integrieren und AWS Lambda verwenden können, um Jobs zu starten, sobald ein Entwickler seine Änderungen in ein CodeCommit AWS-Remote-Repository überträgt.

Wenn ein Entwickler eine Änderung an ein ETL-Repository (Extrahieren, Transformieren und Laden) übermittelt und die Änderungen an AWS überträgt CodeCommit, wird eine neue Pipeline aufgerufen. Die Pipeline initiiert eine Lambda-Funktion, die einen AWS Glue Glue-Job mit diesen Änderungen startet. Der AWS Glue Glue-Job führt die ETL-Aufgabe aus.

Diese Lösung ist in Situationen hilfreich, in denen Unternehmen, Entwickler und Dateningenieure Jobs starten möchten, sobald die Änderungen festgeschrieben und in die Ziel-Repositorys übertragen wurden. Sie trägt zu einem höheren Grad an Automatisierung und Reproduzierbarkeit bei und vermeidet so Fehler bei der Auftragseinführung und im Lebenszyklus.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Git ist auf dem lokalen Computer installiert
- Amazon Cloud Development Kit (Amazon CDK) ist auf dem lokalen Computer installiert
- Python ist auf dem lokalen Computer installiert
- Der Code im Abschnitt Anlagen

Einschränkungen

- Die Pipeline ist abgeschlossen, sobald der AWS Glue Glue-Job erfolgreich gestartet wurde. Es wartet nicht auf den Abschluss des Jobs.

- Der im Anhang enthaltene Code dient nur zu Demo-Zwecken.

Architektur

Zieltechnologie-Stack

- AWS Glue
- AWS Lambda
- AWS CodePipeline
- AWS CodeCommit

Zielarchitektur

Der Prozess besteht aus den folgenden Schritten:

1. Der Entwickler oder Dateningenieur nimmt eine Änderung am ETL-Code vor, überträgt die Änderung und überträgt sie an AWS. CodeCommit
2. Der Push initiiert die Pipeline.
3. Die Pipeline initiiert eine Lambda-Funktion, die das Repository aufruft und die Datei `codecommit:GetFile` auf Amazon Simple Storage Service (Amazon S3) hochlädt.
4. Die Lambda-Funktion startet einen neuen AWS Glue Glue-Job mit dem ETL-Code.
5. Die Lambda-Funktion beendet die Pipeline.

Automatisierung und Skalierung

Der Beispielanhang zeigt, wie Sie AWS Glue in AWS integrieren können CodePipeline. Es bietet ein Basisbeispiel, das Sie für Ihren eigenen Gebrauch anpassen oder erweitern können. Einzelheiten finden Sie im Abschnitt Epics.

Tools

- AWS CodePipeline — AWS CodePipeline ist ein vollständig verwalteter Continuous Delivery Service, der Sie bei der Automatisierung Ihrer Release-Pipelines für schnelle und zuverlässige Anwendungs- und Infrastrukturupdates unterstützt.

- AWS CodeCommit — AWS CodeCommit ist ein vollständig verwalteter Quellcodeverwaltungsservice, der sichere, Git-basierte Repositorys hostet.
- AWS Lambda — AWS Lambda ist ein serverloser Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitzustellen oder zu verwalten.
- AWS Glue — AWS Glue ist ein serverloser Datenintegrationsservice, der es einfach macht, Daten für Analysen, maschinelles Lernen und Anwendungsentwicklung zu entdecken, aufzubereiten und zu kombinieren.
- Git-Client — Git stellt GUI-Tools bereit, oder Sie können die Befehlszeile oder ein Desktop-Tool verwenden, um die erforderlichen Artefakte auszuchecken GitHub.
- AWS CDK — Das AWS CDK ist ein Open-Source-Framework für die Softwareentwicklung, mit dem Sie Ihre Cloud-Anwendungsressourcen mithilfe vertrauter Programmiersprachen definieren können.

Epen

Stellen Sie den Beispielcode bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die AWS CLI.	Konfigurieren Sie die AWS-Befehlszeilenschnittstelle (AWS CLI), um Ihr aktuelles AWS-Konto anzusprechen und sich mit diesem zu authentifizieren. Anweisungen finden Sie in der AWS-CLI-Dokumentation.	Entwickler, DevOps Ingenieur
Extrahieren Sie die Beispielprojektdateien.	Extrahieren Sie die Dateien aus dem Anhang, um einen Ordner zu erstellen, der die Beispielprojektdateien enthält.	Entwickler, DevOps Ingenieur
Stellen Sie den Beispielcode bereit.	Führen Sie nach dem Extrahieren der Dateien die folgenden Befehle vom	Entwickler, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Extraktionsverzeichnis aus, um ein Basisbeispiel zu erstellen:
	
	`cdk bootstrap`
	`cdk deploy`
	`git init`
	`git remote add origin <code-commit-repository-url>`
	`git stage .`
	`git commit -m "adds sample code"`
	`git push --set-upstream origin main`
	
	Nach dem letzten Befehl können Sie den Status der Pipeline und des AWS Glue Glue-Jobs überwachen.	

Passen Sie den Code an.	Passen Sie den Code für die Datei etl.py an Ihre Geschäftsanforderungen an. Sie können den ETL-Code überarbeiten, die Pipeline-Phasen ändern oder die Lösung erweitern.	Dateningenieur

Zugehörige Ressourcen

- Erste Schritte mit dem AWS CDK
- Jobs in AWS Glue hinzufügen
- Finden Sie Action-Integrationen in CodePipeline
- Rufen Sie eine AWS-Lambda-Funktion in einer Pipeline auf in CodePipeline
- AWS Glue Glue-Programmierung

- CodeCommit GetFile AWS-API

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Stellen Sie mithilfe eines EC2 Instanzprofils einen Amazon EKS-Cluster aus AWS Cloud9 bereit

Erstellt von Sagar Panigrahi (AWS)

Übersicht

Hinweis: AWS Cloud9 ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS Cloud9 können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Dieses Muster beschreibt, wie Sie mit AWS Cloud9 und AWS CloudFormation einen Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster erstellen, der betrieben werden kann, ohne den programmatischen Zugriff für Benutzer in Ihrem Amazon Web Services (AWS) -Konto zu aktivieren.

AWS Cloud9 ist eine cloudbasierte integrierte Entwicklungsumgebung (IDE), mit der Sie Ihren Code mithilfe eines Browsers schreiben, ausführen und debuggen können. AWS Cloud9 wird als Kontrollzentrum verwendet, das mithilfe von Amazon Elastic Compute Cloud (Amazon EC2) -Instanzprofilen und CloudFormation AWS-Vorlagen einen Amazon EKS-Cluster bereitstellt.

Sie können dieses Muster verwenden, wenn Sie keine AWS Identity and Access Management (IAM) -Benutzer erstellen und stattdessen IAM-Rollen verwenden möchten. Die rollenbasierte Zugriffskontrolle (RBAC) reguliert den Zugriff auf Ressourcen auf der Grundlage der Rollen der einzelnen Benutzer. Dieses Muster zeigt, wie RBAC innerhalb eines Amazon EKS-Clusters aktualisiert wird, um den Zugriff auf eine bestimmte IAM-Rolle zu ermöglichen.

Die Einrichtung des Musters hilft Ihrem DevOps Team auch dabei, die Funktionen von AWS Cloud9 zur Wartung und Entwicklung von Infrastructure-as-Code (IaC) -Ressourcen für die Erstellung der Amazon EKS-Infrastruktur zu nutzen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Berechtigungen zum Erstellen von IAM-Rollen und -Richtlinien für das Konto. Die IAM-Rolle für den Benutzer muss die `AWSCloud9Administrator` Richtlinie enthalten. Die `eksNodeRoles` Rollen `AWSServiceRoleForAmazonEKS` und müssen ebenfalls erstellt werden, da sie für die Erstellung eines Amazon EKS-Clusters erforderlich sind.
- Kenntnis der Kubernetes-Konzepte.

Einschränkungen

- Dieses Muster beschreibt, wie ein einfacher Amazon EKS-Cluster erstellt wird. Für Produktionscluster müssen Sie die CloudFormation AWS-Vorlage aktualisieren.
- Das Muster stellt keine zusätzlichen Kubernetes-Komponenten bereit (z. B. Fluentd, Ingress-Controller oder Storage-Controller).

Architektur

Technologie-Stack

- AWS Cloud9
- AWS CloudFormation
- Amazon EKS
- IAM

Automatisierung und Skalierung

Sie können dieses Muster erweitern und in CI/CD-Pipelines (Continuous Integration and Continuous Deployment) integrieren, um die vollständige Bereitstellung von Amazon EKS zu automatisieren.

Tools

- AWS CloudFormation — AWS CloudFormation unterstützt Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen, sodass Sie weniger Zeit mit der Verwaltung dieser Ressourcen verbringen und sich mehr auf Ihre Anwendungen konzentrieren können.
- AWS Cloud9 — AWS Cloud9 bietet umfangreiche Funktionen zur Codebearbeitung mit Unterstützung für mehrere Programmiersprachen und Runtime-Debugger sowie einem integrierten Terminal.
- AWS CLI — AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

- Kubectl — `kubectl` ist ein Befehlszeilenprogramm, mit dem Sie mit einem Amazon EKS-Cluster interagieren können.

Epen

Erstellen Sie die IAM-Rollen für das Instanzprofil EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Richtlinie.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die IAM-Konsole, wählen Sie Richtlinien und dann Richtlinie erstellen aus. Wählen Sie die Registerkarte JSON und fügen Sie den Inhalt aus der Datei policy-role-eks-instance profile-for-cloud -9.json (angehängt) ein. Beheben Sie alle Sicherheitswarnungen, Fehler oder allgemeinen Warnungen, die während der Richtlinienvalidierung generiert wurden, und wählen Sie dann Richtlinie überprüfen aus. Füllen Sie das Feld Name für die Richtlinie aus. Wir empfehlen, dass Sie `eks-instance-profile-for-cloud9` für die Richtlinie den Namen verwenden. Überprüfen Sie unter Summary die Richtlinienzusammenfassung, um die	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Berechtigungen einzusehe n, die von Ihrer Richtlinie gewährt werden. Wählen Sie dann Richtlinie erstellen aus.	
Erstellen Sie mithilfe der Richtlinie eine IAM-Rolle.	Wählen Sie in der IAM-Konso le Rollen und anschließend Rolle erstellen aus. Wählen Sie AWS Service und wählen Sie dann EC2aus der Liste. Wählen Sie Weiter: Berechtig ungen und suchen Sie nach der IAM-Richtlinie, die Sie zuvor erstellt haben. Wählen Sie die passenden Tags für Ihre Anforderungen aus. Geben Sie im Abschnitt Überprüfen einen Namen für die Rolle ein. Wir empfehlen , dass Sie `role-eks-instance-profile-f or-cloud9` für die Rolle einen Namen verwenden. Wählen Sie dann Create Role.	Cloud-Administrator

Erstellen Sie eine IAM-Richtlinie und -Rolle für Amazon EKS RBAC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Richt linie.	Wählen Sie in der IAM-Konsole Richtlinien und dann Richtlinie erstellen aus. Wählen Sie die Registerk	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	arte JSON und fügen Sie den Inhalt aus der policy-for-eks-rbac JSON-Datei (angehängt) ein. Beheben Sie alle Sicherhei tswarnungen, Fehler oder allgemeinen Warnungen, die während der Richtlinienvalidie rung generiert wurden, und wählen Sie dann Richtlinie überprüfen aus. Füllen Sie das Feld Name für die Richtlinie aus. Wir empfehlen, dass Sie `policy-for-eks-rbac` für die Richtlinie den Namen verwenden. Überprüfen Sie unter Summary die Richtlini enzusammenfassung, um die Berechtigungen einzusehe n, die von Ihrer Richtlinie gewährt werden. Wählen Sie dann Richtlinie erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie mithilfe der Richtlinie eine IAM-Rolle.	Wählen Sie in der IAM-Konsole Rollen und anschließend Rolle erstellen aus. Wählen Sie AWS Service und wählen Sie dann EC2aus der Liste. Wählen Sie Weiter: Berechtigungen und suchen Sie nach der IAM-Richtlinie, die Sie zuvor erstellt haben. Wählen Sie die passenden Tags für Ihre Anforderungen aus. Geben Sie im Abschnitt Überprüfen einen Namen für die Rolle ein. Wir empfehlen, dass Sie `role-eks-admin-for-rbac` für die Rolle einen Namen verwenden. Wählen Sie dann Create Role.	Cloud-Administrator

Erstellen Sie die AWS Cloud9 Cloud9-Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die AWS Cloud9 Cloud9-Umgebung.	Öffnen Sie die AWS Cloud9 Cloud9-Konsole und wählen Sie Umgebung erstellen. Geben Sie auf der Seite „Umgebung benennen“ einen Namen für Ihre Umgebung ein. Wir empfehlen, dass Sie `eks-management-env` für die Umgebung einen Namen	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	verwenden. Konfigurieren Sie die übrigen Einstellungen entsprechend Ihren Anforderungen und wählen Sie dann Next Step. Wählen Sie auf der Seite Review (Überprüfung) die Option Create environment (Umgebung erstellen) aus. Warten Sie, bis AWS Cloud9 Ihre Umgebung erstellt. Dies kann mehrere Minuten dauern. Weitere Informationen zu den verfügbaren Konfigurationsoptionen finden Sie unter Creating an EC2 environment in der AWS Cloud9 Cloud9-Dokumentation.	
Entfernen Sie die temporären IAM-Anmeldeinformationen für AWS Cloud9.	Nachdem Ihre AWS Cloud9 Cloud9-Umgebung bereitgestellt wurde, wählen Sie im Zahnradsymbol Einstellungen aus. Wählen Sie unter Einstellungen die Option AWS-Einstellungen und dann Anmeldeinformationen aus. Schalten Sie die von AWS verwalteten temporären Anmeldeinformationen aus und schließen Sie die Registerkarte.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Hängen Sie das EC2 Instanzprofil an die zugrunde liegende EC2 Instanz an.	Öffnen Sie die EC2 Amazon-Konsole und wählen Sie die EC2 Instance aus, die zu Ihrer Umgebung in AWS Cloud9 passt. Wenn Sie den von uns empfohlenen Namen verwendet haben, wird die EC2 Instance aufgerufe `naws-cloud9-eks-management-env` . Wählen Sie die EC2 Instanz aus, klicken Sie auf Aktionen und dann auf Instanzeinstellungen. Wählen Sie „IAM-Rolle anfügen/ersetzen“. Suchen Sie nach **`role-eks-instance-profile-for-cloud9`** oder dem Namen der IAM-Rolle, die Sie zuvor erstellt haben, und wählen Sie dann Anwenden.	Cloud-Administrator

Erstellen Sie den Amazon EKS-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Amazon EKS-Cluster.	Laden Sie die Vorlage eks-cfn.yaml (angehängt) für AWS herunter und öffnen Sie sie. CloudFormation Bearbeiten Sie die Vorlage gemäß Ihren Anforderungen.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Öffnen Sie die AWS Cloud9 Cloud9-Umgebung und wählen Sie Neue Datei aus. Fügen Sie die CloudFormation AWS-Vorlage, die Sie zuvor erstellt haben, in das Feld ein. Wir empfehlen, dass Sie eks-cfn.yaml als Vorlagennamen verwenden. Führen Sie im AWS Cloud9-Terminal den folgenden Befehl aus, um den Amazon EKS-Cluster zu erstellen: `aws cloudformation create-stack --stack-name eks-cluster --template-body file://eks-cfn.yaml --region <your_AWS_Region>` Wenn der CloudFormation AWS-Aufruf erfolgreich ist, erhalten Sie den Amazon-Ressourcennamen (ARN) des CloudFormation AWS-Stacks in Ihrer Ausgabe. Die Erstellung des Stacks kann zwischen 10 und 20 Minuten dauern.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Status des Amazon EKS-Clusters.	Öffnen Sie auf der CloudFormation AWS-Konsole die Seite Stacks und wählen Sie dann den Stack-Namen aus. Der Stack wird erstellt, wenn der Stack-Statuscode angezeigt wird`CREATE_COMPLETE` . Weitere Informationen finden Sie in der CloudFormation AWS-Dokumentation unter CloudFormation AWS-Stack-Daten und -Ressourcen anzeigen.	Cloud-Administrator

Greifen Sie auf die Kubernetes-Ressourcen im Amazon EKS-Cluster zu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie kubectl in der AWS Cloud9 Cloud9-Umgebung.	Installieren Sie `kubectl` in Ihrer AWS Cloud9 Cloud9-Umgebung, indem Sie den Anweisungen unter Installation von kubectl in der Amazon EKS-Dokumentation folgen.	Cloud-Administrator
Aktualisieren Sie die neue Amazon EKS-Konfiguration in AWS Cloud9.	Führen Sie den folgenden Befehl im AWS Cloud9-Terminal aus, um die `kubeconfig` vom Amazon EKS-Cluster auf die AWS Cloud9 Cloud9-Umgebung zu aktualisieren:	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws eks update-kubeconfig --name EKS-DEV2 --region <your_AWS_Region>` **Important** `EKS-DEV2`ist der Name des Amazon EKS-Clusters in der CloudFormation AWS-Vorlage, mit der Sie den Cluster erstellt haben. Führen Sie den `kubectl get all -A` Befehl aus, um alle Kubernetes-Ressourcen anzuzeigen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie die Administrator-IAM-Rolle zum Kubernetes RBAC hinzu.	Führen Sie den folgenden Befehl in Ihrem AWS Cloud9-Terminal aus, um die RBAC-Konfigurationsübersicht für Amazon EKS im Bearbeitungsmodus zu öffnen:
	`kubectl edit cm/aws-auth -n kube-system`
	Fügen Sie die folgenden Zeilen unter dem Abschnitt an: `mapRoles`
	`- groups:`
	`- system:masters`
	`rolearn: <ARN_of_IAM_role _from_second_epic>`
	`username: eksadmin`
	Linten Sie die YAML-formatierte Datei, um Syntaxfehler zu vermeiden. Speichern Sie die Datei mithilfe von `vi` Befehlen und beenden Sie sie dann.
	Note
	Indem Sie diesen Abschnitt hinzufügen, teilen Sie der Kubernetes-RBAC mit, dass `<ARN_of_IAM_role`
		Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`_from_sec ond_epic>` sie vollen Administr atorzugriff auf den Amazon EKS-Clust er erhalten soll. Das bedeutet, dass die identifizierte IAM-Rolle administrative Aktionen auf dem Kubernetes-Cluster ausführen kann. AWS fügt den vorhanden en Abschnitt unter „`mapRoles`Während der Amazon EKS-Cluster bereitgestellt wird“ hinzu.	

Zugehörige Ressourcen

Referenzen

- Modulare und skalierbare Amazon EKS-Architektur (Quick Start)
- Verwaltung von Benutzern oder IAM-Rollen für Ihren Amazon EKS-Cluster
- CloudFormation AWS-Vorlage zur Erstellung einer neuen Amazon EKS-Kontrollebene

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Stellen Sie mithilfe von AWS CodePipeline, AWS und AWS Code in mehreren CodeCommit AWS-Regionen bereit CodeBuild

Erstellt von Anand Krishna Varanasi (AWS)

Übersicht

Dieses Muster zeigt, wie mithilfe von AWS eine Infrastruktur oder Architektur in mehreren Amazon Web Services (AWS) -Regionen aufgebaut werden kann CloudFormation. Es umfasst Continuous Integration (CI) /Continuous Deployment (CD) in mehreren AWS-Regionen für schnellere Bereitstellungen. Die Schritte in diesem Muster wurden beispielsweise für die Erstellung eines CodePipeline AWS-Jobs zur Bereitstellung in drei AWS-Regionen getestet. Sie können die Anzahl der Regionen je nach Anwendungsfall ändern.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- • Eine CodeBuild Rolle bei AmazonS3 FullAccess und CloudWatchFullAccessden Richtlinien. Diese Richtlinien ermöglichen CodeBuild den Zugriff auf die Überwachung von AWS-Ereignissen CodeCommit über Amazon CloudWatch und die Nutzung von Amazon Simple Storage Service (Amazon S3) als Artefaktspeicher.
  - Eine CloudFormation AWS-Rolle mit den folgenden Richtlinien, die AWS CloudFormation in der letzten Build-Phase die Möglichkeit geben, AWS Lambda-Funktionen zu erstellen oder zu aktualisieren, CloudWatch Amazon-Protokolle zu übertragen oder zu überwachen und Änderungssätze zu erstellen und zu aktualisieren.
    - AWSLambdaFullAccess
    - AWSCodeDeployFullAccess
    - CloudWatchFullAccess
    - AWSCloudFormationFullAccess
    - AWSCodePipelineFullAccess

> **Note**
>
> Zwei AWS Identity and Access Management (IAM) -Rollen für AWS CodeBuild und AWS CloudFormation mit geeigneten Richtlinien für CodeBuild die parallel Ausführung

der CI-Aufgaben wie Testen, Bündeln, Verpacken der Artefakte und Bereitstellung in mehreren AWS-Regionen. Überprüfen Sie die von erstellten Richtlinien, CodePipeline um sicherzustellen, dass AWS in den CI CodeBuild - und CD-Phasen CloudFormation über die entsprechenden Berechtigungen verfügt.

Architektur

Die Architektur und der Workflow dieses Musters für mehrere Regionen umfassen die folgenden Schritte.

1. Sie senden Ihren Code an ein Repository. CodeCommit
2. Ruft beim Empfang einer Codeaktualisierung oder CodeCommit eines Commits ein CloudWatch Ereignis auf, das wiederum einen CodePipeline Job startet.
3. CodePipeline aktiviert das CI, das von verwaltet wird. CodeBuild Die folgenden Aufgaben werden ausgeführt.
   - Testen der CloudFormation AWS-Vorlagen (optional)
   - Paketierung der CloudFormation AWS-Vorlagen für jede Region, die in der Bereitstellung enthalten ist. Dieses Muster wird beispielsweise parallel in drei AWS-Regionen bereitgestellt, sodass die CloudFormation AWS-Vorlagen in drei S3-Buckets CodeBuild gepackt werden, einen in jeder angegebenen Region. Die S3-Buckets werden nur CodeBuild als Artefakt-Repositorys verwendet.
4. CodeBuild packt die Artefakte als Eingabe für die nächste Bereitstellungsphase, die parallel in den drei AWS-Regionen läuft. Wenn Sie eine andere Anzahl von Regionen angeben, CodePipeline erfolgt die Bereitstellung in diesen Regionen.

Tools

Tools

- AWS CodePipeline — CodePipeline ist ein Continuous Delivery Service, mit dem Sie die Schritte modellieren, visualisieren und automatisieren können, die für die kontinuierliche Veröffentlichung Ihrer Softwareänderungen erforderlich sind.
- AWS CodeBuild — CodeBuild ist ein vollständig verwalteter Build-Service, der Ihren Quellcode kompiliert, Komponententests durchführt und Artefakte erzeugt, die sofort einsatzbereit sind.

- AWS CodeCommit — CodeCommit ist ein von Amazon Web Services gehosteter Service zur Versionskontrolle, mit dem Sie Ressourcen (wie Quellcode und Binärdateien) privat in der Cloud speichern und verwalten können.
- AWS CloudFormation — AWS CloudFormation ist ein Service, der Sie bei der Modellierung und Einrichtung Ihrer Amazon Web Services Services-Ressourcen unterstützt, sodass Sie weniger Zeit mit der Verwaltung dieser Ressourcen verbringen und sich mehr auf Ihre Anwendungen konzentrieren können, die in AWS ausgeführt werden.
- AWS Identity and Access Management — AWS Identity and Access Management (IAM) ist ein Webservice, mit dem Sie den Zugriff auf AWS-Ressourcen sicher kontrollieren können.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist Speicher für das Internet. Der Service ist darauf ausgelegt, Cloud Computing für Entwickler zu erleichtern.

Code

Der folgende Beispielcode bezieht sich auf die `BuildSpec.yaml` Datei (Erstellungsphase).

```
---
artifacts:
discard-paths: true
files:
- packaged-first-region.yaml
- packaged-second-region.yaml
- packaged-third-region.yaml
phases:
build:
commands:
- echo "********BUILD PHASE - CF PACKAGING**********"
- "aws cloudformation package --template-file sam-template.yaml --s3-bucket
 $S3_FIRST_REGION --output-template-file packaged-first-region.yaml --region
 $FIRST_REGION"
- "aws cloudformation package --template-file sam-template.yaml --s3-bucket
 $S3_SECOND_REGION --output-template-file packaged-second-region.yaml --region
 $SECOND_REGION"
- "aws cloudformation package --template-file sam-template-anand.yaml --s3-bucket
 $S3_THIRD_REGION --output-template-file packaged-third-region.yaml --region
 $THIRD_REGION"
install:
commands:
- echo "********BUILD PHASE - PYTHON SETUP**********"
runtime-versions:
```

```
python: 3.8
post_build:
commands:
- echo "********BUILD PHASE - PACKAGING COMPLETION**********"
pre_build:
commands:
- echo "********BUILD PHASE - DEPENDENCY SETUP**********"
- "npm install --silent --no-progress"
- echo "********BUILD PHASE - DEPENDENCY SETUP DONE**********"
version: 0.2
```

Epen

Bereiten Sie den Code und das CodeCommit Repository vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie die primäre AWS-Region für die Bereitstellung aus.	Melden Sie sich bei Ihrem AWS-Konto an und wählen Sie die primäre Region für die Bereitstellung aus. Das CodeCommit Repository wird sich in der primären Region befinden.	DevOps
Erstellen Sie das CodeCommit Repository.	Erstellen Sie das CodeCommit Repository und übertragen Sie den erforderlichen Code hinein. Der Code umfasst im Allgemeinen die AWS CloudFormation - oder AWS-SAM-Vorlagen, Lambda-Code, falls vorhanden, und die CodeBuild `buildspec .yaml` Dateien als Eingabe für AWS CodePipeline.	DevOps
Schieben Sie den Code in das CodeCommit Repository.	Laden Sie im Bereich Anlagen den Code für dieses Beispiel	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	herunter und übertragen Sie dann den erforderlichen Code hinein. Im Allgemeinen kann der Code AWS CloudForm ation - oder AWS-SAM-V orlagen, Lambda-Code und die CodeBuild `buildspec .yaml` Dateien als Eingabe für die Pipeline enthalten.	

Quellphase: Erstellen Sie die Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den CodePipel ine Job.	Wählen Sie in der CodePipel ine Konsole Create Pipeline aus.	DevOps
Geben Sie dem CodePipel ine Job einen Namen und wählen Sie die Einstellung für die Servicerolle aus.	Geben Sie einen Namen für den Job ein und behalten Sie die Standardeinstellung für die Servicerolle bei, sodass die Rolle mit den erforderl ichen Richtlinien CodePipeline erstellt wird.	DevOps
Geben Sie den Speicherort für den Artefaktspeicher an.	Behalten Sie unter Erweiterte Einstellungen die Standardo ption bei, sodass ein S3-Bucket CodePipeline erstellt wird, der für die Speicherung von Codeartefakten verwendet wird. Wenn Sie stattdessen einen vorhandenen S3-Bucket verwenden, muss sich der	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bucket in der primären Region befinden, die Sie im ersten Epic angegeben haben.	
Geben Sie den Verschlüs selungsschlüssel an.	Behalten Sie die Standardo ption AWS Managed Key bei oder entscheiden Sie sich dafür, Ihren eigenen vom Kunden verwalteten AWS Key Management Service (AWS KMS) -Schlüssel zu verwenden.	DevOps
Geben Sie den Quellanbieter an.	Wählen Sie unter Quellanbi eter die Option AWS aus CodeCommit.	DevOps
Geben Sie das Repository an.	Wähle das CodeCommit Repository aus, das du im ersten Epos erstellt hast. Wenn du den Code in einer Filiale platziert hast, wähle die Filiale aus.	DevOps
Geben Sie an, wie Codeänder ungen erkannt werden.	Behalten Sie die Standarde instellung Amazon CloudWatc h Events als Auslöser für die Änderung bei CodeCommit , um den CodePipeline Job zu starten.	DevOps

Erstellungsphase: Konfigurieren Sie die Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den Build-Anbieter an.	Wählen Sie als Build-Anbieter AWS aus CodeBuild.	DevOps
Geben Sie die AWS-Region an.	Wählen Sie die primäre Region aus, die Sie im ersten Epic angegeben haben.	DevOps

Erstellungsphase: Erstellen und konfigurieren Sie das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen des Projekts	Wählen Sie Projekt erstellen und geben Sie einen Namen für das Projekt ein.	DevOps
Geben Sie das Umgebungsbild an.	Verwenden Sie für diese Musterdemonstration das standardmäßige CodeBuild verwaltete Image. Sie haben auch die Möglichkeit, ein benutzerdefiniertes Docker-Image zu verwenden, falls Sie eines haben.	DevOps
Geben Sie das Betriebssystem an.	Wählen Sie entweder Amazon Linux 2 oder Ubuntu. **Note** Amazon Linux 2 nähert sich dem Ende der Unterstützung. Weitere Informati	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	onen finden Sie unter Amazon Linux FAQs 2.	
Geben Sie die Servicerolle an.	Wählen Sie die Rolle aus, für die Sie erstellt haben, CodeBuild bevor Sie mit der Erstellung des CodePipel ine Jobs begonnen haben. (Weitere Informationen finden Sie im Abschnitt Vorausset zungen.)	DevOps
Legen Sie zusätzliche Optionen fest.	Behalten Sie für Timeout und Queued Timeout die Standardwerte bei. Behalten Sie für das Zertifikat die Standardeinstellung bei, es sei denn, Sie haben ein benutzerd efiniertes Zertifikat, das Sie verwenden möchten.	DevOps
Erstellen Sie die Umgebungs variablen.	Erstellen Sie für jede AWS-Region, in der Sie die Bereitstellung durchführ en möchten, Umgebungs variablen, indem Sie den S3-Bucket-Namen und den Regionsnamen angeben (z. B. us-east-1).	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den Namen der Buildspec-Datei an, falls es sich nicht um buildspec.yml handelt.	Lassen Sie dieses Feld leer, wenn der Dateiname der Standardname ist. `buildspec.yaml` Wenn Sie die Buildspec-Datei umbenannt haben, geben Sie den Namen hier ein. Stellen Sie sicher, dass er dem Namen der Datei entsprich t, die sich im Repository befindet. CodeCommit	DevOps
Geben Sie die Protokollierung an.	Um Protokolle für Amazon CloudWatch Events zu sehen, behalten Sie die Standarde instellung bei. Sie können auch beliebige Gruppen- oder Logger-Namen definieren.	DevOps

Überspringen Sie die Bereitstellungsphase

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überspringen Sie die Bereitste llungsphase und schließen Sie die Erstellung der Pipeline ab.	Wenn Sie die Pipeline einrichten, CodePipeline können Sie nur eine Phase in der Bereitstellungsphase erstellen. Um die Bereitste llung in mehreren AWS-Regionen durchzuführen, überspringen Sie diese Phase. Nachdem die Pipeline erstellt wurde, können Sie mehrere	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Phasen der Bereitstellungspha se hinzufügen.	

Bereitstellungsphase: Konfigurieren Sie die Pipeline für die Bereitstellung in der ersten Region

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie der Bereitste llungsphase eine Phase hinzu.	Bearbeiten Sie die Pipeline und wählen Sie in der Bereitstellungsphase die Option Phase hinzufügen aus. Diese erste Phase ist für die primäre Region vorgesehen.	DevOps
Geben Sie einen Aktionsna men für die Phase ein.	Geben Sie einen eindeutig en Namen ein, der die erste (primäre) Phase und Region widerspiegelt. <region>Geben Sie beispielsweise primary_ _deploy ein.	DevOps
Geben Sie den Aktionsan bieter an.	Wählen Sie als Aktionsan bieter AWS aus CloudForm ation.	DevOps
Konfigurieren Sie die Region für die erste Phase.	Wählen Sie die erste (primäre) Region aus, dieselbe Region, in der CodePipeline und eingerichtet CodeBuild sind. Dies ist die primäre Region, in der Sie den Stack bereitstellen möchten.	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie das Eingabeartefakt an.	Wählen Sie BuildArtifact. Dies ist das Ergebnis der Erstellungsphase.	DevOps
Geben Sie die zu ergreifende Aktion an.	Wählen Sie für den Aktionsmodus die Option Stack erstellen oder aktualisieren aus.	DevOps
Geben Sie einen Namen für den CloudFormation Stack ein.		DevOps
Geben Sie die Vorlage für die erste Region an.	Wählen Sie den regionsspezifischen Paketnamen aus, der vom S3-Bucket für die erste (primäre) Region gepackt CodeBuild und dort abgelegt wurde.	DevOps
Geben Sie die Funktionen an.	Funktionen sind erforderlich, wenn die Stack-Vorlage IAM-Ressourcen enthält oder wenn Sie einen Stack direkt aus einer Vorlage erstellen, die Makros enthält. Verwenden Sie für dieses Muster CAPABILITY_IAM, CAPABILITY_NAMED_IAM, CAPABILITY_AUTO_EXPAND.	DevOps

Bereitstellungsphase: Konfigurieren Sie die Pipeline für die Bereitstellung in der zweiten Region

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die zweite Phase zur Bereitstellungsphase hinzu.	Um eine Phase für die zweite Region hinzuzufügen, bearbeiten Sie die Pipeline und wählen Sie in der Bereitstellungsphase die Option Phase hinzufügen aus. Wichtig: Die zweite Region wird genauso erstellt wie die erste Region, mit Ausnahme der folgenden Werte.	DevOps
Geben Sie einen Aktionsnamen für die zweite Phase ein.	Geben Sie einen eindeutigen Namen ein, der die zweite Phase und die zweite Region widerspiegelt.	DevOps
Konfigurieren Sie die Region für die zweite Phase.	Wählen Sie die zweite Region aus, in der Sie den Stack bereitstellen möchten.	DevOps
Geben Sie die Vorlage für die zweite Region an.	Wählen Sie den regionsspezifischen Paketnamen aus, der von der zweiten Region gepackt CodeBuild und in den S3-Bucket abgelegt wurde.	DevOps

Bereitstellungsphase: Konfigurieren Sie die Pipeline für die Bereitstellung in der dritten Region

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die dritte Phase zur Bereitstellungsphase hinzu.	Um eine Phase für die dritte Region hinzuzufügen, bearbeiten Sie die	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Pipeline und wählen Sie in der Bereitstellungsphase die Option Phase hinzufügen aus. Wichtig: Der Vorgang zum Erstellen der zweiten Region entspricht dem der beiden vorherigen Regionen, mit Ausnahme der folgenden Werte.	
Geben Sie einen Aktionsnamen für die dritte Phase ein.	Geben Sie einen eindeutigen Namen ein, der die dritte Phase und die dritte Region widerspiegelt.	DevOps
Konfigurieren Sie die Region für die dritte Stufe.	Wählen Sie die dritte Region aus, in der Sie den Stack bereitstellen möchten.	DevOps
Geben Sie die Vorlage für die dritte Region an.	Wählen Sie den regionsspezifischen Paketnamen aus, der von der dritten Region gepackt CodeBuild und in den S3-Bucket abgelegt wurde.	DevOps

Bereinigen Sie die Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die AWS-Ressourcen.	Um die Bereitstellung zu bereinigen, löschen Sie die CloudFormation Stacks in jeder Region. Löschen Sie anschließend die CodePipeline Ressourcen CodeCommi	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	t CodeBuild, und aus der primären Region.	

Zugehörige Ressourcen

- Was ist AWS CodePipeline?
- Serverloses AWS-Anwendungsmodell
- AWS CloudFormation
- Referenz zur CloudFormation AWS-Architekturstruktur für AWS CodePipeline

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Führen Sie Amazon Redshift SQL-Abfragen mithilfe von Terraform aus

Erstellt von Sylvia Qi (AWS) und Aditya Ambati (AWS)

Übersicht

Die Verwendung von Infrastructure as Code (IaC) für die Bereitstellung und Verwaltung von Amazon Redshift ist in diesem Bereich weit verbreitet. DevOps IaC erleichtert die Bereitstellung und Konfiguration verschiedener Amazon Redshift Redshift-Ressourcen wie Cluster, Snapshots und Parametergruppen. IaC erstreckt sich jedoch nicht auf die Verwaltung von Datenbankressourcen wie Tabellen, Schemas, Ansichten und gespeicherten Prozeduren. Diese Datenbankelemente werden über SQL-Abfragen verwaltet und nicht direkt von IaC-Tools unterstützt. Obwohl es Lösungen und Tools für die Verwaltung dieser Ressourcen gibt, ziehen Sie es möglicherweise vor, keine zusätzlichen Tools in Ihren Technologie-Stack aufzunehmen.

Dieses Muster beschreibt eine Methode, die Terraform verwendet, um Amazon Redshift Redshift-Datenbankressourcen wie Tabellen, Schemas, Ansichten und gespeicherte Prozeduren bereitzustellen. Das Muster unterscheidet zwischen zwei Arten von SQL-Abfragen:

- Nicht wiederholbare Abfragen — Diese Abfragen werden einmal während der ersten Amazon Redshift Redshift-Bereitstellung ausgeführt, um die wesentlichen Datenbankkomponenten einzurichten.
- Wiederholbare Abfragen — Diese Abfragen sind unveränderlich und können erneut ausgeführt werden, ohne die Datenbank zu beeinträchtigen. Die Lösung verwendet Terraform, um Änderungen an wiederholbaren Abfragen zu überwachen und sie entsprechend anzuwenden.

Weitere Informationen finden Sie unter Exemplarische Vorgehensweise zur Lösung unter Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

Sie müssen über ein aktives System verfügen AWS-Konto und Folgendes auf Ihrem Bereitstellungscomputer installieren:

- AWS Command Line Interface (AWS CLI)
- Ein mit Amazon Redshift Redshift-Lese-/Schreibberechtigungen konfiguriertes AWS CLI Profil
- Terraform Version 1.6.2 oder höher

- Python 3
- Boto3

Einschränkungen

- Diese Lösung unterstützt eine einzelne Amazon Redshift Redshift-Datenbank, da Terraform bei der Clustererstellung nur die Erstellung einer Datenbank ermöglicht.
- Dieses Muster beinhaltet keine Tests zur Validierung von Änderungen an den wiederholbaren Abfragen, bevor sie angewendet werden. Wir empfehlen, solche Tests zu integrieren, um die Zuverlässigkeit zu erhöhen.
- Zur Veranschaulichung der Lösung enthält dieses Muster eine `redshift.tf` Beispieldatei, die eine lokale Terraform-Statusdatei verwendet. Für Produktionsumgebungen empfehlen wir jedoch dringend, eine Remote-Statusdatei mit einem Sperrmechanismus zu verwenden, um die Stabilität und Zusammenarbeit zu verbessern.
- Einige AWS-Services sind nicht in allen verfügbar AWS-Regionen. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie unter Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Produktversionen

Diese Lösung wurde auf Amazon Redshift Patch 179 entwickelt und getestet.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub amazon-redshift-sql-deploy-terraform verfügbar.

Architektur

Das folgende Diagramm zeigt, wie Terraform die Amazon Redshift Redshift-Datenbankressourcen verwaltet, indem es sowohl nicht wiederholbare als auch wiederholbare SQL-Abfragen verarbeitet.

Das Diagramm zeigt die folgenden Schritte:

1. Terraform wendet während der ersten Bereitstellung des Amazon Redshift Redshift-Clusters nicht wiederholbare SQL-Abfragen an.
2. Der Entwickler überträgt Änderungen an den wiederholbaren SQL-Abfragen.

3. Terraform überwacht Änderungen in den wiederholbaren SQL-Abfragen.
4. Terraform wendet wiederholbare SQL-Abfragen auf die Amazon Redshift Redshift-Datenbank an.

Die durch dieses Muster bereitgestellte Lösung basiert auf dem Terraform-Modul für Amazon Redshift. Das Terraform-Modul stellt einen Amazon Redshift Redshift-Cluster und eine Datenbank bereit. Um das Modul zu verbessern, haben wir `terraform_data` Ressourcen verwendet, die ein benutzerdefiniertes Python-Skript aufrufen, um SQL-Abfragen mithilfe der Amazon Redshift ExecuteStatementRedshift-API-Operation auszuführen. Infolgedessen kann das Modul Folgendes tun:

- Stellen Sie eine beliebige Anzahl von Datenbankressourcen mithilfe von SQL-Abfragen bereit, nachdem die Datenbank bereitgestellt wurde.
- Überwachen Sie kontinuierlich die wiederholbaren SQL-Abfragen auf Änderungen und wenden Sie diese Änderungen mithilfe von Terraform an.

Weitere Informationen finden Sie unter Exemplarische Vorgehensweise zur Lösung unter Zusätzliche Informationen.

Tools

AWS-Services

- Amazon Redshift ist ein vollständig verwalteter Data-Warehouse-Service im Petabyte-Bereich in der. AWS Cloud

Andere Tools

- Terraform ist ein IaC-Tool (Infrastructure as Code) HashiCorp , mit dem Sie Cloud- und lokale Ressourcen erstellen und verwalten können.
- Python ist eine Allzweck-Programmiersprache, die in diesem Muster zur Ausführung von SQL-Abfragen verwendet wird.

Bewährte Methoden

- Bewährte Methoden für Amazon Redshift
- Verwenden der Amazon Redshift Data API zur Interaktion mit Amazon Redshift Redshift-Clustern

Epen

Stellen Sie die Lösung mit Terraform bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository.	Verwenden Sie den folgenden Befehl, um das Git-Repository zu klonen, das den Terraform -Code für die Bereitstellung eines Amazon Redshift Redshift-Clusters enthält. `git clone https://github.com/aws-samples/amazon-redshift-sql-deploy-terraform.git`	DevOps Ingenieur

Aktualisieren Sie die Terraform-Variablen.	Um die Amazon Redshift Redshift-Cluster-Bereitstellung an Ihre spezifischen Anforderungen anzupassen, aktualisieren Sie die folgenden Parameter in der `terraform.tfvars` Datei.
	`region = "<AWS_REGION>"`
	`cluster_identifier = "<REDSHIFT_CLUSTER_IDENTIFIER>"`
	`node_type = "<REDSHIFT_NODE_TYPE>"`
	`number_of_nodes = "<REDSHIFT_NODE_COUNT>"`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`database_name = "<REDSHIFT_DB_NAME>"`
	`subnet_ids = "<REDSHIFT_SUBNET_IDS>"`
	`vpc_security_group_ids = "<REDSHIFT_SECURITY_GROUP_IDS>"`
	`run_nonrepeatable_queries = true`
	`run_repeatable_queries = true`
	`sql_path_bootstrap = "<BOOTSTRAP_SQLS_PATH>"`
	`sql_path_nonrepeatable = "<NON-REPEATABLE_SQLS_PATH>"`
	`sql_path_repeatable = "<REPEATABLE_SQLS_PATH>"`
	`sql_path_finalize = "<FINALIZE_SQLS_PATH>"`
	`create_random_password = false`
	`master_username = "<REDSHIFT_MASTER_USERNAME>"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die Ressourcen mithilfe von Terraform bereit.	1. Um den Bereitstellungsprozess vorzubereiten, verwenden Sie den folgenden Befehl, um Terraform innerhalb des geklonten Repositorys zu initialisieren.
	`terraform init`
	2. Verwenden Sie den folgenden Befehl, um einen Ausführungsplan zu erstellen, um eine Vorschau der Änderungen anzuzeigen, die Terraform auf die Infrastruktur anwenden wird.
	`terraform plan -var-file terraform.tfvars`
	3. Verwenden Sie den folgenden Befehl, um den Amazon Redshift Redshift-Cluster und die zugehörigen Ressourcen bereitzustellen, um den Terraform-Ausführungsplan anzuwenden.
	`terraform apply -var-file terraform.tfvars`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

(Optional) Führen Sie zusätzliche SQL-Abfragen aus.	Das Beispiel-Repository bietet mehrere SQL-Abfragen für Demo-Zwecke. Um Ihre eigenen SQL-Abfragen auszuführen, fügen Sie sie den folgenden Ordnern hinzu:
	`/bootstrap`
	`/nonrepeatable`
	`/repeatable`
	`/finalize`	

Überwachen Sie die Ausführung von SQL-Anweisungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überwachen Sie die Bereitstellung von SQL-Anweisungen.	Sie können die Ergebnisse der SQL-Ausführungen in einem Amazon Redshift Redshift-Cluster überwachen. Beispiele für Ausgaben, die eine fehlgeschlagene und eine erfolgreiche SQL-Ausführung zeigen, finden Sie unter Beispiel-SQL-Anweisungen unter Zusätzliche Informationen.	DBA, Ingenieur DevOps
Bereinigen von Ressourcen.	Führen Sie den folgenden Befehl aus, um alle von Terraform bereitgestellten Ressourcen zu löschen.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`terraform destroy`	

Validieren Sie die Ergebnisse

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Daten im Amazon Redshift Redshift-Cluster.	1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon Redshift Redshift-Konsole. 2. Wählen Sie im Navigationsmenü Clusters (Cluster) aus. Wählen Sie den entsprechenden Clusternamen in der Liste aus. 3. Folgen Sie den Anweisungen unter Abfragen einer Datenbank mit dem Amazon Redshift Redshift-Abfrage-Editor v2 in der Amazon Redshift Redshift-Dokumentation.	DBA, AWS DevOps

Zugehörige Ressourcen

AWS Dokumentation

- Von Amazon Redshift bereitgestellte Cluster
- Behebung von Problemen mit der Amazon Redshift Data API

Sonstige Ressourcen

- Befehl: apply (Terraform-Dokumentation)

Zusätzliche Informationen

Exemplarische Vorgehensweise zur Lösung

Um die Lösung verwenden zu können, müssen Sie Ihre Amazon Redshift SQL-Abfragen auf eine bestimmte Weise organisieren. Alle SQL-Abfragen müssen in Dateien mit einer `.sql` Erweiterung gespeichert werden.

In dem mit diesem Muster bereitgestellten Codebeispiel sind die SQL-Abfragen in der folgenden Ordnerstruktur organisiert. Sie können den Code (`sql-queries.tf`und`sql-queries.py`) so ändern, dass er mit jeder Struktur funktioniert, die Ihrem individuellen Anwendungsfall entspricht.

```
/bootstrap
     |- Any # of files
     |- Any # of sub-folders
/nonrepeatable
     |- Any # of files
     |- Any # of sub-folders
/repeatable
     /udf
          |- Any # of files
          |- Any # of sub-folders
     /table
          |- Any # of files
          |- Any # of sub-folders
     /view
          |- Any # of files
          |- Any # of sub-folders
     /stored-procedure
          |- Any # of files
          |- Any # of sub-folders
/finalize
     |- Any # of files
     |- Any # of sub-folders
```

Angesichts der obigen Ordnerstruktur führt Terraform während der Bereitstellung von Amazon Redshift Redshift-Clustern die Abfragen in der folgenden Reihenfolge aus:

1. `/bootstrap`

2. `/nonrepeatable`
3. `/repeatable`
4. `/finalize`

Der `/repeatable` Ordner enthält vier Unterordner:`/udf`,, und. `/table` `/view` `/stored-procedure` Diese Unterordner geben die Reihenfolge an, in der Terraform die SQL-Abfragen ausführt.

Das Python-Skript, das die SQL-Abfragen ausführt, ist`sql-queries.py`. Zunächst liest das Skript alle Dateien und Unterordner eines bestimmten Quellverzeichnisses, z. B. den `sql_path_bootstrap` Parameter. Anschließend führt das Skript die Abfragen aus, indem es den Amazon Redshift ExecuteStatementRedshift-API-Vorgang aufruft. Möglicherweise haben Sie eine oder mehrere SQL-Abfragen in einer Datei. Der folgende Codeausschnitt zeigt die Python-Funktion, die in einer Datei gespeicherte SQL-Anweisungen für einen Amazon Redshift Redshift-Cluster ausführt.

```
def execute_sql_statement(filename, cluster_id, db_name, secret_arn, aws_region):
    """Execute SQL statements in a file"""
    redshift_client = boto3.client(
        'redshift-data', region_name=aws_region)
    contents = get_contents_from_file(filename),
    response = redshift_client.execute_statement(
        Sql=contents[0],
        ClusterIdentifier=cluster_id,
        Database=db_name,
        WithEvent=True,
        StatementName=filename,
        SecretArn=secret_arn
    )
    ...
```

Das Terraform-Skript `sql-queries.tf` erstellt die terraform_data-Ressourcen, die das Skript aufrufen. `sql-queries.py` Für jeden der vier Ordner gibt es eine `terraform_data` Ressource:,, und. `/bootstrap` `/nonrepeatable` `/repeatable` `/finalize` Der folgende Codeausschnitt zeigt die `terraform_data` Ressource, die die SQL-Abfragen im `/bootstrap` Ordner ausführt.

```
locals {
  program               = "${path.module}/sql-queries.py"
  redshift_cluster_name = try(aws_redshift_cluster.this[0].id, null)
```

```
}

resource "terraform_data" "run_bootstrap_queries" {
  count      = var.create && var.run_nonrepeatable_queries && (var.sql_path_bootstrap !
= "") && (var.snapshot_identifier == null) ? 1 : 0
  depends_on = [aws_redshift_cluster.this[0]]

  provisioner "local-exec" {
    command = "python3 ${local.program} ${var.sql_path_bootstrap}
 ${local.redshift_cluster_name} ${var.database_name} ${var.redshift_secret_arn}
 ${local.aws_region}"
  }
}
```

Mithilfe der folgenden Variablen können Sie steuern, ob diese Abfragen ausgeführt werden sollen. Wenn Sie keine Abfragen in`sql_path_bootstrap`,, oder ausführen möchten `sql_path_nonrepeatable` `sql_path_repeatable``sql_path_finalize`, legen Sie deren Werte auf fest"".

```
  run_nonrepeatable_queries = true
  run_repeatable_queries    = true
  sql_path_bootstrap        = "src/redshift/bootstrap"
  sql_path_nonrepeatable    = "src/redshift/nonrepeatable"
  sql_path_repeatable       = "src/redshift/repeatable"
  sql_path_finalize         = "src/redshift/finalize"
```

Bei der Ausführung berücksichtigt Terraform die `terraform_data` Ressource`terraform apply`, die nach Abschluss des Skripts hinzugefügt wurde, unabhängig von den Ergebnissen des Skripts. Wenn einige SQL-Abfragen fehlgeschlagen sind und Sie sie erneut ausführen möchten, können Sie die Ressource manuell aus dem Terraform-Status entfernen und erneut ausführen. `terraform apply` Mit dem folgenden Befehl wird die `run_bootstrap_queries` Ressource beispielsweise aus dem Terraform-Status entfernt.

```
terraform state rm module.redshift.terraform_data.run_bootstrap_queries[0]
```

Das folgende Codebeispiel zeigt, wie die `run_repeatable_queries` Ressource Änderungen im `repeatable` Ordner mithilfe des sha256-Hashs überwacht. Wenn eine Datei innerhalb des Ordners aktualisiert wird, markiert Terraform das gesamte Verzeichnis für ein Update. Dann führt Terraform die Abfragen im Verzeichnis im nächsten Schritt erneut aus. `terraform apply`

```
resource "terraform_data" "run_repeatable_queries" {
```

```
  count      = var.create_redshift && var.run_repeatable_queries &&
 (var.sql_path_repeatable != "") ? 1 : 0
  depends_on = [terraform_data.run_nonrepeatable_queries]

  # Continuously monitor and apply changes in the repeatable folder
  triggers_replace = {
    dir_sha256 = sha256(join("", [for f in fileset("${var.sql_path_repeatable}",
 "**") : filesha256("${var.sql_path_repeatable}/${f}")]))
  }

  provisioner "local-exec" {
    command = "python3 ${local.sql_queries} ${var.sql_path_repeatable}
 ${local.redshift_cluster_name} ${var.database_name} ${var.redshift_secret_arn}"
  }
}
```

Um den Code zu verfeinern, können Sie einen Mechanismus implementieren, mit dem Änderungen nur an den Dateien erkannt und angewendet werden, die innerhalb des `repeatable` Ordners aktualisiert wurden, anstatt Änderungen wahllos auf alle Dateien anzuwenden.

Beispiel für SQL-Anweisungen

Die folgende Ausgabe zeigt eine fehlgeschlagene SQL-Ausführung zusammen mit einer Fehlermeldung.

```
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec): Executing:
 ["/bin/sh" "-c" "python3 modules/redshift/sql-queries.py src/redshift/nonrepeatable
 testcluster-1 db1 arn:aws:secretsmanager:us-east-1:XXXXXXXXXXXX:secret:/redshift/
master_user/password-8RapGH us-east-1"]
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec):
 ----------------------------------------------------------------
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec): src/redshift/
nonrepeatable/table/admin/admin.application_family.sql
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec):
 ----------------------------------------------------------------
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec): Status:
 FAILED
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec): SQL execution
 failed.
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec): Error
 message: ERROR: syntax error at or near ")"
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec):   Position:
 244
```

```
module.redshift.terraform_data.run_nonrepeatable_queries[0]: Creation complete after 3s
 [id=ee50ba6c-11ae-5b64-7e2f-86fd8caa8b76]
```

Die folgende Ausgabe zeigt eine erfolgreiche SQL-Ausführung.

```
module.redshift.terraform_data.run_bootstrap_queries[0]: Provisioning with 'local-
exec'...
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec): Executing:
 ["/bin/sh" "-c" "python3 modules/redshift/sql-queries.py src/redshift/bootstrap
 testcluster-1 db1 arn:aws:secretsmanager:us-east-1:XXXXXXXXXXXX:secret:/redshift/
master_user/password-8RapGH us-east-1"]
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec):
 ----------------------------------------------------------------
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec): src/redshift/
bootstrap/db.sql
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec):
 ----------------------------------------------------------------
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec): Status: FINISHED
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec): SQL execution
 successful.
module.redshift.terraform_data.run_bootstrap_queries[0]: Creation complete after 2s
 [id=d565ef6d-be86-8afd-8e90-111e5ea4a1be]
```

Exportieren Sie AWS Backup Backup-Berichte aus einer gesamten Organisation in AWS Organizations als CSV-Datei

Erstellt von Aromal Raj Jayarajan (AWS) und Purushotham G K (AWS)

Übersicht

Dieses Muster zeigt, wie AWS Backup Backup-Jobberichte aus einer gesamten Organisation in AWS Organizations als CSV-Datei exportiert werden. Die Lösung verwendet AWS Lambda und Amazon, EventBridge um AWS Backup Backup-Jobberichte nach ihrem Status zu kategorisieren, was bei der Konfiguration statusbasierter Automatisierungen hilfreich sein kann.

AWS Backup unterstützt Unternehmen dabei, den Datenschutz für alle AWS-Services, in der Cloud und vor Ort zentral zu verwalten und zu automatisieren. Für innerhalb von AWS Organizations konfigurierte AWS-Backup-Jobs ist die konsolidierte Berichterstattung jedoch nur in der AWS-Managementkonsole des Verwaltungskontos der jeweiligen Organisation verfügbar. Wenn Sie diese Berichterstattung außerhalb des Verwaltungskontos platzieren, kann der für die Prüfung erforderliche Aufwand reduziert und der Umfang für Automatisierungen, Benachrichtigungen und Warnmeldungen erweitert werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine aktive Organisation in AWS Organizations, die mindestens ein Verwaltungskonto und ein Mitgliedskonto umfasst
- AWS Backup, konfiguriert auf Organisationsebene in AWS Organizations (weitere Informationen finden Sie im AWS-Blog unter Automatisieren zentraler Backups in großem Umfang für alle AWS-Services mithilfe von AWS Backup).
- Git, auf Ihrem lokalen Computer installiert und konfiguriert

Einschränkungen

Die in diesem Muster bereitgestellte Lösung identifiziert AWS-Ressourcen, die nur für AWS-Backup-Jobs konfiguriert sind. Der Bericht kann keine AWS-Ressourcen identifizieren, die nicht für die Sicherung über AWS Backup konfiguriert sind.

Architektur

Zieltechnologie-Stack

- AWS Backup
- AWS CloudFormation
- Amazon EventBridge
- AWS Lambda
- AWS Security Token Service (AWS STS)
- Amazon Simple Storage Service (Amazon-S3)
- AWS Identity and Access Management (IAM)

Zielarchitektur

Das folgende Diagramm zeigt einen Beispiel-Workflow für den Export von AWS Backup Backup-Jobberichten aus einer gesamten Organisation in AWS Organizations als CSV-Datei.

Das Diagramm zeigt den folgenden Workflow:

1. Eine Regel für geplante EventBridge Ereignisse ruft eine Lambda-Funktion im AWS-Mitgliedskonto (Berichtskonto) auf.
2. Die Lambda-Funktion verwendet dann AWS STS, um eine IAM-Rolle anzunehmen, die über die erforderlichen Berechtigungen verfügt, um eine Verbindung mit dem Verwaltungskonto herzustellen.
3. Die Lambda-Funktion macht dann Folgendes:
   - Fordert den konsolidierten Bericht über AWS-Backup-Jobs vom AWS Backup Backup-Service an
   - Kategorisiert die Ergebnisse basierend auf dem Status des AWS Backup Backup-Jobs
   - Konvertiert die Antwort in eine CSV-Datei
   - Lädt die Ergebnisse in einen Amazon S3 S3-Bucket im Berichtskonto in Ordnern hoch, die anhand ihres Erstellungsdatums gekennzeichnet sind

Tools

Tools

- AWS Backup ist ein vollständig verwalteter Service, mit dem Sie den Datenschutz für alle AWS-Services, in der Cloud und vor Ort zentralisieren und automatisieren können.
- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS-Lambda-Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen AWS-Konten.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie kontrollieren, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code

Der Code für dieses Muster ist im GitHub aws-backup-report-generatorRepository verfügbar.

Bewährte Methoden

- Bewährte Sicherheitsmethoden für Amazon S3 (Amazon S3 S3-Benutzerhandbuch)
- Bewährte Methoden für die Arbeit mit AWS Lambda-Funktionen (AWS Lambda Developer Guide)
- Bewährte Methoden für das Verwaltungskonto (AWS Organizations User Guide)

Epen

Stellen Sie die Lösungskomponenten bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	Klonen Sie das GitHub aws-backup-report-generator Repository, indem Sie den	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	folgenden Befehl in einem Terminalfenster ausführen: `git clone https://github.com/aws-samples/aws-backup-report-generator.git` Weitere Informationen finden Sie in der GitHub Dokumentation unter Ein Repository klonen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Lösungskomponenten im AWS-Mitgliedskonto (Berichtskonto) bereit.	1. Melden Sie sich im Mitgliedskonto (Berichtskonto) bei der AWS-Managementkonsole an und öffnen Sie dann die CloudFormation Konsole. 2. Wählen Sie Create stack (Stack erstellen) und dann With new resources (standard) (Mit neuen Ressourcen (Standard)). 3. Wählen Sie auf der Seite Stack erstellen im Abschnitt Vorlage angeben die Option Vorlagendatei hochladen aus. 4. Wählen Sie Datei auswählen aus. Navigieren Sie dann zum Stammordner des geklonten GitHub Repositorys auf Ihrer lokalen Workstation und wählen Sie template-reporting.yaml. 5. Wählen Sie Öffnen und dann Weiter. 6. Geben Sie auf der Seite „Stack-Details angeben“ unter Stackname einen Namen für Ihren CloudFormation Stack ein. 7. Geben Sie als ManagementAccountID die AWS-Konto	DevOps Ingenieur, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	-ID für das Verwaltungskonto Ihrer Organisation in AWS Organizations ein. 8. Wählen Sie Weiter aus. 9. Wählen Sie auf der Seite „Stack-Optionen konfigurieren“ die Option Weiter aus. 10. Aktivieren Sie auf der Seite Überprüfen das Kontrollkästchen, um zu bestätigen, dass Sie die Konfiguration überprüft haben. 11. Wählen Sie Stack erstellen aus. Der Stack zeigt den Status CREATE_COMPLETE an, wenn die Lösungskomponenten im Mitgliedskonto (Berichtskonto) bereitgestellt werden.	

Testen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie vor dem Testen sicher, dass die EventBridge Regel ausgeführt wird.	Stellen Sie sicher, dass die EventBridge Regel ausgeführt wird, indem Sie mindestens 24 Stunden warten oder indem Sie die Häufigkeit der Berichte in der Datei CloudFormation template-reporting.yml der Vorlage erhöhen.	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Um die Häufigkeit der Berichte zu erhöhen 1. Öffnen Sie die Datei template-reporting.yml im geklonten Repository. 2. Suchen Sie in der Ereignisregel mit der logischen ID " nach dem 'LambdaSchedule'. ScheduleExpression 3. Bearbeiten Sie den Schlüssel ScheduleExpression" so, dass er einen gültigen Cron-Ausdruck enthält. Der folgende Cron-Ausdruck plant beispielsweise, dass die Ereignisregel alle fünf Minuten ausgeführt wird: `“cron (* /5 * * * *)”`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Suchen Sie im Amazon S3 S3-Bucket nach dem generierten Bericht.	1. Melden Sie sich im Mitgliedskonto (Berichtskonto) bei der AWS-Managementkonsole an und öffnen Sie dann die CloudFormation Konsole. 2. Wählen Sie im Bereich Stacks den Namen des von Ihnen erstellten Stacks aus. Wählen Sie dann die Registerkarte Ressourcen. 3. Suchen Sie im Bereich Ressourcen in der Spalte Logische ID nach BackupReportS3Bucket. Öffnen Sie dann den zugehörigen Amazon S3 S3-Bucket in einer neuen Registerkarte, indem Sie den Link in der Spalte Physikalische ID neben dieser logischen ID auswählen. 4. Stellen Sie sicher, dass der Bucket einen Bericht enthält, der im folgenden Format generiert wurde: BackupReports////BackupReport- - - .csv <yyyy><mm><dd><BACKUP JOB STATUS><dd><Mon><yyyy>	AWS DevOps, DevOps Ingenieur

Bereinigen Ihrer Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die Lösungskomponenten aus dem Mitgliedskonto (Berichtskonto).	1. Öffnen Sie im Mitgliedskonto (Berichtskonto) den Amazon S3 S3-Bucket der Lösung. Anweisungen dazu finden Sie in den Schritten 2 bis 4 im Abschnitt Überprüfen Sie den S3-Bucket auf den generierten Bericht im Abschnitt Lösung testen dieses Musters. 2. Löschen Sie den Inhalt des Buckets und leeren Sie den Bucket. Anweisungen finden Sie unter Leeren eines Buckets im Amazon S3 S3-Benutzerhandbuch. 3. Melden Sie sich im Mitgliedskonto (Berichtskonto) bei der AWS-Managementkonsole an und öffnen Sie dann die CloudFormation Konsole. 4. Aktivieren Sie im Bereich Stacks das Kontrollkästchen neben dem Namen des von Ihnen erstellten Stacks. Wählen Sie dann Löschen aus.	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die Lösungskomponenten aus dem Verwaltungskonto.	1. Melden Sie sich im Verwaltungskonto bei der AWS-Managementkonsole an und öffnen Sie dann die CloudFormation Konsole. 2. Aktivieren Sie im Bereich Stacks das Kontrollkästchen neben dem Namen des von Ihnen erstellten Stacks. Wählen Sie dann Löschen aus.	AWS DevOps, DevOps Ingenieur

Zugehörige Ressourcen

- Tutorial: Verwenden von AWS Lambda mit geplanten Ereignissen (AWS Lambda Lambda-Dokumentation)
- Erstellen von geplanten Ereignissen zur Ausführung von AWS Lambda Lambda-Funktionen (AWS-SDK zur JavaScript Dokumentation)
- IAM-Tutorial: Delegieren des Zugriffs über AWS-Konten hinweg mithilfe von IAM-Rollen (IAM-Dokumentation)
- Terminologie und Konzepte von AWS Organizations (Dokumentation zu AWS Organizations)
- Erstellen von Berichtsplänen mit der AWS Backup Backup-Konsole (AWS Backup Backup-Dokumentation)
- Einen Auditbericht erstellen (AWS Backup Backup-Dokumentation)
- Erstellung von On-Demand-Berichten (AWS Backup Backup-Dokumentation)
- Was ist AWS Backup? (AWS-Backup-Dokumentation)
- Automatisieren Sie zentralisierte Backups in großem Umfang für alle AWS-Services mithilfe von AWS Backup (AWS-Blogbeitrag)

Tags für eine Liste von EC2 Amazon-Instances in eine CSV-Datei exportieren

Erstellt von Sida Ju (AWS) und Pac Joonhyun (AWS)

Übersicht

Dieses Muster zeigt, wie Tags für eine Liste von Amazon Elastic Compute Cloud (Amazon EC2) - Instances programmgesteuert in eine CSV-Datei exportiert werden.

Mithilfe des bereitgestellten Python-Beispielskripts können Sie den Zeitaufwand für die Überprüfung und Kategorisierung Ihrer EC2 Amazon-Instances nach bestimmten Tags reduzieren. Sie könnten das Skript beispielsweise verwenden, um schnell eine Liste von Instances zu identifizieren und zu kategorisieren, die Ihr Sicherheitsteam für Softwareupdates gekennzeichnet hat.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Python 3 installiert und konfiguriert
- AWS-Befehlszeilenschnittstelle (AWS CLI) installiert und konfiguriert

Einschränkungen

Das in diesem Muster bereitgestellte Beispiel-Python-Skript kann EC2 Amazon-Instances nur anhand der folgenden Attribute durchsuchen:

- Instanz IDs
- Private IPv4 Adressen
- Öffentliche IPv4 Adressen

Tools

- Python ist eine Allzweck-Computerprogrammiersprache.
- virtualenv hilft Ihnen, isolierte Python-Umgebungen zu erstellen.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

Code-Repository

Das Python-Skript für dieses Muster ist im GitHub search-ec2-Repository verfügbar. instances-export-tags

Epen

Installieren und konfigurieren Sie die Voraussetzungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	**Note** Wenn Sie beim Ausführen von AWS-CLI-Befehlen Fehler erhalten, stellen Sie sicher, dass Sie die neueste AWS-CLI-Version verwenden. Klonen GitHub Sie das instances-export-tags search-ec2-Repository, indem Sie den folgenden Git-Befehl in einem Terminalfenster ausführen: `git clone https://github.com/aws-samples/search-ec2-instances-export-tags.git`	DevOps Ingenieur
Installieren und aktivieren Sie virtualenv.	1. Installieren Sie virtualenv, indem Sie den folgenden Befehl ausführen:	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`python3 -m pip install virtualenv`
	2. Erstellen Sie eine neue virtuelle Umgebung, indem Sie den folgenden Befehl ausführen:
	`python3 -m venv env`
	3. Aktivieren Sie die neue virtuelle Umgebung, indem Sie den folgenden Befehl ausführen:
	`source env/bin/activate`
	Weitere Informationen finden Sie im virtualenv-Benutzerhandbuch.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie die Abhängigkeiten.	1. Öffnen Sie das Codeverzeichnis, indem Sie den folgenden Befehl im Terminal ausführen:
	`cd search-ec2-instances-export-tags`
	2. Installieren Sie die `requirements.txt` Datei, indem Sie den folgenden Pip-Befehl ausführen:
	`pip3 install -r requirements.txt`
		DevOps Ingenieur

Konfigurieren Sie ein benanntes AWS-Profil.	Falls Sie dies noch nicht getan haben, konfigurieren Sie ein benanntes AWS-Profil, das die erforderlichen Anmeldeinformationen für die Ausführung des Skripts enthält. Um ein benanntes Profil zu erstellen, führen Sie den Befehl aws configure aus. Weitere Informationen finden Sie unter Verwenden benannter Profile in der AWS-CLI-Dokumentation.	DevOps Ingenieur

Das Python-Skript konfigurieren und ausführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Eingabedatei.	Erstellen Sie eine Eingabedatei, die eine Liste der EC2 Amazon-Instances enthält, nach denen das Skript Tags suchen und exportieren soll. Sie können Instances IDs, private IPv4 Adressen oder öffentliche IPv4 Adressen auflisten.
	
	Important
	Stellen Sie sicher, dass jede EC2 Amazon-Instance in der Eingabedatei in einer eigenen Zeile aufgeführt ist.
	
	Beispiel für eine Eingabedatei
	
	`i-0547c351bdfe85b9f`
	`54.157.194.156`
	`172.31.85.33`
	`54.165.198.144`
	`i-0b6223b5914111a4b`
	`172.31.85.44`
	`54.165.198.145`
	`172.31.80.219`
	`172.31.94.199`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das Python-Skript aus.	Führen Sie das Skript aus, indem Sie den folgenden Befehl im Terminal ausführen: `python search_instances.py -i INPUTFILE -o OUTPUTFILE -r REGION [-p PROFILE]` **Note** `INPUTFILE` Ersetzen Sie es durch den Namen Ihrer Eingabedatei. `OUTPUTFILE` Ersetzen Sie durch den Namen, den Sie der CSV-Ausgabedatei geben möchten. `REGION`Ersetzen Sie durch die AWS-Region, in der sich Ihre EC2 Amazon-Ressourcen befinden. Wenn Sie ein benanntes AWS-Profil verwenden, `PROFILE` ersetzen Sie es durch das benannte Profil, das Sie verwenden.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Führen Sie den folgenden Befehl aus, um eine Liste der unterstützten Parameter und deren Beschreibung abzurufen : `python search_instances.py -h` Weitere Informationen und ein Beispiel für eine Ausgabedatei finden Sie in der `README.md` Datei im GitHub search-ec2-Repository. instances-export-tags	

Zugehörige Ressourcen

- Konfiguration der AWS-CLI (AWS-CLI-Benutzerhandbuch)

Generieren Sie mithilfe von Troposphere eine CloudFormation AWS-Vorlage, die von AWS Config verwaltete Regeln enthält

Erstellt von Lucas Nation (AWS) und Freddie Wilson (AWS)

Übersicht

Viele Organisationen verwenden verwaltete Regeln von AWS Config, um die Konformität ihrer Amazon Web Services (AWS) -Ressourcen anhand gängiger bewährter Methoden zu bewerten. Die Pflege dieser Regeln kann jedoch zeitaufwändig sein, und dieses Muster hilft Ihnen, Troposphere, eine Python-Bibliothek, zu nutzen, um verwaltete AWS Config-Regeln zu generieren und zu verwalten.

Das Muster hilft Ihnen bei der Verwaltung Ihrer von AWS Config verwalteten Regeln, indem Sie ein Python-Skript verwenden, um eine Microsoft Excel-Tabelle mit verwalteten AWS-Regeln in eine CloudFormation AWS-Vorlage zu konvertieren. Troposphere fungiert als Infrastruktur als Code (IaC). Das bedeutet, dass Sie die Excel-Tabelle mit verwalteten Regeln aktualisieren können, anstatt eine Datei im JSON- oder YAML-Format zu verwenden. Anschließend verwenden Sie die Vorlage, um einen CloudFormation AWS-Stack zu starten, der die verwalteten Regeln in Ihrem AWS-Konto erstellt und aktualisiert.

Die CloudFormation AWS-Vorlage definiert jede von AWS Config verwaltete Regel mithilfe der Excel-Tabelle und hilft Ihnen, die manuelle Erstellung einzelner Regeln in der AWS-Managementkonsole zu vermeiden. Das Skript verwendet für die Parameter jeder verwalteten Regel standardmäßig ein leeres Wörterbuch und für den Geltungsbereich die *`ComplianceResourceTypes`* Standardwerte von. *`THE_RULE_IDENTIFIER.template file`* Weitere Informationen zur Regel-ID finden Sie unter Creating AWS Config managed Rules with CloudFormation AWS-Vorlagen in der AWS Config-Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Vertrautheit mit der Verwendung von CloudFormation AWS-Vorlagen zur Erstellung von verwalteten AWS Config-Regeln. Weitere Informationen dazu finden Sie unter Creating AWS Config Managed Rules with CloudFormation AWS-Vorlagen in der AWS Config-Dokumentation.
- Python 3, installiert und konfiguriert. Weitere Informationen dazu finden Sie in der Python-Dokumentation.

- Eine bestehende integrierte Entwicklungsumgebung (IDE).
- Identifizieren Sie Ihre Organisationseinheiten (OUs) in einer Spalte in der `excel_config_rules.xlsx` Excel-Beispieltabelle (im Anhang).

Epen

Passen Sie die verwalteten Regeln von AWS Config an und konfigurieren Sie sie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Excel-Beispieltabelle.	Laden Sie die `excel_config_rules.xlsx` Excel-Beispieltabelle (beigefügt) herunter und kennzeichnen Sie sie als `Implemented` die von AWS Config verwalteten Regeln, die Sie verwenden möchten. Als markierte Regeln `Implemented` werden der CloudFormation AWS-Vorlage hinzugefügt.	Developer
(Optional) Aktualisieren Sie die Datei config_rules_params.json mit den AWS Config-Regelparametern.	Einige von AWS Config verwaltete Regeln erfordern Parameter und sollten mithilfe der `--param-file` Option als JSON-Datei an das Python-Skript übergeben werden. Die `access-keys-rotated` verwaltete Regel verwendet beispielsweise den folgenden `maxAccessKeyAge` Parameter: `{`	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"access-keys-rotated": {
	"InputParameters": {
	"maxAccessKeyAge": 90
	}
	}
	}</pre>
	In diesem Beispielparameter `maxAccessKeyAge` ist der auf 90 Tage festgelegt. Das Skript liest die Parameterdatei und fügt alle gefundenen Parameter `InputParameters` hinzu.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Aktualisieren Sie die Datei config_rules_params.json mit AWS Config. ComplianceResourceTypes	Standardmäßig ruft das Python-Skript die `ComplianceResourceTypes` von AWS definierten Vorlagen ab. Wenn Sie den Geltungsbereich einer bestimmten verwalteten AWS Config-Regel überschreiben möchten, müssen Sie sie mit der `--param-file` Option als JSON-Datei an das Python-Skript übergeben. Der folgende Beispielcode zeigt beispielsweise, wie der Wert `ComplianceResourceTypes` für in der `["AWS::EC2::Volume"]` Liste festgelegt `ec2-volume-inuse-check` ist: `{ "ec2-volume-inuse-check": { "Scope": { "ComplianceResourceTypes": [ "AWS::EC2::Volume" ] } } }`	Developer

Führen Sie das Python-Skript aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die Pip-Pakete aus der Datei requirements.txt.	Laden Sie die `requirements.txt` Datei (angehängt) herunter und führen Sie den folgenden Befehl in Ihrer IDE aus, um die Python-Pakete zu installieren: `pip3 install -r requirements.txt`	Developer
Führen Sie das Python-Skript aus.	1. Laden Sie die `aws_config_rules.py` Datei (angehängt) auf Ihren lokalen Computer herunter. 2. **Note** Führen Sie den `- python3 aws_config_rules.py --ou <OU_NAME>` Befehl aus.: `--ou` Definiert, welche OU-Spalte in der Excel-Tabelle ausgewählt werden soll. Sie können auch die folgenden optionalen Parameter hinzufügen:	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `--config-rule-option` — Definiert die Regeln, die aus der Excel-Tabelle ausgewählt werden können. Die Standardeinstellung ist der `Implemented` Parameter. • `--excel-file` — Der Pfad für die Excel-Tabelle. Der Standardwert ist `aws_config_rules.xlsx` . • `--param-file` — Der Pfad der Parameter-JSON-Datei. Der Standardwert ist `config_rules_params.json` . • `--max-execution-frequency` — Definiert, wie oft die von AWS Config verwalteten Regeln ausgewertet werden. Die Auswahlmöglichkeiten sind `One_Hour` `Three_Hours` ,`Six_Hours` ,`Twelve_Hours` , oder`TwentyFour_Hours` . Der Standardwert ist `TwentyFour_Hours` .	

Stellen Sie die verwalteten Regeln von AWS Config bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den CloudFormation AWS-Stack.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die CloudFormation AWS-Konsole und wählen Sie dann Stack erstellen. 2. Wählen Sie auf der Seite Vorlage angeben die Option Vorlagendatei hochladen aus und laden Sie dann Ihre CloudFormation AWS-Vorlage hoch. 3. Geben Sie einen Stack-Namen an und wählen Sie dann Weiter. 4. Geben Sie Tags an und wählen Sie dann Weiter. 5. Wählen Sie Stack erstellen aus.	Developer

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Geben Sie SageMaker Notebook-Instances temporären Zugriff auf ein CodeCommit Repository in einem anderen AWS-Konto

Erstellt von Helge Aufderheide (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Dieses Muster zeigt, wie Amazon SageMaker Notebook-Instances und Benutzern temporären Zugriff auf ein CodeCommit AWS-Repository gewährt wird, das sich in einem anderen AWS-Konto befindet. Dieses Muster zeigt auch, wie Sie detaillierte Berechtigungen für bestimmte Aktionen gewähren können, die jede Entität in jedem Repository ausführen kann.

Organizations speichern CodeCommit Repositorys häufig in einem anderen AWS-Konto als dem Konto, das ihre Entwicklungsumgebung hostet. Diese Einrichtung mit mehreren Konten hilft bei der Kontrolle des Zugriffs auf die Repositorys und reduziert das Risiko, dass sie versehentlich gelöscht werden. Um diese kontoübergreifenden Berechtigungen zu gewähren, empfiehlt es sich, AWS Identity and Access Management (IAM) -Rollen zu verwenden. Anschließend können vordefinierte IAM-Identitäten in jedem AWS-Konto vorübergehend die Rollen übernehmen, um eine kontrollierte Vertrauenskette zwischen den Konten aufzubauen.

> **Note**
>
> Sie können ein ähnliches Verfahren anwenden, um anderen IAM-Identitäten kontoübergreifenden Zugriff auf ein Repository zu gewähren. CodeCommit Weitere Informationen finden Sie unter Kontenübergreifendes Zugriff auf ein CodeCommit AWS-Repository mithilfe von Rollen konfigurieren im CodeCommit AWS-Benutzerhandbuch.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit einem CodeCommit Repository (Konto A)
- Ein zweites aktives AWS-Konto mit einer SageMaker Notebook-Instance (Konto B)
- Ein AWS-Benutzer mit ausreichenden Berechtigungen zum Erstellen und Ändern von IAM-Rollen in Konto A

- Ein zweiter AWS-Benutzer mit ausreichenden Berechtigungen zum Erstellen und Ändern von IAM-Rollen in Konto B

Architektur

Das folgende Diagramm zeigt einen Beispiel-Workflow, um einer SageMaker Notebook-Instance und Benutzern in einem AWS-Konto kontoübergreifenden Zugriff auf ein CodeCommit Repository zu gewähren:

Das Diagramm zeigt den folgenden Workflow:

1. Die AWS-Benutzerrolle und die SageMaker Notebook-Instance-Rolle in Konto B gehen von einem benannten Profil aus.
2. Die Berechtigungsrichtlinie des benannten Profils spezifiziert eine CodeCommit Zugriffsrolle in Konto A, die das Profil dann annimmt.
3. Die Vertrauensrichtlinie der CodeCommit Zugriffsrolle in Konto A ermöglicht es dem benannten Profil in Konto B, die CodeCommit Zugriffsrolle zu übernehmen.
4. Die IAM-Berechtigungsrichtlinie des CodeCommit Repositorys in Konto A ermöglicht der CodeCommit Zugriffsrolle den Zugriff auf das CodeCommit Repository.

Technologie-Stack

- CodeCommit
- Git
- IAM
- pip
- SageMaker

Tools

- AWS CodeCommit ist ein Versionskontrollservice, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.

- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Git ist ein verteiltes Versionskontrollsystem zur Nachverfolgung von Änderungen im Quellcode während der Softwareentwicklung.
- git-remote-codecommitist ein Hilfsprogramm, mit dem du Code aus CodeCommit Repositorys pushen und abrufen kannst, indem es Git erweitert.
- pip ist der Paket-Installer für Python. Sie können pip verwenden, um Pakete aus dem Python-Paketindex und anderen Indizes zu installieren.

Bewährte Methoden

Wenn Sie Berechtigungen mit IAM-Richtlinien festlegen, stellen Sie sicher, dass Sie nur die für die Ausführung einer Aufgabe erforderlichen Berechtigungen gewähren. Weitere Informationen finden Sie unter Geringste Berechtigungen anwenden in der IAM-Dokumentation.

Achten Sie bei der Implementierung dieses Musters darauf, dass Sie wie folgt vorgehen:

- Stellen Sie sicher, dass die IAM-Prinzipien nur über die Berechtigungen verfügen, die für die Durchführung bestimmter, erforderlicher Aktionen in jedem Repository erforderlich sind. Es wird beispielsweise empfohlen, genehmigten IAM-Prinzipien die Übertragung und Zusammenführung von Änderungen an bestimmten Repository-Branches zu gestatten, aber nur Zusammenführungen mit geschützten Branches anzufordern.
- Vergewissern Sie sich, dass den IAM-Prinzipien je nach ihren jeweiligen Rollen und Verantwortlichkeiten für jedes Projekt unterschiedliche IAM-Rollen zugewiesen werden. Ein Entwickler hat beispielsweise andere Zugriffsberechtigungen als ein Release-Manager oder AWS-Administrator.

Epen

Konfigurieren Sie die IAM-Rollen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die CodeCommit Zugriffsrolle und die Berechtigungsrichtlinie.	**Note** Um den in diesem Epos dokumenti erten manuellen Einrichtungsprozes s zu automatisieren, können Sie eine CloudFormation AWS-Vorlage verwenden. Gehen Sie in dem Konto, das das CodeCommit Repository enthält (Konto A), wie folgt vor: 1. Erstellen Sie eine IAM-Rolle , die von der SageMaker Notebook-Instanzrolle in Konto B übernommen werden kann. 2. Erstellen Sie eine IAM-Richtlinie, die Zugriff auf das Repository gewährt, und fügen Sie die Richtlini e der Rolle hinzu. Wählen Sie nur zu Testzweck en die von AWSCodeCo mmitPowerUserAWS verwaltete Richtlinie. Diese Richtlinie gewährt alle	Allgemein AWS, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CodeCommit Berechtigungen mit Ausnahme der Möglichkeit, Ressourcen zu löschen. 3. Ändern Sie die Vertrauensrichtlinie der Rolle, sodass Konto B als vertrauenswürdige Entität aufgeführt wird. **Important** Bevor Sie dieses Setup in Ihre Produktionsumgebung verschieben, empfiehlt es sich, Ihre eigene IAM-Richtlinie zu schreiben, die Berechtigungen mit den geringsten Rechten anwendet. Weitere Informationen finden Sie im Abschnitt Zusätzliche Informationen dieses Musters.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erteilen Sie der Rolle der SageMaker Notebook-Instance in Konto B die Berechtigungen, um die CodeCommit Zugriffsrolle in Konto A zu übernehmen.	Gehen Sie in dem Konto, das die IAM-Rolle der SageMaker Notebook-Instanz enthält (Konto B), wie folgt vor: 1. Erstellen Sie eine IAM-Richtlinie, die es einer IAM-Rolle oder einem IAM-Benutzer ermöglicht, die CodeCommit Zugriffsrolle in Konto A zu übernehmen. Beispiel für eine IAM-Berechtigungsrichtlinie, die es einer IAM-Rolle oder einem IAM-Benutzer ermöglicht, eine kontoübergreifende Rolle anzunehmen `{ "Version": "2012-10-17", "Statement": [ { "Sid": "VisualEditor0", "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "arn:aws:iam:::accountA_ID:role/accountArole_ID" } }` 2. Ordnen Sie die Richtlinie der Rolle Ihrer SageMaker	Allgemein AWS, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Notebook-Instanz in Konto B zu. 3. Lassen Sie die Rolle der SageMaker Notebook-Instanz in Konto B die CodeCommit Zugriffsrolle in Konto A übernehmen. **Note** Informationen zum Amazon-Ressourcennamen (ARN) Ihres Repositorys finden Sie unter CodeCommit Repository-Details anzeigen im CodeCommit AWS-Benutzerhandbuch.	

Richten Sie Ihre SageMaker Notebook-Instanz in Konto B ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie ein Benutzerprofil auf der SageMaker AWS-Notebook-Instance ein, um die Rolle in Konto A zu übernehmen.	**Important** Stellen Sie sicher, dass Sie die neueste Version der AWS-Befehlszeilenschnittstelle (AWS CLI) installiert haben.	Allgemein AWS, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Gehen Sie in dem Konto, das die SageMaker Notebook-Instance enthält (Konto B), wie folgt vor:
	
	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die SageMaker -Konsole.
	2. Greifen Sie auf Ihre SageMaker Notebook-Instanz zu. Die Jupyter-Schnittstelle wird geöffnet.
	3. Wählen Sie Neu und dann Terminal. In Ihrer Jupyter-Umgebung wird ein neues Terminalfenster geöffnet.
	4. Navigieren Sie zur Datei SageMaker ~/.aws/config der Notebook-Instanz. Fügen Sie dann der Datei ein Benutzerprofil hinzu, indem Sie die folgende Anweisung eingeben:
	
	`------.aws/config-------------`
	`[profile remoterepouser]`
	`role_arn = arn:aws:iam::<ID of Account A>:role/<rolename>`
	`role_session_name = remoteaccesssession`
	`region = eu-west-1`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`credential_source = Ec2InstanceMetadata`
	`----------`
	`----------`	

Installieren Sie das git-remote-codecommit Hilfsprogramm.	Folgen Sie den Anweisungen in Schritt 2: Installation git-remote-codecommit im CodeCommit AWS-Benutzerhandbuch.	Data Scientist

Greifen Sie auf das Repository zu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Greifen Sie mit Git-Befehlen oder auf das CodeCommit Repository zu SageMaker.	Um Git zu verwenden IAM-Prinzipale, die die Rolle der SageMaker Notebook-Instanz in Konto B übernehmen, können jetzt Git-Befehle ausführen, um auf das CodeCommit Repository in Konto A zuzugreifen. Benutzer können beispielsweise Befehle wie `git clonegit pull`, und ausführen. `git push` Anweisungen finden Sie unter Connect zu einem CodeCommit AWS-Repository herstellen im CodeCommit AWS-Benutzerhandbuch. Informationen zur Verwendung von Git mit CodeCommit	Git, Bash-Konsole

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	finden Sie unter Erste Schritte mit AWS CodeCommit im CodeCommit AWS-Benut zerhandbuch. Zu verwenden SageMaker Um Git von der SageMaker Konsole aus zu verwenden , müssen Sie Git erlauben, Anmeldeinformationen aus Ihrem CodeCommi t Repository abzurufen. Anweisungen finden Sie in der SageMaker Dokumenta tion unter Verknüpfen eines CodeCommit Repositorys in einem anderen AWS-Konto mit einer Notebook-Instance.	

Zugehörige Ressourcen

- Kontenübergreifenden Zugriff auf ein CodeCommit AWS-Repository mithilfe von Rollen konfigurieren (CodeCommit AWS-Dokumentation)
- IAM-Tutorial: Delegieren des Zugriffs über AWS-Konten hinweg mithilfe von IAM-Rollen (IAM-Dokumentation)

Zusätzliche Informationen

Beschränken CodeCommit von Berechtigungen auf bestimmte Aktionen

Um die Aktionen einzuschränken, die ein IAM-Principal im CodeCommit Repository ausführen kann, ändern Sie die Aktionen, die in der CodeCommit Zugriffsrichtlinie zulässig sind.

Weitere Informationen zu CodeCommit API-Vorgängen finden Sie in der CodeCommit Berechtigungsreferenz im CodeCommit AWS-Benutzerhandbuch.

> **Note**
>
> Sie können die von AWSCodeCommitPowerUserAWS verwaltete Richtlinie auch an Ihren Anwendungsfall anpassen.

Beschränkung der CodeCommit Berechtigungen auf bestimmte Repositorys

Gehen Sie wie folgt vor, um eine mandantenfähige Umgebung zu erstellen, in der mehr als ein Code-Repository nur bestimmten Benutzern zugänglich ist:

1. Erstellen Sie mehrere CodeCommit Zugriffsrollen in Konto A. Konfigurieren Sie anschließend die Vertrauensrichtlinie jeder Zugriffsrolle so, dass bestimmte Benutzer in Konto B die Rolle übernehmen können.
2. Schränken Sie ein, welche Code-Repositorys jede Rolle annehmen kann, indem Sie der Richtlinie jeder CodeCommit Zugriffsrolle die Bedingung „Ressource“ hinzufügen.

Beispiel für eine „Ressource“ -Bedingung, die den Zugriff eines IAM-Prinzipals auf ein bestimmtes Repository einschränkt CodeCommit

```
"Resource" : [<REPOSITORY_ARN>,<REPOSITORY_ARN> ]
```

> **Note**
>
> Um mehrere Code-Repositorys in demselben AWS-Konto identifizieren und unterscheiden zu können, können Sie den Namen der Repositorys unterschiedliche Präfixe zuweisen. Beispielsweise können Sie Code-Repositorys mit Präfixen benennen, die unterschiedlichen Entwicklergruppen zugeordnet sind, wie myproject-subproject1-repo1 und myproject-subproject2-repo1. Anschließend können Sie eine IAM-Rolle für jede Entwicklergruppe auf der Grundlage der ihnen zugewiesenen Präfixe erstellen. Sie könnten beispielsweise eine Rolle mit dem Namen myproject-subproject1-repoaccess erstellen und ihr Zugriff auf alle Code-Repositorys gewähren, die das Präfix myproject-subproject1 enthalten.

Beispiel für eine „Ressource“ -Bedingung, die sich auf einen Code-Repository-ARN bezieht, der ein bestimmtes Präfix enthält

```
"Resource" : arn:aws:codecommit:<region>:<account-id>:myproject-subproject1-*
```

Implementieren Sie eine GitHub Flow-Branching-Strategie für Umgebungen mit mehreren Konten DevOps

Erstellt von Mike Stephens (AWS) und Abhilash Vinod (AWS)

Übersicht

Bei der Verwaltung eines Quellcode-Repositorys wirken sich unterschiedliche Verzweigungsstrategien auf die Softwareentwicklungs- und Veröffentlichungsprozesse aus, die Entwicklungsteams verwenden. Beispiele für gängige Branching-Strategien sind Trunk, GitHub Flow und Gitflow. Diese Strategien verwenden unterschiedliche Branches, und die Aktivitäten, die in jeder Umgebung ausgeführt werden, sind unterschiedlich. Organizations, die DevOps Prozesse implementieren, würden von einem visuellen Leitfaden profitieren, der ihnen hilft, die Unterschiede zwischen diesen Verzweigungsstrategien zu verstehen. Die Verwendung dieser Grafik in Ihrem Unternehmen hilft Entwicklungsteams dabei, ihre Arbeit besser aufeinander abzustimmen und die Unternehmensstandards einzuhalten. Dieses Muster bietet dieses Bild und beschreibt den Prozess der Implementierung einer GitHub Flow-Branching-Strategie in Ihrem Unternehmen.

Dieses Muster ist Teil einer Dokumentationsserie über die Auswahl und Implementierung von DevOps Branching-Strategien für Organisationen mit mehreren. AWS-Konten Diese Serie soll Ihnen helfen, von Anfang an die richtige Strategie und die richtigen Best Practices anzuwenden, um Ihre Erfahrung in der Cloud zu optimieren. GitHub Flow ist nur eine mögliche Verzweigungsstrategie, die Ihr Unternehmen anwenden kann. Diese Dokumentationsreihe behandelt auch Trunk - und Gitflow-Verzweigungsmodelle. Falls Sie dies noch nicht getan haben, empfehlen wir Ihnen, den Artikel Auswahl einer Git-Branching-Strategie für DevOps Umgebungen mit mehreren Konten zu lesen, bevor Sie die Anleitung in diesem Muster implementieren. Bitte wählen Sie mit der gebotenen Sorgfalt die richtige Branching-Strategie für Ihr Unternehmen aus.

Dieser Leitfaden enthält ein Diagramm, das zeigt, wie eine Organisation die GitHub Flow-Strategie umsetzen könnte. Es wird empfohlen, die AWS Well-Architected DevOps Guidance zu lesen, um sich über bewährte Verfahren zu informieren. Dieses Muster enthält empfohlene Aufgaben, Schritte und Einschränkungen für jeden Schritt im DevOps Prozess.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Git, installiert. Dies wird als Quellcode-Repository-Tool verwendet.

- Draw.io, installiert. Diese Anwendung wird verwendet, um das Diagramm anzuzeigen und zu bearbeiten.

Architektur

Zielarchitektur

Das folgende Diagramm kann wie ein Punnett-Quadrat (Wikipedia) verwendet werden. Sie richten die Zweige auf der vertikalen Achse mit den AWS Umgebungen auf der horizontalen Achse aus, um zu bestimmen, welche Aktionen in den einzelnen Szenarien ausgeführt werden sollen. Die Zahlen geben die Reihenfolge der Aktionen im Workflow an. Dieses Beispiel führt Sie von einer `feature` Filiale bis zur Bereitstellung in der Produktion.

Weitere Informationen zu Umgebungen und Branches in einem GitHub Flow-Ansatz findest du unter Auswahl einer Git-Branching-Strategie für Umgebungen mit mehreren Konten DevOps . AWS-Konten

Automatisierung und Skalierung

Kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) is the process of automating the software release lifecycle. It automates much or all of the manual processes traditionally required to get new code from an initial commit into production. A CI/CD pipeline encompasses the sandbox, development, testing, staging, and production environments. In each environment, the CI/CD pipeline provisions any infrastructure that is needed to deploy or test the code. By using CI/CD, development teams can make changes to code that are then automatically tested and deployed. CI/CDPipelines) bieten den Entwicklungsteams auch Kontrolle und Richtlinien, indem sie Konsistenz, Standards, bewährte Verfahren und Mindestakzeptanzniveaus für die Akzeptanz und Bereitstellung von Funktionen durchsetzen. Weitere Informationen finden Sie unter Practicing Continuous Integration and Continuous Delivery am. AWS

AWS bietet eine Reihe von Entwicklerservices, die Sie beim Aufbau von CI/CD-Pipelines unterstützen sollen. AWS CodePipelineIst beispielsweise ein vollständig verwalteter Continuous Delivery Service, der Sie bei der Automatisierung Ihrer Release-Pipelines für schnelle und zuverlässige Anwendungs- und Infrastrukturupdates unterstützt. AWS CodeBuildkompiliert Quellcode, führt Tests durch und produziert ready-to-deploy Softwarepakete. Weitere Informationen finden Sie unter Entwicklertools unter AWS.

Tools

AWS Dienste und Tools

AWS stellt eine Suite von Entwicklerdiensten bereit, mit denen Sie dieses Muster implementieren können:

- AWS CodeArtifactist ein hoch skalierbarer, verwalteter Artefakt-Repository-Service, mit dem Sie Softwarepakete für die Anwendungsentwicklung speichern und gemeinsam nutzen können.
- AWS CodeBuildist ein vollständig verwalteter Build-Service, der Sie beim Kompilieren von Quellcode, beim Ausführen von Komponententests und beim Erstellen von Artefakten unterstützt, die sofort einsatzbereit sind.
- AWS CodeDeployautomatisiert Bereitstellungen in Amazon Elastic Compute Cloud (Amazon EC2) oder lokalen Instances, AWS Lambda Funktionen oder Amazon Elastic Container Service (Amazon ECS) -Services.
- AWS CodePipelinehilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.

Andere Tools

- Draw.io Desktop ist eine Anwendung zum Erstellen von Flussdiagrammen und Diagrammen. Das Code-Repository enthält Vorlagen im .drawio-Format für Draw.io.
- Figma ist ein Online-Designtool, das für die Zusammenarbeit entwickelt wurde. Das Code-Repository enthält Vorlagen im .fig-Format für Figma.

Code-Repository

Diese Quelldatei für das Diagramm in diesem Muster ist im Repository GitHub Git Branching Strategy for GitHub Flow verfügbar. Sie enthält Dateien in den Formaten PNG, Draw.io und Figma. Sie können diese Diagramme ändern, um die Prozesse Ihres Unternehmens zu unterstützen.

Bewährte Methoden

Folgen Sie den Best Practices und Empfehlungen in AWS Well-Architected DevOps Guidance und Choosing a Git Branching Strategy for Multi-Account-Umgebungen. DevOps Diese helfen Ihnen dabei, die GitHub Flow-basierte Entwicklung effektiv zu implementieren, die Zusammenarbeit zu fördern, die Codequalität zu verbessern und den Entwicklungsprozess zu rationalisieren.

Epen

Überprüfung der GitHub Flow-Workflows

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den GitHub Standard-Flow-Prozess.	1. In der Sandbox-U mgebung erstellt der Entwickler aus dem `feature` Branch einen Branch und verwendet das `main` Benennung smuster`feature/<ticket>_<initials>_<short description>` . 2. Der Entwickler fügt dem `feature` Branch einen oder mehrere Commits hinzu, die jeweils eine eigenständige Änderung oder Verbesserung darstellen. 3. Der Entwickler öffnet eine Merge-Anfrage (MR), um die Änderungen im `main` Branch zusammenzuführen. Dadurch wird ein Überprüfu ngsprozess eingeleitet. 4. Während des Überprüfu ngsprozesses bespreche n die Entwickler die Codeänderungen und geben Feedback. Ziel ist es, sicherzustellen, dass die Änderungen von hoher	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Qualität sind und den Projektstandards entsprechen. 5. Nachdem der Entwickler die Merge-Anfrage erstellt hat, wird ein automatisierter Build-Prozess gestartet und die Änderungen in der `feature` Filiale in der Entwicklungsumgebung bereitgestellt. 6. Automatisierte Tests überprüfen die Integrität und Qualität der in der Merge-Anfrage enthaltenen Änderungen. Ein erfolgreicher Build, eine erfolgreiche Bereitstellung und erfolgreiche Tests sind erforderlich, um die Zusammenführungsanforderung abzuschließen. 7. Wenn der Überprüfungsprozess abgeschlossen ist, werden die Änderungen in der `main` Filiale zusammengeführt. 8. Ein Genehmiger genehmigt manuell die Bereitstellung der Release-Artefakte in der Testumgebung. 9. Ein Genehmiger genehmigt manuell die Bereitstellung	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Release-Artefakte in der Staging-Umgebung. 10. Ein Genehmiger genehmigt manuell die Bereitstellung der Release-Artefakte in der Produktionsumgebung.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Bugfix GitHub Flow-Prozess.	1. Der Entwickler erstellt aus dem `bugfix` Zweig einen `main` Zweig und verwendet das Benennung smusterbugfix/<ticket number>_<developer initials>_<descriptor> . 2. Der Entwickler behebt das Problem, überträgt den Fix und erstellt den `bugfix` Branch. 3. Der Entwickler öffnet eine Merge-Anfrage, um den Branch mit dem `bugfix` Branch zusammenzuführen. `main` Dadurch wird ein Überprüfungsprozess eingeleitet. 4. Während des Überprüfungsprozesses besprechen die Entwickler die Codeänderungen und geben Feedback. 5. Nach Abschluss und Genehmigung der Überprüfung schließt der Entwickler die Anfrage zur Zusammenführung der `bugfix` Filiale mit der `main` Filiale ab. 6. Ein Genehmiger genehmigt manuell die Bereitstellung	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Release-Artefakte in höheren Umgebungen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Hotfix GitHub Flow-Prozess.	GitHub Flow ist so konzipier t, dass es eine kontinuierliche Bereitstellung ermöglicht, bei der Codeänderungen häufig und zuverlässig in höheren Umgebungen implementiert werden. Der Schlüssel ist, dass jede `feature` Filiale jederzeit einsatzbereit ist. `Hotfix`Zweige, die `feature` `bugfix` OD-Zweigen ähneln, können dem gleichen Prozess folgen wie jeder dieser anderen Zweige. Aufgrund ihrer Dringlichkeit haben Hotfixes jedoch in der Regel eine höhere Priorität . Abhängig von den Richtlini en des Teams und der Unmittelbarkeit der Situation können bestimmte Schritte im Prozess beschleunigt werden. Beispielsweise könnten Codeüberprüfungen für Hotfixes beschleunigt werden. Daher entspricht der Hotfix-Prozess zwar dem Feature- oder Bugfix-Prozess, die Dringlichkeit der Hotfixes kann jedoch Änderungen bei der Einhaltung der Verfahren rechtfertigen. Es ist wichtig, Richtlinien für die Verwaltun g von Hotfixes festzulegen,	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	um sicherzustellen, dass diese effizient und sicher behandelt werden.	

Fehlerbehebung

Problem	Lösung
Konflikte in der Branche	Ein häufiges Problem, das beim GitHub Flow-Modell auftreten kann, besteht darin, dass ein Hotfix in der Produktion ausgeführt werden muss, aber eine entsprechende Änderung in einem `featurebugfix`, oder `hotfix` -Zweig erfolgen muss, in dem dieselben Ressource n geändert werden. Wir empfehlen, dass Sie Änderungen häufig aus `main` untergeordneten Zweigen zusammenführen, um erhebliche Konflikte beim Zusammenführen mit zu `main` vermeiden.
Reife des Teams	GitHub Flow fördert tägliche Implement ierungen in höheren Umgebungen und setzt auf echte Continuous Integration und Continuou s Delivery (CI/CD). Es ist unerlässlich, dass das Team über die nötige technische Reife verfügt, um Funktionen zu entwickeln und Automatisierungstests für diese zu erstellen . Das Team muss eine umfassende Prüfung der Zusammenführungsanfrage durchführen, bevor die Änderungen genehmigt werden. Dies fördert eine solide technische Kultur, die Qualität, Rechenschaftspflicht und Effizienz im Entwicklungsprozess fördert.

Zugehörige Ressourcen

In diesem Leitfaden sind keine Schulungen für Git enthalten. Es stehen jedoch viele hochwertige Ressourcen im Internet zur Verfügung, falls Sie diese Schulung benötigen. Wir empfehlen, dass Sie mit der Git-Dokumentationsseite beginnen.

Die folgenden Ressourcen können Ihnen bei Ihrer Reise zur GitHub Flow-Verzweigung in der AWS Cloud helfen.

AWS DevOps Anleitung

- AWS DevOps Beratung
- AWS Referenzarchitektur für die Bereitstellungspipeline
- Was ist DevOps?
- DevOps Ressourcen

GitHub Strömungsführung

- GitHub Flow-Schnellstart-Tutorial () GitHub
- Warum GitHub Flow?

Sonstige Ressourcen

- Zwölf-Faktoren-App-Methodik (12factor.net)

Implementieren Sie eine Gitflow-Branching-Strategie für Umgebungen mit mehreren Konten DevOps

Erstellt von Mike Stephens (AWS), Stephen DiCato (AWS), Tim Wondergem (AWS) und Abhilash Vinod (AWS)

Übersicht

Bei der Verwaltung eines Quellcode-Repositorys wirken sich unterschiedliche Verzweigungsstrategien auf die Softwareentwicklungs- und Veröffentlichungsprozesse aus, die Entwicklungsteams verwenden. Beispiele für gängige Branching-Strategien sind Trunk, Gitflow und Flow. GitHub Diese Strategien verwenden unterschiedliche Branches, und die Aktivitäten, die in jeder Umgebung ausgeführt werden, sind unterschiedlich. Organizations, die DevOps Prozesse implementieren, würden von einem visuellen Leitfaden profitieren, der ihnen hilft, die Unterschiede zwischen diesen Verzweigungsstrategien zu verstehen. Die Verwendung dieser Grafik in Ihrem Unternehmen hilft Entwicklungsteams dabei, ihre Arbeit besser aufeinander abzustimmen und die Unternehmensstandards einzuhalten. Dieses Muster bietet dieses Bild und beschreibt den Prozess der Implementierung einer Gitflow-Branching-Strategie in Ihrer Organisation.

Dieses Muster ist Teil einer Dokumentationsserie über die Auswahl und Implementierung von DevOps Branching-Strategien für Organisationen mit mehreren. AWS-Konten Diese Serie soll Ihnen helfen, von Anfang an die richtige Strategie und die richtigen Best Practices anzuwenden, um Ihre Erfahrung in der Cloud zu optimieren. Gitflow ist nur eine mögliche Branching-Strategie, die Ihr Unternehmen anwenden kann. Diese Dokumentationsreihe behandelt auch Trunk - und GitHub Flow-Verzweigungsmodelle. Falls Sie dies noch nicht getan haben, empfehlen wir Ihnen, den Artikel Auswahl einer Git-Branching-Strategie für DevOps Umgebungen mit mehreren Konten zu lesen, bevor Sie die Anleitung in diesem Muster implementieren. Bitte wählen Sie mit der gebotenen Sorgfalt die richtige Branching-Strategie für Ihr Unternehmen aus.

Dieser Leitfaden enthält ein Diagramm, das zeigt, wie eine Organisation die Gitflow-Strategie umsetzen könnte. Es wird empfohlen, die AWS Well-Architected DevOps Guidance zu lesen, um sich über bewährte Verfahren zu informieren. Dieses Muster enthält empfohlene Aufgaben, Schritte und Einschränkungen für jeden Schritt im DevOps Prozess.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Git, installiert. Dies wird als Quellcode-Repository-Tool verwendet.

- Draw.io, installiert. Diese Anwendung wird verwendet, um das Diagramm anzuzeigen und zu bearbeiten.
- (Optional) Gitflow-Plugin, installiert.

Architektur

Zielarchitektur

Das folgende Diagramm kann wie ein Punnett-Quadrat (Wikipedia) verwendet werden. Sie richten die Zweige auf der vertikalen Achse mit den AWS Umgebungen auf der horizontalen Achse aus, um zu bestimmen, welche Aktionen in den einzelnen Szenarien ausgeführt werden sollen. Die Zahlen geben die Reihenfolge der Aktionen im Workflow an. Dieses Beispiel führt Sie von einem Feature-Branch bis zur Bereitstellung in der Produktion.

Weitere Informationen zu den AWS-Konten Umgebungen und Branches in einem Gitflow-Ansatz findest du unter Auswahl einer Git-Branching-Strategie für Umgebungen mit mehreren DevOps Konten.

Automatisierung und Skalierung

Kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) is the process of automating the software release lifecycle. It automates much or all of the manual processes traditionally required to get new code from an initial commit into production. A CI/CD pipeline encompasses the sandbox, development, testing, staging, and production environments. In each environment, the CI/CD pipeline provisions any infrastructure that is needed to deploy or test the code. By using CI/CD, development teams can make changes to code that are then automatically tested and deployed. CI/CDPipelines) bieten den Entwicklungsteams auch Kontrolle und Richtlinien, indem sie Konsistenz, Standards, bewährte Verfahren und Mindestakzeptanzniveaus für die Akzeptanz und Bereitstellung von Funktionen durchsetzen. Weitere Informationen finden Sie unter Practicing Continuous Integration and Continuous Delivery auf. AWS

AWS bietet eine Reihe von Entwicklerservices, die Sie beim Aufbau von CI/CD-Pipelines unterstützen sollen. AWS CodePipelineIst beispielsweise ein vollständig verwalteter Continuous Delivery Service, der Sie bei der Automatisierung Ihrer Release-Pipelines für schnelle und zuverlässige Anwendungs- und Infrastrukturupdates unterstützt. AWS CodeBuildkompiliert Quellcode, führt Tests durch und produziert ready-to-deploy Softwarepakete. Weitere Informationen finden Sie unter Entwicklertools unter AWS.

Tools

AWS Dienste und Tools

AWS stellt eine Suite von Entwicklerdiensten bereit, mit denen Sie dieses Muster implementieren können:

- AWS CodeArtifactist ein hoch skalierbarer, verwalteter Artefakt-Repository-Service, mit dem Sie Softwarepakete für die Anwendungsentwicklung speichern und gemeinsam nutzen können.
- AWS CodeBuildist ein vollständig verwalteter Build-Service, der Sie beim Kompilieren von Quellcode, beim Ausführen von Komponententests und beim Erstellen von Artefakten unterstützt, die sofort einsatzbereit sind.
- AWS CodeDeployautomatisiert Bereitstellungen in Amazon Elastic Compute Cloud (Amazon EC2) oder lokalen Instances, AWS Lambda Funktionen oder Amazon Elastic Container Service (Amazon ECS) -Services.
- AWS CodePipelinehilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.

Andere Tools

- Draw.io Desktop ist eine Anwendung zum Erstellen von Flussdiagrammen und Diagrammen. Das Code-Repository enthält Vorlagen im .drawio-Format für Draw.io.
- Figma ist ein Online-Designtool, das für die Zusammenarbeit entwickelt wurde. Das Code-Repository enthält Vorlagen im .fig-Format für Figma.
- (Optional) Das Gitflow-Plugin ist eine Sammlung von Git-Erweiterungen, die Repository-Operationen auf hoher Ebene für das Gitflow-Verzweigungsmodell bereitstellen.

Code-Repository

Diese Quelldatei für das Diagramm in diesem Muster ist in der GitHub Git Branching Strategy for GitFlow Repository verfügbar. Sie enthält Dateien in den Formaten PNG, Draw.io und Figma. Sie können diese Diagramme ändern, um die Prozesse Ihres Unternehmens zu unterstützen.

Bewährte Methoden

Folgen Sie den Best Practices und Empfehlungen in AWS Well-Architected DevOps Guidance und Choosing a Git Branching Strategy for Multi-Account-Umgebungen. DevOps Diese helfen dir dabei, die GitFlow-basierte Entwicklung effektiv zu implementieren, die Zusammenarbeit zu fördern, die Codequalität zu verbessern und den Entwicklungsprozess zu rationalisieren.

Epen

Überprüfung der Gitflow-Workflows

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfe den Standard-Gitflow-Prozess.	1. In der Sandbox-Umgebung erstellt der Entwickler aus dem `feature` Branch einen Branch und verwendet das `develop` Benennungsmuster. `feature/<ticket>_<initials>_<short description>` 2. Der Entwickler entwickelt Code und stellt den Code iterativ in der Sandbox-Umgebung bereit, um das Ticket abzuschließen. **Note** Der Entwickler kann optional einen `sandbox` Branch erstellen, um eine automatisierte Build- oder Deploy-Pipeline in der Sandbox-U	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	mgebung auszuführ en. 3. Der Entwickler erstellt mithilfe einer Squash-Merge eine Merge-Anf rage von der `feature` `develop` Verzweigung in die Verzweigung. 4. Eine CI/CD-Pipeline (Continuous Integration and Continuous Delivery) erstellt den `develop` Branch automatisch und stellt ihn in der Entwicklungsumgebung bereit. 5. (Optional) Ein Entwickler integriert weitere `feature` Branches in den Develop-Branch, bevor er mit den Release-Aktivitäten fortfährt . 6. Wenn Sie bereit sind, die Funktionen im `develop` Branch zu veröffentlichen, erstellt der Entwickler einen `release` Branch, der nach `release/v<number>` dem `develop` Branch benannt ist. 7. Der Entwickler erstellt den Release-Zweig, in dem Artefakte zur Wiederver wendung in anderen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Umgebungen veröffentlicht werden. 8. Ein Genehmiger genehmigt manuell die Bereitstellung der Release-Artefakte in der Testumgebung. 9. Ein Genehmiger genehmigt manuell die Bereitstellung der Release-Artefakte in der Staging-Umgebung. 10. Ein Genehmiger genehmigt manuell die Bereitstellung der Release-Artefakte in der Produktionsumgebung. 11. Der Entwickler führt den Zweig mit dem `release` Zweig zusammen. `main` Im Idealfall verwendet der Entwickler ein automatisiertes Skript, um eine schnelle Zusammenführung durchzuführen. Verwenden Sie keinen Squash-Merge. 12. Der Entwickler führt den Zweig mit dem `release` Zweig zusammen. `develop` Im Idealfall verwendet der Entwickler ein automatisiertes Skript, um eine schnelle Zusammenführung durchzuführen. Verwenden Sie keinen Squash-Merge.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Hotfix-Gitflow-Prozess.	1. Der Entwickler erstellt aus dem `hotfix` Branch einen `main` Branch und verwendet das Benennungsmuster. `hotfix/<ticket>_<initials>_<short description>` 2. Der Entwickler erstellt aus dem `release` Zweig einen `main` Zweig und benennt ihn `release/v<number>` . 3. Der Entwickler behebt das Problem, überträgt den Fix und erstellt den `hotfix` Branch. 4. Der Entwickler erstellt mithilfe eines Squash-Merge-Verfahrens `hotfix` eine Merge-Anfrage vom `release/v<number>` Branch in den Branch. 5. Der Entwickler erstellt den `release` Branch, der Artefakte zur Wiederverwendung in anderen Umgebungen veröffentlicht. 6. Ein Genehmiger genehmigt manuell die Bereitstellung der Release-Artefakte in der Testumgebung. 7. Ein Genehmiger genehmigt manuell die Bereitstellung	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Release-Artefakte in der Staging-Umgebung. 8. Ein Genehmiger genehmigt manuell die Bereitstellung der Release-Artefakte in der Produktionsumgebung. 9. Der Entwickler führt den Zweig mit dem `release` Zweig zusammen. `main` Im Idealfall verwendet der Entwickler ein automatis iertes Skript, um eine schnelle Zusammenführung durchzuführen. Verwenden Sie keinen Squash-Merge. 10. Der Entwickler führt den Zweig mit dem `release` Zweig zusammen. `develop` Im Idealfall verwendet der Entwickle r ein automatisiertes Skript, um eine schnelle Zusammenführung durchzuführen. Verwenden Sie keinen Squash-Merge. 11. Wenn ein Konflikt erkannt wird, erhalten Entwickler eine Warnung und lösen den Konflikt mit einer Merge-Anfrage.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfe den Bugfix-Gitflow-Prozess.	1. Der Entwickler erstellt einen `bugfix` Branch aus dem aktuellen `release/v<number>` Branch und verwendet das Benennungsmuster. `bugfix/<ticket number>_<developer initials>_<descriptor>` 2. Der Entwickler behebt das Problem, überträgt den Fix und erstellt den `bugfix` Branch. 3. Der Entwickler erstellt mithilfe eines Squash-Merge-Verfahrens `bugfix` eine Merge-Anfrage vom `release/v<number>` Branch in den Branch. 4. Der Entwickler erstellt den `release` Branch, der Artefakte zur Wiederverwendung in anderen Umgebungen veröffentlicht. 5. Ein Genehmiger genehmigt manuell die Bereitstellung der Release-Artefakte in der Testumgebung. 6. Ein Genehmiger genehmigt manuell die Bereitstellung der Release-Artefakte in der Stage-Umgebung.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Ein Genehmiger genehmigt manuell die Bereitstellung der Release-Artefakte in der Produktionsumgebung. 8. Der Entwickler führt den Zweig mit dem `release` Zweig zusammen. `main` Im Idealfall verwendet der Entwickler ein automatis iertes Skript, um eine schnelle Zusammenführung durchzuführen. Verwenden Sie keinen Squash-Merge. 9. Der Entwickler führt den Zweig mit dem `release` Zweig zusammen. `develop` Im Idealfall verwendet der Entwickle r ein automatisiertes Skript, um eine schnelle Zusammenführung durchzuführen. Verwenden Sie keinen Squash-Merge. 10. Wenn ein Konflikt erkannt wird, erhalten Entwickler eine Warnung und lösen den Konflikt mit einer Merge-Anfrage.	

Fehlerbehebung

Problem	Lösung
Konflikte in der Branche	Ein häufiges Problem, das beim Gitflow-Modell auftreten kann, besteht darin, dass ein Hotfix in der Produktion ausgeführt werden muss, eine entsprechende Änderung jedoch in einer niedrigeren Umgebung vorgenommen werden muss, in der ein anderer Zweig dieselben Ressourcen ändert. Wir empfehlen, dass jeweils nur ein einziger Release-Zweig aktiv ist. Wenn mehr als ein Branch gleichzeitig aktiv ist, kollidieren die Änderungen in den Umgebungen möglicherweise und Sie können einen Branch möglicherweise nicht in die Produktion überführen.
Zusammenführen	Releases sollten so schnell wie möglich wieder in die Hauptversionen integriert und weiterentwickelt werden, um die Arbeit wieder in den primären Zweigen zu konsolidieren.
Zusammenführung von Squash	Verwenden Sie eine Squash-Merge nur, wenn Sie von einem `feature` Zweig zu einem Zweig zusammenführen. `develop` Die Verwendung von Squash-Merges in höheren Zweigen führt zu Schwierigkeiten, wenn Änderungen wieder in niedrigere Zweige zurückgeführt werden.

Zugehörige Ressourcen

In diesem Leitfaden sind keine Schulungen für Git enthalten. Es stehen jedoch viele hochwertige Ressourcen im Internet zur Verfügung, falls Sie diese Schulung benötigen. Wir empfehlen, dass Sie mit der Git-Dokumentationsseite beginnen.

Die folgenden Ressourcen können Ihnen bei Ihrer Reise nach Gitflow-Branches in der helfen. AWS Cloud

AWS DevOps Anleitung

- AWS DevOps Beratung
- AWS Referenzarchitektur für die Bereitstellungspipeline
- Was ist DevOps?
- DevOps Ressourcen

Gitflow-Anleitung

- Der ursprüngliche Gitflow-Blog (Blogbeitrag von Vincent Driessen)
- Gitflow-Workflow (Atlassian)
- Gitflow on GitHub: So verwendest du Git Flow-Workflows mit GitHub Based Repos (Video) YouTube
- Beispiel für Git Flow Init (YouTube Video)
- Der Gitflow-Release-Zweig von Anfang bis Ende (Video) YouTube

Sonstige Ressourcen

Zwölf-Faktoren-App-Methodik (12factor.net)

Implementieren Sie eine Trunk-Branching-Strategie für Umgebungen mit mehreren Konten DevOps

Erstellt von Mike Stephens (AWS) und Rayjan Wilson (AWS)

Übersicht

Bei der Verwaltung eines Quellcode-Repositorys wirken sich unterschiedliche Verzweigungsstrategien auf die Softwareentwicklungs- und Release-Prozesse aus, die von Entwicklungsteams verwendet werden. Beispiele für gängige Branching-Strategien sind Trunk, GitHub Flow und Gitflow. Diese Strategien verwenden unterschiedliche Branches, und die Aktivitäten, die in jeder Umgebung ausgeführt werden, sind unterschiedlich. Organizations, die DevOps Prozesse implementieren, würden von einem visuellen Leitfaden profitieren, der ihnen hilft, die Unterschiede zwischen diesen Verzweigungsstrategien zu verstehen. Die Verwendung dieser Grafik in Ihrem Unternehmen hilft Entwicklungsteams dabei, ihre Arbeit besser aufeinander abzustimmen und die Unternehmensstandards einzuhalten. Dieses Muster bietet dieses Bild und beschreibt den Prozess der Implementierung einer Trunk-Branching-Strategie in Ihrer Organisation.

Dieses Muster ist Teil einer Dokumentationsreihe über die Auswahl und Implementierung von DevOps Branching-Strategien für Organisationen mit mehreren Filialen. AWS-Konten Diese Serie soll Ihnen helfen, von Anfang an die richtige Strategie und die richtigen Best Practices anzuwenden, um Ihre Erfahrung in der Cloud zu optimieren. Trunk ist nur eine mögliche Verzweigungsstrategie, die Ihr Unternehmen anwenden kann. Diese Dokumentationsreihe behandelt auch die GitHub Branching-Modelle Flow und Gitflow. Falls Sie dies noch nicht getan haben, empfehlen wir Ihnen, den Artikel Auswahl einer Git-Branching-Strategie für DevOps Umgebungen mit mehreren Konten zu lesen, bevor Sie die Anleitung in diesem Muster implementieren. Bitte wählen Sie mit der gebotenen Sorgfalt die richtige Branching-Strategie für Ihr Unternehmen aus.

Dieser Leitfaden enthält ein Diagramm, das zeigt, wie ein Unternehmen die Trunk-Strategie umsetzen könnte. Es wird empfohlen, die offiziellen AWS DevOps Well-Architected-Leitlinien zu lesen, um sich über bewährte Verfahren zu informieren. Dieses Muster enthält empfohlene Aufgaben, Schritte und Einschränkungen für jeden Schritt im DevOps Prozess.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Git, installiert. Dies wird als Quellcode-Repository-Tool verwendet.

- Draw.io, installiert. Diese Anwendung wird verwendet, um das Diagramm anzuzeigen und zu bearbeiten.

Architektur

Zielarchitektur

Das folgende Diagramm kann wie ein Punnett-Quadrat (Wikipedia) verwendet werden. Sie richten die Zweige auf der vertikalen Achse mit den AWS Umgebungen auf der horizontalen Achse aus, um zu bestimmen, welche Aktionen in den einzelnen Szenarien ausgeführt werden sollen. Die Zahlen geben die Reihenfolge der Aktionen im Workflow an. Dieses Beispiel führt Sie von einer `feature` Filiale bis zur Bereitstellung in der Produktion.

Weitere Informationen zu Umgebungen und Branches in einem Trunk-Ansatz finden Sie unter Auswahl einer Git-Branching-Strategie für Umgebungen mit mehreren Konten DevOps . AWS-Konten

Automatisierung und Skalierung

Kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) is the process of automating the software release lifecycle. It automates much or all of the manual processes traditionally required to get new code from an initial commit into production. A CI/CD pipeline encompasses the sandbox, development, testing, staging, and production environments. In each environment, the CI/CD pipeline provisions any infrastructure that is needed to deploy or test the code. By using CI/CD, development teams can make changes to code that are then automatically tested and deployed. CI/CDPipelines) bieten den Entwicklungsteams auch Kontrolle und Richtlinien, indem sie Konsistenz, Standards, bewährte Verfahren und Mindestakzeptanzniveaus für die Akzeptanz und Bereitstellung von Funktionen durchsetzen. Weitere Informationen finden Sie unter Practicing Continuous Integration and Continuous Delivery auf. AWS

AWS bietet eine Reihe von Entwicklerservices, die Sie beim Aufbau von CI/CD-Pipelines unterstützen sollen. AWS CodePipelineIst beispielsweise ein vollständig verwalteter Continuous Delivery Service, der Sie bei der Automatisierung Ihrer Release-Pipelines für schnelle und zuverlässige Anwendungs- und Infrastrukturupdates unterstützt. AWS CodeBuildkompiliert Quellcode, führt Tests durch und produziert ready-to-deploy Softwarepakete. Weitere Informationen finden Sie unter Entwicklertools unter AWS.

Tools

AWS Dienste und Tools

AWS stellt eine Suite von Entwicklerdiensten bereit, mit denen Sie dieses Muster implementieren können:

- AWS CodeArtifactist ein hoch skalierbarer, verwalteter Artefakt-Repository-Service, mit dem Sie Softwarepakete für die Anwendungsentwicklung speichern und gemeinsam nutzen können.
- AWS CodeBuildist ein vollständig verwalteter Build-Service, der Sie beim Kompilieren von Quellcode, beim Ausführen von Komponententests und beim Erstellen von Artefakten unterstützt, die sofort einsatzbereit sind.
- AWS CodeDeployautomatisiert Bereitstellungen in Amazon Elastic Compute Cloud (Amazon EC2) oder lokalen Instances, AWS Lambda Funktionen oder Amazon Elastic Container Service (Amazon ECS) -Services.
- AWS CodePipelinehilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.

Andere Tools

- Draw.io Desktop — Eine Anwendung zum Erstellen von Flussdiagrammen und Diagrammen.
- Figma ist ein Online-Design-Tool, das für die Zusammenarbeit entwickelt wurde. Das Code-Repository enthält Vorlagen im .fig-Format für Figma.

Code-Repository

Diese Quelldatei für das Diagramm in diesem Muster ist im Repository GitHub Git Branching Strategy for Trunk verfügbar. Sie enthält Dateien in den Formaten PNG, Draw.io und Figma. Sie können diese Diagramme ändern, um die Prozesse Ihres Unternehmens zu unterstützen.

Bewährte Methoden

Folgen Sie den Best Practices und Empfehlungen in AWS Well-Architected DevOps Guidance und Choosing a Git Branching Strategy for Multi-Account-Umgebungen. DevOps Diese helfen dir dabei, Trunk-basierte Entwicklung effektiv zu implementieren, die Zusammenarbeit zu fördern, die Codequalität zu verbessern und den Entwicklungsprozess zu rationalisieren.

Epen

Überprüfung des Trunk-Workflows

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Standard-Trunk-Prozess.	1. In der Sandbox-Umgebung erstellt der Entwickler aus dem `feature` Branch einen Branch und verwendet das `main` Benennung smuster`feature/<ticket>_<initials>_<short description>` . 2. Der Entwickler entwickelt Code und stellt den Code iterativ in der Sandbox-Umgebung bereit, um das Ticket abzuschließen. **Note** Der Entwickler kann optional einen `sandbox` Branch erstellen, um eine automatisierte Build- oder Deploy-Pipeline in der Sandbox-Umgebung auszuführen. 3. Der Entwickler erstellt mithilfe einer Squash-Merge	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eine Merge-Anfrage von der `feature` `main` Verzweigung in die Verzweigung. 4. Eine CI/CD-Pipeline (Continuous Integration and Continuous Delivery) erstellt und veröffentlicht die Artefakte aus dem `main` Branch automatisch in der Entwicklungsumgebung. 5. Ein Genehmiger genehmigt manuell die Bereitstellung der Release-Artefakte in der Entwicklungsumgebung. 6. Ein Genehmiger genehmigt manuell die Bereitstellung der Release-Artefakte in der Testumgebung. 7. Ein Genehmiger genehmigt manuell die Bereitstellung der Release-Artefakte in der Staging-Umgebung. 8. Ein Genehmiger genehmigt manuell die Bereitstellung der Release-Artefakte in der Produktionsumgebung.	

Fehlerbehebung

Problem	Lösung
Konflikte in der Branche	Ein häufiges Problem, das beim Trunk-Mod ell auftreten kann, besteht darin, dass ein

Problem	Lösung
	Hotfix in der Produktion ausgeführt werden muss, eine entsprechende Änderung jedoch in einer `feature` Filiale vorgenommen werden muss, in der dieselben Ressourcen geändert werden. Wir empfehlen, dass Sie Änderunge n häufig aus `main` untergeordneten Zweigen zusammenführen, um erhebliche Konflikte beim Zusammenführen zu `main` vermeiden.

Zugehörige Ressourcen

In diesem Leitfaden sind keine Schulungen für Git enthalten. Es stehen jedoch viele hochwertige Ressourcen im Internet zur Verfügung, falls Sie diese Schulung benötigen. Wir empfehlen, dass Sie mit der Git-Dokumentationsseite beginnen.

Die folgenden Ressourcen können Ihnen bei Ihrer Trunk-Branching-Reise in der AWS Cloud helfen.

AWS DevOps Anleitung

- AWS DevOps Beratung
- AWS Deployment Pipeline Reference Architecture
- Was ist DevOps?
- DevOps Ressourcen

Führung des Rumpfes

- Entwicklung auf Trunk-Basis

Sonstige Ressourcen

- Zwölf-Faktor-App-Methodik (12factor.net)

Implementieren Sie zentralisiertes benutzerdefiniertes Checkov-Scanning, um Richtlinien vor der Bereitstellung AWS der Infrastruktur durchzusetzen

Erstellt von Benjamin Morris (AWS)

Übersicht

Dieses Muster bietet ein GitHub Actions-Framework für das Schreiben benutzerdefinierter Checkov-Richtlinien in einem Repository, die unternehmensweit wiederverwendet werden können. GitHub Wenn dieses Muster befolgt wird, kann ein Informationssicherheitsteam benutzerdefinierte Richtlinien auf der Grundlage der Unternehmensanforderungen schreiben, hinzufügen und verwalten. Die benutzerdefinierten Richtlinien können automatisch in alle Pipelines der GitHub Organisation übernommen werden. Dieser Ansatz kann verwendet werden, um Unternehmensstandards für Ressourcen durchzusetzen, bevor die Ressourcen eingesetzt werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Eine GitHub Organisation, die GitHub Aktionen verwendet
- AWS Infrastruktur, die entweder mit HashiCorp Terraform oder AWS CloudFormation

Einschränkungen

- Dieses Muster wurde für GitHub Aktionen geschrieben. Es kann jedoch an ähnliche Frameworks für Continuous Integration und Continuous Delivery (CI/CD) angepasst werden, wie z. GitLab Es ist keine spezielle kostenpflichtige Version von GitHub erforderlich.
- Einige AWS-Services sind nicht in allen verfügbar AWS-Regionen. Informationen zur regionalen Verfügbarkeit finden Sie in der AWS Dokumentation unter Dienstendpunkte und Kontingente und wählen Sie den Link für den Dienst aus.

Architektur

Dieses Muster ist für die Bereitstellung als GitHub Repository konzipiert, das einen GitHub wiederverwendbaren Workflow und benutzerdefinierte Checkov-Richtlinien enthält. Der wiederverwendbare Workflow kann sowohl Terraform- als auch CloudFormation Infrastructure-as-Code-Repositorys (IaC) scannen.

Das folgende Diagramm zeigt das Repository für wiederverwendbare GitHub Workflows und das Repository für benutzerdefinierte Checkov-Richtlinien als separate Symbole. Sie können diese Repositorys jedoch entweder als separate Repositorys oder als einzelnes Repository implementieren. Der Beispielcode verwendet ein einzelnes Repository mit Dateien für Workflows (`.github/workflows`) und Dateien für benutzerdefinierte Richtlinien (`custom_policies`Ordner und `.checkov.yml` Konfigurationsdatei) im selben Repository.

Das Diagramm zeigt den folgenden Workflow:

1. Ein Benutzer erstellt eine Pull-Anfrage in einem GitHub Repository.
2. Pipeline-Workflows beginnen in GitHub Aktionen, einschließlich eines Verweises auf einen wiederverwendbaren Checkov-Workflow.
3. Der Pipeline-Workflow lädt den referenzierten wiederverwendbaren Checkov-Workflow aus einem externen Repository herunter und führt diesen Checkov-Workflow mithilfe von Aktionen aus. GitHub
4. Der wiederverwendbare Checkov-Workflow lädt die benutzerdefinierten Richtlinien aus einem externen Repository herunter.
5. Der wiederverwendbare Checkov-Workflow bewertet die IaC im GitHub Repository anhand integrierter und benutzerdefinierter Checkov-Richtlinien. Der wiederverwendbare Checkov-Workflow ist erfolgreich oder schlägt fehl, je nachdem, ob Sicherheitsprobleme gefunden wurden.

Automatisierung und Skalierung

Dieses Muster ermöglicht die zentrale Verwaltung der Checkov-Konfiguration, sodass Richtlinienaktualisierungen an einem Ort angewendet werden können. Dieses Muster erfordert jedoch, dass jedes Repository einen Workflow verwendet, der einen Verweis auf den zentralen wiederverwendbaren Workflow enthält. Sie können diesen Verweis manuell hinzufügen oder Skripts verwenden, um die Datei in den `.github/workflows` Ordner für jedes Repository zu verschieben.

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend AWS-Konten zu verwalten. Checkov kann scannen CloudFormation.

Andere Tools

- Checkov ist ein statisches Codeanalyse-Tool, das IaC auf Sicherheits- und Compliance-Fehlkonfigurationen überprüft.
- GitHub Actions ist in die GitHub Plattform integriert, um Sie bei der Erstellung, gemeinsamen Nutzung und Ausführung von Workflows in Ihren Repositorys zu unterstützen. GitHub Sie können GitHub Aktionen verwenden, um Aufgaben wie das Erstellen, Testen und Bereitstellen Ihres Codes zu automatisieren.
- Terraform ist ein IaC-Tool von HashiCorp , mit dem Sie Cloud- und lokale Ressourcen erstellen und verwalten können. Checkov kann Terraform scannen.

Code-Repository

Der Code für dieses Muster ist im GitHub centralized-custom-checkov-sastRepository verfügbar.

Bewährte Methoden

- Um einen konsistenten Sicherheitsstatus aufrechtzuerhalten, sollten Sie die Sicherheitsrichtlinien Ihres Unternehmens an die Checkov-Richtlinien anpassen.
- In den frühen Phasen der Implementierung der benutzerdefinierten Richtlinien von Checkov können Sie die Soft-Fail-Option in Ihrem Checkov-Scan verwenden, damit IaC und Sicherheitsprobleme zusammengeführt werden können. Wenn der Prozess ausgereift ist, wechseln Sie von der Soft-Fail-Option zur Hard-Fail-Option.

Epen

Erstellen Sie ein zentrales Checkov-Repository für benutzerdefinierte Richtlinien

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein zentrales Checkov-Repository.	Erstellen Sie ein Repository, um benutzerdefinierte Checkov-Richtlinien zu speichern, die innerhalb der Organisation verwendet werden.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Für einen schnellen Start können Sie den Inhalt des Repositorys dieses Patterns in Ihr zentrales GitHub centraliz ed-custom-checkov-sast Checkov-Repository kopieren.	
Erstellen Sie ein Repositor y für wiederverwendbare Workflows.	Wenn bereits ein Repositor y für wiederverwendbare Workflows existiert oder Sie planen, wiederverwendbare Workflow-Dateien in dasselbe Repository aufzunehmen wie die benutzerdefinierten Checkov-Richtlinien, können Sie diesen Schritt übersprin gen. Erstellen Sie ein GitHub Repository für wiederver wendbare Workflows. Die Pipelines anderer Repositorien werden auf dieses Repository verweisen.	DevOps Ingenieur

Erstellen Sie wiederverwendbare Checkov-Workflows und Beispielworkflows

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie einen wiederver wendbaren Checkov-Workflow hinzu.	Erstellen Sie einen wiederver wendbaren GitHub Checkov-Aktions-Workflow (YAML-Dat ei) im Repository für wiederver wendbare Workflows. Sie können diesen wiederver	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wendbaren Workflow anhand der in diesem Muster bereitgestellten Workflow-Datei anpassen. Ein Beispiel für eine Änderung, die Sie möglicher weise vornehmen möchten, besteht darin, den wiederver wendbaren Workflow so zu ändern, dass er die Soft-Fail-Option verwendet. `true`Durch die Einstellung `soft-fail` auf kann der Job auch dann erfolgreich abgeschlossen werden, wenn ein Checkov-Scan fehlschlägt. Anweisung en dazu finden Sie unter Hard and Soft Fail in der Checkov-D okumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie einen Beispiel-Workflow hinzu.	Fügen Sie einen Checkov-Beispiel-Workflow hinzu, der auf den `reusable` Workflow verweist. Dadurch wird eine Vorlage für die Wiederverwendung des `reusable` Workflows bereitgestellt. Im Beispiel-Repository `checkov-source.yaml` befindet sich der wiederverwendbare Workflow und `checkov-scan.yaml` ist das Beispiel, das verbraucht. `checkov-source` Weitere Informationen zum Schreiben eines Checkov-Beispiel-Workflows finden Sie unter Zusätzliche Informationen.	DevOps Ingenieur

Ordnen Sie Unternehmensrichtlinien den benutzerdefinierten Richtlinien von Checkov zu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie Richtlinien, die mit Checkov durchgesetzt werden können.	1. Informieren Sie sich über Unternehmensrichtlinien, die sich auf die Infrastruktursicherheit beziehen und welche Anforderungen gelten sollten. 2. Ermitteln Sie, welche Anforderungen mithilfe der benutzerdefinierten Richtlini	Sicherheit und Compliance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en von Checkov implement iert werden können. 3. Erstellen Sie eine Namenskonvention, die die Richtliniensteuerung der benutzerdefinierte n Checkov-Richtlinie zuordnet. In der Regel haben benutzerdefinierte Checkov-Richtlinien eine Kennung mit einem Checkov-Namen, der Richtlinienquelle (benutzer definiert) und einer Richtlini ennummer (zum Beispiel). `CKV2_CUSTOM_123` Weitere Informationen zur Erstellung von benutzerd efinierten Checkov-Richtlinie n finden Sie unter Übersicht über benutzerdefinierte Richtlinien in der Checkov-D okumentation.	
Fügen Sie benutzerdefinierte Checkov-Richtlinien hinzu.	Konvertieren Sie die identifiz ierten Unternehmensrichtl inien in benutzerdefinierte Checkov-Richtlinien im zentralen Repository. Sie können einfache Checkov-R ichtlinien entweder in Python oder YAML schreiben.	Sicherheit

Implementieren Sie zentralisierte benutzerdefinierte Checkov-Richtlinien

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie den wiederver wendbaren Checkov-Workflow zu allen Repositorys hinzu.	Zu diesem Zeitpunkt sollten Sie über ein Beispiel für einen Checkov-Workflow verfügen, der auf den wiederver wendbaren Workflow verweist. Kopieren Sie den Checkov-B eispiel-Workflow, der auf den wiederverwendbaren Workflow verweist, in jedes Repository, das ihn benötigt.	DevOps Ingenieur
Erstellen Sie einen Mechanismus, um sicherzus tellen, dass Checkov vor Zusammenführungen ausgeführt wird.	Um sicherzustellen, dass der Checkov-Workflow für jede Pull-Anfrage ausgeführt wird, erstellen Sie eine Statusprü fung, die einen erfolgreichen Checkov-Workflow vorausset zt, bevor Pull-Requests zusammengeführt werden können. GitHub ermöglich t es Ihnen, zu verlangen, dass bestimmte Workflows ausgeführt werden, bevor Pull-Requests zusammengeführt werden können.	DevOps Ingenieur
Erstellen Sie eine unternehm ensweite PAT und geben Sie sie als geheim weiter.	Wenn Ihre GitHub Organisat ion öffentlich sichtbar ist, können Sie diesen Schritt überspringen. Dieses Muster erfordert, dass der Checkov-Workflow in der Lage ist, benutzerd	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	efinierte Richtlinien aus dem Repository für benutzerd efinierte Richtlinien in Ihrer GitHub Organisation herunterz uladen. Sie müssen Berechtig ungen bereitstellen, damit der Checkov-Workflow auf diese Repositorys zugreifen kann. Erstellen Sie dazu ein Personal Access Token (PAT) mit Berechtigungen zum Lesen von Organisat ions-Repositorys. Teilen Sie dieses PAT mit Repositor ys, entweder als organisat ionsweites Geheimnis (bei einem kostenpflichtigen Tarif) oder als Geheimnis in jedem Repository (kostenlo se Version). Im Beispielcode lautet der Standardname für das Geheimnis. `ORG_PAT`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Schützen Sie die Checkov-Workflow-Dateien vor Änderungen.	Um die Checkov-Workflow-Dateien vor unerwünschten Änderungen zu schützen, können Sie eine `CODEOWNERS` Datei verwenden. Die `CODEOWNERS` Datei wird normalerweise im Stammverzeichnis bereitgestellt. Um beispielsweise Genehmigungen von der `secEng` Gruppe Ihrer GitHub Organisation einzuholen, wenn die `checkov-scan.yaml` Datei geändert wird, fügen Sie Folgendes an die Datei eines Repositorys `CODEOWNERS` an: `[Checkov] .github/workflows/checkov-scan.yaml @myOrg/secEng` Eine `CODEOWNERS` Datei ist spezifisch für das Repository, in dem sie sich befindet. Um den vom Repository verwendeten Checkov-Workflow zu schützen, müssen Sie in jedem Repository eine `CODEOWNERS` Datei hinzufügen (oder aktualisieren).	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen zum Schutz von Checkov-W orkflow-Dateien finden Sie unter Zusätzliche Informati onen. Weitere Informationen zu `CODEOWNERS` Dateien finden Sie in der offiziellen Dokumentation Ihres CI/CD-Anbieters (z. B.). GitHub	

Zugehörige Ressourcen

- Überblick über die benutzerdefinierten Richtlinien von Checkov
- CloudFormation Scannen von Konfigurationen
- GitHub Aktionen Wiederverwendbare Workflows

Zusätzliche Informationen

Checkov-Workflow-Dateien schreiben

Überlegen Sie sich beim Schreiben`checkov-scan.yaml`, wann es ausgeführt werden soll. Der `on` Schlüssel der obersten Ebene bestimmt, wann der Workflow ausgeführt wird. Im Beispiel-Repository wird der Workflow ausgeführt, wenn eine Pull-Anfrage auf den `main` Branch abzielt (und jedes Mal, wenn der Quell-Branch dieser Pull-Anfrage geändert wird). Aufgrund des `workflow_dispatch` Schlüssels kann der Workflow auch nach Bedarf ausgeführt werden.

Sie können die Workflow-Auslösebedingungen ändern, je nachdem, wie oft der Workflow ausgeführt werden soll. Sie könnten beispielsweise den Workflow so ändern, dass er jedes Mal ausgeführt wird, wenn Code an einen Zweig übertragen wird, indem Sie den Schlüssel durch den `branches` Schlüssel `pull_request` ersetzen `push` und ihn entfernen.

Sie können die Workflow-Beispieldatei ändern, die Sie in einem einzelnen Repository erstellt haben. Sie könnten beispielsweise den Namen des Ziel-Branches von bis ändern`main`, `production` wenn ein Repository um einen `production` Branch herum strukturiert ist.

Schutz der Checkov-Workflow-Dateien

Der Checkov-Scan liefert nützliche Informationen über mögliche Sicherheitsfehler. Einige Entwickler könnten dies jedoch als Hindernis für ihre Produktivität empfinden und versuchen, den Scan-Workflow zu entfernen oder zu deaktivieren.

Es gibt mehrere Möglichkeiten, dieses Problem zu lösen, darunter bessere Informationen über den langfristigen Wert von Sicherheitsscans und eine klarere Dokumentation zur Bereitstellung einer sicheren Infrastruktur. Dies sind wichtige „sanfte“ Ansätze für die DevSecOps Zusammenarbeit, die als Lösung für die eigentliche Ursache dieses Problems angesehen werden können. Sie können jedoch auch technische Kontrollen wie eine `CODEOWNERS` Datei als Leitplanken verwenden, um Entwickler auf dem richtigen Weg zu halten.

Testmuster in einer Sandbox

Gehen Sie folgendermaßen vor, um dieses Muster in einer Sandbox-Umgebung zu testen:

1. Erstellen Sie eine neue GitHub Organisation. Erstellen Sie ein Token mit schreibgeschütztem Zugriff auf alle Repositorys in der Organisation. Da dieses Token für eine Sandbox-Umgebung und nicht für eine kostenpflichtige Umgebung bestimmt ist, können Sie dieses Token nicht in einem unternehmensweiten Geheimnis speichern.
2. Erstellen Sie ein `checkov` Repository für die Checkov-Konfiguration und ein `github-workflows` Repository für die wiederverwendbare Workflow-Konfiguration. Füllen Sie die Repositorys mit dem Inhalt des Beispiel-Repositorys.
3. Erstellen Sie ein Anwendungs-Repository, kopieren Sie den `checkov-scan.yaml` Workflow und fügen Sie ihn in den entsprechenden Ordner ein. `.github/workflows` Fügen Sie dem Repository einen geheimen Schlüssel hinzu, der die PAT enthält, die Sie für den schreibgeschützten Organisationszugriff erstellt haben. Das Standardgeheimnis ist. `ORG_PAT`
4. Erstellen Sie eine Pull-Anfrage, die dem Anwendungs-Repository etwas Terraform oder CloudFormation Code hinzufügt. Checkov sollte scannen und ein Ergebnis zurückgeben.

Automatische Erkennung von Änderungen und Initiierung verschiedener CodePipeline Pipelines für ein Monorepo in CodeCommit

Erstellt von Helton Ribeiro (AWS), Petrus Batalha (AWS) und Ricardo Morais (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Hinweis: AWS Cloud9 steht Neukunden nicht mehr zur Verfügung. Bestandskunden von AWS Cloud9 können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Dieses Muster hilft Ihnen dabei, Änderungen am Quellcode einer Monorepo-basierten Anwendung automatisch zu erkennen AWS CodeCommit und dann eine Pipeline zu initiieren, in der die Continuous Integration and Continuous Delivery (CI/CD) automation for each microservice. This approach means that each microservice in your monorepo-based application can have a dedicated CI/CDPipeline) ausgeführt wird. Dadurch wird eine bessere Sichtbarkeit, einfachere gemeinsame Nutzung von Code und eine verbesserte Zusammenarbeit, Standardisierung und Auffindbarkeit gewährleistet. AWS CodePipeline

Die in diesem Muster beschriebene Lösung führt keine Abhängigkeitsanalyse zwischen den Microservices im Monorepo durch. Sie erkennt nur Änderungen im Quellcode und initiiert die passende CI/CD-Pipeline.

Das Muster dient AWS Cloud9 als integrierte Entwicklungsumgebung (IDE) und AWS Cloud Development Kit (AWS CDK) zur Definition einer Infrastruktur mithilfe von zwei AWS CloudFormation Stacks: und. `MonoRepoStack` `PipelinesStack` Der `MonoRepoStack` Stack erstellt den Monorepo-Eingang AWS CodeCommit und die AWS Lambda Funktion, die die CI/CD-Pipelines initiiert. Der `PipelinesStack` Stack definiert Ihre Pipeline-Infrastruktur.

> **Important**
>
> Der Workflow dieses Musters ist ein Machbarkeitsnachweis (PoC). Wir empfehlen, es nur in einer Testumgebung zu verwenden. Wenn Sie den Ansatz dieses Musters in einer Produktionsumgebung verwenden möchten, finden Sie in der AWS Identity and Access Management (IAM-) Dokumentation unter Bewährte Sicherheitsmethoden in IAM weitere Informationen und nehmen Sie die erforderlichen Änderungen an Ihren IAM-Rollen und vor. AWS-Services

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Konto. AWS
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert. Weitere Informationen finden Sie AWS CLI in der AWS CLI Dokumentation unter Installation, Aktualisierung und Deinstallation von.
- Python 3 und`pip`, auf Ihrem lokalen Computer installiert. Weitere Informationen finden Sie in der Python-Dokumentation.
- AWS CDK, installiert und konfiguriert. Weitere Informationen finden Sie AWS CDK in der AWS CDK Dokumentation unter Erste Schritte mit dem.
- Eine AWS Cloud9 IDE, installiert und konfiguriert. Weitere Informationen finden Sie AWS Cloud9 in der AWS Cloud9 Dokumentation unter Einrichtung.
- Die GitHub AWS CodeCommit Monorepo-Multi-Pipeline löst ein Repository aus, das auf Ihrem lokalen Computer geklont wurde.
- Ein vorhandenes Verzeichnis, das Anwendungscode enthält, mit dem Sie ihn erstellen und bereitstellen möchten. CodePipeline
- Vertrautheit und Erfahrung mit DevOps bewährten Methoden auf dem AWS Cloud. Um sich besser damit vertraut zu machen DevOps, können Sie das Muster Build a loose coupled architecture with microservices using DevOps practices und AWS Cloud9 auf der Prescriptive Guidance-Website verwenden. AWS

Architektur

Das folgende Diagramm zeigt, wie Sie mithilfe von eine Infrastruktur mit zwei AWS CDK Stacks definieren können: und. AWS CloudFormation `MonoRepoStack` `PipelinesStack`

Das Diagramm zeigt den folgenden Workflow:

1. Der Bootstrap-Prozess verwendet die, AWS CDK um die Stacks zu erstellen und. AWS CloudFormation `MonoRepoStack` `PipelinesStack`
2. Der `MonoRepoStack` Stack erstellt das CodeCommit Repository für Ihre Anwendung und die `monorepo-event-handler` Lambda-Funktion, die nach jedem Commit initiiert wird.

3. Der `PipelinesStack` Stack erstellt die Pipelines CodePipeline , die von der Lambda-Funktion initiiert werden. Jeder Microservice muss über eine definierte Infrastrukturpipeline verfügen.
4. Die Pipeline für `microservice-n` wird von der Lambda-Funktion initiiert und startet ihre isolierten CI/CD-Stufen, die auf dem Quellcode in basieren. CodeCommit
5. Die Pipeline für `microservice-1` wird von der Lambda-Funktion initiiert und startet ihre isolierten CI/CD-Stufen, die auf dem Quellcode in basieren. CodeCommit

Das folgende Diagramm zeigt die Bereitstellung der AWS CloudFormation Stacks `MonoRepoStack` und `PipelinesStack` in einem Konto.

1. Ein Benutzer ändert den Code in einem der Microservices der Anwendung.
2. Der Benutzer überträgt die Änderungen von einem lokalen Repository in ein CodeCommit Repository.
3. Die Push-Aktivität initiiert die Lambda-Funktion, die alle Pushs an das Repository empfängt. CodeCommit
4. Die Lambda-Funktion liest einen Parameter im Parameter Store, eine Fähigkeit von AWS Systems Manager, um die neueste Commit-ID abzurufen. Der Parameter hat das Benennungsformat:`/MonoRepoTrigger/{repository}/{branch_name}/LastCommit`. Wenn der Parameter nicht gefunden wird, liest die Lambda-Funktion die letzte Commit-ID aus dem CodeCommit Repository und speichert den zurückgegebenen Wert im Parameter Store.
5. Nach der Identifizierung der Commit-ID und der geänderten Dateien identifiziert die Lambda-Funktion die Pipelines für jedes Microservice-Verzeichnis und initiiert die erforderliche Pipeline. CodePipeline

Tools

- AWS Cloud Development Kit (AWS CDK)ist ein Framework für die Softwareentwicklung, mit dem Cloud-Infrastruktur im Code definiert und bereitgestellt werden kann. AWS CloudFormation
- Python ist eine Programmiersprache, mit der Sie schnell arbeiten und Systeme effektiver integrieren können.

Code

Der Quellcode und die Vorlagen für dieses Muster sind im GitHub AWS CodeCommit Monorepo Multi-Pipeline-Trigger-Repository verfügbar.

Bewährte Methoden

- Diese Beispielarchitektur beinhaltet keine Überwachungslösung für die bereitgestellte Infrastruktur. Wenn Sie diese Lösung in einer Produktionsumgebung einsetzen möchten, empfehlen wir Ihnen, die Überwachung zu aktivieren. Weitere Informationen finden Sie unter Überwachen Ihrer serverlosen Anwendungen mit CloudWatch Application Insights in der Dokumentation AWS Serverless Application Model (AWS SAM).
- Wenn Sie den in diesem Muster enthaltenen Beispielcode bearbeiten, befolgen Sie die bewährten Methoden für die Entwicklung und Bereitstellung der Cloud-Infrastruktur in der AWS CDK Dokumentation.
- Lesen Sie bei der Definition Ihrer Microservice-Pipelines die bewährten Sicherheitsmethoden in der AWS CodePipeline Dokumentation.
- Sie können Ihren AWS CDK Code auch mithilfe des Dienstprogramms cdk-nag auf bewährte Methoden überprüfen. Dieses Tool verwendet eine Reihe von Regeln, die nach Paketen gruppiert sind, um Ihren Code auszuwerten. Die verfügbaren Pakete sind:
  - AWS Lösungsbibliothek
  - Sicherheit nach dem Gesetz über die Portabilität und Rechenschaftspflicht von Krankenversicherungen (HIPAA)
  - Nationales Institut für Standards und Technologie (NIST) 800-53 Rev. 4
  - NIST 800-53 Rev. 5
  - Datensicherheitsstandard der Zahlungskartenindustrie (PCI DSS) 3.2.1

Epen

Richte die Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine virtuelle Python-Umgebung.	Erstellen Sie in Ihrer AWS Cloud9 IDE eine virtuelle Python-Umgebung und installieren Sie die erforderl ichen Abhängigkeiten, indem	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie den folgenden Befehl ausführen: `make install`	
Bootstrap das AWS-Konto und AWS-Region für das AWS CDK.	Führen Sie das Bootstrap ping für die erforderlichen AWS-Konto Daten und die Region durch, indem Sie den folgenden Befehl ausführen: `make bootstrap account-id=<your-AWS-account-ID> region=<required-region>`	Developer

Fügen Sie eine neue Pipeline für einen Microservice hinzu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Ihren Beispielcode zu Ihrem Anwendungsverzeichnis hinzu.	Fügen Sie das Verzeichnis, das Ihren Beispielanwendungscode enthält, dem `monorepo-sample` Verzeichnis im GitHub AWS CodeCommit geklonten Monorepo-Multi-Pipeline-Trigger-Repository hinzu.	Developer
Bearbeiten Sie die `monorepo-main.json` -Datei.	Fügen Sie den Verzeichnisnamen des Codes Ihrer Anwendung und den Namen der Pipeline zur `monorepo-main.json` Datei im geklonten Repository hinzu.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Pipeline.	Fügen Sie im `Pipelines` Verzeichnis für das Repository die Pipeline `class` für Ihre Anwendung hinzu. Das Verzeichnis enthält zwei Beispieldateien `pipeline_hotsite.py` und`pipeline_demo.py` . Jede Datei besteht aus drei Phasen: Quelle, Erstellung und Bereitstellung. Sie können eine der Dateien kopieren und entsprechend den Anforderungen Ihrer Anwendung Änderungen daran vornehmen.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bearbeiten Sie die `monorepo_config.py` - Datei.	Fügen Sie `service_map` unter den Verzeichnisnamen für Ihre Anwendung und die Klasse hinzu, die Sie für die Pipeline erstellt haben.
	
	Der folgende Code zeigt beispielsweise eine Pipeline-Definition in dem `Pipelines` Verzeichnis, die eine `pipeline_mysample.py` mit einer `MySamplePipeline` Klasse benannte Datei verwendet:
	
	`...`
	`# Pipeline definition imports`
	`from pipelines.pipeline_demo import DemoPipeline`
	`from pipelines.pipeline_hotsite import HotsitePipeline`
	`from pipelines.pipeline_mysample import MySamplePipeline`
	
	`### Add your pipeline configuration here`
	`service_map: Dict[str, ServicePipeline] = {`
	`# folder-name -> pipeline-class`
	`'demo': DemoPipeline(),`
	`'hotsite': HotsitePipeline(),`
		Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`'mysample': MySamplePipeline() }`	

Stellen Sie den MonoRepoStack Stack bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den AWS CloudFormation Stack bereit.	Stellen Sie den AWS CloudFormation `MonoRepoStack` Stack mit Standardparameterwerten im Stammverzeichnis des geklonten Repositorys bereit, indem `make deploy-core` Sie den Befehl ausführen. Sie können den Namen des Repositorys ändern, indem Sie den `make deploy-core monorepo-name=<repo_name>` Befehl ausführen. **Note** Mit dem `make deploy monorepo-name=<repo_name>` Befehl können Sie beide Pipelines gleichzeitig bereitstellen.	Developer
Überprüfen Sie das CodeCommit Repository.	Stellen Sie sicher, dass Ihre Ressourcen erstellt wurden,	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	indem `aws codecommit get-repository --repository-name <repo_name>` Sie den Befehl ausführen. **Important** Da der AWS CloudFormation Stack das CodeCommit Repository erstellt, in dem das Monorepo gespeichert ist, führen Sie den `cdk destroy MonoRepoStack` Befehl nicht aus, wenn Sie damit begonnen haben, Änderungen in ihn zu übertragen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die AWS CloudFormation Stack-Ergebnisse.	Stellen Sie sicher, dass der AWS CloudFormation `MonoRepoStack` Stack korrekt erstellt und konfiguriert wurde, indem Sie den folgenden Befehl ausführen: `aws cloudformation list-stacks --stack-status-filter CREATE_COMPLETE --query 'StackSummaries[?StackName == 'MonoRepoStack']'`	Developer

Stellen Sie den PipelinesStack Stack bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den AWS CloudFormation Stack bereit.	Der AWS CloudFormation `PipelinesStack` Stack muss bereitgestellt werden, nachdem Sie den `MonoRepoStack` Stack bereitgestellt haben. Der Stack nimmt an Größe zu, wenn der Codebasis des Monorepo neue Microservices hinzugefügt werden, und er wird erneut bereitgestellt, wenn ein neuer Microservice hinzugefügt wird. Stellen Sie den Stack bereit, indem Sie den Befehl	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ausführen. PipelinesStack `make deploy-pipelines` **Note** Sie können auch beide Pipelines gleichzeitig bereitstellen, indem Sie den `make deploy monorepo-name=<repo_name>` Befehl ausführen. Die folgende Beispielausgabe zeigt, wie die `Pipelines Stacks` Bereitstellung die URLs für die Microservices am Ende der Implementierung ausgibt: `Outputs: PipelinesStack.dem ourl = .cloudfront.net PipelinesStack.hotsi teurl = .cloudfro nt.net`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die AWS CloudFormation Stack-Ergebnisse.	Stellen Sie sicher, dass der AWS CloudFormation `PipelinesStacks` Stack korrekt erstellt und konfiguriert wurde, indem Sie den folgenden Befehl ausführen: `aws cloudformation list-stacks --stack-status-filter CREATE_COMPLETE UPDATE_COMPLETE --query 'StackSummaries[?StackName == 'PipelinesStack']'`	Developer

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Lösche deine AWS CloudFormation Stapel.	Führen Sie den Befehl `make destroy` aus.	Developer
Löschen Sie die S3-Buckets für Ihre Pipelines.	1. Melden Sie sich bei der Amazon Simple Storage Service (Amazon S3) -Konsole an AWS Management Consoleund öffnen Sie sie. 2. Löschen Sie die S3-Buckets, die Ihren Pipelines zugeordnet sind, und verwenden Sie den folgenden Namen:	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`pipelinesstack-codepipeline*`	

Fehlerbehebung

Problem	Lösung
Ich bin auf Probleme gestoßen AWS CDK .	Weitere Informationen finden Sie in der AWS CDK-Dokumentation unter Behebung häufiger AWS CDK Probleme.
Ich habe meinen Microservice-Code übertragen, aber die Microservice-Pipeline lief nicht.	Überprüfung des Setups Überprüfen Sie die Zweigkonfiguration: • Stellen Sie sicher, dass Sie Ihren Code in den richtigen Zweig übertragen. Diese Pipeline ist so konfiguriert, dass sie nur ausgeführt wird, wenn Änderungen an der `main` Verzweigung vorgenommen werden. Pushs an andere Zweige initiieren die Pipeline nur, wenn sie speziell konfiguriert wurden. • Nachdem Sie Ihren Code übertragen haben, überprüfen Sie, ob der Commit sichtbar ist, AWS CodeCommit um sicherzustellen, dass der Push erfolgreich war und dass die Verbindung zwischen Ihrer lokalen Umgebung und dem Repository intakt ist. Aktualisieren Sie Ihre Anmeldedaten, falls es Probleme beim Übertragen von Code gibt. Überprüfen Sie die Konfigurationsdateien:

Problem	Lösung
	• Vergewissern Sie sich, dass die `service_map` Variable in die aktuelle Verzeichnisstruktur Ihrer Microservices `monorepo_config.py` korrekt wiedergibt. Diese Variable spielt eine entscheidende Rolle bei der Zuordnung Ihres Code-Pushs zur jeweiligen Pipeline. • Stellen Sie sicher, dass `monorepo-main.json` es aktualisiert wird und das neue Mapping für Ihren Microservice enthält. Diese Datei ist wichtig, damit die Pipeline Änderungen an Ihrem Microservice erkennt und korrekt verarbeitet. Fehlerbehebung auf der Konsole AWS CodePipeline prüft: • Bestätigen Sie auf dem AWS Management Console, dass Sie sich an dem AWS-Region Ort befinden, an dem Ihre Pipeline gehostet wird. Öffnen Sie die CodePipeline Konsole und überprüfen Sie, ob die Pipeline, die Ihrem Microservice entspricht, initiiert wurde. Fehleranalyse: Wenn die Pipeline initiiert wurde, aber fehlgeschlagen ist, überprüfen Sie alle von bereitgestellten Fehlermeldungen oder Protokolle, CodePipeline um herauszufinden, was schief gelaufen ist. AWS Lambda Problembehandlung: • Öffnen Sie auf der AWS Lambda Konsole die `monorepo-event-handler` Lambda-Fu

Problem	Lösung
	nktion. Stellen Sie sicher, dass die Funktion als Reaktion auf den Code-Push initiiert wurde. Protokollanalyse: Untersuchen Sie die Logs der Lambda-Funktion auf etwaige Probleme. Die Protokolle bieten detaillierte Einblicke in die Ereignisse, als die Funktion ausgeführ t wurde, und helfen dabei, festzustellen, ob die Funktion das Ereignis erwartungsgemäß verarbeitet hat.

Problem	Lösung
Ich muss alle meine Microservices erneut bereitstellen.	Es gibt zwei Ansätze, um die Umverteilung aller Microservices zu erzwingen. Wählen Sie die Option, die Ihren Anforderungen entspricht. Ansatz 1: Löschen Sie einen Parameter im Parameterspeicher Bei dieser Methode wird ein bestimmter Parameter im Systems Manager Parameter Store gelöscht, der die letzte für die Bereitste llung verwendete Commit-ID verfolgt. Wenn Sie diesen Parameter entfernen, ist das System gezwungen, alle Microservices beim nächsten Trigger erneut bereitzustellen, da es diesen als neuen Zustand wahrnimmt. Schritte: 1. Suchen Sie den spezifischen Parameter Store-Eintrag, der die Commit-ID oder eine zugehörige Bereitstellungsmarkierung für Ihr Monorepo enthält. Der Parametername folgt dem Format: `"/MonoRepoTrigger/{repository}/{branch_name}/LastCommit"` 2. Erwägen Sie, den Parameterwert zu sichern, wenn er kritisch ist oder wenn Sie den Bereitstellungsstatus aufzeichnen möchten, bevor Sie ihn zurücksetzen. 3. Verwenden Sie, oder AWS Management Console AWS CLI, um den identifizierten Parameter SDKs zu löschen. Diese Aktion setzt die Bereitstellungsmarkierung zurück. 4. Nach dem Löschen sollte das System beim nächsten Push zum Repository alle

Problem	Lösung
	Microservices bereitstellen, da es nach dem letzten Commit sucht, das für die Bereitstellung in Betracht gezogen werden soll. Vorteile: • Einfach und schnell mit minimalen Schritten zu implementieren. • Erfordert keine willkürlichen Codeänderungen, um Bereitstellungen zu initiieren. Nachteile: • Weniger detaillierte Kontrolle über den Bereitstellungsprozess. • Potenziell riskant, wenn der Parameterspeicher für die Verwaltung anderer kritischer Konfigurationen verwendet wird. Ansatz 2: Push einen Commit in jeden Monorepo-Unterordner Bei dieser Methode wird eine geringfügige Änderung vorgenommen und diese in jeden Microservice-Unterordner innerhalb des Monorepos verschoben, um die einzelnen Pipelines zu initiieren. Schritte: 1. Listet alle Microservices innerhalb des Monorepo auf, die erneut bereitgestellt werden müssen. 2. Nehmen Sie für jeden Microservice eine minimale Änderung in seinem Unterordner

Problem	Lösung
	vor, die keine Auswirkungen hat. Dabei kann es sich um das Aktualisieren einer `README` Datei, das Hinzufügen eines Kommentars zu einer Konfigurationsdatei oder um eine Änderung handeln, die die Funktionalität des Dienstes nicht beeinträchtigt. 3. Bestätigen Sie diese Änderungen mit einer klaren Botschaft (z. B. „Initiieren Sie die erneute Bereitstellung von Microservices“) und übertragen Sie sie per Push in das Repository. Stellen Sie sicher, dass Sie die Änderungen an den Branch übertragen, der die Bereitstellung initiiert. 4. Überwachen Sie die Pipelines für jeden Microservice, um sicherzustellen, dass sie erfolgreich initiiert und abgeschlossen wurden. Vorteile: • Bietet eine detaillierte Kontrolle darüber, welche Microservices erneut bereitgestellt werden. • Sicherer, da dabei keine Konfigurationspara meter gelöscht werden müssen, die für andere Zwecke verwendet werden könnten. Nachteile: • Zeitaufwändiger, insbesondere bei einer großen Anzahl von Microservices. • Erfordert unnötige Codeänderungen, die den Commit-Verlauf überladen könnten.

Zugehörige Ressourcen

- Kontinuierliche Integration und Bereitstellung (CI/CD) mithilfe von CDK Pipelines (Dokumentation)AWS CDK
- aws-cdk/pipelines-Modul (API-Referenz)AWS CDK

Integrieren Sie mithilfe von AWS ein Bitbucket-Repository mit AWS Amplify CloudFormation

Erstellt von Alwin Abraham (AWS)

Übersicht

Mit AWS Amplify können Sie statische Websites schnell bereitstellen und testen, ohne die normalerweise erforderliche Infrastruktur einrichten zu müssen. Sie können den Ansatz dieses Musters verwenden, wenn Ihr Unternehmen Bitbucket für die Quellcodeverwaltung verwenden möchte, sei es, um vorhandenen Anwendungscode zu migrieren oder eine neue Anwendung zu erstellen. Indem Sie AWS CloudFormation zur automatischen Einrichtung von Amplify verwenden, bieten Sie Einblick in die von Ihnen verwendeten Konfigurationen.

Dieses Muster beschreibt, wie Sie mithilfe von AWS eine Pipeline und Bereitstellungsumgebung für Continuous Integration and Continuous Deployment (CI/CD) im Front-End einrichten, CloudFormation um ein Bitbucket-Repository mit AWS Amplify zu integrieren. Der Ansatz des Musters bedeutet, dass Sie eine Amplify-Frontend-Pipeline für wiederholbare Bereitstellungen erstellen können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS) -Konto
- Ein aktives Bitbucket-Konto mit Administratorzugriff
- Zugriff auf ein Terminal, das cURL oder die Postman-Anwendung verwendet
- Vertrautheit mit Amplify
- Vertrautheit mit AWS CloudFormation
- Vertrautheit mit Dateien im YAML-Format

Architektur

Technologie-Stack

- Amplify
- AWS CloudFormation
- Bitbucket

Tools

- AWS Amplify — Amplify unterstützt Entwickler bei der Entwicklung und Bereitstellung cloudgestützter Mobil- und Web-Apps.
- AWS CloudFormation — AWS CloudFormation ist ein Service, der Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen unterstützt, sodass Sie weniger Zeit mit der Verwaltung dieser Ressourcen verbringen und sich mehr auf Ihre Anwendungen konzentrieren können, die in AWS ausgeführt werden.
- Bitbucket — Bitbucket ist eine Git-Repository-Management-Lösung, die für professionelle Teams entwickelt wurde. Es bietet dir einen zentralen Ort, um Git-Repositorys zu verwalten, gemeinsam an deinem Quellcode zu arbeiten und dich durch den Entwicklungsablauf zu führen.

Code

Die `bitbucket-amplify.yml` Datei (angehängt) enthält die CloudFormation AWS-Vorlage für dieses Muster.

Epen

Konfiguriere das Bitbucket-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Erstelle ein Bitbucket-Repository.	1. Melde dich mit deinem Bitbucket-Konto an und erstelle ein neues Repository. Weitere Informationen dazu findest du in der Bitbucket-Dokumentation unter Ein Git-Repository erstellen. 2. Notiere dir den Namen des Workspace.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Du kannst auch ein vorhandenes Bitbucket-Repository verwenden.	
Öffnen Sie die Workspace-Einstellungen.	1. Öffnen Sie den Workspace und wählen Sie den Tab Repository. 2. Wählen Sie das Repository aus, das Sie in Amplify integrieren möchten. 3. Wählen Sie den Namen des Workspace, der über dem Namen des Repositorys steht. 4. Wähle in der Seitenleiste Einstellungen.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schaffen Sie einen OAuth Verbraucher.	1. Wählen Sie im Abschnitt Apps und Funktionen die Option OAuth Verbraucher und dann Verbraucher hinzufügen aus. 2. Geben Sie einen Namen für Ihren Verbraucher ein, `Amplify Integration` z. B. 3. Geben Sie eine Rückruf-URL ein. Dieses Feld ist zwar eine Pflichteingabe, wird aber nicht verwendet, um die Integration abzuschließen. Der Wert könnte also `http://localhost:3000` 4. Markieren Sie das Kästchen für Dies ist ein Privatverbraucher. 5. Wählen Sie die folgenden Berechtigungen aus: • Projekt — `Read` • Repositorien — `Admin` • Pull-Anfragen — `Read` • Webhooks — `Read` und `Write` 6. Behalten Sie die Standardauswahl für alle anderen Felder bei und wählen Sie Senden.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Notieren Sie sich den Schlüssel und das Geheimnis, die generiert wurden.	
Besorgen Sie sich ein OAuth Zugriffstoken	1. Öffnen Sie ein Terminalf enster und führen Sie den folgenden Befehl aus: `curl -X POST -u "KEY:SECRET" https://bitbucket.org/site/oauth2/access_token -d grant_type=client_credentials` **Important** Ersetzen Sie `KEY` und `SECRET` durch den Schlüssel und das Geheimnis, die Sie zuvor aufgezeichnet haben. 2. Notieren Sie das Zugriffst oken ohne die Anführung szeichen. Das Token ist nur für eine begrenzte Zeit gültig und die Standardzeit beträgt zwei Stunden. Sie müssen die CloudFormation AWS-Vorlage in diesem Zeitraum ausführen.	DevOps Ingenieur

CloudFormation AWS-Stack erstellen und bereitstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die CloudFormation AWS-Vorlage herunter.	Laden Sie die `bitbucket-amplify.yml` CloudFormation AWS-Vorlage herunter (im Anhang). Diese Vorlage erstellt zusätzlich zum Amplify-Projekt und dem Amplify-Zweig die CI/CD-Pipeline in Amplify.	
Erstellen und implementieren Sie den CloudFormation AWS-Stack.	1. Melden Sie sich bei der AWS-Managementkonsole in der AWS-Region an, in der Sie die Bereitstellung durchführen möchten, und öffnen Sie die CloudFormation AWS-Konsole. 2. Wählen Sie Create Stack (mit neuen Ressourcen) und dann Upload a Template File aus. 3. Hochladen der `bitbucket-amplify.yml` -Datei 4. Wählen Sie Weiter, geben Sie einen Stack-Namen ein und geben Sie dann die folgenden Parameter ein: • Zugriffstoken: Fügen Sie das OAuth Zugriffstoken ein, das Sie zuvor erstellt haben. • Repository-URL: Füge die URL des	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bitbucket-Projekt-Repositorys hinzu. Die URL hat normalerweise das folgende Format: `https://bitbucket.org/<WORKSPACE_NAME>/<REPO_NAME>` • Branch-Name: Dieser muss mit dem Namen eines Branches in deinem Bitbucket-Repository übereinstimmen. Dieser Zweig muss nicht existieren, wenn Sie den CloudFormation AWS-Stack ausführen, aber er ist für die Bereitstellung von Code in der Umgebung erforderlich. • Projektname: Dies ist der Name, der dem Amplify-Projekt zugeordnet werden soll. 5. Wählen Sie Weiter und dann Stapel erstellen.	

Testen Sie die CI/CD-Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Code für den Branch in Ihrem Repository bereit.	1. Klonen Sie Ihr Bitbucket-Repository, indem Sie den folgenden Befehl ausführen: `git clone https://bitbucket.org/<WORKSPACE_NAME>/<REPO_NAME>` 2. Schauen Sie sich den Branch-Namen an, der bei der Ausführung des CloudFormation AWS-Skripts verwendet wurde. Führen Sie den `git checkout -b <BRANCH_NAME>` Befehl aus, um einen neuen Branch zu erstellen und auszuchecken. Führen Sie den folgenden `git checkout <BRANCH_NAME>` Befehl aus, um einen vorhandenen Zweig auszuchecken 3. Übergeben Sie den Code in den Branch und übertragen Sie ihn in den Remote-Zweig, indem Sie die `git push` Befehle `git commit` und ausführen. 4. Amplify erstellt dann die Anwendung und stellt sie bereit.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen dazu findest du unter Grundlegende Git-Befehle in der Bitbucket-Dokumentation.	

Zugehörige Ressourcen

Authentifizierungsmethoden (Atlassian-Dokumentation)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacke die folgende Datei: attachment.zip

Starten Sie mithilfe von Step Functions und einer Lambda-Proxyfunktion ein CodeBuild Projekt für alle AWS-Konten

Erstellt von Richard Milner-Watts (AWS) und Amit Anjarlekar (AWS)

Übersicht

Dieses Muster zeigt, wie ein CodeBuild AWS-Projekt mithilfe von AWS AWS Step Functions und einer AWS Lambda-Proxyfunktion asynchron über mehrere AWS-Konten hinweg gestartet wird. Sie können die Step Functions-Beispielstatusmaschine des Musters verwenden, um den Erfolg Ihres CodeBuild Projekts zu testen.

CodeBuild hilft Ihnen dabei, betriebliche Aufgaben mithilfe der AWS-Befehlszeilenschnittstelle (AWS CLI) in einer vollständig verwalteten Laufzeitumgebung zu starten. Sie können das Verhalten Ihres CodeBuild Projekts zur Laufzeit ändern, indem Sie Umgebungsvariablen überschreiben. Darüber hinaus können Sie es CodeBuild zur Verwaltung von Workflows verwenden. Weitere Informationen finden Sie unter Service Catalog Tools auf der AWS Workshop-Website und Schedule jobs in Amazon RDS for PostgreSQL using AWS CodeBuild and EventBridge Amazon im AWS Database Blog.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zwei aktive AWS-Konten: ein Quellkonto zum Aufrufen einer Lambda-Proxyfunktion mit Step Functions und ein Zielkonto zum Erstellen eines Remote-Beispielprojekts CodeBuild

Einschränkungen

- Dieses Muster kann nicht verwendet werden, um Artefakte zwischen Konten zu kopieren.

Architektur

Das folgende Diagramm zeigt die Architektur, die dieses Muster aufbaut.

Das Diagramm zeigt den folgenden Workflow:

1. Die Step Functions Functions-Zustandsmaschine analysiert die bereitgestellte Eingabemap und ruft die Lambda-Proxyfunktion (`codebuild-proxy-lambda`) für jedes Konto, jede Region und jedes Projekt auf, das Sie definiert haben.
2. Die Lambda-Proxyfunktion verwendet AWS Security Token Service (AWS STS), um eine IAM-Proxyrolle (`codebuild-proxy-role`) anzunehmen, die mit einer IAM-Richtlinie (`codebuild-proxy-policy`) im Zielkonto verknüpft ist.
3. Unter Verwendung der angenommenen Rolle startet die Lambda-Funktion das CodeBuild Projekt und gibt die CodeBuild Job-ID zurück. Die Step Functions Functions-Zustandsmaschine wiederholt den CodeBuild Job und fragt ihn ab, bis er einen Erfolgs- oder Fehlerstatus erhält.

Die Logik der Zustandsmaschine ist in der folgenden Abbildung dargestellt.

Technologie-Stack

- AWS CloudFormation
- CodeBuild
- IAM
- Lambda
- Step Functions
- X-Ray

Tools

- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.
- AWS CloudFormation Designer bietet einen integrierten JSON- und YAML-Editor, mit dem Sie CloudFormation Vorlagen anzeigen und bearbeiten können.
- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Komponententests ausführen und bereitstellungsbereite Artefakte erstellen können.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie kontrollieren, wer authentifiziert und autorisiert ist, diese zu verwenden.

- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Step Functions ist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen.
- AWS X-Ray hilft Ihnen dabei, Daten über die Anfragen zu sammeln, die Ihre Anwendung bedient, und bietet Tools, mit denen Sie diese Daten anzeigen, filtern und Einblicke in sie gewinnen können, um Probleme und Optimierungsmöglichkeiten zu identifizieren.

Code

Der Beispielcode für dieses Muster ist im GitHub Cross Account CodeBuild Proxy Repository verfügbar. Dieses Muster verwendet die Bibliothek AWS Lambda Powertools for Python, um Protokollierungs- und Ablaufverfolgungsfunktionen bereitzustellen. Weitere Informationen zu dieser Bibliothek und ihren Dienstprogrammen finden Sie unter Powertools for AWS Lambda (Python).

Bewährte Methoden

1. Passen Sie die Wartezeitwerte in der Step Function-Zustandsmaschine an, um die Anzahl der Abfragen für den Jobstatus zu minimieren. Verwenden Sie die erwartete Ausführungszeit für das CodeBuild Projekt.
2. Passen Sie die `MaxConcurrency` Eigenschaft der Map in Step Functions an, um zu steuern, wie viele CodeBuild Projekte parallel ausgeführt werden können.
3. Prüfen Sie bei Bedarf den Beispielcode auf Produktionsreife. Überlegen Sie, welche Daten von der Lösung protokolliert werden könnten und ob die standardmäßige CloudWatch Amazon-Verschlüsselung ausreichend ist.

Epen

Erstellen Sie die Lambda-Proxyfunktion und die zugehörige IAM-Rolle im Quellkonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erfassen Sie das AWS-Konto IDs.	AWS-Konten IDs sind erforderl ich, um den kontenübe	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	rgreifenden Zugriff einzurich ten. Notieren Sie sich die AWS-Konto-ID für Ihre Quell- und Zielkonten. Weitere Informati onen finden Sie in der IAM-Dokumentation unter Finden Ihrer AWS-Konto-ID.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die CloudFormation AWS-Vorlagen herunter.	1. Laden Sie die `sample_target_codebuild_template.yaml` CloudFormation AWS-Vorlage für dieses Muster aus dem GitHub Repository herunter. 2. Laden Sie die `codebuild_lambda_proxy_template.yaml` CloudFormation AWS-Vorlage für dieses Muster aus dem GitHub Repository herunter. **Note** In den CloudFormation AWS-Vorlagen `<SourceAccountId>` ist dies die AWS-Konto-ID für das Quellkonto und `<TargetAccountId>` die AWS-Konto-ID für das Zielkonto.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und implementieren Sie den CloudFormation AWS-Stack.	1. Melden Sie sich bei der AWS-Managementkonsole für Ihr Quellkonto an, öffnen Sie die CloudFormation AWS-Konsole und wählen Sie dann Stacks aus. 2. Wählen Sie Stack erstellen und dann Mit neuen Ressourcen (Standard) aus. 3. Wählen Sie unter Templete source (Vorlagenquelle) den Wert Upload a template file (Vorlagendatei hochladen) aus. 4. Wählen Sie unter Vorlagendatei hochladen die Option Datei und dann Ihre heruntergeladene `codebuild_lambda_proxy_template.yaml` Datei aus. Wählen Sie Weiter aus. 5. Geben Sie unter Stackname einen Namen für den Stapel ein (z. B.`codebuild-lambda-proxy`). 6. **Note** Ersetzen Sie den `crossAccountTargetRoleArn`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Parameter durch Ihren `<TargetAccountId>` (z. B.`<arn:aws:iam::123456789012:role/proxy-lambda-codebuild-role>`). : Sie müssen den Standardwert für den **`targetCodeBuildProject`** Parameter nicht aktualisieren. 7. Wählen Sie Weiter, akzeptieren Sie die Standardoptionen für die Stapelerstellung und wählen Sie dann Weiter. 8. Aktivieren Sie das Kontrollkästchen Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen mit benutzerdefinierten Namen erstellt, und wählen Sie dann Stack erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Sie müssen den CloudFormation AWS-Stack für die Proxy-Lambda-Funktion erstellen, bevor Sie Ressourcen in Zielkonten erstellen. Wenn Sie eine Vertrauensrichtlinie in einem Zielkonto erstellen, wird die IAM-Rolle vom Rollennamen in eine interne Kennung übersetzt. Aus diesem Grund muss die IAM-Rolle bereits existieren.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie die Erstellung der Proxyfunktion und der State-Machine.	1. Warten Sie, bis der CloudFormation AWS-Stack den Status CREATE_COMPLETE erreicht hat. Dies sollte weniger als eine Minute dauern. 2. Öffnen Sie die AWS Lambda Lambda-Konsole, wählen Sie Functions und suchen Sie dann nach der `lambda-proxy-ProxyLambda-<GUID>` Funktion. 3. Öffnen Sie die AWS Step Functions Functions-Konsole, wählen Sie State Machines und suchen Sie dann den `sample-crossaccount-codebuild-state-machine` State Machine.	AWS DevOps

Erstellen Sie eine IAM-Rolle im Zielkonto und starten Sie ein Beispielprojekt CodeBuild

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und implementieren Sie den CloudFormation AWS-Stack.	1. Melden Sie sich bei der AWS-Managementkonsole für Ihr Zielkonto an, öffnen Sie die CloudFormation AWS-Konsole und wählen Sie dann Stacks aus.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie Create Stack und dann With new resources (Standard) aus. 3. Wählen Sie unter Templete source (Vorlagenquelle) den Wert Upload a template file (Vorlagendatei hochladen) aus. 4. Wählen Sie für „Eine Vorlagendatei hochladen “ die Option „Datei auswählen“ und wählen Sie dann die `sample_target_codebuild_template.yaml` Datei aus. Wählen Sie Weiter aus. 5. Geben Sie unter Stackname einen Namen für den Stapel ein (zum Beispiel:`sample-codebuild-stack`). 6. Ersetzen Sie den `crossAccountSourceRoleArn` Parameter durch Ihren `<SourceAccountId>` (zum Beispiel`<arn:aws:iam::123456789012:role/codebuild-proxy-lambda-role>`). 7. Wählen Sie Weiter, akzeptieren Sie die Standardoptionen für	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Stapelerstellung und wählen Sie dann Weiter. 8. Aktivieren Sie das Kontrollkästchen Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen mit benutzerdefinierten Namen erstellt, und wählen Sie dann Stack erstellen aus.	
Überprüfen Sie die Erstellung des CodeBuild Beispielprojekts.	1. Warten Sie, bis der CloudFormation AWS-Stack den Status CREATE_COMPLETE erreicht hat. Dies sollte weniger als eine Minute dauern. 2. Öffnen Sie die CodeBuild AWS-Konsole und suchen Sie dann das `sample-codebuild-project` Projekt.	AWS DevOps

Testen Sie die kontoübergreifende Lambda-Proxyfunktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Zustandsmaschine.	1. Melden Sie sich bei der AWS-Managementkonsole für Ihr Quellkonto an, öffnen Sie die AWS Step Functions-Konsole und wählen Sie dann State machines aus.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie die `sample-crossaccount-codebuild-state-machine` Zustandsmaschine aus und klicken Sie dann auf Ausführung starten. 3. Geben Sie im Eingabe-Editor den folgenden JSON-Code ein und `<TargetAccountID>` ersetzen Sie ihn durch die AWS-Konto-ID des Kontos, das das CodeBuild Projekt enthält. `{ "crossAccountTargetRoleArns": [ { "arn": "arn:aws:iam::<TargetAccountID>:role/proxy-lambda-codebuild-role", "region": "eu-west-1", "codeBuildProject": "sample-codebuild-project", "SampleValue1": "Value1", "SampleValue2": "Value2" } ] }`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Die Schlüssel-Wert-Paare werden als Umgebungsvariablen von der Funktion im Quellkonto an das CodeBuild Projekt im Zielkonto übergeben. 4. Wählen Sie Start execution (Ausführung starten) aus. 5. Überprüfen Sie auf der State-Machine-Seite auf der Registerkarte Details, ob der Ausführungsstatus auf Erfolgreich gesetzt ist. Dadurch wird bestätigt, dass Ihr Zustandsmaschine läuft. Hinweis: Es kann etwa 30 Sekunden dauern, bis die Zustandsmaschine den Status Erfolgreich erreicht hat. 6. Um die Ausgabe und Eingabe eines Schritts in der Zustandsmaschine zu sehen, erweitern Sie diesen Schritt im Abschnitt Verlauf der Ausführungsereignisse. Erweitern Sie beispielsweise den Schritt Lambda	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	— CodeBuild Proxy — Start. Die Ausgabe enthält Details zu den überschri ebenen Umgebungs variablen, der ursprüngl ichen Nutzlast und der Job-ID. CodeBuild	
Validieren Sie die Umgebungs variablen.	1. Melden Sie sich bei der AWS-Managementkonsole für Ihr Zielkonto an. 2. Öffnen Sie die CodeBuild AWS-Konsole, erweitern Sie Build und wählen Sie dann Build projects aus. 3. Wählen Sie das `sample-codebuild-project` Projekt und dann Details anzeigen aus. 4. Wählen Sie auf der Registerkarte Build-Verlauf den neuesten Build des Projekts und dann Logs anzeigen aus. 5. Stellen Sie in der Protokoll ausgabe sicher, dass die auf STDOUT ausgegebe nen Umgebungsvariablen mit den Umgebungs variablen aus der Step Functions Functions-Beispielstatusmaschine übereinstimmen.	AWS DevOps

Fehlerbehebung

Problem	Lösung
Die Ausführung von Step Functions dauert länger als erwartet.	Passen Sie die `MaxConcurrency` Eigenschaft der Map in der Step Function-Zustandsmaschine an, um zu steuern, wie viele CodeBuild Projekte parallel ausgeführt werden können.
Die Ausführung der CodeBuild Jobs dauert länger als erwartet.	1. Passen Sie die Wartezeitwerte in der Step Functions Functions-Zustandsmaschine an, um Abrufanforderungen für den Jobstatus zu minimieren. Verwenden Sie die erwartete Ausführungszeit für das CodeBuild Projekt. 2. Überlegen Sie, ob CodeBuild das geeignete Tool verwendet werden soll. Beispielsweise kann die Zeit, die für die Initialisierung eines CodeBuild Jobs benötigt wird, erheblich länger sein als bei AWS Lambda. Wenn ein hoher Durchsatz und schnelle Abschluss zeiten erforderlich sind, sollten Sie erwägen, die Geschäftslogik auf AWS Lambda zu migrieren und eine Fan-Out-Architektur zu verwenden.

Multi-AZ-Failover für EMR-Cluster mithilfe von Application Recovery Controller verwalten

Erstellt von Aarti Rajput (AWS), Ashish Bhatt (AWS), Neeti Mishra (AWS) und Nidhi Sharma (AWS)

Übersicht

Dieses Muster bietet eine effiziente Disaster-Recovery-Strategie für Amazon EMR-Workloads, um eine hohe Verfügbarkeit und Datenkonsistenz in mehreren Availability Zones innerhalb einer einzigen sicherzustellen. AWS-Region Das Design verwendet Amazon Application Recovery Controller und einen Application Load Balancer, um Failover-Operationen und die Verkehrsverteilung für einen Apache Spark-basierten EMR-Cluster zu verwalten.

Unter Standardbedingungen hostet die primäre Availability Zone einen aktiven EMR-Cluster und eine Anwendung mit voller Lese-/Schreibfunktionalität. Wenn eine Availability Zone unerwartet ausfällt, wird der Datenverkehr automatisch zur sekundären Availability Zone umgeleitet, wo ein neuer EMR-Cluster gestartet wird. Beide Availability Zones greifen über spezielle Gateway-Endpunkte auf einen gemeinsamen Amazon Simple Storage Service (Amazon S3) -Bucket zu, wodurch eine konsistente Datenverwaltung gewährleistet wird. Dieser Ansatz minimiert Ausfallzeiten und ermöglicht eine schnelle Wiederherstellung kritischer Big-Data-Workloads bei Ausfällen in der Availability Zone. Die Lösung ist in Branchen wie dem Finanzwesen oder dem Einzelhandel nützlich, in denen Echtzeitanalysen von entscheidender Bedeutung sind.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Amazon EMR auf Amazon Elastic Compute Cloud (Amazon EC2)
- Zugriff vom Master-Knoten des EMR-Clusters auf Amazon S3.
- AWS Multi-AZ-Infrastruktur

Einschränkungen

- Einige AWS-Services sind nicht in allen AWS-Regionen verfügbar. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie auf der Seite Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Produktversionen

- Amazon EMR 6.x und spätere Versionen

Architektur

Zieltechnologie-Stack

- Amazon EMR-Cluster
- Amazon Application Recovery Controller
- Application Load Balancer
- Amazon-S3-Bucket
- Gateway-Endpunkte für Amazon S3

Zielarchitektur

Diese Architektur bietet Ausfallsicherheit für Anwendungen, indem sie mehrere Availability Zones verwendet und einen automatisierten Wiederherstellungsmechanismus über den Application Recovery Controller implementiert.

1. Der Application Load Balancer leitet den Datenverkehr an die aktive Amazon EMR-Umgebung weiter, bei der es sich in der Regel um den primären EMR-Cluster in der primären Availability Zone handelt.
2. Der aktive EMR-Cluster verarbeitet die Anwendungsanfragen und stellt über seinen speziellen Amazon S3-Gateway-Endpunkt für Lese- und Schreibvorgänge eine Verbindung zu Amazon S3 her.
3. Amazon S3 dient als zentrales Datenrepository und wird möglicherweise als Checkpoint oder als gemeinsam genutzter Speicher zwischen EMR-Clustern verwendet. EMR-Cluster behalten die Datenkonsistenz bei, wenn sie über `s3://` das Protokoll und das EMR-Dateisystem (EMRFS) direkt in Amazon S3 schreiben.
4. Application Recovery Controller überwacht kontinuierlich den Zustand der primären Availability Zone und verwaltet bei Bedarf automatisch Failover-Operationen.
5. Wenn der Application Recovery Controller einen Fehler im primären EMR-Cluster feststellt, ergreift er die folgenden Aktionen:

- Initiiert den Failover-Prozess für den sekundären EMR-Cluster in Availability Zone 2.
- Aktualisiert die Routingkonfigurationen, um den Verkehr zum sekundären Cluster weiterzuleiten.

Tools

AWS-Services

- Amazon Application Recovery Controller unterstützt Sie bei der Verwaltung und Koordination der Wiederherstellung Ihrer Anwendungen in allen AWS-Regionen Availability Zones. Dieser Service vereinfacht den Prozess und verbessert die Zuverlässigkeit der Anwendungswiederherstellung, indem er die manuellen Schritte reduziert, die bei herkömmlichen Tools und Prozessen erforderlich sind.
- Application Load Balancer arbeitet auf der Anwendungsebene, der siebten Schicht des Open Systems Interconnection (OSI) -Modells. Er verteilt den eingehenden Anwendungsdatenverkehr auf mehrere Ziele, z. B. EC2 Instanzen, in mehreren Availability Zones. Dies erhöht die Verfügbarkeit Ihrer Anwendung.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie AWS-Services über Befehle in Ihrer Befehlszeilen-Shell interagieren können.
- Amazon EMR ist eine Big-Data-Plattform, die Datenverarbeitung, interaktive Analyse und maschinelles Lernen für Open-Source-Frameworks wie Apache Spark, Apache Hive und Presto bietet.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem es kontrolliert, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Amazon S3 bietet eine einfache Webservice-Schnittstelle, mit der Sie beliebige Datenmengen zu jeder Zeit und von überall speichern und abrufen können. Mit diesem Service können Sie ganz einfach Anwendungen erstellen, die Cloud-nativen Speicher nutzen.
- Gateway-Endpunkte für Amazon S3 sind Gateways, die Sie in Ihrer Routing-Tabelle angeben, um von Ihrer Virtual Private Cloud (VPC) aus über das Netzwerk auf Amazon S3 zuzugreifen. AWS

Bewährte Methoden

- Folgen Sie den AWS Best Practices für Sicherheit, Identität und Compliance, um eine robuste und sichere Architektur zu gewährleisten.
- Richten Sie die Architektur auf das AWS Well-Architected Framework aus.

- Verwenden Sie Amazon S3 Access Grants, um den Zugriff von Ihrem Spark-basierten EMR-Cluster auf Amazon S3 zu verwalten. Einzelheiten finden Sie im Blogbeitrag Use Amazon EMR with S3 Access Grants to Scale Spark access to Amazon S3.
- Verbessern Sie die Spark-Leistung mit Amazon S3.

Epen

So richten Sie Ihre Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie sich bei der an AWS Management Console.	Melden Sie sich als IAM-Benutzer bei der AWS Management Console an. Anweisungen finden Sie in der AWS Dokumentation.	AWS DevOps
Konfigurieren Sie die AWS CLI.	Installieren Sie die AWS CLI oder aktualisieren Sie sie auf die neueste Version, damit Sie mit AWS-Services der interagieren können AWS Management Console. Anweisungen finden Sie in der AWS CLI Dokumentation.	AWS DevOps

Stellen Sie eine Spark-Anwendung auf Ihrem EMR-Cluster bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	1. Erstellen Sie einen S3-Bucket, um den Eingabedatensatz, die Protokolle, die Anwendung und die Ausgabedaten zu speichern. Anweisungen finden Sie in	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Amazon S3 S3-Dokumentation. 2. Organisieren Sie den Bucket in separate Ordner für Eingabedaten (`dataset`), Logs (`logs`), Spark-Anwendung (`spark-app `) und Ausgabedaten (`output`).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie einen EMR-Cluster.	1. Verwenden Sie die folgenden AWS CLI Befehle, um einen EMR-Cluster (z. B. Version 6.12 oder höher) mit Instances zu erstellen, die sich über zwei Availability Zones (wie `us-east-1a` und `us-east-1b`) erstrecken, um Hochverfügbarkeit zu gewährleisten. Der Befehl gibt den `m4.large` Instanztyp als Beispiel an.
	
	`aws emr create-cluster \ --ec2-attributes AvailabilityZone=<AZ-name-1> \ --release-label emr-6.12.0 \ --instance-groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE,InstanceCount=2,InstanceType=m4.large`
	
	`aws emr create-cluster \ --ec2-attributes AvailabilityZone=<AZ-name-2> \ --release-label emr-6.12.0 \`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>--instance-groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE,InstanceCount=2,InstanceType=m4.large</pre> Weitere Informationen finden Sie im Befehl create-cluster und in der Amazon EMR-Dokumentation. 2. Stellen Sie das key pair, die Servicerolle und das Instanzprofil nach Bedarf mit den erforderlichen Berechtigungen bereit.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Sicherheitseinstellungen für den EMR-Cluster.	1. Identifizieren Sie die Sicherheitsgruppe, die dem Master-Knoten des EMR-Clusters zugeordnet ist, indem Sie den Befehl AWS CLI describe-cluster verwenden: `aws emr describe-cluster --cluster-id j-XXXXXXXX` 2. Um die Sicherheit zu erhöhen, ändern Sie die Einstellungen der Sicherheitsgruppe so, dass SSH-Zugriff (TCP-Port 22) auf den Master-Knoten zulässig ist, dieser jedoch auf Ihre spezifische IP-Adresse beschränkt ist. Weitere Informationen finden Sie in der Amazon EMR-Dokumentation.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Connect zum EMR-Cluster her.	Stellen Sie mithilfe des bereitgestellten key pair über SSH eine Connect zum Master-Knoten des EMR-Clusters her.
	
	Stellen Sie sicher, dass sich die Schlüsselpaardatei im selben Verzeichnis wie Ihre Anwendung befindet.
	
	Führen Sie die folgenden Befehle aus, um die richtigen Berechtigungen für das key pair festzulegen und die SSH-Verbindung herzustellen:
	
	`chmod 400 <key-pair-name>`
	`ssh -i ./<key-pair-name> hadoop@<master-node-public-dns>`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die Spark-Anwendung bereit.	Nachdem Sie die SSH-Verbindung hergestellt haben, befinden Sie sich in der Hadoop-Konsole.
	
	1. Erstellen oder bearbeiten Sie die Spark-Anwendungsdatei (`main.py`) mit einem Texteditor wie vim:
	
	`vim main.py`
	
	Weitere Informationen zum Erstellen und Ändern der Spark-Anwendung finden Sie in der Amazon EMR-Dokumentation.
	2. Senden Sie die Spark-Anwendung an den EMR-Cluster und geben Sie dabei die Speicherorte der Eingabe- und Ausgabedaten im S3-Bucket an:
	
	`spark-submit main.py –data_source <input-data-folder-in-s3> –output_uri <output-folder-in-s3>`
	
	Hier ist ein Beispiel, das auf den Ordnern basiert, die Sie zuvor eingerichtet haben:
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`spark-submit main.py –data_source dataset –output_uri output`
	3. Überwachen Sie den Fortschritt der Anwendung , indem Sie die Anwendung sprotokolle überprüfen:
	`yarn logs -applicationId <application-id>`	

Überwachen Sie die Spark-Anwendung.	1. Öffnen Sie ein weiteres Terminalfenster und richten Sie einen SSH-Tunnel zur Resource Manager-Weboberfläche des EMR-Clusters ein: `ssh -i <key-pair-name> -N -L 8157:<resource-manager-public-dns>:8088 hadoop@<resource-manager-public-dns>` 2. Um die Anwendung zu überwachen, greifen Sie auf die Resource Manager-Weboberfläche zu, indem Sie `http://localhost:8157` in Ihrem Webbrowser zu navigieren.	AWS DevOps

Verkehr in eine andere Availability Zone verlagern

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Application Load Balancer.	Richten Sie die Zielgruppe ein, die den Datenverkehr zwischen Amazon EMR-Masterknoten weiterleitet, die in zwei Availability Zones innerhalb einer AWS-Region bereitgestellt werden. Eine Anleitung finden Sie in der Elastic Load Balancing -Dokumentation unter Eine Zielgruppe für Ihren Application Load Balancer erstellen.	AWS DevOps
Konfigurieren Sie die Zonenverschiebung im Application Recovery Controller.	In diesem Schritt verwenden Sie die Zonal Shift-Funktion in Application Recovery Controller, um den Datenverkehr in eine andere Availability Zone zu verlagern. 1. Öffnen Sie die Application Recovery Controller-Konsole. 2. Wählen Sie unter Erste Schritte die Optionen Zonal Shift und Start Zonal Shift aus. 3. Wählen Sie die Availability Zone aus, von der Sie den Verkehr wegverlagern möchten.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie in der Tabelle Ressourcen eine unterstützte Ressource (z. B. Application Load Balancer) für die Zonenverschiebung aus. 5. Wählen Sie unter Ablauf der Zonenschicht festlegen eine Ablaufzeit für die Zonenschicht aus, oder geben Sie sie ein. Sie können eine Dauer zwischen 1 Minute und drei Tagen (72 Stunden) festlegen. Alle Zonenverschiebungen sind temporär. Sie müssen ein Ablaufdatum festlegen, aber Sie können aktive Schichten später aktualisieren, um einen neuen Ablaufzeitraum von bis zu drei Tagen festzulegen. 6. Geben Sie einen Kommentar zu dieser Zonenschicht ein. 7. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass durch den Start einer Zonenverschiebung die verfügbare Kapazität für Ihre Anwendung reduziert wird, da der Datenverkehr	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	von der Availability Zone weg verlagert wird. 8. Wählen Sie Starten. Informationen zur AWS CLI Verwendung von finden Sie unter Beispiele für die Verwendung von AWS CLI with Zonal Shift in der Dokumentation zu Application Recovery Controller.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Konfiguration und den Fortschritt der Zonenschicht.	1. Überprüfen Sie die Ressourcen, die bei Zonal Shift registriert sind:
	`aws arc-zonal-shift list-managed-resources --region <AWS-region-name>`
	Die folgende Ausgabe bestätigt beispielsweise, dass die Ressourcen in beiden Availability Zones betriebsbereit sind.
	`"appliedWeights": { "use1-az1": 1.0, "use1-az2": 1.0 },`
	2. Um die Zonenverschiebung zu visualisieren, verwenden Sie den folgenden AWS CLI Befehl, um die Zonenverschiebung zu starten:
	`aws arc-zonal-shift start-zonal-shift \ --resource-identifier <application-load-balancer-arn> \ --away-from <source-AZ> \ --expires-in 10m --comment "testing" \`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>--region <AWS-regi
	on-name></pre>
	wo `<source-AZ>` ist der Identifier der Availabil ity Zone, von der Sie den Traffic wegverlagern möchten, und `<applicat ion-load-balancer-arn>` ist der Amazon Resource Name (ARN) Ihres Application Load Balancer.
	3. Stellen Sie sicher, dass der Datenverkehr in eine andere Availability Zone verlagert wurde.
	<pre>aws arc-zonal-shift
	get-managed-resour
	ce \
	--resource-identif
	ier <application-
	load-balancer-arn> \
	--region <AWS-regi
	on-name></pre>
	Sie können sehen, dass die Zonenverschiebung anhand dieser Gewichtun gen bestätigt wird:
	<pre>"appliedWeights": {
	"use1-az1":
	0.0,
	"use1-az2":
	1.0</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>},</pre>	

Zugehörige Ressourcen

- AWS CLI Befehle:
  - create-cluster
  - Cluster beschreiben
  - arc-zonal-shift
- Konfiguration von Amazon EMR-Cluster-Instance-Typen und Best Practices für Spot-Instances (Amazon EMR-Dokumentation)
- Bewährte Sicherheitsmethoden in IAM (IAM-Dokumentation)
- Verwenden Sie Instanzprofile (IAM-Dokumentation)
- Verwenden Sie Zonal Shift und Zonal Autoshift, um Anwendungen in ARC wiederherzustellen (Application Recovery Controller-Dokumentation)

Verwalten Sie Blau/Grün-Bereitstellungen von Microservices für mehrere Konten und Regionen mithilfe von AWS-Code-Services und AWS KMS-Regionsschlüsseln für mehrere Regionen

Erstellt von Balaji Vedagiri (AWS), Ashish Kumar (AWS), Faisal Shahdad (AWS), Anand Krishna Varanasi (AWS), Vanitha Dontireddy (AWS) und Vivek Thangamuthu (AWS)

Übersicht

AWS CodeCommit Hinweis: ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Dieses Muster beschreibt, wie eine globale Microservices-Anwendung von einem zentralen AWS-Konto auf mehrere Workload-Konten und Regionen gemäß einer Blau/Grün-Bereitstellungsstrategie bereitgestellt wird. Das Muster unterstützt Folgendes:

- Software wird in einem zentralen Konto entwickelt, wohingegen Workloads und Anwendungen auf mehrere Konten und AWS-Regionen verteilt sind.
- Ein einziger regionsübergreifender AWS Key Management System (AWS KMS) -Schlüssel wird für die Verschlüsselung und Entschlüsselung verwendet, um die Notfallwiederherstellung abzudecken.
- Der KMS-Schlüssel ist regionsspezifisch und muss für Pipeline-Artefakte in drei verschiedenen Regionen verwaltet oder erstellt werden. Ein regionsübergreifender KMS-Schlüssel hilft dabei, dieselbe Schlüssel-ID in allen Regionen beizubehalten.
- Das Git-Workflow-Verzweigungsmodell ist mit zwei Branches (Development und Main) implementiert und der Code wird mithilfe von Pull-Requests (PRs) zusammengeführt. Die AWS Lambda Lambda-Funktion, die von diesem Stack aus bereitgestellt wird, erstellt eine PR vom Entwicklungszweig zum Hauptzweig. Die PR-Zusammenführung mit der Hauptzweig initiiert eine CodePipeline AWS-Pipeline, die den CI/CD-Fluss (Continuous Integration and Continuous Delivery) orchestriert und die Stacks kontenübergreifend bereitstellt.

Dieses Muster bietet ein Beispiel für die Einrichtung einer Infrastruktur als Code (IaC) über CloudFormation AWS-Stacks, um diesen Anwendungsfall zu demonstrieren. Die blaue/grüne Bereitstellung von Microservices wird mithilfe von AWS implementiert. CodeDeploy

Voraussetzungen und Einschränkungen

Voraussetzungen

- Vier aktive AWS-Konten:
  - Ein Tools-Konto zur Verwaltung der Code-Pipeline und zur Wartung des CodeCommit AWS-Repositorys.
  - Drei Workload-Konten (Testkonten) für die Bereitstellung des Microservices-Workloads.
- Dieses Muster verwendet die folgenden Regionen. Wenn Sie andere Regionen verwenden möchten, müssen Sie die entsprechenden Änderungen an den mehrregionalen AWS CodeDeploy - und AWS KMS KMS-Stacks vornehmen.
  - Tools-Konto (AWS CodeCommit): `ap-south-1`
  - Workload- (Test-) Konto 1: `ap-south-1`
  - Workload- (Test-) Konto 2: `eu-central-1`
  - Workload- (Test-) Konto 3: `us-east-1`
- Drei Amazon Simple Storage Service (Amazon S3) -Buckets für die Bereitstellungsregionen in jedem Workload-Konto. (Diese werden aufgerufen `S3BUCKETNAMETESTACCOUNT1` `S3BUCKETNAMETESTACCOUNT2` und `S3BUCKETNAMETESTACCOUNT3` später in diesem Muster aufgeführt.)

  Sie können diese Buckets beispielsweise in bestimmten Konten und Regionen mit eindeutigen Bucket-Namen wie folgt erstellen (ersetzen Sie xxxx durch eine Zufallszahl):

```
##In Test Account 1
aws s3 mb s3://ecs-codepipeline-xxxx-ap-south-1 --region ap-south-1
##In Test Account 2
aws s3 mb s3://ecs-codepipeline-xxxx-eu-central-1 --region eu-central-1
##In Test Account 3
aws s3 mb s3://ecs-codepipeline-xxxx-us-east-1 --region us-east-1

#Example
##In Test Account 1
aws s3 mb s3://ecs-codepipeline-18903-ap-south-1 --region ap-south-1
##In Test Account 2
aws s3 mb s3://ecs-codepipeline-18903-eu-central-1 --region eu-central-1
##In Test Account 3
aws s3 mb s3://ecs-codepipeline-18903-us-east-1 --region us-east-1
```

Einschränkungen

Das Muster verwendet AWS CodeBuild und andere Konfigurationsdateien, um einen Beispiel-Microservice bereitzustellen. Wenn Sie einen anderen Workload-Typ verwenden (z. B. serverlos), müssen Sie alle relevanten Konfigurationen aktualisieren.

Architektur

Zieltechnologie-Stack

- AWS CloudFormation
- AWS CodeCommit
- AWS CodeBuild
- AWS CodeDeploy
- AWS CodePipeline

Zielarchitektur

Automatisierung und Skalierung

Die Einrichtung wird mithilfe von CloudFormation AWS-Stack-Vorlagen (IaC) automatisiert. Es kann problemlos für mehrere Umgebungen und Konten skaliert werden.

Tools

AWS-Services

- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.
- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Komponententests ausführen und bereitstellungsbereite Artefakte erstellen können.
- AWS CodeCommit ist ein Versionskontrollservice, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodeDeploy automatisiert Bereitstellungen auf Amazon Elastic Compute Cloud (Amazon EC2) oder lokalen Instances, AWS Lambda Lambda-Funktionen oder Amazon Elastic Container Service (Amazon ECS) -Services.

- AWS CodePipeline hilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Beenden und Verwalten von Containern in einem Cluster vereinfacht.
- AWS Key Management Service (AWS KMS) unterstützt Sie bei der Erstellung und Kontrolle kryptografischer Schlüssel, um Ihre Daten zu schützen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Zusätzliche Tools

- Git ist ein verteiltes Open-Source-Versionskontrollsystem, das mit dem CodeCommit AWS-Repository zusammenarbeitet.
- Docker ist eine Reihe von Platform-as-a-Service (PaaS) -Produkten, die Virtualisierung auf Betriebssystemebene nutzen, um Software in Containern bereitzustellen. Dieses Muster verwendet Docker, um Container-Images lokal zu erstellen und zu testen.
- cfn-lint und cfn-nag sind Open-Source-Tools, mit denen Sie CloudFormation Stacks auf Fehler und Sicherheitsprobleme überprüfen können.

Code-Repository

Der Code für dieses Muster ist im Repository für GitHub globale Blue/Green-Bereitstellungen in mehreren Regionen und Konten verfügbar.

Epen

Richten Sie Umgebungsvariablen ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Exportieren Sie Umgebungsvariablen für die CloudFormation Stack-Bereitstellung.	Definieren Sie Umgebungsvariablen, die später in diesem Muster als Eingabe für die CloudFormation Stacks verwendet werden.
	
	1. Aktualisieren Sie die Bucket-Namen, die Sie in den drei Konten und Regionen erstellt haben, wie weiter oben im Abschnitt Voraussetzungen beschrieben:
	
	`export S3BUCKETNAMETESTACCOUNT1=<S3BUCKETACCOUNT1>`
	`export S3BUCKETNAMETESTACCOUNT2=<S3BUCKETACCOUNT2>`
	`export S3BUCKETNAMETESTACCOUNT3=<S3BUCKETACCOUNT3>`
	
	2. Definieren Sie eine zufällige Zeichenfolge, um Artefakt-Buckets zu erstellen, da Bucket-Namen weltweit eindeutig sein müssen:
	
	`export BUCKETSTARTNAME=ecs-codepip`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>eline-artifacts-19
	992</pre>
	3. Definieren und exportieren Sie das Konto IDs und die Regionen:
	<pre>export TOOLSACCO
	UNT=<TOOLSACCOUNT>
	export CODECOMMI
	TACCOUNT=<CODECOMM
	ITACCOUNT>
	export CODECOMMI
	TREGION=ap-south-1
	export CODECOMMI
	TREPONAME=Poc
	export TESTACCOU
	NT1=<TESTACCOUNT1>
	export TESTACCOU
	NT2=<TESTACCOUNT2>
	export TESTACCOU
	NT3=<TESTACCOUNT3>
	export TESTACCOU
	NT1REGION=ap-south
	-1
	export TESTACCOU
	NT2REGION=eu-centr
	al-1
	export TESTACCOU
	NT3REGION=us-east-1
	export TOOLSACCO
	UNTREGION=ap-south
	-1
	export ECRREPOSI
	TORYNAME=web</pre>	

Package und Bereitstellen der CloudFormation Stacks für die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Klonen Sie das Repository	Klonen Sie das Beispiel-Repository in ein neues Repository an Ihrem Arbeitsplatz:
	`##In work location`
	`git clone https://github.com/aws-samples/ecs-blue-green-global-deployment-with-multiregion-cmk-codepipeline.git`
		AWS DevOps

Package Sie die Cloudformation-Ressourcen.	In diesem Schritt packen Sie die lokalen Artefakte, auf die sich die CloudFormation Vorlagen beziehen, um die Infrastrukturressourcen zu erstellen, die für Dienste wie Amazon Virtual Private Cloud (Amazon VPC) und Application Load Balancer erforderlich sind.
	Die Vorlagen sind im `Infra` Ordner des Code-Repositorys verfügbar.
	`##In TestAccount1##`
	`aws cloudformation package \`
	`--template-file mainInfraStack.yaml \`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	--s3-bucket $S3BUCKETNAMETESTACCOUNT1 \ --s3-prefix infraStack \ --region $TESTACCOUNT1REGION \ --output-template-file infrastructure_${TESTACCOUNT1}.template ##In TestAccount2## aws cloudformation package \ --template-file mainInfraStack.yaml \ --s3-bucket $S3BUCKETNAMETESTACCOUNT2 \ --s3-prefix infraStack \ --region $TESTACCOUNT2REGION \ --output-template-file infrastructure_${TESTACCOUNT2}.template ##In TestAccount3## aws cloudformation package \ --template-file mainInfraStack.yaml \ --s3-bucket $S3BUCKETNAMETESTACCOUNT3 \ --s3-prefix infraStack \	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--region $TESTACCOUNT3REGION \` `--output-template-file infrastructure_${TESTACCOUNT3}.template`	

Validieren Sie die Paketvorlagen.	Überprüfen Sie die Paketvorlagen:
	`aws cloudformation validate-template \`
	`--template-body file://infrastructure_${TESTACCOUNT1}.template`
	
	`aws cloudformation validate-template \`
	`--template-body file://infrastructure_${TESTACCOUNT2}.template`
	
	`aws cloudformation validate-template \`
	`--template-body file://infrastructure_${TESTACCOUNT3}.template`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die Paketdateien in den Workload-Konten bereit,	1. Aktualisieren Sie die Platzhalterwerte und Kontonamen im `nfraParameters.jso n` i-Skript basierend auf Ihrem Setup.
	2. Stellen Sie die Paketvorl agen in Ihren drei Workload-Konten bereit.
	
	`##In TestAccount1## aws cloudformation deploy \ --template-file infrastructure_${T ESTACCOUNT1}.templ ate \ --stack-name mainInfrastack \ --parameter- overrides file://in fraParameters.json \ --region $TESTACCO UNT1REGION \ --capabilities CAPABILITY_IAM CAPABILITY_NAMED_I AM`
	
	`##In TestAccount2## aws cloudformation deploy \ --template-file infrastructure_${T ESTACCOUNT2}.templ ate \ --stack-name mainInfrastack \`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`--parameter-overrides file://infraParameters.json \`
	`--region $TESTACCOUNT2REGION \`
	`--capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM`
	
	`##In TestAccount3##`
	`aws cloudformation deploy \`
	`--template-file infrastructure_${TESTACCOUNT3}.template \`
	`--stack-name mainInfrastack \`
	`--parameter-overrides file://infraParameters.json \`
	`--region $TESTACCOUNT3REGION \`
	`--capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM`	

Senden Sie ein Beispielbild und skalieren Sie Amazon ECS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie ein Beispielbild in das Amazon ECR-Repository.	Senden Sie ein Beispielbild (NGINX) in das Amazon Elastic Container Registry (Amazon ECR) -Repository mit dem Namen `web` (wie in	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	den Parametern festgeleg t). Sie können das Bild nach Bedarf anpassen.
	
	Folgen Sie den Anweisungen in der Amazon ECR-Dokum entation, um sich anzumelde n und die Anmeldeinformation en für die Übertragung eines Bilds an Amazon ECR festzulegen.
	
	Die Befehle lauten:
	
	`docker pull nginx`
	`docker images`
	`docker tag <imageid> aws_account_id.dkr .ecr.region.amazon aws.com/<web>:latest`
	`docker push <aws_acco unt_id>.dkr.ecr.<r egion>.amazonaws.com/ <web>:tag`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Skalieren Sie Amazon ECS und überprüfen Sie den Zugriff.	1. Skalieren Sie Amazon ECS, um zwei Replikate zu erstellen: `aws ecs update-service --cluster QA-Cluster --service Poc-Service --desired-count 2` wo `Poc-Service` bezieht sich auf Ihre Beispielanwendung. 2. Stellen Sie sicher, dass über den Application Load Balancer auf die Dienste zugegriffen werden kann, indem Sie einen vollqualifizierten Domänennamen (FQDN) oder DNS in einem Browser oder mithilfe des Befehls curl verwenden.	AWS DevOps

Richten Sie Code-Services und Ressourcen ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein CodeCommit Repository im Tools-Konto.	Erstellen Sie mithilfe der `codecommit.yaml` Vorlage, die sich im `code` Ordner des CodeCommit Repositorys befindet, ein GitHub Repository im Tools-Konto. Sie dürfen dieses Repository nur in der	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Region erstellen, in der Sie den Code entwickeln möchten. `aws cloudformation deploy --stack-name codecommitrepoStack --parameter-overrides CodeCommitReponame=$CODECOMMITREPONAME \ ToolsAccount=$TOOLSACCOUNT --template-file codecommit.yaml --region $TOOLSACCOUNTREGION \ --capabilities CAPABILITY_NAMED_IAM`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket für die Verwaltung von Artefakten, die von generiert wurden CodePipeline.	Erstellen Sie einen S3-Bucket für die Verwaltung CodePipeline von Artefakten, die mithilfe der `pre-reqs-bucket.yaml` Vorlage generiert wurden, die sich im `code` Ordner des GitHub Repositorys befindet. Die Stacks müssen in allen drei Workload- (Test-) und Tools-Konten und Regionen bereitgestellt werden. `aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TESTACCOUNT1REGION --capabilities CAPABILITY_NAMED_IAM`  `aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketSta`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	rtName=$BUCKETSTAR TNAME \ TestAccount1=$TE STACCOUNT1 TestAccou nt2=$TESTACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tAccount=$CODECOMM ITACCOUNT ToolsAcco unt=$TOOLSACCOUNT \ --template-file pre- reqs_bucket.yaml --region $TESTACCO UNT2REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts -bucket --parameter- overrides BucketSta rtName=$BUCKETSTAR TNAME \ TestAccount1=$TE STACCOUNT1 TestAccou nt2=$TESTACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tAccount=$CODECOMM ITACCOUNT ToolsAcco unt=$TOOLSACCOUNT \ --template-file pre- reqs_bucket.yaml --region $TESTACCO UNT3REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TOOLSACCOUNTREGION --capabilities CAPABILITY_NAMED_IAM	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie einen KMS-Schlüssel für mehrere Regionen ein.	1. Erstellen Sie einen KMS-Schlüssel für mehrere Regionen mit Primär- und Replikatschlüsseln, die CodePipeline verwendet werden. In unserem Beispiel `ToolsAccount1region - ap-south-1` wird das die primäre Region sein. `aws cloudformation deploy --stack-name ecs-codepipeline-pre-reqs-KMS \ --template-file pre-reqs_KMS.yaml --parameter-overrides \ TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT --region $TOOLSACCOUNTREGION` 2. Legen Sie die CMKARN-Variablen fest, die an Projekte übergeben werden sollen CodeBuild . Die Werte sind in der Ausgabe des ecs-codepipeline-pre-reqs-KMS-Vorlagenstapels verfügbar (die Schlüssel-ID	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	ist in allen Regionen gleich und beginnt mit). `mrk-` Sie können die CMKARN-Werte auch aus dem Tools-Konto abrufen. Exportieren Sie sie in alle Kontositzungen:
	`export CMKARN1=arn:aws:kms:ap-south-1:<TOOLSACCOUNTID>:key/mrk-xxx`
	`export CMKARN2=arn:aws:kms:eu-central-1:<TOOLSACCOUNTID>:key/mrk-xxx`
	`export CMKARN3=arn:aws:kms:us-east-1:<TOOLSACCOUNTID>:key/mrk-xxx`
	`export CMARNTOOLS=arn:aws:kms:ap-south-1:<TOOLSACCOUNTID>:key/mrk-xxx`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie das CodeBuild Projekt im Tools-Konto ein.	1. Verwenden Sie die `codebuild_IAM.yaml` Vorlage aus dem `code` Ordner des GitHub Repositorys, um AWS Identity and Access Management (IAM) für AWS CodeBuild in einer einzigen Region im Tools-Konto einzurichten:
	`#In ToolsAccount aws cloudformation deploy --stack-name ecs-codebuild-iam \ --template-file codebuild_IAM.yaml --region $TOOLSACCOUNTREGION \ --capabilities CAPABILITY_NAMED_IAM`
	2. Verwenden Sie die `codebuild.yaml` Vorlage, um Ihr Build-Projekt einzurichten CodeBuild . Stellen Sie diese Vorlage in allen drei Regionen wie folgt bereit:
	`aws cloudformation deploy --stack-name ecscodebuildstack -- parameter-overrides ToolsAccount=$TOOLSACCOUNT \`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CodeCommitRepoName= $CODECOMMITREPONAME ECRRepositoryName= $ECRREPOSITORYNAME APPACCOUNTID=$TEST ACCOUNT1 \ TestAccount3=$TE STACCOUNT3 CodeCommi tRegion=$CODECOMMI TREGION CMKARN=$C MKARN1 \ --template-file codebuild.yaml --region $TESTACCO UNT1REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name ecscodebuildstack -- parameter-overrides ToolsAccount=$TOOL SACCOUNT \ CodeCommitRepoName= $CODECOMMITREPONAME ECRRepositoryName= $ECRREPOSITORYNAME APPACCOUNTID=$TEST ACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tRegion=$CODECOMMI TREGION CMKARN=$C MKARN2 \ --template-file codebuild.yaml --region $TESTACCO UNT2REGION --capabil ities CAPABILIT Y_NAMED_IAM	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws cloudformation deploy --stack-name ecscodebuildstack --parameter-overrides ToolsAccount=$TOOLSACCOUNT \ CodeCommitRepoName=$CODECOMMITREPONAME ECRRepositoryName=$ECRREPOSITORYNAME APPACCOUNTID=$TESTACCOUNT3 \ CodeCommitRegion=$CODECOMMITREGION CMKARN=$CMKARN3 \ --template-file codebuild.yaml --region $TESTACCOUNT3REGION --capabilities CAPABILITY_NAMED_IAM`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
CodeDeploy In Workload-Konten einrichten.	Verwenden Sie die `codedeploy.yaml` Vorlage im `code` Ordner des GitHub Repositorys, um sie CodeDeploy in allen drei Workload-Konten einzurichten. Die Ausgabe von `mainInfra Stack` umfasst die Amazon-Ressourcennamen (ARNs) des Amazon ECS-Clusters und des Application Load Balancer Balancer-Listeners. **Note** Die Werte aus den Infrastruktur-Stac ks wurden bereits exportiert, sodass sie von den CodeDeplo y Stack-Vorlagen importiert werden. `##WorkloadAccount1## aws cloudformation deploy --stack-name ecscodedeploystack \ --parameter-overrides ToolsAccount=$TOOL SACCOUNT mainInfra stackname=mainInfr astack \ --template-file codedeploy.yaml --region $TESTACCO`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	UNT1REGION --capabil ities CAPABILIT Y_NAMED_IAM ##WorkloadAccount2## aws cloudformation deploy --stack-name ecscodedeploystack \ --parameter-overrides ToolsAccount=$TOOL SACCOUNT mainInfra stackname=mainInfr astack \ --template-file codedeploy.yaml --region $TESTACCO UNT2REGION --capabil ities CAPABILIT Y_NAMED_IAM ##WorkloadAccount3## aws cloudformation deploy --stack-name ecscodedeploystack \ --parameter-overrides ToolsAccount=$TOOL SACCOUNT mainInfra stackname=mainInfr astack \ --template-file codedeploy.yaml --region $TESTACCO UNT3REGION --capabil ities CAPABILIT Y_NAMED_IAM	

CodePipeline Im Tools-Konto einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Code-Pipeline im Tools-Konto.	Führen Sie im Tools-Konto den folgenden Befehl aus: `aws cloudformation deploy --stack-name ecscodepipelinestack --parameter-overrides \ TestAccount1=$TESTACCOUNT1 TestAccount1Region=$TESTACCOUNT1REGION \ TestAccount2=$TESTACCOUNT2 TestAccount2Region=$TESTACCOUNT2REGION \ TestAccount3=$TESTACCOUNT3 TestAccount3Region=$TESTACCOUNT3REGION \ CMKARNTools=$CMKTROOLSARN CMKARN1=$CMKARN1 CMKARN2=$CMKARN2 CMKARN3=$CMKARN3 \ CodeCommitRepoName=$CODECOMMITREPONAME BucketStartName=$BUCKETSTARTNAME \ --template-file codepipeline.yaml --capabilities CAPABILITY_NAMED_IAM`	AWS DevOps
Stellen Sie Zugriff auf CodePipeline und CodeBuild Rollen in der AWS-KMS-S	1. Stellen Sie Zugriff CodePipeline und CodeBuild Rollen in der	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
chlüsselrichtlinie und der S3-Bucket-Richtlinie bereit.	AWS KMS KMS-Schlü sselrichtlinie bereit: `aws cloudformation deploy --stack-name ecs-codepipeline-pre-reqs-KMS \ --template-file pre-reqs_KMS.yaml --parameter-overrides \ CodeBuildCondition=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT --region $TOOLSACCOUNTREGION`  2. Aktualisieren Sie die S3-Bucket-Richtlinie, um den Zugriff für CodePipeline und CodeDeploy Rollen zu ermöglichen:  `aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ PutS3BucketPolicy=true TestAccount1=$TESTACCOUNT1`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	TestAccount2=$TEST ACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tAccount=$CODECOMM ITACCOUNT ToolsAcco unt=$TOOLSACCOUNT \ --template-file pre- reqs_bucket.yaml --region $TESTACCO UNT1REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts -bucket --parameter- overrides BucketSta rtName=$BUCKETSTAR TNAME \ PutS3BucketPolic y=true TestAccou nt1=$TESTACCOUNT1 TestAccount2=$TEST ACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tAccount=$CODECOMM ITACCOUNT ToolsAcco unt=$TOOLSACCOUNT \ --template-file pre- reqs_bucket.yaml --region $TESTACCO UNT2REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts -bucket --parameter-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	overrides BucketStartName=$BUCKETSTARTNAME \ PutS3BucketPolicy=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TESTACCOUNT3REGION --capabilities CAPABILITY_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ PutS3BucketPolicy=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TOOLSACCOUNTREGION --capabil	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`ities CAPABILIT Y_NAMED_IAM`	

Rufen Sie an und testen Sie die Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Änderungen in das CodeCommit Repository übertragen.	1. Klonen Sie das CodeCommit Repositor y, das in der `codecommi trepoStack` mithilfe des `git clone` Befehls erstellt wurde, wie in der CodeCommit AWS-Dokum entation beschrieben. 2. Aktualisieren Sie die Eingabeartefakte mit den erforderlichen Details: • JSON-Datei: Aktualisi eren Sie `AccountID` die Datei an drei Stellen dieser Datei. Benennen Sie die drei Dateien um, sodass sie das Konto enthalten IDs. • YAML-Dateien: Aktualisi eren Sie den ARN und die Version der Aufgabendefinition. Benennen Sie die drei Dateien um, sodass sie das Konto IDs enthalten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	3. Ändern Sie die `index.html` Datei, um einige kleinere Änderungen an der Startseite vorzunehmen.
	4. Kopieren Sie die folgenden Dateien in das Repository und übertragen Sie sie:
	`index.html`
	`Dockerfile`
	`buildspec.yaml`
	`appspec_<accountid>.yaml (3 files - one per account )`
	`taskdef<accountid>.json (3 files - one per account)`
	5. Starten oder starten Sie die Pipeline neu und überprüfen Sie die Ergebnisse.
	6. Greifen Sie über den Application Load Balancer mithilfe eines FQDN oder DNS auf den Dienst zu und überprüfen Sie, ob die Updates bereitgestellt wurden.	

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen Sie alle eingesetzten Ressourcen.	1. Skalieren Sie Amazon ECS auf Null Instances:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`aws ecs update-service --cluster QA-Cluster --service Poc-Service --desired-count 0`
	2. Löschen Sie die CloudFormation Stacks in jedem Konto und jeder Region:
	`##In Tools Account##`
	`aws cloudformation delete-stack --stack-name ecscodepipelinestack --region $TOOLSACCOUNTREGION`
	`aws cloudformation delete-stack --stack-name ecscodebuildstack --region $TESTACCOUNT1REGION`
	`aws cloudformation delete-stack --stack-name ecscodebuildstack --region $TESTACCOUNT2REGION`
	`aws cloudformation delete-stack --stack-name ecscodebuildstack --region $TESTACCOUNT3REGION`
	`aws cloudformation delete-stack --stack-name ecs-codepipeline-pre-reqs-KMS --region $TOOLSACCOUNTREGION`
	`aws cloudformation delete-stack --stack-name codecommi`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	trepoStack --region $TOOLSACCOUNTREGION aws cloudformation delete-stack -- stack-name pre-reqs- artifacts-bucket --region $TESTACCO UNT1REGION aws cloudformation delete-stack -- stack-name pre-reqs- artifacts-bucket --region $TESTACCO UNT2REGION aws cloudformation delete-stack -- stack-name pre-reqs- artifacts-bucket --region $TESTACCO UNT3REGION aws cloudformation delete-stack -- stack-name pre-reqs- artifacts-bucket --region $TOOLSACC OUNTREGION aws cloudformation delete-stack -- stack-name ecs-codeb uild-iam --region $TOOLSACCOUNTREGION ##NOTE: Artifact buckets will not get deleted if there are artifacts so it has to be emptied manually before deleting.##	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	``` ##In Workload / Test Accounts## ##Account:1## aws cloudformation delete-stack -- stack-name ecscodede ploystack --region $TESTACCOUNT1REGION aws cloudformation delete-stack -- stack-name mainInfra stack --region $TESTACCOUNT1REGION ##Account:2## aws cloudformation delete-stack -- stack-name ecscodede ploystack --region $TESTACCOUNT2REGION aws cloudformation delete-stack -- stack-name mainInfra stack --region $TESTACCOUNT2REGION ##Account:3## aws cloudformation delete-stack -- stack-name ecscodede ploystack --region $TESTACCOUNT3REGION aws cloudformation delete-stack -- stack-name mainInfra stack --region $TESTACCOUNT3REGION ##NOTE: Amazon ECR (web) will not get deleted if the registry still includes images. It can be manually ```	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cleaned up if not required.`	

Fehlerbehebung

Problem	Lösung
Änderungen, die Sie für das Repository übernommen haben, werden nicht bereitgestellt.	• Überprüfen Sie die CodeBuild Protokolle auf Fehler bei der Docker-Build-Aktion. Weitere Informationen finden Sie in der CodeBuild - Dokumentation. • Überprüfen Sie die CodeDeploy Bereitstellung auf etwaige Probleme mit der Amazon ECS-Bereitstellung.

Zugehörige Ressourcen

- Ein Docker-Image pushen (Amazon ECR-Dokumentation)
- Stellen Sie eine Connect zu einem CodeCommit AWS-Repository her (CodeCommit AWS-Dokumentation)
- AWS-Fehlerbehebung CodeBuild (CodeBuild AWS-Dokumentation)

Überwachen Sie Amazon ECR-Repositorys mit AWS und AWS CloudFormation Config auf Platzhalterberechtigungen

Erstellt von Vikrant Telkar (AWS), Sajid Momin (AWS) und Wassim Benhallam (AWS)

Übersicht

In der Amazon Web Services (AWS) -Cloud ist Amazon Elastic Container Registry (Amazon ECR) ein verwalteter Container-Image-Registry-Service, der private Repositorys mit ressourcenbasierten Berechtigungen mithilfe von AWS Identity and Access Management (IAM) unterstützt.

IAM unterstützt den Platzhalter „*“ sowohl in den Ressourcen- als auch in den Aktionsattributen, was die automatische Auswahl mehrerer übereinstimmender Elemente erleichtert. In Ihrer Testumgebung können Sie allen authentifizierten AWS-Benutzern den Zugriff auf ein Amazon ECR-Repository ermöglichen, indem Sie die `ecr:*` Platzhalterberechtigung in einem Hauptelement für Ihre Repository-Richtlinienerklärung verwenden. Die `ecr:*` Platzhalterberechtigung kann nützlich sein, wenn Sie in Entwicklungskonten entwickeln und testen, die nicht auf Ihre Produktionsdaten zugreifen können.

Sie müssen jedoch sicherstellen, dass die `ecr:*` Platzhalterberechtigung in Ihren Produktionsumgebungen nicht verwendet wird, da sie schwerwiegende Sicherheitslücken verursachen kann. Der Ansatz dieses Musters hilft Ihnen dabei, Amazon ECR-Repositorys zu identifizieren, die die `ecr:*` Platzhalterberechtigung in Repository-Richtlinienerklärungen enthalten. Das Muster enthält Schritte und eine CloudFormation AWS-Vorlage zum Erstellen einer benutzerdefinierten Regel in AWS Config. Eine AWS Lambda Lambda-Funktion überwacht dann Ihre Amazon ECR-Repository-Richtlinienerklärungen auf `ecr:*` Platzhalterberechtigungen. Wenn Lambda nicht konforme Repository-Richtlinienerklärungen findet, benachrichtigt es AWS Config, ein Ereignis an Amazon zu senden, EventBridge und leitet EventBridge dann ein Amazon Simple Notification Service (Amazon SNS) -Thema ein. Das SNS-Thema informiert Sie per E-Mail über die nicht konformen Repository-Richtlinienerklärungen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert. Weitere Informationen dazu finden Sie unter Installation, Aktualisierung und Deinstallation der AWS-CLI in der AWS-CLI-Dokumentation.

- Ein vorhandenes Amazon ECR-Repository mit einer angehängten Richtlinienerklärung, das in Ihrer Testumgebung installiert und konfiguriert wurde. Weitere Informationen dazu finden Sie unter Erstellen eines privaten Repositorys und Einrichten einer Repository-Richtlinienerklärung in der Amazon ECR-Dokumentation.
- AWS Config, konfiguriert in Ihrer bevorzugten AWS-Region. Weitere Informationen dazu finden Sie unter Erste Schritte mit AWS Config in der AWS Config-Dokumentation.
- Die `aws-config-cloudformation.template` Datei (angehängt), die auf Ihren lokalen Computer heruntergeladen wurde.

Einschränkungen

- Die Lösung dieses Musters ist Regional und Ihre Ressourcen müssen in derselben Region erstellt werden.

Architektur

Das folgende Diagramm zeigt, wie AWS Config die Amazon ECR-Repository-Richtlinienerklärungen auswertet.

Das Diagramm zeigt den folgenden Workflow:

1. AWS Config initiiert eine benutzerdefinierte Regel.
2. Die benutzerdefinierte Regel ruft eine Lambda-Funktion auf, um die Einhaltung der Amazon ECR-Repository-Richtlinienerklärungen zu bewerten. Die Lambda-Funktion identifiziert dann nicht konforme Repository-Richtlinienanweisungen.
3. Die Lambda-Funktion sendet den Status der Nichtkonformität an AWS Config.
4. AWS Config sendet ein Ereignis an EventBridge.
5. EventBridge veröffentlicht die Benachrichtigungen über Verstöße zu einem SNS-Thema.
6. Amazon SNS sendet eine E-Mail-Benachrichtigung an Sie oder einen autorisierten Benutzer.

Automatisierung und Skalierung

Die Lösung dieses Musters kann eine beliebige Anzahl von Amazon ECR-Repository-Richtlinienerklärungen überwachen, aber alle Ressourcen, die Sie auswerten möchten, müssen in derselben Region erstellt werden.

Tools

- AWS CloudFormation — AWS CloudFormation hilft Ihnen dabei, Ihre AWS-Ressourcen zu modellieren und einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus zu verwalten. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben und sie zusammen als Stack zu starten und zu konfigurieren, anstatt Ressourcen einzeln zu verwalten. Sie können Stacks für mehrere AWS-Konten und AWS-Regionen verwalten und bereitstellen.
- AWS Config — AWS Config bietet eine detaillierte Ansicht der Konfiguration der AWS-Ressourcen in Ihrem AWS-Konto. Dazu gehört auch, wie die Ressourcen jeweils zueinander in Beziehung stehen und wie sie in der Vergangenheit konfiguriert wurden, damit Sie sehen können, wie sich die Konfigurationen und Beziehungen im Laufe der Zeit verändern.
- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) ist ein von AWS verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist. Amazon ECR unterstützt private Container-Image-Repositories mit ressourcenbasierten Berechtigungen unter Verwendung von IAM.
- Amazon EventBridge — Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen verbinden können. EventBridge liefert einen Stream von Echtzeitdaten aus Ihren Anwendungen, SaaS-Anwendungen (Software as a Service) und AWS-Services an Ziele wie AWS Lambda-Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen Konten.
- AWS Lambda — AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Code

Der Code für dieses Muster ist in der `aws-config-cloudformation.template` Datei (angehängt) verfügbar.

Epen

Den CloudFormation AWS-Stack erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den CloudFormation AWS-Stack.	Erstellen Sie einen CloudFormation AWS-Stack, indem Sie den folgenden Befehl in der AWS-CLI ausführen: `$ aws cloudformation create-stack --stack-name=AWSConfigECR \ --template-body file://aws-config-cloudformation.template \ --parameters ParameterKey=<email>,ParameterValue=<myemail@example.com> \ --capabilities CAPABILITY_NAMED_IAM`	AWS DevOps

Testen Sie die benutzerdefinierte AWS Config-Regel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die benutzerdefinierte AWS Config-Regel.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die AWS Config-Konsole und wählen Sie dann Ressourcen aus.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Auf der Seite mit dem Ressourcenbestand können Sie nach Ressource nkategorie, Ressourcentyp und Compliance-Status filtern. 3. Ein Amazon ECR-Repos itory, das `ecr:*` ist enthält, `NON-COMPLIANT?` und ein Amazon ECR-Repository, das is nicht enthält`ecr:*`. `COMPLIANT` 4. Die E-Mail-Adresse, die das SNS-Thema abonniert hat, erhält Benachrichtigungen , wenn ein Amazon ECR-Repository nicht konforme Richtlinienerklärungen enthält.	

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Optimieren Sie serverlose Bereitstellungen mit mehreren Konten mithilfe der AWS CDK Workflows und Aktionen GitHub

Erstellt von Sarat Chandra Pothula (AWS) und VAMSI KRISHNA SUNKAVALLI (AWS)

Übersicht

Organizations, die eine serverlose Infrastruktur in mehreren AWS-Konten Umgebungen einsetzen, stehen häufig vor Herausforderungen wie Codeduplizierung, manuellen Prozessen und inkonsistenten Praktiken. Die Lösung dieses Musters zeigt, wie die wiederverwendbaren Workflows AWS Cloud Development Kit (AWS CDK) In Go und GitHub Actions verwendet werden können, um die serverlose Infrastrukturverwaltung für mehrere Konten zu optimieren. Diese Lösung zeigt, wie Sie Cloud-Ressourcen als Code definieren, standardisierte (kontinuierlicheintegration/continuous deployment (CI/CD) Prozesse implementieren und modulare, wiederverwendbare Komponenten erstellen können.

Mithilfe dieser Tools können Unternehmen kontenübergreifende Ressourcen effizient verwalten, konsistente Bereitstellungspipelines implementieren und komplexe serverlose Architekturen vereinfachen. Der Ansatz verbessert auch die Sicherheit und die Einhaltung der Vorschriften, indem standardisierte Verfahren für die Verwendung durchgesetzt werden AWS-Konten, was letztendlich die Produktivität verbessert und Fehler bei der Entwicklung und Bereitstellung serverloser Anwendungen reduziert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver. AWS-Konto
- AWS Identity and Access Management (IAM) -Rollen und -Berechtigungen sind für den Bereitstellungsprozess vorhanden. Dazu gehören Berechtigungen für den Zugriff auf Amazon Elastic Container Registry (Amazon ECR) -Repositorys, zum Erstellen von AWS Lambda Funktionen und für alle anderen erforderlichen Ressourcen im gesamten Ziel. AWS-Konten
- AWS Command Line Interface (AWS CLI) Version 2.9.11 oder höher, installiert und konfiguriert.
- AWS Cloud Development Kit (AWS CDK) Version 2.114.1 oder höher, installiert und gebootet.
- Go 1.22 oder höher, installiert.
- Docker 24.0.6 oder höher, installiert.

Einschränkungen

- Sprachkompatibilität — Go ist eine beliebte Sprache für serverlose Anwendungen. Neben Go AWS CDK unterstützt der jedoch auch andere Programmiersprachen, darunter C#, Java, Python und TypeScript. Wenn Ihr Unternehmen bereits über Codebasen oder Kenntnisse in anderen Sprachen verfügt, müssen Sie Go möglicherweise anpassen oder lernen, um die im Muster beschriebene Lösung vollständig nutzen zu können.
- Lernkurve — Die Einführung von Workflows AWS CDK, Go-Workflows (sofern sie für das Unternehmen neu sind) und GitHub wiederverwendbaren Workflows kann für Entwickler und DevOps Teams eine gewisse Lernkurve mit sich bringen. Möglicherweise sind Schulungen und Unterlagen erforderlich, um eine reibungslose Einführung und effektive Nutzung dieser Technologien zu gewährleisten.

Architektur

Das folgende Diagramm zeigt den Workflow und die Architekturkomponenten für dieses Muster.

Diese Lösung führt die folgenden Schritte aus:

1. Der Entwickler klont das Repository, erstellt einen neuen Branch und nimmt Änderungen am Anwendungscode in seiner lokalen Umgebung vor.
2. Der Entwickler überträgt diese Änderungen und überträgt den neuen Branch in das Repository. GitHub
3. Der Entwickler erstellt eine Pull-Anfrage im GitHub Repository und schlägt vor, sein Feature oder seinen neuen Feature-Branch mit dem Haupt-Branch zusammenzuführen.
4. Dieser Pull-Request löst den Workflow für Continuous Integration (CI) GitHub -Aktionen aus. Die CI- und die Continuous Deployment (CD) -Workflows in diesem Muster verwenden wiederverwendbare Workflows, bei denen es sich um vordefinierte, modulare Vorlagen handelt, die gemeinsam genutzt und in verschiedenen Projekten oder Repositorys ausgeführt werden können. Wiederverwendbare Workflows fördern die Standardisierung und Effizienz der CI/CD-Prozesse.
5. Der CI-Workflow richtet die erforderliche Umgebung ein, generiert ein Docker-Tag für das Image und erstellt das Docker-Image mithilfe des Anwendungscodes.
6. Der CI-Workflow authentifiziert sich AWS mithilfe der zentralen AWS-Konto GitHub OIDC-Rolle. Für CI-Workflows verwendet die zentrale AWS-Konto GitHub OIDC-Rolle AWS

Security Token Service (AWS STS), um temporäre Anmeldeinformationen abzurufen. Diese Anmeldeinformationen ermöglichen es der Rolle, Docker-Images zu erstellen und in das Amazon ECR-Repository der Zentrale zu übertragen. AWS-Konto

7. Der CI-Workflow überträgt das erstellte Docker-Image an Amazon ECR.
8. Der CI-Workflow speichert das Image-Tag im Systems Manager Manager-Parameterspeicher.
9. Nachdem der CI-Workflow erfolgreich abgeschlossen wurde, wird das Docker-Image-Tag ausgegeben.
10. Beim Auslösen des CD-Workflows gibt der Entwickler das Image-Tag des Docker-Images, das er bereitstellen möchte, manuell ein. Dieses Image-Tag entspricht dem Tag, das während des CI-Workflows generiert und an Amazon ECR übertragen wurde.
11. Der Entwickler löst den CD-Workflow manuell aus, wobei der Workflow für wiederverwendbare CDs verwendet wird.
12. Der CD-Workflow authentifiziert sich AWS mithilfe der zentralen AWS-Konto GitHub OIDC-Rolle. Für den CD-Workflow AWS STS wird zunächst die zentrale AWS-Konto GitHub OIDC-Rolle übernommen. Anschließend übernimmt diese Rolle die CDK-Bootstrap-Rollen für die Bereitstellung von Zielkonten.
13. Der CD-Workflow verwendet die, um Vorlagen AWS CDK zu synthetisieren. AWS CloudFormation
14. Der CD-Workflow stellt die Anwendung mithilfe AWS-Konto von CDK Deploy auf dem Ziel bereit, wobei das manuell angegebene Image-Tag für die Lambda-Funktion verwendet wird.

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK)ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung von AWS Cloud Infrastruktur im Code unterstützt.
- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und zu verwalten AWS-Regionen. CloudFormation ist ein integraler Bestandteil des AWS CDK Bereitstellungsprozesses. Das CDK synthetisiert CloudFormation Vorlagen und verwendet sie dann CloudFormation , um die Ressourcen in der Umgebung zu erstellen oder zu aktualisieren. AWS
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.

- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Systems Manager Parameter Store bietet sicheren, hierarchischen Speicher für die Verwaltung von Konfigurationsdaten und Geheimnissen.

Andere Tools

- Docker ist eine Reihe von Platform-as-a-Service (PaaS) -Produkten, die Virtualisierung auf Betriebssystemebene nutzen, um Software in Containern bereitzustellen.
- GitHub Actions ist eine CI/CD-Plattform (Continuous Integration and Continuous Delivery), die eng in Repositorys integriert ist. GitHub Sie können GitHub Actions verwenden, um Ihre Build-, Test- und Bereitstellungspipeline zu automatisieren.
- Go ist eine Open-Source-Programmiersprache, die Google unterstützt.

Code-Repository

Der Code für dieses Muster ist im GitHub aws-cdk-golang-serverlesscicd-github-actions-Repository verfügbar.

Bewährte Methoden

- Modularer Aufbau — Organisieren Sie Ihren AWS CDK Code in modulare und wiederverwendbare Konstrukte oder Stapel und fördern so die Wiederverwendung und Wartbarkeit von Code über mehrere Konten und Projekte hinweg.
- Trennung von Problemen — Trennen Sie den Infrastrukturcode vom Anwendungscode, sodass jede Komponente unabhängig bereitgestellt und verwaltet werden kann.
- Versionierung und Unveränderlichkeit — Behandle deine Infrastruktur als Code (IaC) und verwende Git für die Versionskontrolle. Machen Sie sich unveränderliche Infrastrukturprinzipien zunutze, indem Sie neue Ressourcen erstellen, anstatt bestehende zu modifizieren.
- Testen und Validieren — Implementieren Sie umfassende Teststrategien, einschließlich Komponententests, Integrationstests und end-to-end Tests, um die Richtigkeit und Zuverlässigkeit Ihres AWS CDK Codes und Ihrer Implementierungen zu gewährleisten.

- Sicherheit und Compliance — Halten Sie sich an bewährte AWS Sicherheitsmethoden wie den Zugriff mit geringsten Rechten, sichere Kommunikation und Datenverschlüsselung. Implementieren Sie Compliance-Prüfungen und Auditmechanismen, um die Einhaltung der Unternehmensrichtlinien und behördlichen Anforderungen sicherzustellen. Implementieren Sie bewährte Sicherheitsmethoden für Container-Images, z. B. das Scannen nach Sicherheitslücken, die Durchsetzung der Image-Signierung und die Einhaltung der Compliance-Anforderungen für Ihr Unternehmen.
- Überwachung und Protokollierung — Richten Sie Überwachungs- und Protokollierungsmechanismen ein, um den Zustand und die Leistung Ihrer serverlosen Anwendungen und Infrastruktur zu verfolgen. Verwenden Sie AWS-Services es wie Amazon CloudWatch und AWS X-Ray für Überwachungs- und Prüfungszwecke. AWS CloudTrail
- Automatisierung und CI/CD — Verwenden Sie GitHub wiederverwendbare Workflows und andere CI/CD-Tools, um die Erstellungs-, Test- und Bereitstellungsprozesse zu automatisieren, wodurch konsistente und wiederholbare Bereitstellungen über mehrere Konten hinweg unterstützt werden können.
- Umgebungsmanagement — Pflegen Sie separate Umgebungen (z. B. Entwicklung, Staging und Produktion). Implementieren Sie Strategien zur Förderung von Änderungen zwischen Umgebungen und stellen Sie sicher, dass vor der Bereitstellung in der Produktion ordnungsgemäße Tests und Validierungen durchgeführt werden.
- Dokumentation und Zusammenarbeit — Dokumentieren Sie Ihren Infrastrukturcode, Ihre Bereitstellungsprozesse und Best Practices, um den Wissensaustausch und die Zusammenarbeit innerhalb Ihres Teams zu erleichtern.
- Kostenoptimierung — Implementieren Sie Strategien zur Kostenüberwachung und -optimierung, z. B. die richtige Dimensionierung von Ressourcen, die Nutzung der auto-scaling und die Nutzung von AWS Kostenoptimierungsdiensten wie AWS Budgets und. AWS Cost Explorer
- Notfallwiederherstellung und Backup — Planen Sie Notfallwiederherstellungsszenarien, indem Sie Sicherungs- und Wiederherstellungsmechanismen für Ihre serverlosen Anwendungen und Infrastrukturressourcen implementieren.
- Kontinuierliche Verbesserung — Überprüfen und aktualisieren Sie Ihre Verfahren, Tools und Prozesse regelmäßig, um sie an die neuesten Best Practices, Sicherheitsempfehlungen und technologischen Fortschritte im serverlosen Ökosystem anzupassen.
- Verbessern Sie die Sicherheitslage — Verwenden Sie diese Option, AWS PrivateLinkum die Sicherheitslage Ihrer Virtual Private Cloud (VPC) zu verbessern, indem Sie VPC-Schnittstellen-Endpunkte für Amazon ECR und Parameter Store AWS Lambda konfigurieren. AWS Systems Manager

Epen

Richten Sie die Umgebungen ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon ECR-Repository in der Zentrale AWS-Konto.	Um Container-Images für mehrere freizugeben AWS-Konten, müssen Sie den kontoübergreifenden Zugriff für Amazon ECR konfiguri eren. Erstellen Sie zunächst ein Amazon ECR-Repository in der Zentrale AWS-Konto. Führen Sie den folgenden Befehl aus, um ein Amazon ECR-Repository zu erstellen: `aws ecr create-re pository --repository- name sample-repo` Gewähren Sie in einer späteren Aufgabe den anderen Benutzern, die das Container-Image verwenden müssen AWS-Konten , Pull-Zugriff.	AWS DevOps
Fügen Sie kontoübergreifende Berechtigungen zum Amazon ECR-Repository hinzu.	Um kontoübergreifende Berechtigungen zum Amazon ECR-Repository in der Zentrale hinzuzufügen AWS-Konto, führen Sie den folgenden Code aus: `{`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"Version": "2008-10-17", "Statement": [{ "Sid": "LambdaECRImageRetrievalPolicy", "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, "Action": ["ecr:BatchGetImage", "ecr:GetDownloadUrlForLayer",], "Condition": { "StringLike": { "aws:sourceArn": "arn:aws:lambda:<Target_Region>:<Target_Account_ID>:function:*" } } }, { "Sid": "new statement", "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::<Target_Account_ID>:root" }, "Action": ["ecr:BatchGetImage",	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"ecr:GetD
	ownloadUrlForLayer",
	],
	}
	]
	}</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie eine Rolle für die GitHub OIDC-Rolle in der Zentrale. AWS-Konto	1. Konfigurieren Sie GitHub das OIDC so, dass es sich AWS um eine föderiert e Identität handelt. Dazu gehört auch das Hinzufüge n des GitHub OIDC-Anbi eters und die Konfigura tion der Rollen AWS - und Vertrauensrichtlinie in IAM. Folgen Sie dazu den Anweisungen unter Konfiguration von OpenID Connect in Amazon Web Services in der GitHub Dokumentation. 2. Nachdem die Rolle erstellt wurde, fügen Sie der Rolle die erforderlichen Berechtigungen hinzu. Fügen Sie beispielsweise Berechtigungen für Amazon ECR und AWS Systems Manager Parameter Store hinzu. Weitere Informati onen finden Sie in der IAM-Dokumentation unter Konfiguration einer Rolle für den GitHub OIDC-Iden titätsanbieter.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bootstrapping der AWS Umgebung im Ziel AWS-Konten.	Richten Sie eine CDK-Umgebung in einer bestimmten AWS-Konto Umgebung ein AWS-Region , die kontoüber greifende Bereitstellungen von einem zentralen Konto aus ermöglicht und bei der Ausführungsrolle die Prinzipien der geringsten Rechte anwendet. CloudFormation Führen Sie den folgenden Befehl aus, um eine AWS Umgebung zu booten: `cdk bootstrap aws://<Target_Account_ID>/<Target_Region> --trust <Central_Account_ID> --cloudformation-execution-policies arn:aws:iam::aws:policy/<Least_Privilege_Policy>`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gewähren Sie der zentralen AWS-Konto OIDC-Rolle Zugriff auf die AWS-Konto Bootstrap-Zielrollen.	Der CDK-Bootstrap erstellt die folgenden IAM-Rolle n, die so konzipiert sind, dass sie von der zentralen Stelle in verschiedenen Phasen des AWS-Konto CDK-Bereitstellungsprozesses übernommen werden: • Rolle beim Veröffentlichen von Dateien • Rolle beim Veröffentlichen von Bildern • Rolle „Nachschlagen“ • Rolle bei der Bereitstellung Jede Rolle verfügt über spezifische Berechtigungen, die auf ihren Zweck zugeschni tten sind und dem Prinzip der geringsten Rechte folgen. Das „`Target_Account_ID` und“ `Target_Region` in jedem Rollennamen weist darauf hin, dass diese Rollen in verschiedenen AWS-Konte n Regionen einzigartig sind. Dieser Ansatz unterstützt eine klare Identifizierung und Verwaltung in Konfigurationen mit mehreren Konten und mehreren Regionen.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`Target Account CDK Bootstrap Roles`
	`arn:aws:iam::<Target_Account_ID>:role/cdk-deploy-role-<Target_Account_ID>-<Target_Region>`
	`arn:aws:iam::<Target_Account_ID>:role/cdk-file-publishing-role-<Target_Account_ID>-<Target_Region>`
	`arn:aws:iam::<Target_Account_ID>:role/cdk-image-publishing-role-<Target_Account_ID>-<Target_Region>`
	`arn:aws:iam::<Target_Account_ID>:role/cdk-lookup-role-<Target_Account_ID>-<Target_Region>`
	• Aktualisieren Sie die Berechtigungsrichtlinie für die OIDC-Rolle im zentralen Konto, damit sie Rollen im Zielkonto übernehmen kann. Diese Konfiguration ermöglicht die Bereitstellung von CDK-Stacks auf verschiedenen Ebenen. AWS-Konten Indem Sie der OIDC-Rolle des zentralen Kontos erlauben, die erforderlichen Berechtigungen des Zielkontos zu übernehmen, schaffen Sie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eine sichere Brücke für kontenübergreifende CDK-Bereitstellungen. Dieser Ansatz gewährleistet eine angemessene Zugriffsk ontrolle und ermöglicht gleichzeitig ein nahtloses Infrastrukturmanagement für mehrere Konten. Verwenden Sie den folgenden Code, um die Berechtig ungsrichtlinie für die OIDC-Rolle in der Zentrale AWS-Konto zu aktualisieren: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": [ "arn:aws:iam::<Target_Account_ID>:role/cdk-deploy-role-<Target_Account_ID>-<Target_Region>”, “arn:aws:iam::<Target_Account_ID>:role/cdk-file-publishing-`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	role-<Target_Account_ID>-<Target_Region>”, “arn:aws:iam::<Target_Account_ID>:role/cdk-image-publishing-role-<Target_Account_ID>-<Target_Region>”, “arn:aws:iam::<Target_Account_ID>:role/cdk-lookup-role-<Target_Account_ID>-<Target_Region>”] }] }	

Erstellen Sie das Docker-Image

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Projekt-Repository.	Führen Sie den folgenden Befehl aus, um das GitHub Repository dieses Musters zu klonen: `git clone https://github.com/aws-samples/aws-cdk-golang-serverless-cicd-github-actions.git`	AWS DevOps
Gehen Sie zum Dockerfile-Pfad.	Führen Sie den folgenden Befehl aus, um zum Dockerfile-Pfad zu navigieren:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cd lambda`	
Authentifizieren Sie Docker mit Amazon ECR.	Amazon ECR benötigt sicheren Zugriff auf Ihre privaten Container-Reposito rys. Wenn Sie sich auf diese Weise anmelden, ermöglichen Sie Docker auf Ihrem lokalen Computer oder Ihrer CI/CD-Umgebung, sicher mit Amazon ECR zu interagieren. Führen Sie den folgenden Befehl aus, um Docker mit Amazon ECR zu authentif izieren: `aws ecr get-login -password --region <AWS_REGION> | docker login --username AWS --password-stdin <AWS_ACCOUNT_ID>.dkr.ecr.<AWS_REGION>.amazonaws.com` Überarbeiten Sie die Platzhalter `AWS_REGION` und `AWS_Account_ID` und fügen Sie Ihre Informationen hinzu.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Docker-Image.	Führen Sie den folgenden Befehl aus, um das Docker-Image zu erstellen: `docker build --platform linux/arm64 -t sample-app .`	AWS DevOps

Markieren und übertragen Sie das Docker-Image.	Führen Sie die folgenden Befehle aus, um das Docker-Image zu taggen und in das Amazon ECR-Repository zu übertragen:
	`docker tag sample-app:latest <AWS_ACCOUNT_ID>.dkr.ecr.<AWS_REGION>.amazonaws.com/<ECR_REPOSITORY>:<DOCKER_TAG>`
	`docker push <AWS_ACCOUNT_ID>.dkr.ecr.<AWS_REGION>.amazonaws.com/<ECR_REPOSITORY>:<DOCKER_TAG>`
	Überarbeiten Sie die Platzhalter `AWS_Account_ID` , `AWS_REGION` `ECR_REPOSITORY` , und `DOCKER_TAG` mit Ihren Informationen.
		AWS DevOps

Stellen Sie die AWS CDK App bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Synthetisieren Sie den CDK-Stack mit umgebungsspezifischen Variablen.	Führen Sie den folgenden Befehl aus, um die CloudFormation Vorlage für Ihre Infrastruktur zu generieren, wie sie in Ihrem CDK-Code definiert ist: `ENV=<environment> IMAGETAG=<image_tag> ECR_ARN=<ecr_repo_arn> cdk synth` Überarbeiten Sie die folgenden Platzhalter mit Ihren Informationen: • `environment` — Ersetzt durch einen bestimmten Umgebungsnamen wie `devstaging`, oder. `prod` • `image_tag` — Ersetzt durch ein bestimmtes Tag für ein Docker-Image wie `v1.0.0` oder`latest`. • `ecr_repo_arn` — Durch den Amazon-Ressourcennamen (ARN) eines Amazon ECR-Repositorys ersetzen.	AWS DevOps
Stellen Sie den CDK-Stack bereit.	Führen Sie den folgenden Befehl aus AWS-Konto , um den CDK-Stack auf Ihrem bereitzustellen. Das `--require-approval`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`never` Flag bedeutet, dass das CDK alle Änderungen automatisch genehmigt und ausführt. Dazu gehören auch Änderungen, die das CDK normalerweise als manuell überprüfbar kennzeichnen würde (z. B. Änderungen der IAM-Richtlinien oder das Entfernen von Ressource n). Stellen Sie sicher, dass Ihr CDK-Code und Ihre CI/CD-Pipeline gut getestet und sicher sind, bevor Sie das Flag in Produktionsumgebungen verwenden. `--require-approval never` `ENV=<environment> IMAGETAG=<image_tag> ECR_ARN=<ecr_repo_arn> cdk deploy --require-approval never`	

Automatisieren Sie CI/CD mithilfe von Aktions-Workflows GitHub

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Feature-Branch und fügen Sie Ihre Änderungen hinzu.	Verwenden Sie das geklonte Repository, das Sie zuvor erstellt haben, erstellen Sie einen Feature-Branch und fügen Sie dann Ihre Änderungen zum Anwendung	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	scode hinzu. Verwenden Sie die folgenden Befehle:
	
	`git checkout -b <feature_branch>`
	`git add .`
	`git commit -m “add your changes”`
	`git push origin <feature_branch>`
	
	Im Folgenden finden Sie Beispiele für Änderungen:
	
	• Änderungen an der Lambda-Funktionslogik
	• Hinzufügen neuer Features oder Funktionen zum Lambda-Code
	• Behebung von Fehlern oder Optimierung des vorhanden en Codes innerhalb der Lambda-Funktion
	
	GitHub Aktionen verwenden die wiederverwendbaren Workflows und lösen die CI/ CD-Pipelines aus.	

Führen Sie Ihre Änderungen zusammen.	Erstelle einen Pull-Request und füge deine Änderungen mit dem Hauptteil zusammen.	AWS DevOps

Fehlerbehebung

Problem	Lösung
`AccessDenied` Fehler beim Bereitstellen von Ressourcen auf AWS-Konten, zum Beispiel`AccessDenied: User not authorized to perform: “sts:AssumeRole" .`	Gehen Sie wie folgt vor, um die kontoüber greifenden Berechtigungen zu überprüfen, um dieses Problem zu beheben: • Stellen Sie sicher, dass die erforderlichen IAM-Rollen und -Richtlinien für kontoüber greifende Bereitstellungen vorhanden sind. • Überprüfen Sie, ob die `assume` Rollenber echtigungen korrekt konfiguriert sind.
Kompatibilitätsprobleme aufgrund von Versionskonflikten, z. B. `undefined: awscdkStack` Fehler mit einer veralteten CDK-Version.	Gehen Sie wie folgt vor, um zu überprüfen, ob Sie die erforderlichen Versionen von AWS CDK and Go verwenden, um dieses Problem zu lösen: • Stellen Sie sicher, dass Sie kompatible Versionen von The AWS CDK and Go verwenden. • Suchen Sie nach bekannten Problemen oder wichtigen Änderungen in den letzten Versionen.
CI/CD-Pipeline-Fehler, z. B. `Error: No such file or directory` aufgrund einer falschen YAML-Konfiguration oder `Permission denied` aufgrund geschützter Zweige.	Um Probleme mit der GitHub Aktionskonfiguration zu lösen, stellen Sie sicher, dass die wiederverwendbaren Workflows ordnungsgemäß referenziert und konfiguriert sind.

Zugehörige Ressourcen

AWS-Ressourcen

- AWS Bewährte Methoden für Sicherheit, Identität und Compliance
- AWS CDK Workshop

- AWS Bibliothek Cloud Development Kit
- Erstellen Sie eine Lambda-Funktion mit einem Container-Image
- Identity and Access Management für Amazon Elastic Container Registry
- Arbeiten mit dem AWS CDK in Go

Sonstige Ressourcen

- Konfiguration von OpenID Connect in Amazon Web Services (GitHub Dokumentation)
- Golang-Dokumentation
- Schnellstart für GitHub Aktionen (Dokumentation) GitHub
- Wiederverwendung von Workflows (Dokumentation) GitHub

Führen Sie benutzerdefinierte Aktionen aus CodeCommit AWS-Ereignissen durch

Erstellt von Abdullahi Olaoye (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Wenn Sie ein CodeCommit AWS-Repository zum Speichern von Code verwenden, möchten Sie möglicherweise das Repository überwachen und bei bestimmten Ereignissen einen Aktionsablauf einleiten. Beispielsweise möchten Sie möglicherweise eine E-Mail-Benachrichtigung senden, wenn ein Benutzer eine Codezeile in einem Commit kommentiert, oder eine AWS-Lambda-Funktion initiieren, um nach einem Commit Sicherheitsscans der Repository-Inhalte durchzuführen. Dieses Muster beschreibt die Schritte zur Konfiguration eines CodeCommit Repositorys für benutzerdefinierte Aktionen. Das Muster verwendet CodeCommit AWS-Benachrichtigungsregeln, um die relevanten Ereignisse zu erfassen, und sendet diese Ereignisse dann an ein konfiguriertes Ziel.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Vertrautheit mit Git-Befehlen.
- AWS CodeCommit, eingerichtet. Anweisungen finden Sie unter Einrichtung für AWS CodeCommit.
- (Empfohlen) AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert. Anweisungen finden Sie unter Erste Schritte mit der AWS-CLI.

Architektur

Tools

AWS-Services

- AWS CodeCommit ist ein vollständig verwalteter Quellcodeverwaltungsservice, der sichere Git-basierte Repositorys hostet. Es erleichtert Teams die Zusammenarbeit an Code in einem

sicheren und hoch skalierbaren Ökosystem. CodeCommit macht es überflüssig, Ihr eigenes Quellcodeverwaltungssystem zu betreiben oder sich Gedanken über die Skalierung der Infrastruktur zu machen

- Amazon Simple Notification Service (Amazon SNS) ist ein Webservice, der es Anwendungen, Endbenutzern und Geräten ermöglicht, sofort Benachrichtigungen aus der Cloud zu senden und zu empfangen. Amazon SNS bietet Themen (Kommunikationskanäle) für Push-basiertes Messaging mit hohem Durchsatz. many-to-many Mithilfe von Amazon SNS SNS-Themen können Herausgeber Nachrichten zur parallel Verarbeitung an eine große Anzahl von Abonnenten verteilen, einschließlich Amazon Simple Queue Service (Amazon SQS) -Warteschlangen, AWS Lambda Lambda-Funktionen und HTTP/S-Webhooks. Sie können Amazon SNS auch verwenden, um Benachrichtigungen per Push, SMS und E-Mail an Endbenutzer zu senden.

Epen

Richten Sie ein Repository ein CodeCommit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein CodeCommit Repository.	Verwenden Sie die CodeCommit Konsole oder die AWS-CLI, um ein CodeCommit Repository zu erstellen. Anweisungen finden Sie unter Erstellen eines CodeCommit Repositorys.	DevOps Ingenieur
Inhalte in das CodeCommit Repository übertragen.	Nachdem Sie ein Repository erstellt haben, fügen Sie ihm mithilfe von Git-Befehlen Inhalte hinzu. Sie können den Inhalt eines vorhandenen Git-Repositorys oder lokale, unversionierte Inhalte von Ihrem Computer migrieren. Anweisungen finden Sie unter Dateien zu Ihrem Repositor	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	y hinzufügen oder Zu AWS migrieren CodeCommit.	

Einrichten von Amazon SNS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein SNS-Thema.	Dieses SNS-Thema erhält die Ereignisse von CodeCommit. Anweisungen finden Sie unter Erstellen eines Amazon SNS SNS-Themas.	Cloud-Architekt, Ingenieur DevOps
Erstellen Sie eine Ressource für eine benutzerdefinierte Aktion.	Damit die benutzerdefinierte Aktion ausgeführt werden kann, müssen Sie die entsprechende Ressource erstellen. Wenn Ihre benutzerd efinierte Aktion beispielsweise darin besteht, Lambda-Code auszuführen und Nachrichten an eine SQS-Warteschlange zu senden, müssen Sie die Lambda-Funktion und die SQS-Warteschlange erstellen . Aktionen wie E-Mail- und SMS-Benachrichtigungen benötigen keine Ressource n. Weitere Informationen finden Sie in der AWS-Dokum entation für den Ressource ntyp, den Sie erstellen.	Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Abonnieren Sie die Ressource für benutzerdefinierte Aktionen zum SNS-Thema.	Abhängig von der benutzerd efinierten Aktion erstellen Sie ein Abonnement für das entsprechende Protokoll. Sie abonnieren beispielsweise eine E-Mail-Adresse für E-Mail-Benachrichtigungen, eine Lambda-Funktion zum Ausführen von benutzerd efiniertem Code oder eine SQS-Warteschlange, um Ereignisse an Amazon SQS zu senden. Bei Abonnemen tprotokollen wie E-Mail und SMS müssen Sie das Abonnement über den Link bestätigen, der an die E-Mail bzw. Telefonnummer gesendet wird. Anweisungen finden Sie unter Amazon SNS abonnieren.	Cloud-Architekt, Ingenieur DevOps

Benachrichtigungsregeln konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Benachric htigungsregel für das CodeCommit Repository.	Wenn Sie die Benachric htigungsregel erstellen, wählen Sie die Git-Ereignisse aus, die die Benachrichtigung auslösen sollen, wählen Sie das SNS-Thema als Zieltyp aus und wählen dann das SNS-Thema aus, das Sie	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zuvor erstellt haben. Sie können auch mehrere Ziele für das Repository konfigurieren. Anweisungen finden Sie unter Eine Benachrichtigungsregel erstellen.	
Testen Sie benutzerdefinierte Aktionen.	Führen Sie eines der Ereignisse aus, die für die Initiierung der Benachrichtigung konfiguriert wurden. Erstellen Sie beispielsweise eine Pull-Anfrage, wenn Sie dieses Ereignis als Auslöser ausgewählt haben. Sie sollten sehen, dass Ihre benutzerdefinierte Aktion ausgeführt wird. Wenn Sie beispielsweise eine E-Mail-Adresse für das SNS-Thema abonniert haben, sollten Sie eine E-Mail-Benachrichtigung erhalten.	DevOps Ingenieur

Zugehörige Ressourcen

- CodeCommit AWS-Dokumentation
- Amazon SNS SNS-Dokumentation
- Git-Dokumentation

Bereitstellen von AWS Service Catalog Produkten auf der Grundlage von AWS CloudFormation Vorlagen mithilfe von GitHub Aktionen

Erstellt von Ashish Bhatt (AWS) und Ruchika Modi (AWS)

Übersicht

Dieses Muster bietet Unternehmen einen optimierten Ansatz, bei dem AWS Service CatalogProdukte und Portfolios verwendet werden, um teamübergreifend standardisierte und konforme Lösungen bereitzustellen. AWS-Services AWS CloudFormationhilft dabei, wichtige Komponenten in Service Catalog-Produkten und -Portfolios für die Bereitstellung der Basisnetzwerkinfrastruktur zu AWS Cloud kombinieren. Dieses Muster fördert auch DevOps Praktiken, indem Infrastructure-as-Code (IaC) mithilfe GitHub von Aktionen in automatisierte Entwicklungsworkflows integriert wird.

AWS Service Catalog ermöglicht es Unternehmen, genehmigte IT-Services zu erstellen und zu verwalten AWS, was Vorteile wie Standardisierung, zentrale Steuerung, Self-Service-Bereitstellung und Kostenmanagement bietet. Durch die Automatisierung der Bereitstellung von Service Catalog-Portfolios und -Produkten durch GitHub Aktionen können Unternehmen Folgendes tun:

- Erzielen Sie konsistente und wiederholbare Bereitstellungen.
- Verwenden Sie die Versionskontrolle für IaC.
- Integrieren Sie das Cloud-Ressourcenmanagement in bestehende Entwicklungsworkflows.

Diese Kombination rationalisiert den Cloud-Betrieb, sorgt für die Einhaltung von Vorschriften und beschleunigt die Bereitstellung genehmigter Dienste. Gleichzeitig werden manuelle Fehler reduziert und die Gesamteffizienz verbessert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Zugriff auf das GitHub Repository
- Grundlegendes Verständnis von AWS CloudFormation und AWS Service Catalog
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket zum Hosten von CloudFormation Vorlagen

- Eine benannte AWS Identity and Access Management (IAM-) Rolle`github-actions`, die für die Konnektivität zwischen und GitHub verwendet wird AWS

Einschränkungen

- Der wiederverwendbare Code dieses Musters wurde nur mit GitHub Aktionen getestet.
- Einige AWS-Services sind nicht in allen verfügbar AWS-Regionen. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie unter Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Produktversionen

Die Lösung dieses Musters wurde mithilfe der folgenden GitHub Marketplace-Aktionen und ihrer jeweiligen Versionen erstellt:

- `actions/checkout@v4`
- `aws-actions/configure-aws-credentials@v2`
- `aws-actions/aws-cloudformation-github-deploy@v1.2.0`

Architektur

Das folgende Diagramm zeigt die Architektur für diese Lösung.

1. Administratoren oder Plattformingenieure übertragen standardisierte CloudFormation Vorlagen in ein GitHub Repository, in dem die Vorlagen verwaltet werden. Das GitHub Repo enthält auch Workflows, die die Bereitstellung von AWS Service Catalog Using GitHub Actions automatisieren.
2. GitHub Aktionen lösen einen Workflow aus, der eine Verbindung AWS Cloud mit dem herstellt, der einen OpenID Connect (OIDC) -Anbieter verwendet, um Service Catalog bereitzustellen.
3. Der Service Catalog enthält das Portfolio und die Produkte, mit denen Entwickler direkt standardisierte AWS Ressourcen bereitstellen können. Dieses Muster bündelt AWS Ressourcen wie virtuelle private Clouds (VPCs), Subnetze, NAT- und Internet-Gateways sowie Routing-Tabellen.

4. Nachdem der Entwickler ein Service Catalog-Produkt erstellt hat, konvertiert Service Catalog es in vorkonfigurierte und standardisierte AWS Ressourcen. Dadurch sparen Entwickler Zeit, da sie keine einzelnen Ressourcen bereitstellen und manuell konfigurieren müssen.

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und zu verwalten AWS-Regionen. Es handelt sich um einen Infrastructure-as-Code-Service (IaC), der problemlos als einer der Produkttypen mit AWS Service Catalog verwendet werden kann.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Service Catalogunterstützt Sie bei der zentralen Verwaltung des Katalogs von IT-Services, für die eine Genehmigung erteilt wurde. AWS Endbenutzer können schnell nur die jeweils benötigten genehmigten IT-Services bereitstellen, wobei die Einschränkungen Ihrer Organisation berücksichtigt werden.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere

- GitHub Actions ist eine CI/CD-Plattform (Continuous Integration and Continuous Delivery), die eng in Repositorien integriert GitHub ist. Sie können GitHub Actions verwenden, um Ihre Build-, Test- und Bereitstellungspipeline zu automatisieren.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub service-catalog-with-github-actions verfügbar. Das Repo enthält die folgenden interessanten Dateien:

- `github/workflows`:
  - `e2e-test.yaml`— Diese Datei ruft auf`workflow.yaml`, was der wiederverwendbare Workflow ist. Dieser Workflow wird ausgelöst, sobald ein Commit und ein Push für einen Branch erfolgt.

  - `workflow.yaml`— Diese Datei enthält den wiederverwendbaren Workflow für diese Lösung und ist `workflow_call` als Auslöser konfiguriert. Als wiederverwendbarer Workflow `workflow.yaml` kann er von jedem anderen Workflow aus aufgerufen werden.
- `templates`:
  - `servicecatalog-portfolio.yaml`— Diese CloudFormation Vorlage enthält Ressourcen, die das Service Catalog-Portfolio und das Service Catalog-Produkt bereitstellen. Die Vorlage enthält eine Reihe von Parametern, die bei der Bereitstellung des Service Catalog-Portfolios und der Produkte verwendet werden. Ein Parameter akzeptiert eine Amazon S3 S3-Datei-URL, in die die Vorlage hochgeladen `vpc.yaml` wird. Dieses Muster beinhaltet zwar die `vpc.yaml` Datei zur Bereitstellung von AWS Ressourcen, Sie können jedoch auch den Parameter S3-Datei-URL für die Konfiguration verwenden.
  - `vpc.yaml`— Diese CloudFormation Vorlage enthält AWS Ressourcen, die dem Service Catalog-Produkt hinzugefügt werden sollen. AWS Zu den Ressourcen gehören VPCs Subnetze, Internet-Gateways, NAT-Gateways und Routing-Tabellen. Die `vpc.yaml` Vorlage ist ein Beispiel dafür, wie Sie eine beliebige CloudFormation Vorlage mit einer Produkt- und Portfoliovorlage für einen Service Catalog verwenden können.

Bewährte Methoden

- Weitere Informationen finden Sie AWS Service Catalog in der AWS Service Catalog Dokumentation unter Bewährte Sicherheitsmethoden für.
- Weitere Informationen finden Sie in der GitHub Dokumentation unter Sicherheitshärtung für GitHub Aktionen.

Epen

Richten Sie eine lokale Workstation ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Einrichtung von Git auf Ihrer lokalen Workstation.	Um Git auf deiner lokalen Workstation zu installieren und zu konfigurieren, verwende die Anleitung Erste Schritte —	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Installation von Git in der Git-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Projekt-Repo.	Gehen Sie wie folgt vor, um das GitHub Projekt-Repo zu klonen: 1. Öffnen Sie das GitHub Repo für dieses Muster 2. Wählen Sie Code, um die Klonoptionen zu sehen, und kopieren Sie die auf der Registerkarte HTTPS angegebene URL. 3. Erstellen Sie einen Ordner für Ihr Projekt auf Ihrer Workstation. 4. Öffnen Sie ein Terminal und navigieren Sie zu diesem Ordner 5. Um das GitHub Repo zu klonen, führen Sie den folgenden Befehl mit der URL aus, die Sie in Schritt 2 kopiert haben: `git clone https://github.com/aws-samples/service-catalog-with-github-actions.git` 6. Wenn das Klonen abgeschlossen ist, führen Sie den folgenden Befehl aus, um zum geklonten Repo in Ihrem Projektordner zu wechseln:	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cd <folder-name>/service-catalog-with-github-actions` 7. Öffnen Sie das Projekt in einer integrierten Entwicklungsumgebung (IDE) Ihrer Wahl.	

Richten Sie den OIDC-Anbieter ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie einen OIDC-Anbieter.	Erstellen Sie einen OpenID Connect (OIDC) -Anbieter, der den GitHub Actions-Workflows den Zugriff auf Ressourcen ermöglicht AWS, ohne dass die AWS Anmeldeinformationen als langlebige Geheimnisse gespeichert werden müssen. GitHub Anweisungen finden Sie in der GitHub Dokumentation unter Konfiguration von OpenID Connect in Amazon Web Services. Nach der Konfiguration eines OIDC-Anbieters wird die Vertrauensrichtlinie der IAM-Rolle`github-actions` , die bereits in den Voraussetzungen erwähnt wurde, aktualisiert.	AWS-Administrator, AWS DevOps, Allgemeines AWS

Trigger GitHub Actions-Pipeline zur Bereitstellung des Service Catalog-Portfolios und der Produkte

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisieren von `e2e-test.yaml` .	Die `e2e-test.yaml` Datei löst den wiederverwendbaren Workflow unter aus`workflow.yaml` . Aktualisieren und validieren Sie die Werte für die folgenden Eingabeparameter in`e2e-test.yaml` :
	• `aws_account_id` — Geben Sie das Richtige an AWS-Konto.
	• `aws_region` — Geben Sie das Richtige an AWS-Region.
	• `s3BucketName` — Geben Sie den Amazon S3 S3-Bucket an, der die CloudFormation Vorlagen enthalten soll.
	• Für die Workflow-Datei sind zwei IAM-Rollen als Eingabe erforderlich:
	  • `LaunchConstraintRole` - Die IAM-Rolle, die AWS Service Catalog übernommen wird, wenn ein Endbenutzer ein Produkt startet, aktualisiert oder beendet.
	  • `PrincipalArn` — Der Amazon-Ressourcenn
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ame (ARN) des Prinzipal s (IAM-Benutzer, Rolle oder Gruppe), der dem Service Catalog-Portfolio zugeordnet wird. Wenn ja`IAM`, `Principal Type` ist der unterstüt zte Wert ein vollständig definierter IAM-Amazon-Ressourcenname (ARN). Wenn ja`IAM_PATTERN` , `PrincipalType` ist der unterstützte Wert ein IAM-ARN ohne `AccountID` im folgenden Format: `arn:partition:iam: ::resource-type/ resource-id`	

Bereitstellung validieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Service Catalog-Ressourcen.	Gehen Sie wie folgt vor, um die Service Catalog-R essourcen zu validieren: 1. Melden Sie sich bei AWS Management Console der an AWS-Konto, und vergewissern Sie sich, dass der korrekt AWS-Region ist. 2. Navigieren Sie zu Verwaltung, Portfolios,	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	AWS Service Catalogund überprüfen Sie, ob ein Portfolio vorhanden ist. 3. Wählen Sie das Portfolio aus und überprüfen Sie die Informationen auf den Registerkarten Produkte, Einschränkungen und Zugriff.	

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie den CloudFormation Stapel.	Gehen Sie wie folgt vor, um den CloudFormation Stapel zu löschen: 1. Öffnen Sie die AWS CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation. 2. Wählen Sie in der Navigationsleiste oben auf dem Bildschirm aus, AWS-Region wo sich der Stapel befindet. 3. Wählen Sie auf der Seite Stapel den Stapel aus, den Sie löschen möchten. Der Stack muss aktuell ausgeführt werden.	DevOps Ingenieur, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie im Stack-Detailbereich Delete (Löschen) aus. 5. Wählen Sie Delete stack (Stack löschen) aus, wenn Sie dazu aufgefordert werden. Weitere Informationen finden Sie in der Dokumentation unter Löschen eines Stacks aus der CloudFormation CloudFormation Konsole	

Fehlerbehebung

Problem	Lösung

`e2e-test`
 	
`Can't find 'action.yml', 'action.yaml' or 'Dockerfile' under '*/home/runner/work/service-catalog-with-github-actions/service-catalog-with-github-actions`
 	
`Did you forget to run actions/checkout before running your local action?`
	Gehen Sie wie folgt vor, um sicherzustellen, dass Sie die richtigen Repository-Einstellungen aktiviert haben:
	
	1. Navigiere zum Github-Repository auf der Registerkarte Einstellungen.
	2. Wählen Sie im Menü auf der linken Seite Aktionen, Allgemein
	3. Gehen Sie zum Bereich Zugriff und wählen Sie die Option Zugänglich aus Repositorys in der Organisation „XXX“.

Zugehörige Ressourcen

AWS Dokumentation

- Überblick über den Service Catalog

Sonstige Ressourcen

- Informationen zu Ereignissen, die Workflows auslösen (GitHub Dokumentation)
- Wiederverwendung von Workflows (GitHub Dokumentation)

Zusätzliche Informationen

Screenshots zu den Epics finden Sie im Ordner Images im Repo dieses Patterns GitHub . Die folgenden Screenshots sind verfügbar:

- AWS Service Catalog Portfolio, Bereich Verwaltung
- AWS Service Catalog Produkt, Bereich Verwaltung
- AWS Service Catalog Produkt, Bereich Benutzer/Bereitstellung

Stellen Sie IAM-Rollen mit den geringsten Rechten bereit, indem Sie eine Rollenautomatenlösung bereitstellen

Erstellt von Benjamin Morris (AWS), Aman Kaur Gandhi (AWS), Tschad Moon (AWS) und Nima Fotouhi (AWS)

Übersicht

Rollenberechtigungen mit übermäßigem Geltungsbereich AWS Identity and Access Management (IAM) für Pipelines können zu unnötigen Risiken für ein Unternehmen führen. Entwickler gewähren manchmal während der Entwicklung weitreichende Berechtigungen, vernachlässigen es jedoch, nach der Fehlerbehebung im Code die Zugriffsrechte einzuschränken. Dies führt zu Problemen, wenn leistungsstarke Rollen ohne geschäftliche Notwendigkeit vorhanden sind und möglicherweise noch nie von einem Sicherheitsingenieur überprüft wurden.

Dieses Muster bietet eine Lösung für dieses Problem: der Rollenverkaufsautomat (RVM). Mithilfe eines sicheren und zentralisierten Bereitstellungsmodells demonstriert das RVM, wie IAM-Rollen mit den geringsten Rechten für die Pipelines einzelner GitHub Repositorys mit minimalem Aufwand für Entwickler bereitgestellt werden können. Da es sich bei der RVM um eine zentrale Lösung handelt, können Sie Ihre Sicherheitsteams als Prüfer konfigurieren, die Änderungen genehmigen müssen. Dieser Ansatz ermöglicht es der Sicherheitsabteilung, zu viele Anfragen an Pipeline-Rollen zurückzuweisen.

Die RVM verwendet Terraform-Code als Eingabe und generiert Pipeline-bereite IAM-Rollen als Ausgabe. Die erforderlichen Eingaben sind die AWS-Konto ID, der GitHub Repository-Name und die Berechtigungsrichtlinie. Die RVM verwendet diese Eingaben, um die Vertrauens- und Berechtigungsrichtlinie der Rolle zu erstellen. Die daraus resultierende Vertrauensrichtlinie ermöglicht es dem angegebenen GitHub Repository, die Rolle zu übernehmen und sie für Pipeline-Operationen zu verwenden.

Die RVM verwendet eine IAM-Rolle (die beim Bootstrap konfiguriert wurde). Diese Rolle hat die Berechtigung, role-provisioning-role in jedem Konto in der Organisation eine anzunehmen. Die Rolle wird entweder über AWS Control Tower Account Factory for Terraform (AFT) oder konfiguriert. AWS CloudFormation StackSets Dies role-provisioning-roles sind die Rollen, die tatsächlich die Pipeline-Rollen für Entwickler erstellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto.
- Eine GitHub Organisation, die zur Bereitstellung von Infrastructure as Code (IaC) im Rahmen von GitHub Aktionen verwendet wird. (GitHub Enterprise/Premium/Ultimatesind nicht erforderlich.)
- Eine AWS Umgebung mit mehreren Konten. Diese Umgebung muss nicht Teil davon AWS Organizations sein.
- Ein Mechanismus für die Bereitstellung einer IAM-Rolle in allen Bereichen AWS-Konten (z. B. AFT oder CloudFormation StackSets).
- Terraform Version 1.3 oder höher wurde installiert und konfiguriert.
- Terraform AWS Provider Version 4 oder höher wurde installiert und konfiguriert.

Einschränkungen

- Der Code dieses Musters ist spezifisch für GitHub Actions und Terraform. Die allgemeinen Konzepte des Musters können jedoch in anderen Continuous Integration and Delivery (CI/CD) - Frameworks wiederverwendet werden.
- Einige AWS-Services sind nicht in allen verfügbar. AWS-Regionen Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie unter AWS Dienste nach Regionen. Informationen zu bestimmten Endpunkten finden Sie unter Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Architektur

Das folgende Diagramm veranschaulicht den Arbeitsablauf für dieses Muster.

Der Arbeitsablauf für die typische Verwendung der Rolle Verkaufsautomat besteht aus den folgenden Schritten:

1. Ein Entwickler überträgt Code, der Terraform-Code für eine neu angeforderte IAM-Rolle enthält, in das RVM-Repository. GitHub Diese Aktion löst die RVM-Aktionspipeline aus. GitHub
2. Die Pipeline verwendet eine OpenID Connect (OIDC) -Vertrauensrichtlinie, um die Rolle der RVM-Rollenübernahme zu übernehmen.
3. Bei der Ausführung der RVM-Pipeline übernimmt sie die RVM-Workflow-Rolle in dem Konto, in dem sie die neue IAM-Rolle des Entwicklers bereitstellt. (Die RVM-Workflow-Rolle wurde mithilfe von AFT oder bereitgestellt.) CloudFormation StackSets

4. Die RVM erstellt die IAM-Rolle des Entwicklers mit den entsprechenden Berechtigungen und der entsprechenden Vertrauensstellung, sodass die Rolle von anderen Anwendungspipelines übernommen werden kann.
5. App-Entwickler können ihre App-Pipelines so konfigurieren, dass sie diese vom RVM bereitgestellte Rolle übernehmen.

Die erstellte Rolle umfasst die vom Entwickler angeforderten Berechtigungen und eine Richtlinie. `ReadOnlyAccess` Die Rolle kann nur von Pipelines übernommen werden, die für den `main` Zweig des vom Entwickler angegebenen Repositorys ausgeführt werden. Dieser Ansatz trägt dazu bei, dass Branch-Schutz und Überprüfungen erforderlich sein können, um die Rolle nutzen zu können.

Automatisierung und Skalierung

Bei den Berechtigungen mit den geringsten Rechten ist für jede Rolle, die bereitgestellt wird, besondere Aufmerksamkeit erforderlich. Dieses Modell reduziert die Komplexität, die für die Erstellung dieser Rollen erforderlich ist, und ermöglicht es Entwicklern, die Rollen zu erstellen, die sie benötigen, ohne dass viel zusätzliches Lernen oder Aufwand erforderlich ist.

Tools

AWS-Services

- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Organizationsist ein Kontoverwaltungsservice, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie erstellen und zentral verwalten.

Andere Tools

- Git ist ein verteiltes Open-Source-Versionskontrollsystem. Es beinhaltet die Möglichkeit, ein Organisationskonto zu erstellen.
- GitHub Actions ist eine CI/CD-Plattform (Continuous Integration and Continuous Delivery), die eng in Repositorys integriert GitHub ist. Sie können GitHub Actions verwenden, um Ihre Build-, Test- und Bereitstellungspipeline zu automatisieren.
- Terraform ist ein IaC-Tool (Infrastructure as Code) HashiCorp , mit dem Sie Cloud- und lokale Ressourcen erstellen und verwalten können.

Code-Repository

Der Code für dieses Muster ist im GitHub role-vending-machineRepository verfügbar.

Bewährte Methoden

- Machen Sie den richtigen Weg einfach und den falschen Weg schwer — Machen Sie es einfach, das Richtige zu tun. Wenn Entwickler Probleme mit dem RVM-Bereitstellungsprozess haben, versuchen sie möglicherweise, Rollen auf andere Weise zu erstellen, wodurch der zentrale Charakter von RVM untergraben wird. Stellen Sie sicher, dass Ihr Sicherheitsteam klare Anweisungen zur sicheren und effektiven Verwendung der RVM gibt.

  Sie sollten es Entwicklern auch schwer machen, das Falsche zu tun. Verwenden Sie Dienststeuerungsrichtlinien (SCPs) oder Berechtigungsgrenzen, um einzuschränken, welche Rollen andere Rollen erstellen können. Dieser Ansatz kann dazu beitragen, die Rollenerstellung auf RVM und andere vertrauenswürdige Quellen zu beschränken.
- Nennen Sie gute Beispiele — Es ist unvermeidlich, dass einige Entwickler bestehende Rollen im RVM-Repository als informelle Vorlagen für die Erteilung von Berechtigungen für ihre neuen Rollen anpassen. Wenn Sie über Beispiele mit den geringsten Berechtigungen verfügen, von denen sie kopieren können, kann das Risiko verringert werden, dass Entwickler umfassende Berechtigungen mit Platzhaltern anfordern. Wenn Sie mit Rollen mit hohen Rechten und vielen Platzhaltern beginnen, kann sich dieses Problem mit der Zeit noch vergrößern.
- Benennungskonventionen und -bedingungen verwenden — Selbst wenn ein Entwickler nicht alle Ressourcennamen kennt, die seine Anwendung erstellen wird, sollte er dennoch die Rollenberechtigungen mithilfe einer Namenskonvention einschränken. Wenn sie beispielsweise Amazon S3 S3-Buckets erstellen, könnte der Wert ihres Ressourcenschlüssels `arn:aws:s3:::myorg-myapp-dev-*` so aussehen, dass ihre Rolle keine Berechtigungen hat, die über Buckets hinausgehen, die diesem Namen entsprechen. Die Durchsetzung der Namenskonvention durch eine IAM-Richtlinie hat den zusätzlichen Vorteil, dass die Einhaltung der Namenskonvention verbessert wird. Diese Verbesserung ist darauf zurückzuführen, dass nicht übereinstimmende Ressourcen nicht erstellt werden dürfen.
- Pull-Request-Reviews (PR) erforderlich — Der Vorteil der RVM-Lösung besteht darin, dass sie einen zentralen Ort schafft, an dem neue Pipeline-Rollen überprüft werden können. Dieses Design ist jedoch nur dann sinnvoll, wenn es Schutzmaßnahmen gibt, die sicherstellen, dass sicherer, qualitativ hochwertiger Code an die RVM übergeben wird. Schützt die Branches, die zum Bereitstellen von Code verwendet werden (z. B.`main`), vor direkten Pushs und erfordert Genehmigungen für alle Merge-Anfragen, die auf sie abzielen.

- Schreibgeschützte Rollen konfigurieren — Standardmäßig stellt die RVM eine `readonly` Version jeder angeforderten Rolle bereit. Diese Rolle kann in CI/CD-Pipelines verwendet werden, die keine Daten schreiben, z. B. in einem Pipeline-Workflow. `terraform plan` Dieser Ansatz trägt dazu bei, unerwünschte Änderungen zu verhindern, wenn sich ein schreibgeschützter Workflow schlecht verhält.

  Standardmäßig ist die AWS verwaltete `ReadOnlyAccess` Richtlinie sowohl den Rollen mit Schreibzugriff als auch den Rollen mit Lese-/Schreibzugriff zugeordnet. Diese Richtlinie reduziert den Bedarf an Wiederholungen bei der Festlegung der erforderlichen Berechtigungen, kann jedoch für einige Organisationen zu freizügig sein. Wenn Sie möchten, können Sie die Richtlinie aus dem Terraform-Code entfernen.
- Mindestberechtigungen gewähren — Folgen Sie dem Prinzip der geringsten Rechte und gewähren Sie die Mindestberechtigungen, die zur Ausführung einer Aufgabe erforderlich sind. Weitere Informationen finden Sie in der IAM-Dokumentation unter Gewährung der geringsten Rechte und bewährte Methoden zur Sicherheit.

Epen

Bereite die Umgebung vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopieren Sie das Beispiel-Repository in Ihre GitHub Organisation.	Klonen Sie das Repository dieses Musters oder teilen Sie dieses Repository auf Ihre GitHub Organisation ab, sodass Sie es an Ihre Bedürfnisse anpassen können. • Wenn Sie dieses Repository klonen möchten, können Sie den folgenden Befehl verwenden: `git clone https://github.com/aws-samples/role-vending-machine`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wenn Sie sich dafür entscheiden, das Repository an Ihre GitHub Organisation weiterzugeben, können Sie den folgenden Befehl verwenden: `gh repo fork aws-samples/role-vending-machine --org YOUR_ORGANIZATION_NAME`	
Ermitteln Sie den AWS-Konto für das RVM.	Ermitteln Sie, welche Infrastrukturbereitstellung für die RVM verwendet werden AWS-Konto soll. Verwenden Sie nicht das Management- oder Root-Konto.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Erlauben Sie, dass die Pipelines der Organisation erstellt PRs werden.	**Note** Dieser Schritt ist nur erforderlich, wenn Sie die Erstellung PRs des `generate_providers_and_account_vars` Workflows zulassen möchten. Gehen Sie wie folgt vor PRs, damit die Pipelines Ihrer Organisation erstellt werden können: 1. Wechseln Sie zu `https://github.com/organizations/YOUR_ORG/settings/actions` . 2. Wähle GitHub Aktionen zulassen aus, um Pull Requests zu erstellen und zu genehmigen. Weitere Informationen finden Sie in der GitHub Dokumentation unter GitHub Aktionseinstellungen für ein Repository verwalten.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gewähren Sie dem RVM-Konto nur Leseberechtigungen .	Erstellen Sie in Ihrem Verwaltungskonto eine Delegierungsrichtlinie, die Ihrem RVM-Konto nur Leseberechtigungen gewährt. Auf diese Weise können Ihre GitHub RVM-Workflows dynamisch eine Liste der Konten Ihrer AWS Organisation abrufen, wenn das Skript ausgeführt wird. `generate_providers_and_account_vars.py` Verwenden Sie den folgenden Code und `<YOUR RVM Account ID>` ersetzen Sie ihn durch die AWS-Konto ID, die Sie in Schritt 2 ausgewählt haben: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "Statement", "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::<YOUR RVM Account ID>:root" }, "Action": [ "organizations:ListAccounts",`	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"organizations:DescribeOrganization",
	"organizations:DescribeOrganizationalUnit",
	"organizations:ListRoots",
	"organizations:ListAWSServiceAccessForOrganization",
	"organizations:ListDelegatedAdministrators"
	],
	"Resource": "*"
	}
	]
	}</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Standardwerte aus dem Beispiel-Repository.	Gehen Sie wie folgt vor, um die RVM für den Betrieb in Ihrer spezifischen Umgebung zu konfigurieren: AWS-Region 1. Aktualisieren Sie `scripts/generate_providers_and_account_vars.py` und andere Dateien (z. B. den `bootstrap` Ordner) mit der entsprechenden Region, in der Sie arbeiten. 2. Aktualisieren Sie die `.github/workflows/.env` Datei mit der AWS-Konto ID, der Region und allen anderen Variablen, die Sie angeben möchten.	DevOps Ingenieur

Infrastruktur initialisieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bootstrap für das RVM-Repo.	Dieser Schritt ist erforderlich, um die OIDC-Vertrauens- und IAM-Rollen zu erstellen, die von der RVM-Pipeline selbst verwendet werden, sodass sie den Betrieb aufnehmen und andere Rollen verkaufen kann. Führen Sie im Kontext Ihres RVM-Kontos manuell einen	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`terraform apply` Befehl aus dem Verzeichnis aus. `scripts/bootstrap` Geben Sie alle erforderlichen Werte auf der Grundlage der Variablendokumentation an.	

Operationen konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die `github-workflow-rvm-readonly` Rollen `github-workflow-rvm` und für alle Konten bereit.	Wählen Sie eine Bereitstellungsmethode, die den Praktiken Ihres Unternehmens entspricht, z. B. AFT oder StackSets. Verwenden Sie diese Methode, um die beiden IAM-Rollen in der `scripts/assumed_role/main.tf` Datei (Standardnamen `github-workflow-rvm` und `github-workflow-rvm-readonly`) für jedes Konto bereitzustellen, für das die RVM Pipeline-Rollen erstellen soll. Diese IAM-Rollen verfügen über Vertrauensrichtlinien, die es der Rolle des RVM-Kontos (oder einer gleichwertigen Rolle) ermöglichen, diese Rolle zu übernehmen. `readonly` Die Rollen	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	verfügen außerdem über IAM-Berechtigungsrichtlinie n, die es ihnen ermöglichen, übereinstimmende Rollen zu lesen und zu schreiben (sofern sie nicht die `readonly` Rolle verwenden). `github-wo rkflow-role-*`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den `generate_providers_and_account_vars` Workflow aus.	Gehen Sie wie folgt vor, um Ihre RVM so zu konfigurieren, dass sie bereit ist, Pipeline-Rollen zu erstellen: 1. Führen Sie den `generate_providers_and_account_vars` Workflow mithilfe von workflow_dispatch aus. 2. Führen Sie den PR zusammen, den der Workflow erstellt. Nach Abschluss des Workflows ist die RVM bereit für: • Akzeptieren Sie Anfragen für neue Pipeline-Rollen. • Erstellen Sie je nach Anforderung entweder Rollen mit Lese-/Schreibzugriff oder Rollen mit Lese-/Schreibzugriff. • Stellen Sie Rollen für die angegebenen Rollen bereit. AWS-Konten	DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Ich habe mit dem RVM eine Rolle erstellt, kann sie aber GitHub nicht übernehmen.	Stellen Sie sicher, dass der Name des GitHub Repositorys mit dem Namen übereinstimmt, der dem `github_workflow_roles` Modul zur Verfügung gestellt wurde. Rollen sind so begrenzt, dass sie nur von einem Repository übernommen werden können. Stellen Sie auf ähnliche Weise sicher, dass der in der GitHub Pipeline verwendete Branch mit dem Namen des Branches übereinstimmt, der dem Modul zur Verfügung gestellt wurde. `github_workflow_roles` In der Regel können von RVM erstellte Rollen mit Schreibbe rechtigungen nur von Workflows verwendet werden, die auf den `main` Branch beschränk t sind (d. h. Bereitstellungen, aus denen sie stammen). `main`
Meine schreibgeschützte Rolle kann ihre Pipeline nicht ausführen, da ihr die Berechtig ungen zum Lesen einer bestimmten Ressource fehlen.	Die `ReadOnlyAccess` Richtlinie bietet zwar umfangreiche Leseberechtigungen, einige Leseaktionen (z. B. bestimmte Aktionen) sind in der Richtlinie jedoch nicht vorgesehen. AWS Security Hub Sie können spezifische Aktionsberechtigun gen hinzufügen, indem Sie den `inline_po licy_readonly` Parameter des `github-workflow-roles` Moduls verwenden.

Zugehörige Ressourcen

- Bewährte Methoden für die Verwendung AWS CloudFormation StackSets
- Organisieren Sie Ihre AWS Umgebung mithilfe mehrerer Konten

- Überblick über AWS Control Tower Account Factory for Terraform (AFT)
- Bewährte Methoden für Richtlinien

Zusätzliche Informationen

GitHub Umgebungen verwenden

GitHub Umgebungen sind ein alternativer Ansatz zu branchenbasierten Einschränkungen des Rollenzugriffs. Wenn Sie lieber eine GitHub Umgebung verwenden möchten, finden Sie im Folgenden ein Beispiel für die Syntax für eine zusätzliche Bedingung in der IAM-Vertrauensrichtlinie. Diese Syntax gibt an, dass die Rolle nur verwendet werden kann, wenn die GitHub Aktion in der `Production` Umgebung ausgeführt wird.

```
"StringLike": {
    "token.actions.githubusercontent.com:sub": "repo:octo-org/octo-
repo:environment:Production"
}
```

Die Beispielsyntax verwendet die folgenden Platzhalterwerte:

- `octo-org`ist der Name der GitHub Organisation.
- `octo-repo`ist der Name des Repositorys.
- `Production`ist der spezifische GitHub Umgebungsname.

Veröffentlichen Sie CloudWatch Amazon-Metriken in einer CSV-Datei

Erstellt von Abdullahi Olaoye (AWS)

Übersicht

Dieses Muster verwendet ein Python-Skript, um CloudWatch Amazon-Metriken abzurufen und die Metrikinformationen zur besseren Lesbarkeit in eine Datei mit kommagetrennten Werten (CSV) zu konvertieren. Das Skript verwendet den AWS-Service, dessen Metriken abgerufen werden sollen, als erforderliches Argument. Sie können die AWS-Region und das AWS-Anmeldeinformationsprofil als optionale Argumente angeben. Wenn Sie diese Argumente nicht angeben, verwendet das Skript die Standardregion und das Standardprofil, die für die Workstation konfiguriert sind, auf der das Skript ausgeführt wird. Nachdem das Skript ausgeführt wurde, generiert und speichert es eine CSV-Datei im selben Verzeichnis.

Im Abschnitt Anlagen finden Sie das Skript und die zugehörigen Dateien, die mit diesem Muster bereitgestellt werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Python 3.x
- AWS-Befehlszeilenschnittstelle (AWS Command Line Interface, AWS CLI)

Einschränkungen

Das Skript unterstützt derzeit die folgenden AWS-Services:

- AWS Lambda
- Amazon Elastic Compute Cloud (Amazon EC2)
  - Standardmäßig erfasst das Skript keine Volumenmetriken für Amazon Elastic Block Store (Amazon EBS). Um Amazon EBS-Metriken zu sammeln, müssen Sie die angehängte `metrics.yaml` Datei ändern.
- Amazon Relational Database Service (Amazon RDS)
  - Das Skript unterstützt Amazon Aurora jedoch nicht.
- Application Load Balancer

- Network Load Balancer
- Amazon API Gateway

Tools

- Amazon CloudWatch ist ein Überwachungsservice, der sich an DevOps Ingenieure, Entwickler, Techniker für die Zuverlässigkeit von Standorten (SREs) und IT-Manager richtet. CloudWatch bietet Daten und umsetzbare Erkenntnisse, die Ihnen helfen, Ihre Anwendungen zu überwachen, auf systemweite Leistungsänderungen zu reagieren, die Ressourcennutzung zu optimieren und einen einheitlichen Überblick über den Betriebsstatus zu erhalten. CloudWatch sammelt Überwachungs- und Betriebsdaten in Form von Protokollen, Metriken und Ereignissen und bietet eine einheitliche Ansicht der AWS-Ressourcen, -Anwendungen und -Services, die auf AWS- und lokalen Servern ausgeführt werden.

Epen

Installieren und konfigurieren Sie die Voraussetzungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die Vorausset zungen.	Führen Sie den folgenden Befehl aus: `$ pip3 install -r requirements.txt`	Developer
Konfigurieren Sie die AWS CLI.	Führen Sie den folgenden Befehl aus: `$ aws configure`	Developer

Das Python-Skript konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Öffnen Sie das Skript.	Um die Standardkonfiguration des Skripts zu ändern, öffnen Sie `metrics.yaml` .	Developer
Stellen Sie den Zeitraum für das Skript ein.	Dies ist der Zeitraum, der abgerufen werden soll. Der Standardzeitraum beträgt 5 Minuten (300 Sekunden). Sie können den Zeitraum ändern, beachten Sie jedoch die folgenden Einschränkungen: • Wenn der angegebene Stundenwert zwischen 3 Stunden und 15 Tagen liegt, verwenden Sie ein Vielfaches von 60 Sekunden (1 Minute) für den Zeitraum. • Wenn der angegebene Stundenwert zwischen 15 Stunden und 63 Tagen liegt, verwenden Sie ein Vielfache s von 300 Sekunden (5 Minuten) für den Zeitraum. • Wenn der angegebene Stundenwert größer als vor 63 Tagen ist, verwenden Sie ein Vielfaches von 3.600 Sekunden (1 Stunde) für den Zeitraum.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Andernfalls gibt der API-Vorga ng keine Datenpunkte zurück.	
Legen Sie die Stunden für das Skript fest.	Dieser Wert gibt an, wie viele Stunden an Messwerten Sie abrufen möchten. Die Standardeinstellung ist 1 Stunde. Um Messwerte für mehrere Tage abzurufen , geben Sie den Wert in Stunden an. Geben Sie beispielsweise für 2 Tage 48 an.	Developer
Ändern Sie die Statistikwerte für das Skript.	(Optional) Der globale Statistik wert ist. Er wird verwendet `Average`, wenn Metriken abgerufen werden, denen kein bestimmter Statistikwert zugewiesen ist. Das Skript unterstützt die Statistikwerte `MaximumSampleCount` , und`Sum`.	Developer

Führen Sie das Python-Skript aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das Skript aus.	Verwenden Sie den folgenden Befehl: `$ python3 cwreport.py <service>`	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Führen Sie den folgenden Befehl aus, um eine Liste der Dienstwerte `region` und der optionalen `profile` Parameter anzuzeigen: `$ python3 cwreport.py -h` Weitere Informationen zu den optionalen Parametern finden Sie im Abschnitt Zusätzliche Informationen.	

Zugehörige Ressourcen

- Konfiguration der AWS-CLI
- Verwenden von CloudWatch Amazon-Metriken
- CloudWatch Amazon-Dokumentation
- EC2 CloudWatch Metriken
- AWS Lambda Lambda-Metriken
- Amazon RDS-Metriken
- Metriken für den Application Load Balancer
- Metriken für den Network Load Balancer
- Amazon API Gateway Gateway-Metriken

Zusätzliche Informationen

Verwendung von Skripten

```
$ python3 cwreport.py -h
```

Beispiel für eine Syntax

```
python3 cwreport.py <service> <--region=Optional Region> <--profile=Optional credential
 profile>
```

Parameter

- service (erforderlich) – Der Dienst, für den Sie das Skript ausführen möchten. Das Skript unterstützt derzeit diese Dienste: AWS Lambda, Amazon, Amazon RDS EC2, Application Load Balancer, Network Load Balancer und API Gateway.
- Region (optional) – Die AWS-Region, aus der Metriken abgerufen werden sollen. Die Standardregion ist`ap-southeast-1`.
- profile (optional) – Das zu verwendende AWS-CLI benannte Profil. Wenn dieser Parameter nicht angegeben ist, wird das standardmäßig konfigurierte Anmeldeinformationsprofil verwendet.

Beispiele

- So verwenden Sie die Standardregion `ap-southeast-1` und die konfigurierten Standardanmeldedaten zum Abrufen von EC2 Amazon-Metriken: `$ python3 cwreport.py ec2`
- So geben Sie eine Region an und rufen API-Gateway-Metriken ab: `$ python3 cwreport.py apigateway --region us-east-1`
- So geben Sie ein AWS-Profil an und rufen EC2 Amazon-Metriken ab: `$ python3 cwreport.py ec2 --profile testprofile`
- So geben Sie sowohl die Region als auch das Profil zum Abrufen von EC2 Amazon-Metriken an: `$ python3 cwreport.py ec2 --region us-east-1 --profile testprofile`

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Entfernen Sie EC2 Amazon-Einträge AWS Managed Microsoft AD mithilfe AWS-Konten von AWS Lambda Automatisierung

Erstellt von Dr. Rahul Sharad Gaikwad (AWS) und Tamilselvan P (AWS)

Übersicht

Active Directory (AD) ist ein Microsoft-Skripttool, das Domäneninformationen und Benutzerinteraktionen mit Netzwerkdiensten verwaltet. Es wird häufig von Managed Services Providern (MSPs) verwendet, um die Anmeldeinformationen und Zugriffsberechtigungen von Mitarbeitern zu verwalten. Da AD-Angreifer mit inaktiven Konten versuchen können, sich in ein Unternehmen zu hacken, ist es wichtig, inaktive Konten zu finden und sie im Rahmen eines routinemäßigen Wartungsplans zu deaktivieren. Mit AWS Directory Service for Microsoft Active Directory können Sie Microsoft Active Directory als verwalteten Dienst ausführen. Dieses Muster kann Ihnen helfen, die AWS Lambda Automatisierung so zu konfigurieren, dass inaktive Konten schnell gefunden und entfernt werden.

Wenn die folgenden Szenarien auf Ihr Unternehmen zutreffen, kann Ihnen dieses Muster helfen:

- Zentralisierte AD-Verwaltung — Wenn Ihr Unternehmen mehrere hat AWS-Konten, von denen jedes über eine eigene AD-Bereitstellung verfügt, kann es schwierig sein, Benutzerkonten und Zugriffsberechtigungen für alle Konten einheitlich zu verwalten. Mit einer kontenübergreifenden AD-Bereinigungslösung können Sie inaktive Konten aus allen AD-Instanzen zentral deaktivieren oder entfernen.
- AD-Restrukturierung oder -Migration — Wenn Ihr Unternehmen plant, seine AD-Bereitstellung umzustrukturieren oder zu migrieren, kann Ihnen eine kontenübergreifende AD-Bereinigungslösung dabei helfen, die Umgebung vorzubereiten. Die Lösung kann Ihnen helfen, unnötige oder inaktive Konten zu entfernen, den Migrationsprozess zu vereinfachen und potenzielle Konflikte oder Probleme zu reduzieren.

Wenn Sie dieses Muster verwenden, können Sie die folgenden Vorteile nutzen:

- Verbessern Sie die Datenbank- und Serverleistung und beheben Sie Sicherheitslücken, die auf inaktive Konten zurückzuführen sind.
- Wenn Ihr AD-Server in der Cloud gehostet wird, kann das Entfernen inaktiver Konten auch die Speicherkosten senken und gleichzeitig die Leistung verbessern. Ihre monatlichen Rechnungen könnten sinken, da sowohl die Bandbreitenkosten als auch die Rechenressourcen sinken können.

- Halten Sie potenzielle Angreifer mit einem sauberen Active Directory in Schach.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Elternkonto AWS-Konto und ein oder mehrere Kinderkonten. In diesem Muster wird Active Directory für ein übergeordnetes Konto erstellt. Untergeordnete Konten hosten Windows-Server und werden über das übergeordnete Konto Active Directory miteinander verbunden.
- Git wurde auf einer lokalen Workstation installiert und konfiguriert.
- Terraform wurde auf einer lokalen Workstation installiert und konfiguriert.
- AWS Managed Microsoft AD Verzeichnis, das im übergeordneten Konto konfiguriert und für alle untergeordneten Konten gemeinsam genutzt wird. Weitere Informationen finden Sie im AWS Directory Service Administratorhandbuch unter Tutorial: Teilen Ihres AWS Managed Microsoft AD Verzeichnisses für einen nahtlosen EC2 Domänenbeitritt.
- Eine Virtual Private Cloud (VPC) -Peering-Verbindung oder AWS Transit Gateway Verbindung, die zwischen der VPC von AWS Directory Service (übergeordnetem Konto) und der VPC der Amazon Elastic Compute Cloud (Amazon EC2) -Instances (untergeordnete Konten) verfügbar ist. Weitere Informationen finden Sie unter Konfigurieren einer VPC-Peering-Verbindung zwischen dem Verzeichnisbesitzer und dem Directory-Consumer-Konto im AWS Directory Service Administratorhandbuch.
- Ein Windows-Computer, der mit dem `EC2WindowsUserdata` Skript für alle Eltern- und Kinderkonten konfiguriert wurde. Die Skriptdatei ist im Stammverzeichnis des Code-Repositorys dieses Musters verfügbar.
- Eine kontoübergreifende Rolle AWS Identity and Access Management (IAM), die für jedes untergeordnete Konto verfügbar ist und mit einer Vertrauensrichtlinie konfiguriert ist, die die Verwendung einer AWS Lambda Funktion aus dem übergeordneten Konto ermöglicht. Weitere Informationen finden Sie unter Senden und Empfangen von Ereignissen zwischen AWS-Konten EventBridge in Amazon im EventBridge Amazon-Benutzerhandbuch.
- Die folgenden geheimen Werte sind im AWS Systems Manager Parameter Store des übergeordneten Kontos verfügbar:
  - `domainJoinUser`— Benutzername des Verzeichnisdienstes
  - `domainJoinPassword`— Passwort des Verzeichnisdienstes

Weitere Informationen zu Geheimnissen finden Sie unter Create an AWS Secrets Manager Secret im AWS Secrets Manager Benutzerhandbuch.

Einschränkungen

- Das Erstellen einer Ressource in einem Kinderkonto ist mit Terraform nicht automatisiert. Sie müssen die folgenden Ressourcen manuell mithilfe von erstellen: AWS Management Console
  - EventBridge Amazon-Regel zum Senden der EC2 Kündigungsereignisse von Amazon an das übergeordnete Konto
  - Erstellung einer EC2 kontoübergreifenden Amazon-Rolle im Kinderkonto mit Vertrauensrichtlinie
  - VPC-Peering oder Transit Gateway Gateway-Verbindung
- Einige AWS-Services sind nicht in allen verfügbar. AWS-Regionen Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie unter Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Produktversionen

- Terraform Version 1.1.9 oder höher
- Terraform AWS Provider Version 3.0 oder höher

Architektur

Das folgende Diagramm zeigt die High-Level-Architektur der Lösung.

Das Architekturdiagramm veranschaulicht den folgenden Prozess:

1. Bei Kinderkonten erfasst die EventBridge Regel alle EC2 Kündigungsereignisse von Amazon. Die Regel sendet die Ereignisse, EventBridge die im übergeordneten Konto vorhanden sind.
2. EventBridge Sammelt aus dem übergeordneten Konto alle Ereignisse und enthält die Regel zum Auslösen der Lambda-Funktion`ADcleanup-Lambda`.
3. Das übergeordnete Konto empfängt alle Kündigungsereignisse vom Eltern- oder Kinderkonto und löst die Lambda-Funktion aus.

4. Die Lambda-Funktion ruft Amazon EC2 Auto Scaling Scaling-Gruppen mithilfe des Python-Boto-Moduls auf und ruft die zufällige Instanz-ID ab. Die Instanz-ID wird verwendet, um Systems Manager Manager-Befehle auszuführen.
5. Die Lambda-Funktion ruft Amazon EC2 mithilfe des Boto-Moduls erneut auf. Die Lambda-Funktion ruft die privaten IP-Adressen der laufenden Windows-Server ab und speichert die Adressen in einer temporären Variablen. In den Schritten 5.1 und 5.2 werden die laufenden EC2 Windows-Instanzen von untergeordneten Konten erfasst.
6. Die Lambda-Funktion ruft Systems Manager erneut auf, um die Computerinformationen abzurufen, mit denen eine Verbindung hergestellt ist. AWS Directory Service
7. Ein AWS Systems Manager Dokument hilft dabei, den PowerShell Befehl auf Amazon EC2 Windows-Servern auszuführen, um die privaten IP-Adressen der Computer abzurufen, die mit AD verbunden sind. (Das Systems Manager Manager-Dokument verwendet die Instanz-ID, die in Schritt 4 abgerufen wurde.)
8. Der Benutzername und die Kennwörter der AD-Domäne werden im AWS Systems Manager Parameterspeicher gespeichert. AWS Lambda und Systems Manager rufen Parameter Store auf und rufen die Werte für Benutzername und Passwort ab, die für die Verbindung mit AD verwendet werden sollen.
9. Mithilfe des Systems Manager Manager-Dokuments wird das PowerShell Skript auf dem Amazon EC2 Windows-Server unter Verwendung der zuvor in Schritt 4 abgerufenen Instance-ID ausgeführt.
10. Amazon EC2 stellt mithilfe AWS Directory Service von PowerShell Befehlen eine Verbindung her und entfernt die Computer, die nicht verwendet oder inaktiv sind.

Tools

AWS Dienstleistungen

- AWS Directory Servicebietet mehrere Möglichkeiten, Microsoft Active Directory (AD) mit anderen AWS-Services wie Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS) für SQL Server und Amazon FSx für Windows File Server zu verwenden.
- AWS Directory Service for Microsoft Active Directoryermöglicht Ihren verzeichnissensitiven Workloads und AWS Ressourcen die Verwendung von Microsoft Active Directory in der. AWS Cloud

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS Lambda Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen. AWS-Konten
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden. Mit IAM können Sie festlegen, wer oder was auf Dienste und Ressourcen zugreifen kann AWS, detaillierte Berechtigungen zentral verwalten und den Zugriff analysieren, um die Berechtigungen zu verfeinern. AWS
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Systems Managerhilft Ihnen bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der ausgeführt AWS Cloud werden. Es vereinfacht das Anwendungs- und Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme und hilft Ihnen, Ihre AWS Ressourcen sicher und in großem Umfang zu verwalten.
- AWS Systems Manager Dokumente definieren die Aktionen, die Systems Manager auf Ihren verwalteten Instanzen ausführt. Systems Manager umfasst mehr als 100 vorkonfigurierter Dokumente, die Sie verwenden können, indem Sie zur Laufzeit Parameter angeben.
- AWS Systems Manager Parameter Store ist eine Funktion von AWS Systems Manager und bietet sicheren, hierarchischen Speicher für die Verwaltung von Konfigurationsdaten und Geheimnissen.

Andere Tools

- HashiCorp Terraform ist ein Infrastructure-as-Code-Tool (IaC), mit dem Sie mithilfe von Code Cloud-Infrastruktur und -Ressourcen bereitstellen und verwalten können.
- PowerShellist ein Automatisierungs- und Konfigurationsverwaltungsprogramm von Microsoft, das unter Windows, Linux und macOS läuft.
- Python ist eine Allzweck-Computerprogrammiersprache.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub aws-lambda-ad-cleanup-terraform-samples verfügbar.

Bewährte Methoden

- Automatisch Domains beitreten.Wenn Sie eine Windows-Instanz starten, die Teil einer AWS Directory Service Domäne sein soll, treten Sie der Domäne während der Instanzerstellung bei, anstatt die Instanz später manuell hinzuzufügen. Um einer Domäne automatisch beizutreten, wählen Sie beim Starten einer neuen Instanz das richtige Verzeichnis aus der Dropdownliste zum Domänenbeitrittsverzeichnis aus. Weitere Informationen finden Sie unter Nahtloses Hinzufügen einer Amazon EC2 Windows-Instance zu Ihrem AWS Managed Microsoft AD Active Directory im AWS Directory Service Administratorhandbuch.
- Löschen Sie ungenutzte Konten.Es ist üblich, in AD Konten zu finden, die noch nie verwendet wurden. Wie deaktivierte oder inaktive Konten, die im System verbleiben, können vernachlässigte, ungenutzte Konten Ihr AD-System verlangsamen oder Ihr Unternehmen anfällig für Datenschutzverletzungen machen.
- Automatisieren Sie Active Directory-Säuberungen.Um Sicherheitsrisiken zu minimieren und zu verhindern, dass veraltete Konten die AD-Leistung beeinträchtigen, sollten AD-Bereinigungen in regelmäßigen Abständen durchgeführt werden. Sie können die meisten AD-Verwaltungs- und Bereinigungsaufgaben erledigen, indem Sie Skripts schreiben. Zu den Aufgaben gehören beispielsweise das Entfernen deaktivierter und inaktiver Konten, das Löschen leerer und inaktiver Gruppen und das Auffinden abgelaufener Benutzerkonten und Kennwörter.

Epen

Richten Sie Kinderkonten ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine kontoüber greifende Rolle im Kinderkon to.	Gehen Sie wie folgt vor, um eine kontoübergreifende Rolle in einem Kinderkonto zu erstellen: 1. Erstellen Sie für jedes Kinderkonto eine Rolle, die `ec2crossaccountrol`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	e mithilfe der verwaltet en Richtlinie benannt `AmazonEC2ReadOnlyA ccess` wird. (Weitere Informationen finden Sie in der IAM-Dokumentation unter Erstellen einer Rolle mithilfe benutzerdefinierter Vertrauensrichtlinien.) 2. Fügen Sie im Abschnitt Benutzerdefinierte Vertrauensrichtlinie den folgenden Code hinzu: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "ec2.amazonaws.com" }, "Action": "sts:AssumeRole" }, { "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::${Parentaccountid}:role/ADcleanuprole"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> },
	            "Action":
	"sts:AssumeRole"
	        }
	    ]
	}</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Ereignisregel im Kinderkonto.	Gehen Sie wie folgt vor, um für jedes Kinderkonto eine EventBridge Regel zu erstellen: 1. Melden Sie sich bei dem Kind AWS-Konto an und öffnen Sie dann die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/. 2. Wählen Sie im Navigationsbereich Regeln aus. 3. Wählen Sie Regel erstellen aus. 4. Geben Sie einen Namen und optional eine Beschreibung für die Regel ein. 5. Wählen Sie für Event Bus den AWS-Standardereignisbus aus. 6. Wählen Sie als Regeltyp die Option Regel mit einem Ereignismuster aus. 7. Wählen Sie Weiter aus. 8. Fügen Sie für Ereignismuster den folgenden Code ein: `{ "source": ["aws.ec2"],`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"detail-type": ["EC2 Instance State-change Notification"], "detail": { "state": ["terminated"] } }</pre> 9. Wählen Sie Weiter aus. 10. Wählen Sie als Zieltyp die Option Eventbus in einem anderen Konto oder einer anderen Region aus.Geben Sie für Event Bus als Ziel den Amazon Resource Name (ARN) für den Eventbus für das übergeordnete Konto ein. 11. Wählen Sie für Ausführungsrolle die Option Neue Rolle für diese spezifische Ressource erstellen aus. 12. Wählen Sie Weiter, um die Details für die neue Regel zu überprüfen, und klicken Sie dann auf Erstellen. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch unter Regeln erstellen, die auf Ereignisse EventBridge in Amazon reagieren.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine EC2 Instanz und treten Sie AD bei.	Gehen Sie wie folgt vor, um eine EC2 Instanz für Windows zu erstellen: 1. Verwenden Sie das `EC2WindowsUserdata` Skript, das im Code-Repository dieses Musters verfügbar ist. 2. Überarbeiten Sie im Benutzerdatenskript den folgenden Code, um Ihre `Directory service addresses` Werte aus dem übergeordneten Konto zu verwenden: `set-DnsClientServerAddress -InterfaceIndex 6 -ServerAddresses $(Directory service addresses)`	DevOps Ingenieur

Richten Sie die lokale Workstation ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Projektordner und fügen Sie die Dateien hinzu.	Gehen Sie wie folgt vor, um das Repository zu klonen und einen Projektordner zu erstellen: 1. Öffnen Sie das GitHub Repository dieses Musters.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	2. Wählen Sie die Code-Schaltfläche, um die Optionen zum Klonen in der Dropdownliste „Klonen“ zu sehen.
	3. Kopieren Sie auf der Registerkarte HTTPS die unter Clone angegebene URL mithilfe der Web-URL.
	4. Erstellen Sie einen Ordner auf Ihrem Computer und benennen Sie ihn mit Ihrem Projektnamen.
	5. Öffnen Sie ein Terminal auf Ihrem lokalen Computer und navigieren Sie zu diesem Ordner.
	6. Verwenden Sie den folgenden Befehl, um das Git-Repository zu klonen.
	`git clone <repository-URL>.git`
	7. Nachdem das Repository geklont wurde, verwenden Sie den folgenden Befehl, um zum geklonten Verzeichnis zu wechseln.
	`cd <directory name>/terraform-aws-lambda-ad-cleanup/multiple-account-cleanup`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Öffnen Sie dieses Projekt im geklonten Repository in einer integrierten Entwicklungsumgebung (IDE) Ihrer Wahl.	
Erstellen Sie die `adcleanup.zip` Datei.	Führen Sie den folgenden Befehl aus, um die `lambda_function.py` Datei zu komprimieren: `zip -r adcleanup.zip lambda_function.py`	DevOps Ingenieur

Stellen Sie die Zielarchitektur mithilfe der Terraform-Konfiguration bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie Werte für die Terraform-Variablen an.	Geben Sie für das untergeordnete Konto Werte für die folgenden `arn` Variablen als Zeichenfolgentypen in der `terraform.tfvars` Datei an: • `lambda_env_cross_role_arn` • `child_account_cross_role_arn`	DevOps Ingenieur
Initialisieren Sie die Terraform-Konfiguration.	Führen Sie den folgenden Befehl aus, um Ihr Arbeitsverzeichnis zu initialisieren, das die Terraform-Dateien enthält:	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`terraform init`	
Änderungen in der Vorschau anzeigen.	Sie können eine Vorschau der Änderungen anzeigen, die Terraform an der Infrastruktur vornehmen wird, bevor Ihre Infrastruktur bereitgestellt wird. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob Terraform die Änderungen nach Bedarf vornimmt: `terraform plan –- var-file=examples/ terraform.tfvars`	DevOps Ingenieur
Führen Sie die vorgeschl agenen Aktionen aus.	Gehen Sie wie folgt vor, um zu überprüfen, ob die Ergebniss e des `terraform plan` Befehls den Erwartungen entsprechen: 1. Führen Sie den folgenden Befehl aus: `terraform apply` 2. Melden Sie sich bei der an AWS Management Console, und stellen Sie sicher, dass die Ressource n vorhanden sind.	DevOps Ingenieur

Überprüfen der Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Lambda-Funktion aus und testen Sie sie.	Gehen Sie wie folgt vor, um zu überprüfen, ob die Bereitstellung erfolgreich durchgeführt wurde: 1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Lambda-Konsole. Öffnen Sie die Seite Funktionen und wählen Sie den Funktionsnamen aus, der mit ADcleanup-Lambda-* beginnt. 2. Wählen Sie auf der Funktionsübersichtsseite auf der Registerkarte Code im Abschnitt Codequelle die Option Test aus. 3. Um das Testereignis zu speichern, geben Sie einen Namen für das Ereignis ein und wählen Sie Speichern. Um das Ereignis zu testen, wählen Sie erneut Testen. Die Ausführungsergebnisse zeigen die Ausgabe der Funktion.	DevOps Ingenieur
Ergebnisse der EventBridge Regelausführung vom	Gehen Sie wie folgt vor, um die Ergebnisse der EventBridge Regel anzuzeigen, die auf	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
übergeordneten Konto aus anzeigen.	EC2 Kündigungsereignissen durch Amazon vom übergeordneten Konto aus basiert: 1. Kündigen Sie EC2 Instances vom übergeordneten Konto aus. 2. Öffnen Sie die Lambda-Konsole des übergeordneten Kontos. Öffnen Sie die Seite Funktionen und wählen Sie den Funktionsnamen aus, der mit ADcleanup-Lambda-* beginnt. 3. Wählen Sie die Registerkarte „Überwachen“ und dann „Protokolle anzeigen“. CloudWatch In der CloudWatch Konsole werden auf der Seite Protokollgruppen die Ergebnisse der Lambda-Funktion angezeigt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Die Ergebnisse der EventBridge Regelausführung vom untergeordneten Konto aus anzeigen.	Gehen Sie wie folgt vor, um die Ergebnisse der EventBridge Regel anzuzeigen, die auf EC2 Kündigungsereignissen von Amazon für das Kinderkonto basiert: 1. Beenden Sie EC2 Instances über das Kinderkonto. 2. Öffnen Sie die Lambda-Konsole des übergeordneten Kontos. Öffnen Sie die Seite Funktionen und wählen Sie den Funktionsnamen aus, der mit ADcleanup-Lambda-* beginnt. 3. Wählen Sie die Registerkarte „Überwachen“ und dann „Protokolle anzeigen“. CloudWatch In der CloudWatch Konsole werden auf der Seite Protokollgruppen die Ergebnisse der Lambda-Funktion angezeigt.	DevOps Ingenieur

Reinigen Sie die Infrastruktur nach dem Gebrauch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Säubere die Infrastruktur.	Verwenden Sie den folgenden Befehl, um die von Ihnen	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	erstellte Infrastruktur zu bereinigen: `terraform destroy` Um den `destroy` Befehl zu bestätigen, geben Sie ein`yes`.	
Nach der Säuberung überprüfen.	Stellen Sie sicher, dass die Ressourcen erfolgreich entfernt wurden.	DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Verbindungsproblem zwischen AWS Directory Service (übergeordnetes Konto) und EC2 Amazon-Instance (untergeordnetes Konto) — Sie können die Computer des untergeordneten Kontos nicht mit AD verbinden, obwohl VPC-Peering verfügbar ist.	Fügen Sie Routing hinzu in. VPCs Anweisung en finden Sie in der Dokumentation unter Konfigurieren einer VPC-Peering-Verbindung zwischen dem Verzeichnisbesitzer und dem Directory-Consumer-Konto. AWS Directory Service

Zugehörige Ressourcen

AWS Dokumentation

- Amazon EventBridge und AWS Identity and Access Management
- Erforderliche Instance-Berechtigungen für Systems Manager konfigurieren
- Identitäts- und Zugriffsmanagement für AWS Directory Service
- Identitätsbasierte IAM-Richtlinien für Lambda
- Manuelles Hinzufügen einer Amazon EC2 Windows-Instance zu Ihrem AWS Managed Microsoft AD Active Directory

- Entfernen Sie EC2 Amazon-Einträge in derselben AWS-Konto Form AWS Managed Microsoft AD mithilfe von AWS Lambda Automatisierung

Sonstige Ressourcen

- AWS Anbieter (Terraform-Dokumentation)
- Backend-Konfiguration (Terraform-Dokumentation)
- Installieren Sie Terraform (Terraform-Dokumentation)
- Python-Boto-Modul (Python-Paketindex-Repository)
- Laden Sie die Terraform-Binärdatei herunter (Terraform-Dokumentation)

Entfernen Sie EC2 Amazon-Einträge in derselben AWS-Konto Form AWS Managed Microsoft AD mithilfe von AWS Lambda Automatisierung

Erstellt von Dr. Rahul Sharad Gaikwad (AWS) und Tamilselvan P (AWS)

Übersicht

Active Directory (AD) ist ein Microsoft-Skripttool, das Domäneninformationen und Benutzerinteraktionen mit Netzwerkdiensten verwaltet. Es wird häufig von Managed Services Providern (MSPs) verwendet, um die Anmeldeinformationen und Zugriffsberechtigungen von Mitarbeitern zu verwalten. Da AD-Angreifer mit inaktiven Konten versuchen können, sich in ein Unternehmen zu hacken, ist es wichtig, inaktive Konten zu finden und sie im Rahmen eines routinemäßigen Wartungsplans zu deaktivieren. Mit AWS Directory Service for Microsoft Active Directory können Sie Microsoft Active Directory als verwalteten Dienst ausführen.

Dieses Muster kann Ihnen helfen, die AWS Lambda Automatisierung so zu konfigurieren, dass inaktive Konten schnell gefunden und entfernt werden. Wenn Sie dieses Muster verwenden, können Sie die folgenden Vorteile nutzen:

- Verbessern Sie die Datenbank- und Serverleistung und beheben Sie Sicherheitslücken, die auf inaktive Konten zurückzuführen sind.
- Wenn Ihr AD-Server in der Cloud gehostet wird, kann das Entfernen inaktiver Konten auch die Speicherkosten senken und gleichzeitig die Leistung verbessern. Ihre monatlichen Rechnungen könnten sinken, da sowohl die Bandbreitenkosten als auch die Rechenressourcen sinken können.
- Halten Sie potenzielle Angreifer mit einem sauberen Active Directory in Schach.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto.
- Git wurde auf einer lokalen Workstation installiert und konfiguriert.
- Terraform wurde auf einer lokalen Workstation installiert und konfiguriert.
- Windows-Computer mit Active Directory-Modulen ()`ActiveDirectory`.
- Ein Verzeichnis in AWS Managed Microsoft AD und Anmeldeinformationen, die in einem Parameter im AWS Systems Manager Parameter Store gespeichert sind.

- AWS Identity and Access Management (IAM) -Rolle mit Berechtigungen für die in Tools AWS-Services aufgelisteten Rollen. Weitere Informationen zu IAM finden Sie unter Verwandte Ressourcen.

Einschränkungen

- Dieses Muster unterstützt keine kontenübergreifende Einrichtung.
- Einige AWS-Services sind nicht in allen AWS-Regionen verfügbar. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie unter Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Produktversionen

- Terraform Version 1.1.9 oder höher
- Terraform AWS Provider Version 3.0 oder höher

Architektur

Das folgende Diagramm zeigt den Workflow und die Architekturkomponenten für dieses Muster.

Das Diagramm zeigt den folgenden Workflow:

1. Amazon EventBridge löst die AWS Lambda Funktion auf der Grundlage eines Cron-Ausdrucks aus. (Bei diesem Muster erfolgt der Zeitplan für Cron-Ausdrücke einmal täglich.)
2. Die erforderliche IAM-Rolle und -Richtlinie werden AWS Lambda über Terraform erstellt und angehängt.
3. Die AWS Lambda Funktion wird ausgeführt und ruft Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Groups mithilfe des Python-Boto-Moduls auf. Die Lambda-Funktion ruft die zufällige Instanz-ID ab. Die Instanz-ID wird zur Ausführung von AWS Systems Manager Befehlen verwendet.
4. AWS Lambda ruft Amazon EC2 mithilfe des Boto-Moduls erneut auf und ruft die privaten IP-Adressen der laufenden Windows-Server ab und speichert die Adressen in einer temporären Variablen.

5. AWS Lambda ruft Systems Manager erneut auf, um die Computerinformationen abzurufen, mit denen eine Verbindung hergestellt ist AWS Directory Service.
6. Ein AWS Systems Manager Dokument hilft dabei, das PowerShell Skript auf Amazon EC2 Windows-Servern auszuführen, um die privaten IP-Adressen der Computer abzurufen, die mit AD verbunden sind.
7. Der Benutzername und die Passwörter der AD-Domain werden im AWS Systems Manager Parameter Store gespeichert. AWS Lambda und Systems Manager rufen Parameter Store auf und rufen die Werte für Benutzername und Passwort ab, die für die Verbindung mit AD verwendet werden sollen.
8. Mithilfe des Systems Manager Manager-Dokuments wird das PowerShell Skript auf dem Amazon EC2 Windows-Server unter Verwendung der zuvor in Schritt 3 abgerufenen Instance-ID ausgeführt.
9. Amazon EC2 stellt mithilfe AWS Directory Service von PowerShell Befehlen eine Verbindung her und entfernt die Computer, die nicht verwendet oder inaktiv sind.

Tools

AWS-Services

- AWS Directory Servicebietet mehrere Möglichkeiten, Microsoft Active Directory (AD) mit anderen AWS-Services wie Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS) für SQL Server und Amazon FSx für Windows File Server zu verwenden.
- AWS Directory Service for Microsoft Active Directoryermöglicht Ihren verzeichnissensitiven Workloads und AWS Ressourcen die Verwendung von Microsoft Active Directory in der. AWS Cloud
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS Lambda Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen. AWS-Konten
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden. Mit IAM können Sie festlegen, wer oder was auf Dienste und Ressourcen

zugreifen kann AWS, detaillierte Berechtigungen zentral verwalten und den Zugriff analysieren, um die Berechtigungen zu verfeinern. AWS

- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Systems Managerhilft Ihnen bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der ausgeführt AWS Cloud werden. Es vereinfacht das Anwendungs- und Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme und hilft Ihnen, Ihre AWS Ressourcen sicher und in großem Umfang zu verwalten.
- AWS Systems Manager Dokumente definieren die Aktionen, die Systems Manager auf Ihren verwalteten Instanzen ausführt. Systems Manager umfasst mehr als 100 vorkonfigurierter Dokumente, die Sie verwenden können, indem Sie zur Laufzeit Parameter angeben.
- AWS Systems Manager Parameter Store ist eine Funktion von AWS Systems Manager und bietet sicheren, hierarchischen Speicher für die Verwaltung von Konfigurationsdaten und Geheimnissen.

Andere Tools

- HashiCorp Terraform ist ein Open-Source-Tool für Infrastruktur als Code (IaC), mit dem Sie mithilfe von Code Cloud-Infrastruktur und -Ressourcen bereitstellen und verwalten können.
- PowerShellist ein Automatisierungs- und Konfigurationsverwaltungsprogramm von Microsoft, das unter Windows, Linux und macOS läuft.
- Python ist eine Allzweck-Computerprogrammiersprache.

C-Code-Repository

Der Code für dieses Muster ist im Lösungs-Repository für GitHub benutzerdefinierte AD Cleanup Automation verfügbar.

Bewährte Methoden

- Automatisch Domänen beitreten.Wenn Sie eine Windows-Instanz starten, die Teil einer AWS Directory Service Domäne sein soll, treten Sie der Domäne während der Instanzerstellung bei, anstatt die Instanz später manuell hinzuzufügen. Um einer Domäne automatisch beizutreten, wählen Sie beim Starten einer neuen Instanz das richtige Verzeichnis aus der Dropdownliste zum Domänenbeitrittsverzeichnis aus. Weitere Informationen finden Sie unter Nahtloses Hinzufügen

einer Amazon EC2 Windows-Instance zu Ihrem AWS Managed Microsoft AD Active Directory im AWS Directory Service Administratorhandbuch.

- Löschen Sie ungenutzte Konten.Es ist üblich, in AD Konten zu finden, die noch nie verwendet wurden. Wie deaktivierte oder inaktive Konten, die im System verbleiben, können vernachlässigte, ungenutzte Konten Ihr AD-System verlangsamen oder Ihr Unternehmen anfällig für Datenschutzverletzungen machen.
- Automatisieren Sie Active Directory-Säuberungen.Um Sicherheitsrisiken zu minimieren und zu verhindern, dass veraltete Konten die AD-Leistung beeinträchtigen, sollten AD-Bereinigungen in regelmäßigen Abständen durchgeführt werden. Sie können die meisten AD-Verwaltungs- und Bereinigungsaufgaben erledigen, indem Sie Skripts schreiben. Zu den Aufgaben gehören beispielsweise das Entfernen deaktivierter und inaktiver Konten, das Löschen leerer und inaktiver Gruppen und das Auffinden abgelaufener Benutzerkonten und Kennwörter.

Epen

So richten Sie Ihre Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Projektor dner und fügen Sie die Dateien hinzu.	Gehen Sie wie folgt vor, um das Repository zu klonen und einen Projektordner zu erstellen: 1. Öffnen Sie das GitHub Repository dieses Musters. 2. Wählen Sie die Code-Schaltfläche, um die Optionen zum Klonen in der Dropdownliste „Klonen“ zu sehen. 3. Kopieren Sie auf der Registerkarte HTTPS die unter Clone angegebene URL mithilfe der Web-URL.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	4. Erstellen Sie einen Ordner auf Ihrem Computer und benennen Sie ihn mit Ihrem Projektnamen.
	5. Öffnen Sie ein Terminal auf Ihrem lokalen Computer und navigieren Sie zu diesem Ordner.
	6. Verwenden Sie den folgenden Befehl, um das Git-Repository zu klonen.
	`git clone <repository-URL>.git`
	7. Nachdem das Repository geklont wurde, verwenden Sie den folgenden Befehl, um zum geklonten Verzeichnis zu wechseln.
	`cd <directory name>`
	8. Öffnen Sie dieses Projekt im geklonten Repository in einer integrierten Entwicklungsumgebung (IDE) Ihrer Wahl.	

Stellen Sie die Zielarchitektur mithilfe der Terraform-Konfiguration bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initialisieren Sie die Terraform-Konfiguration.	Führen Sie den folgenden Befehl aus, um Ihr Arbeitsve	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	rzeichnis zu initialisieren, das die Terraform-Dateien enthält. `terraform init`	
Änderungen in der Vorschau anzeigen.	Sie können eine Vorschau der Änderungen anzeigen, die Terraform an der Infrastruktur vornehmen wird, bevor Ihre Infrastruktur bereitgestellt wird. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob Terraform die Änderungen nach Bedarf vornimmt. `terraform plan`	DevOps Ingenieur
Führen Sie die vorgeschl agenen Aktionen aus.	Gehen Sie wie folgt vor, um zu überprüfen, ob die Ergebniss e des `terraform plan` Befehls den Erwartungen entsprechen: 1. Führen Sie den folgenden Befehl aus. `terraform apply` 2. Melden Sie sich bei der an AWS Management Console, und stellen Sie sicher, dass die Ressource n vorhanden sind.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Säubere die Infrastruktur.	Verwenden Sie den folgenden Befehl, um die von Ihnen erstellte Infrastruktur zu bereinigen. `terraform destroy` Geben Sie ein, um den Befehl destroy zu bestätigen`yes`.	DevOps Ingenieur

Überprüfen der Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Lambda-Funktion aus und testen Sie sie.	Gehen Sie wie folgt vor, um zu überprüfen, ob die Bereitstellung erfolgreich durchgeführt wurde: 1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Konsole. Öffnen Sie die Seite Funktionen und wählen Sie den Funktionsnamen aus, der mit ADcleanup-Lambda-* beginnt. 2. Wählen Sie auf der Funktionsübersichtsseite auf der Registerkarte Code im Abschnitt Codequelle die Option Test aus. 3. Um das Testereignis zu speichern, geben Sie einen	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Namen für das Ereignis ein und wählen Sie Speichern. Um das Ereignis zu testen, wählen Sie dann erneut Testen aus. Die Ausführungsergebnisse zeigen die Ausgabe der Funktion.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich die Ergebnisse der Lambda-Funktion an.	In diesem Muster führt eine EventBridge Regel die Lambda-Funktion einmal täglich aus. Gehen Sie wie folgt vor, um die Ergebniss e der Lambda-Funktion anzuzeigen: 1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Lambda Konsole. Öffnen Sie die Seite Funktione n und wählen Sie den Funktionsnamen aus, der mit ADcleanup-Lambda-* beginnt. 2. Wählen Sie die Registerk arte „Überwachen“ und dann „Protokolle anzeigen“. CloudWatch In der CloudWatch Konsole werden auf der Seite Protokoll gruppen die Ergebnisse der Lambda-Funktion angezeigt.	DevOps Ingenieur

Reinigen Sie die Infrastruktur nach dem Gebrauch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Infrastruktur aufräumen.	Verwenden Sie den folgenden Befehl, um die von Ihnen	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	erstellte Infrastruktur zu bereinigen. `terraform destroy` Geben Sie ein, um den Befehl destroy zu bestätigen`yes`.	
Nach der Säuberung überprüfen.	Stellen Sie sicher, dass die Ressourcen erfolgreich entfernt wurden.	DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Wenn Sie versuchen, den AD-Computer zu entfernen, erhalten Sie die Meldung „Zugriff verweigert“. Der AD-Computer kann nicht entfernt werden, da die Aktion standardm äßig versucht, zwei private IP-Adressen zu entfernen, die als Teil der AD-Dienste miteinander verbunden sind.	Um diesen Fehler zu vermeiden, verwenden Sie den folgenden Python-Vorgang, um die ersten beiden Computer zu ignorieren, wenn Sie die Unterschiede zwischen einer AD-Computerausgabe und der Ausgabe Ihres Computers auflisten, auf dem Windows ausgeführt wird. `Difference = Difference[2:]`
Wenn Lambda ein PowerShell Skript auf einem Windows-Server ausführt, erwartet es, dass Active Directory-Module standardm äßig verfügbar sind. Wenn die Module nicht verfügbar sind, erzeugt eine Lambda-Fu nktion einen Fehler, der besagt, dass „Get-AdComputer ist nicht auf der Instanz installiert“.	Um diesen Fehler zu vermeiden, installieren Sie die erforderlichen Module mithilfe der Benutzerdaten der EC2 Instanzen. Verwenden Sie das EC2WindowsUserdataSkript, das sich im GitHub Repository dieses Musters befindet.

Zugehörige Ressourcen

AWS Dokumentation

- Amazon EventBridge und AWS Identity and Access Management
- Erforderliche Instance-Berechtigungen für Systems Manager konfigurieren
- Identitäts- und Zugriffsmanagement für AWS Directory Service
- Manuelles Hinzufügen einer Amazon EC2 Windows-Instance zu Ihrem AWS Managed Microsoft AD Active Directory
- Arbeiten mit identitätsbasierten IAM-Richtlinien in AWS Lambda

Sonstige Ressourcen

- AWS Anbieter (Terraform-Dokumentation)
- Backend-Konfiguration (Terraform-Dokumentation)
- Installieren Sie Terraform (Terraform-Dokumentation)
- Python-Boto-Modul (Python-Paketindex-Repository)
- Laden Sie die Terraform-Binärdatei herunter (Terraform-Dokumentation)

Führen Sie Komponententests für Python-ETL-Jobs AWS Glue mithilfe des Pytest-Frameworks aus

Erstellt von Praveen Kumar Jeyarajan (AWS) und Vaidy Sankaran (AWS)

Übersicht

Sie können Komponententests für Python-Jobs zum Extrahieren, Transformieren und Laden (ETL) für AWS Glue in einer lokalen Entwicklungsumgebung ausführen, aber das Replizieren dieser Tests in einer DevOps Pipeline kann schwierig und zeitaufwändig sein. Unit-Tests können besonders schwierig sein, wenn Sie den Mainframe-ETL-Prozess auf AWS Technologie-Stacks modernisieren. Dieses Muster zeigt Ihnen, wie Sie Komponententests vereinfachen und gleichzeitig die bestehende Funktionalität beibehalten, Unterbrechungen wichtiger Anwendungsfunktionen bei der Veröffentlichung neuer Funktionen vermeiden und hochwertige Software beibehalten können. Sie können die Schritte und Codebeispiele in diesem Muster verwenden, um Komponententests für Python-ETL-Jobs auszuführen, AWS Glue indem Sie das Pytest-Framework in AWS CodePipeline verwenden. Sie können dieses Muster auch verwenden, um mehrere AWS Glue Jobs zu testen und bereitzustellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Eine Amazon Elastic Container Registry (Amazon ECR) -Image-URI für Ihre AWS Glue Bibliothek, heruntergeladen von der Amazon ECR Public Gallery
- Bash-Terminal (auf jedem Betriebssystem) mit einem Profil für das Ziel und AWS-Konto AWS-Region
- Python 3.10 oder höher
- Pytest
- Moto-Python-Bibliothek zum Testen AWS-Services

Architektur

Das folgende Diagramm beschreibt, wie Komponententests für AWS Glue ETL-Prozesse, die auf Python basieren, in eine typische Pipeline auf Unternehmensebene AWS DevOps integriert werden können.

Das Diagramm zeigt den folgenden Workflow:

1. AWS CodePipeline Verwendet in der Quellphase einen versionierten Amazon Simple Storage Service (Amazon S3) -Bucket zum Speichern und Verwalten von Quellcode-Assets. Zu diesen Ressourcen gehören ein Beispiel für einen Python-ETL-Job (`sample.py`), eine Unit-Test-Datei (`test_sample.py`) und eine AWS CloudFormation Vorlage. CodePipeline Überträgt dann den neuesten Code aus dem Hauptzweig zur weiteren Verarbeitung in das AWS CodeBuild Projekt.
2. In der Erstellungs- und Veröffentlichungsphase wird der neueste Code aus der vorherigen Quellphase mithilfe eines AWS Glue öffentlichen Amazon ECR-Images auf Einheiten getestet. Anschließend wird der Testbericht für CodeBuild Berichtsgruppen veröffentlicht. Das Container-Image im öffentlichen Amazon ECR-Repository für AWS Glue Bibliotheken enthält alle Binärdateien, die für die lokale Ausführung und auf Unit-Tests PySparkbasierende ETL-Aufgaben erforderlich sind. AWS Glue Das öffentliche Container-Repository hat drei Image-Tags, einen für jede Version, die von unterstützt wird. AWS Glue Zu Demonstrationszwecken verwendet dieses Muster das `glue_libs_4.0.0_image_01` Image-Tag. Um dieses Container-Image als Runtime-Image zu verwenden CodeBuild, kopieren Sie den Image-URI, der dem Image-Tag entspricht, den Sie verwenden möchten, und aktualisieren Sie dann die `pipeline.yml` Datei im GitHub Repository für die `TestBuild` Ressource.
3. In der Bereitstellungsphase wird das CodeBuild Projekt gestartet und der Code wird in einem Amazon S3 S3-Bucket veröffentlicht, wenn alle Tests erfolgreich sind.
4. Der Benutzer stellt die AWS Glue Aufgabe mithilfe der CloudFormation Vorlage im `deploy` Ordner bereit.

Tools

AWS-Services

- AWS CodeBuildist ein vollständig verwalteter Build-Service, der Sie beim Kompilieren von Quellcode, beim Ausführen von Komponententests und beim Erstellen bereitgestellter Artefakte unterstützt.
- AWS CodePipelinehilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.

- AWS Glueist ein vollständig verwalteter ETL-Service. Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben.
- Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice, der branchenführende Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet.

Andere Tools

- Python ist eine interpretierte Mehrzweck-Programmiersprache auf hohem Niveau.
- Moto ist eine Python-Bibliothek zum Testen AWS-Services.
- Pytest ist ein Framework zum Schreiben kleiner Komponententests, die skaliert werden können, um komplexe Funktionstests für Anwendungen und Bibliotheken zu unterstützen.
- Die Python-ETL-Bibliothek für AWS Glue ist ein Repository für Python-Bibliotheken, die bei der lokalen Entwicklung von PySpark Batch-Jobs für verwendet werden AWS Glue.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub aws-glue-jobs-unit-testing verfügbar. Das Repository umfasst die folgenden Ressourcen:

- Ein Beispiel für einen Python-basierten AWS Glue Job im Ordner `src`
- Zugeordnete Unit-Testfälle (erstellt mit dem Pytest-Framework) im Ordner `tests`
- Eine CloudFormation Vorlage (in YAML geschrieben) im Ordner `deploy`

Bewährte Methoden

Sicherheit für Ressourcen CodePipeline

Es hat sich bewährt, Verschlüsselung und Authentifizierung für die Quell-Repositorys zu verwenden, die eine Verbindung zu Ihren Pipelines herstellen. CodePipeline Weitere Informationen finden Sie in der Dokumentation unter Bewährte Sicherheitsmethoden. CodePipeline

CodePipeline Ressourcen überwachen und protokollieren

Es hat sich bewährt, mithilfe von AWS Protokollierungsfunktionen zu ermitteln, welche Aktionen Benutzer in Ihrem Konto ausführen und welche Ressourcen sie verwenden. Die Protokolldateien zeigen Folgendes:

- Uhrzeit und Datum der Aktionen
- Quell-IP-Adresse der Aktionen
- Welche Aktionen sind aufgrund unzureichender Berechtigungen fehlgeschlagen

Protokollierungsfunktionen sind in Amazon Events AWS CloudTrail und Amazon CloudWatch Events verfügbar. Sie können CloudTrail damit AWS API-Aufrufe und verwandte Ereignisse protokollieren, die von oder in Ihrem Namen getätigt wurden AWS-Konto. Weitere Informationen finden Sie AWS CloudTrail in der CodePipeline Dokumentation unter Protokollieren von CodePipeline API-Aufrufen mit.

Sie können CloudWatch Ereignisse verwenden, um Ihre AWS Cloud Ressourcen und Anwendungen zu überwachen, auf denen sie ausgeführt AWS werden. Sie können auch Benachrichtigungen unter CloudWatch Ereignisse erstellen. Weitere Informationen finden Sie in der CodePipeline Dokumentation unter CodePipeline Ereignisse überwachen.

Epen

Stellen Sie den Quellcode bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie das Codearchiv für die Bereitstellung vor.	1. Laden Sie es `code.zip` aus dem GitHub aws-glue-jobs-unit-testing Repository herunter, oder erstellen Sie die .zip-Datei selbst mithilfe eines Befehlszeilentools. Sie können die .zip-Datei beispielsweise unter Linux oder Mac erstellen, indem Sie die folgenden Befehle im Terminal ausführen: `git clone https://github.com/aws-samples/aws-glue-jobs-unit-testing.git`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>cd aws-glue-jobs-
	unit-testing
	git checkout master
	zip -r code.zip src/
	 tests/ deploy/</pre>
	2. Melden Sie sich bei der an AWS Management Consoleund wählen Sie die Option AWS-Region Ihrer Wahl aus.
	3. Erstellen Sie einen Amazon S3 S3-Bucket und laden Sie dann das ZIP-Paket und die `code.zip` Datei (zuvor heruntergeladen) in den Amazon S3 S3-Bucket hoch, den Sie erstellt haben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den CloudFormation Stapel.	1. Melden Sie sich bei der an AWS Management Console und öffnen Sie dann die CloudFormation Konsole. 2. Wählen Sie Stack erstellen und anschließend Mit vorhandenen Ressourcen (Ressourcen importieren) aus. 3. Wählen Sie auf der Seite „Stack erstellen “ im Abschnitt „Vorlage angeben“ die Option „Eine Vorlagendatei hochladen “ und dann die Vorlage „pipeline.yml“ (aus dem Repository heruntergeladen) aus. GitHub Wählen Sie anschließend Weiter. 4. Geben Sie als Stack-Name einen Stack-Namen Ihrer Wahl ein glue-unit-testing-pipeline, oder wählen Sie einen aus. 5. Verwenden Sie für ApplicationStackNameden bereits ausgefüllten glue-code pipeline-appNamen. Dies ist der Name des CloudFormation Stacks, der von der Pipeline erstellt wird.	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Verwenden Sie für BucketNameden bereits ausgefüllten Bucket-Namen aws-glue-artifacts-us-east-1. Dies ist der Name des Amazon S3 S3-Buckets, der die .zip-Datei enthält und von der Pipeline zum Speichern von Codeartef akten verwendet wird. 7. Verwenden Sie für CodeZipFileden vorab ausgefüllten Wert code.zip. Dies ist der Schlüsselname des Amazon S3 S3-Beispi elcode-Objekts. Das Objekt sollte eine ZIP-Datei sein. 8. Verwenden Sie für TestReportGroupNameden bereits ausgefüllten Namen glue-unittest-report. Dies ist der Name der CodeBuild Testberichtsgruppe, die zum Speichern der Unit-Testberichte erstellt wurde. 9. Wählen Sie Weiter und klicken Sie dann auf der Seite Stack-Optionen konfigurieren erneut auf Weiter. 10. Wählen Sie auf der Seite Überprüfen unter Funktione n die Option Ich bestätige , dass CloudFormation	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	möglicherweise IAM-Ressourcen mit benutzerdefinierten Namen erstellt werden. 11. Wählen Sie Absenden aus. Nachdem die Erstellung des Stacks abgeschlossen ist, können Sie die erstellten Ressourcen auf der Registerkarte Ressourcen sehen. Die Erstellung des Stacks dauert ungefähr 5-7 Minuten. Der Stack erstellt eine CodePipeline Ansicht mit Amazon S3 als Quelle. In den obigen Schritten lautet die Pipeline aws-glue-unit-test-pipeline.	

Führen Sie die Komponententests aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die in der Pipeline befindlichen Komponententests aus.	1. Um die bereitgestellte Pipeline zu testen, melden Sie sich bei der AWS Management Console an und öffnen Sie dann die CodePipeline Konsole. 2. Wählen Sie die Pipeline aus, die durch den CloudFormation Stack erstellt wurde, und klicken	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie dann auf Änderung veröffentlichen. Die Pipeline wird gestartet (mit dem neuesten Code im Amazon S3 S3-Bucket). 3. Nachdem die Test_and_ Build-Phase abgeschlo ssen ist, wählen Sie die Registerkarte Details und überprüfen Sie dann die Protokolle. 4. Wählen Sie die Registerk arte Berichte und dann unter Berichtsverlauf den Testbericht aus, um die Ergebnisse der Komponent entests anzuzeigen. 5. Führen Sie nach Abschluss der Bereitstellungspha se den bereitgestellten AWS Glue Job auf der AWS Glue Konsole aus und überwachen Sie ihn. Weitere Informationen finden Sie AWS Glue in der AWS Glue Dokumentation unter Überwachung.	

Säubere alle AWS Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Säubern Sie die Ressourcen in Ihrer Umgebung.	Um zusätzliche Infrastru kturkosten zu vermeiden,	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	stellen Sie sicher, dass Sie den Stack löschen, nachdem Sie mit den Beispielen in diesem Muster experimentiert haben. 1. Öffnen Sie die CloudFormation Konsole und wählen Sie dann den Stack aus, den Sie erstellt haben. 2. Wählen Sie Löschen aus. Dadurch werden alle Ressourcen gelöscht, die Ihr Stack erstellt hat, einschließlich AWS Identity and Access Management (IAM-) Rollen, IAM-Richtlinien und Projekte. CodeBuild	

Fehlerbehebung

Problem	Lösung
Die CodePipeline Servicerolle kann nicht auf den Amazon S3 S3-Bucket zugreifen.	• Fügen `s3:ListBucket` Sie die mit Ihrer CodePipeline Servicerolle verknüpfte Richtlinie der Liste der Aktionen in Ihrer Richtlinie hinzu. Anweisungen zum Anzeigen der Servicerollenrichtlinie finden Sie unter Pipeline-ARN und Dienstrollen-ARN (Konsole) anzeigen. Bearbeiten Sie die Richtlinienerklärung für Ihre Servicerolle, wie unter Berechtigungen zur CodePipeline Servicerolle hinzufügen beschrieben.

Problem	Lösung
	• Fügen Sie für die ressourcenbasierte Richtlinie, die an den Amazon S3 S3-Artefakt-Bucket für Ihre Pipeline angehängt ist, auch Artifact-Bucket-Richtlinie genannt, eine Anweisung hinzu, die es der CodePipeline Servicerolle ermöglicht, die Berechtigung zu verwenden. `s3:ListBucket`
CodePipeline gibt einen Fehler zurück, dass der Amazon S3 S3-Bucket nicht versioniert ist.	CodePipeline erfordert, dass der Amazon S3 S3-Quell-Bucket versioniert ist. Aktivieren Sie die Versionierung in Ihrem Amazon S3 S3-Bucket. Anweisungen finden Sie unter Versionierung für Buckets aktivieren.

Zugehörige Ressourcen

- AWS Glue
- Jobs lokal entwickeln und testen AWS Glue
- AWS CloudFormation für AWS Glue

Zusätzliche Informationen

Darüber hinaus können Sie die AWS CloudFormation Vorlagen mithilfe von AWS Command Line Interface (AWS CLI) bereitstellen. Weitere Informationen finden Sie in der CloudFormation Dokumentation unter Schnelles Bereitstellen von Vorlagen mit Transformationen.

Richten Sie ein Helm v3-Chart-Repository in Amazon S3 ein

Erstellt von Abhishek Sharma (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Dieses Muster hilft Ihnen, Helm v3-Diagramme effizient zu verwalten, indem Sie das Helm v3-Repository in Amazon Simple Storage Service (Amazon S3) in der Amazon Web Services (AWS) Cloud integrieren. Um dieses Muster verwenden zu können, müssen Sie mit Kubernetes und Helm, einem Kubernetes-Paketmanager, vertraut sein. Die Verwendung von Helm-Repositorys zum Speichern von Diagrammen und zur Steuerung von Diagrammversionen kann die mittlere Wiederherstellungszeit (MTTR) bei Ausfällen verbessern.

Dieses Muster verwendet AWS CodeCommit für die Erstellung von Helm-Repositorys und verwendet einen S3-Bucket als Helm-Diagramm-Repository, sodass die Diagramme zentral verwaltet und von Entwicklern im gesamten Unternehmen abgerufen werden können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Python-Version 2.7.12 oder höher
- pip
- Eine virtuelle private Cloud (VPC) mit Subnetzen und einer Amazon Elastic Compute Cloud (Amazon) -Instanz EC2
- Git ist auf der EC2 Instanz installiert
- Zugriff auf AWS Identity and Access Management (IAM) zur Erstellung des S3-Buckets
- IAM-Zugriff (programmatischer oder Rollenzugriff) auf Amazon S3 vom Client-Computer
- CodeCommit AWS-Repository
- AWS-Befehlszeilenschnittstelle (AWS Command Line Interface, AWS CLI)

Produktversionen

- Helm v3

- Python-Version 2.7.12 oder höher

Architektur

Zieltechnologie-Stack

- Amazon S3
- AWS CodeCommit
- Helm
- Kubectl
- Python und Pip
- Git
- Helm-S3-Plugin

Zielarchitektur

Automatisierung und Skalierung

- Sie können Helm in Ihr bestehendes (kontinuierlichesintegration/continuous delivery (CI/CD) Automatisierungstool integrieren, um die Paketierung und Versionskontrolle von Helm-Diagrammen zu automatisieren (außerhalb des Geltungsbereichs dieses Musters).
- GitVersion oder Jenkins-Build-Nummern können verwendet werden, um die Versionskontrolle der Charts zu automatisieren.

Tools

- Helm — Helm ist ein Paketmanager für Kubernetes, der Sie bei der Installation und Verwaltung von Anwendungen auf Ihrem Kubernetes-Cluster unterstützt.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Speicher für das Internet. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen.
- helm-S3-Plugin — Das helm-S3-Plugin unterstützt die Interaktion mit Amazon S3. Es kann entweder mit Helm v2 oder Helm v3 verwendet werden.

Epen

Installieren und validieren Sie Helm v3

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den Helm v3-Client.	Führen Sie den folgenden Befehl aus, um den Helm-Client herunterzuladen und auf Ihrem lokalen System zu installieren: `sudo curl https://raw.githubusercontent.com/helm/helm/main/scripts/get-helm-3 | bash`	Cloud-Administrator, DevOps Ingenieur
Validieren Sie die Helm-Installation.	Führen Sie den folgenden Befehl aus, um den Helm-Client zu validieren: `helm version --short`	Cloud-Administrator, DevOps Ingenieur

Initialisieren Sie einen S3-Bucket als Helm-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket für Helm-Charts.	Erstellen Sie einen eindeutigen S3-Bucket. Erstellen Sie im Bucket einen Ordner mit dem Namen `stable/myapp` . Das Beispiel in diesem Muster verwendet `s3://my-helm-charts/stable/myapp` als Zieldiagramm-Repository.	Cloud-Administrator, DevOps Ingenieur
Installieren Sie das Helm-S3-Plugin für Amazon S3.	Führen Sie den folgenden Befehl aus, um das Helm-S3-Plugin auf Ihrem Client-	Cloud-Administrator, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Computer zu installieren: `helm plugin install https://github.com/hypnoglow/helm-s3.git`	
Initialisieren Sie das Amazon S3 Helm-Repository.	Verwenden Sie den folgenden Befehl, um den Zielordner als Helm-Repository zu initialisieren: `helm s3 init s3://my-helm-charts/stable/myapp` Der Befehl erstellt eine `index.yaml` Datei im Ziel, um alle Diagramminformationen zu verfolgen, die an diesem Speicherort gespeichert sind.	Cloud-Administrator, DevOps Ingenieur
Überprüfen Sie das neu erstellte Helm-Repository.	Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die `index.yaml` Datei erstellt wurde: `aws s3 ls s3://my-helm-charts/stable/myapp/`	Cloud-Administrator, DevOps Ingenieur
Fügen Sie das Amazon S3 S3-Repository zu Helm auf dem Client-Computer hinzu.	Verwenden Sie den folgenden Befehl, um den Ziel-Repository-Alias zum Helm-Client-Computer hinzuzufügen: `helm repo add stable-myapp s3://my-helm-charts/stable/myapp/`	Cloud-Administrator, DevOps Ingenieur

Verpacken und veröffentlichen Sie Diagramme im Amazon S3 Helm-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie Ihre Helm-Charts.	Wenn in Ihrem CodeCommit Repository keine lokalen Helm-Charts vorhanden sind, klonen Sie sie aus Ihrem GitHub Repo, indem Sie den folgenden Befehl ausführen: `git clone <url_of_your_helm_source_code>.git`	Cloud-Administrator, Ingenieur DevOps
Package Sie die lokale Helm-Karte.	Verwenden Sie den folgenden Befehl, um das Diagramm, das Sie erstellt oder geklont haben, zu verpacken: `helm package ./my-app` Als Beispiel verwendet dieses Muster das `my-app` Diagramm. Der Befehl packt den gesamten Inhalt des `my-app` Diagrammordners in eine Archivdatei, die anhand der Versionsnummer benannt wird, die in der `Chart.yaml` Datei angegeben ist.	Cloud-Administrator, DevOps Ingenieur
Speichern Sie das lokale Paket im Amazon S3 Helm-Repository.	Führen Sie den folgenden Befehl aus, um das lokale Paket in das Helm-Repository in Amazon S3 hochzuladen: `helm s3 push ./my-app-0.1.0.tgz stable-myapp`	Cloud-Administrator, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	In dem Befehl `my-app` steht der Name Ihres Diagrammordners, `0.1.0` die unter erwähnte Diagrammversion und der Alias für `stable-myapp` das Ziel-Repository. `Chart.yaml`	
Suchen Sie nach dem Helm-Diagramm.	Um zu überprüfen, ob das Diagramm sowohl lokal als auch im Amazon S3 Helm-Repository angezeigt wird, führen Sie den folgenden Befehl aus: `helm search repo stable-myapp`	Cloud-Administrator, DevOps Ingenieur

Aktualisieren Sie Ihr Helm-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern und verpacken Sie das Diagramm.	Legen Sie den `replicaCount` Wert auf fest1, und verpacken Sie dann das Diagramm, wobei Sie diesmal die Version in `Chart.yaml` ändern`0.1.1`. `values.yaml` Die Versionskontrolle wird idealerweise durch Automatisierung erreicht, indem Tools wie GitVersion oder Jenkins-Build-Nummern in einer CI/CD-Pipeline verwendet werden. Die Automatisierung der Versionsn	Cloud-Administrator, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ummer ist für dieses Muster nicht vorgesehen. Führen Sie den folgenden Befehl aus, um das Diagramm zu verpacken: `helm package ./my-app/`	
Pushen Sie die neue Version in das Helm-Repository in Amazon S3.	Führen Sie den folgenden Befehl aus, um das neue Paket, Version 0.1.1, in das my-helm-chartsHelm-Repository in Amazon S3 zu übertragen: `helm s3 push ./my-app-0.1.1.tgz stable-myapp`	Cloud-Administrator, Ingenieur DevOps

Überprüfen Sie das aktualisierte Helm-Diagramm.	Führen Sie die folgenden Befehle aus, um zu überprüfen, ob das aktualisierte Diagramm sowohl lokal als auch im Amazon S3 Helm-Repository angezeigt wird.
	`helm repo update`
	`helm search repo stable-myapp`
		Cloud-Administrator, DevOps Ingenieur

Suchen und installieren Sie ein Diagramm aus dem Amazon S3 Helm-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Suchen Sie nach allen Versionen des my-app-Diagramms.	Um alle verfügbaren Versionen eines Diagramms anzuzeigen, führen Sie den folgenden Befehl mit der `--versions` Markierung aus: `helm search repo my-app --versions` Ohne die Markierung zeigt Helm standardmäßig die zuletzt hochgeladene Version eines Diagramms an.	DevOps Ingenieur
Installieren Sie ein Diagramm aus dem Amazon S3 Helm-Repository.	Eine automatische Installation ist für dieses Muster nicht vorgesehen, aber Sie können die Installation manuell durchführen. Die Suchergebnisse der vorherigen Aufgabe zeigen die verschiedenen Versionen des `my-app` Diagramms. Verwenden Sie den folgenden Befehl, um die neue Version (0.1.1) aus dem Amazon S3 Helm-Repository zu installieren: `helm upgrade --install my-app-release stable-myapp/my-app --version 0.1.1 --namespace dev`	DevOps Ingenieur

Gehen Sie mithilfe von Helm zu einer früheren Version zurück

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Details für eine bestimmte Revision.	Ein automatisiertes Rollback ist für dieses Muster nicht vorgesehen, aber Sie können manuell zu einer früheren Version zurückkehren. Bevor Sie zu einer funktionierenden Version wechseln oder ein Rollback durchführen und für eine zusätzliche Überprüfungsebene vor der Installation einer Revision, sollten Sie mit dem folgenden Befehl überprüfen, welche Werte an die einzelnen Versionen übergeben wurden: `helm get values --revision=2 my-app-release`	DevOps Ingenieur
Führen Sie einen Rollback zu einer früheren Version durch.	Ein automatisiertes Rollback ist für dieses Muster nicht vorgesehen. Verwenden Sie den folgenden Befehl, um manuell zu einer früheren Version zurückzukehren: `helm rollback my-app-release 1` In diesem Beispiel wird auf Version 1 zurückgesetzt.	DevOps Ingenieur

Zugehörige Ressourcen

- HELM-Dokumentation

- helm-S3-Plugin (MIT-Lizenz)
- Amazon S3

Richten Sie eine CI/CD-Pipeline mithilfe von AWS CodePipeline und AWS CDK ein

Erstellt von Konstantin Zarudaev (AWS), Cizer Pereira (AWS), Lars Kinder (AWS) und Yasha Dabas (AWS)

Startseite

Hinweis: ist für Neukunden nicht mehr verfügbar. AWS CodeCommit Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen Die Automatisierung Ihres Softwareerstellungs- und -veröffentlichungsprozesses mit kontinuierlicher Integration und kontinuierlicher Bereitstellung (CI/CD) supports repeatable builds and rapid delivery of new features to your users. You can quickly and easily test each code change, and you can catch and fix bugs before releasing your software. By running each change through your staging and release process, you can verify the quality of your application or infrastructure code. CI/CDverkörpert eine Kultur, eine Reihe von Betriebsprinzipien und eine Sammlung von Praktiken), die Anwendungsentwicklungsteams dabei unterstützen, Codeänderungen häufiger und zuverlässiger vorzunehmen. Die Implementierung wird auch als CI/CD-Pipeline bezeichnet.

Dieses Muster definiert eine wiederverwendbare Pipeline für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) auf Amazon Web Services (AWS) mit einem CodeCommit AWS-Repository. Die CodePipeline AWS-Pipeline wurde mit dem AWS Cloud Development Kit (AWS CDK) v2 geschrieben.

Mithilfe CodePipeline können Sie die verschiedenen Phasen Ihres Softwareveröffentlichungsprozesses über die AWS-Managementkonsole, die AWS-Befehlszeilenschnittstelle (AWS CLI) CloudFormation, AWS oder AWS modellieren SDKs. Dieses Muster demonstriert die Implementierung von CodePipeline und seine Komponenten mithilfe von AWS CDK. Zusätzlich zu den Construct-Bibliotheken enthält AWS CDK ein Toolkit (den CLI-Befehl`cdk`), das wichtigste Tool für die Interaktion mit Ihrer AWS-CDK-App. Das Toolkit bietet unter anderem die Möglichkeit, einen oder mehrere Stacks in CloudFormation Vorlagen zu konvertieren und sie auf einem AWS-Konto bereitzustellen.

Die Pipeline umfasst Tests zur Überprüfung der Sicherheit Ihrer Drittanbieter-Bibliotheken und trägt dazu bei, eine beschleunigte, automatisierte Veröffentlichung in den angegebenen Umgebungen sicherzustellen. Sie können die Gesamtsicherheit Ihrer Anwendungen erhöhen, indem Sie sie einem Validierungsprozess unterziehen.

Ziel dieses Musters ist es, die Verwendung von CI/CD-Pipelines zur Bereitstellung Ihres Codes zu beschleunigen und gleichzeitig sicherzustellen, dass die von Ihnen bereitgestellten Ressourcen den Best Practices entsprechen DevOps . Nachdem Sie den Beispielcode implementiert haben, verfügen Sie über ein AWS CodePipeline mit Linting-, Test-, Sicherheitscheck-, Bereitstellungs- und Nachbereitstellungsprozessen. Dieses Muster beinhaltet auch Schritte für Makefile. Mithilfe eines Makefiles können Entwickler CI/CD-Schritte lokal reproduzieren und so den Entwicklungsprozess beschleunigen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein grundlegendes Verständnis im Folgenden:
  - AWS-CDK
  - AWS CloudFormation
  - AWS CodePipeline
  - TypeScript

Einschränkungen

Dieses Muster verwendet AWS CDK TypeScript nur für. Andere Sprachen, die von AWS CDK unterstützt werden, werden nicht abgedeckt.

Produktversionen

Verwenden Sie die neuesten Versionen der folgenden Tools:

- AWS-Befehlszeilenschnittstelle (AWS Command Line Interface, AWS CLI)
- cfn_nag
- git-remote-codecommit
- Node.js

Architektur

Zieltechnologie-Stack

- AWS-CDK
- AWS CloudFormation
- AWS CodeCommit
- AWS CodePipeline

Zielarchitektur

Die Pipeline wird durch eine Änderung im CodeCommit AWS-Repository (`SampleRepository`) ausgelöst. Zu Beginn CodePipeline erstellt es Artefakte, aktualisiert sich selbst und startet den Bereitstellungsprozess. Die daraus resultierende Pipeline stellt eine Lösung für drei unabhängige Umgebungen bereit:

- Dev — Dreistufiger Codecheck in der aktiven Entwicklungsumgebung
- Test — Integrations- und Regressionstestumgebung
- Prod — Produktionsumgebung

Die Entwicklungsphase umfasst drei Schritte: Linting, Sicherheit und Komponententests. Diese Schritte laufen parallel ab, um den Prozess zu beschleunigen. Um sicherzustellen, dass die Pipeline nur funktionierende Artefakte bereitstellt, wird sie beendet, sobald ein Schritt im Prozess fehlschlägt. Nach einer Bereitstellung in der Entwicklungsphase führt die Pipeline Validierungstests durch, um die Ergebnisse zu überprüfen. Im Erfolgsfall stellt die Pipeline die Artefakte dann in der Testumgebung bereit, die die Validierung nach der Bereitstellung beinhaltet. Der letzte Schritt besteht darin, die Artefakte in der Prod-Umgebung bereitzustellen.

Das folgende Diagramm zeigt den Arbeitsablauf vom CodeCommit Repository bis zu den Build- und Aktualisierungsprozessen CodePipeline, die drei Schritte der Entwicklungsumgebung und die anschließende Bereitstellung und Validierung in jeder der drei Umgebungen.

Tools

AWS-Services

- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen

hinweg zu verwalten. In diesem Muster können CloudFormation Vorlagen verwendet werden, um ein CodeCommit Repository und eine CodePipeline CI/CD-Pipeline zu erstellen.

- AWS CodeCommit ist ein Versionskontrollservice, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodePipeline ist ein CI/CD-Service, der Ihnen hilft, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

Andere Tools

- cfn_nag ist ein Open-Source-Tool, das in CloudFormation Vorlagen nach Mustern sucht, um potenzielle Sicherheitsprobleme zu identifizieren.
- git-remote-codecommitist ein Hilfsprogramm zum Pushen und Abrufen von Code aus CodeCommit Repositorys, indem es Git erweitert.
- Node.js ist eine ereignisgesteuerte JavaScript Laufzeitumgebung, die für die Erstellung skalierbarer Netzwerkanwendungen konzipiert wurde.

Code

Der Code für dieses Muster ist im GitHub AWS CodePipeline with CI/CD Practices Repository verfügbar.

Bewährte Methoden

Überprüfen Sie Ressourcen wie die Richtlinien von AWS Identity and Access Management (IAM), um sicherzustellen, dass sie mit den bewährten Methoden Ihres Unternehmens übereinstimmen.

Epen

Tools installieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Tools auf macOS oder Linux.	Wenn Sie macOS oder Linux verwenden, können Sie die	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Tools installieren, indem Sie den folgenden Befehl in Ihrem bevorzugten Terminal ausführen oder Homebrew für Linux verwenden.
	
	`brew install`
	`brew install git-remote-codecommit`
	`brew install ruby brew-gem`
	`brew-gem install cfn-nag`	

Richten Sie die AWS-CLI ein.	Verwenden Sie die Anweisungen für Ihr Betriebssystem, um AWS CLI einzurichten: • Windows: Einrichtungsschritte für HTTPS-Verbindungen zu CodeCommit AWS-Repositorys unter Windows mit dem AWS CLI Credential Helper • Linux, macOS, Unix: Einrichtungsschritte für HTTPS-Verbindungen zu CodeCommit AWS-Repositorys unter Linux, macOS oder Unix mit dem AWS CLI Credential Helper	DevOps Ingenieur

Richten Sie die erste Bereitstellung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Laden Sie den Code herunter oder klonen Sie ihn.	Gehen Sie wie folgt vor, um den Code abzurufen, der von diesem Muster verwendet wird:
	• Laden Sie den neuesten Quellcode aus den Releases im GitHub Repo herunter und entpacken Sie die heruntergeladene Datei in einen Ordner.
	• Klonen Sie das Projekt, indem Sie den folgenden Befehl ausführen.
	`git clone --depth 1 https://github.com/aws-samples/aws-codepipeline-cicd.git`
	Entfernen Sie das `.git` Verzeichnis aus dem geklonten Repository.
	`cd ./aws-codepipeline-cicd`
	`rm -rf ./.git`
	Später werden Sie ein neu erstelltes CodeCommit AWS-Repository als Remote-Ursprung verwenden.
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Connect zum AWS-Konto her.	Sie können eine Verbindung herstellen, indem Sie ein temporäres Sicherheitstoken oder eine Landingzone-Authentifizierung verwenden. Führen Sie die folgenden Befehle aus, um zu bestätigen, dass Sie das richtige Konto und die richtige AWS-Region verwenden.
	`AWS_REGION="eu-west-1"`
	`ACCOUNT_NUMBER=$(aws sts get-caller-identity --query Account --output text)`
	`echo "${ACCOUNT_NUMBER}"`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bootstrapping für die Umwelt.	Führen Sie die folgenden Befehle aus, um eine AWS-CDK-Umgebung zu booten.
	`npm install`
	`npm run cdk bootstrap "aws://${ACCOUNT_NUMBER}/${AWS_REGION}"`
	Nachdem Sie die Umgebung erfolgreich gebootet haben, sollte die folgende Ausgabe angezeigt werden.
	`# Bootstrapping environment aws://{account}/{region}...`
	`# Environment aws://{account}/{region} bootstrapped`
	Weitere Informationen zu AWS CDK-Bootstrapping finden Sie in der AWS CDK-Dokumentation.
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Synthetisieren Sie eine Vorlage.	Verwenden Sie den Befehl, um eine AWS CDK-App zu synthetisieren. `cdk synth`
	
	`npm run cdk synth`
	
	Die Ausgabe sollte folgender maßen aussehen.
	
	`Successfully synthesized to <path-to-directory>/aws-codepipeline-cicd/cdk.out`
	`Supply a stack id (CodePipeline, Dev-MainStack) to display its template.`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie den CodePipeline Stack bereit.	Nachdem Sie die CloudFormation Vorlage nun gebootet und synthetisiert haben, können Sie sie bereitstellen. Bei der Bereitstellung werden die CodePipeline Pipeline und ein CodeCommit Repository erstellt, das als Quelle und Auslöser der Pipeline dient.
	`npm run cdk -- deploy CodePipeline --require-approval never`
	Nachdem Sie den Befehl ausgeführt haben, sollten Sie sehen, dass der CodePipeline Stack erfolgreich bereitgestellt und die Informationen ausgegeben wurden. Das `CodePipeline.RepositoryName` gibt Ihnen den Namen des CodeCommit Repositorys im AWS-Konto.
	`CodePipeline: deploying...`
	`CodePipeline: creating CloudFormation changeset...`
	`# CodePipeline`
	`Outputs:`
	`CodePipeline.RepositoryName = SampleRepository`
	`Stack ARN:`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`arn:aws:cloudformation:REGION:ACCOUNT-ID:stack/CodePipeline/STACK-ID`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie das CodeCommit Remote-Repository und den Branch ein.	Nach einer erfolgreichen Bereitstellung CodePipeline wird der erste Lauf der Pipeline initiiert, den Sie in der CodePipeline AWS-Konsole finden. Da AWS CDK und CodeCommit kein Standard-Branch initiieren, schlägt dieser erste Pipeline-Lauf fehl und gibt die folgende Fehlermeldung zurück.
	`The action failed because no branch named main was found in the selected AWS CodeCommit repository SampleRepository. Make sure you are using the correct branch name, and then try again. Error: null`
	Um diesen Fehler zu beheben, richten Sie einen Remote-Ursprung als `SampleRepository` ein und erstellen Sie den erforderlichen `main` Branch.
	`RepoName=$(aws cloudformation describe-stacks --stack-name CodePipeline --query "Stacks[0].Outputs[?OutputKey=='RepositoryNam`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`e'].OutputValue" --`
	`output text)`
	`echo "${RepoName}"`
	`#`
	`git init`
	`git branch -m master`
	` main`
	`git remote add origin`
	` codecommit://${Rep`
	`oName}`
	`git add .`
	`git commit -m "Initial`
	` commit"`
	`git push -u origin main`	

Testen Sie die bereitgestellte CodePipeline Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie eine Änderung, um die Pipeline zu aktivieren.	Nach einer erfolgreichen ersten Bereitstellung sollten Sie über eine vollständige CI/CD-Pipeline mit einem `main` Zweig `SampleRepository` als Quellzweig verfügen. Sobald Sie die Änderunge n an der `main` Verzweigung vorgenommen haben, initiiert die Pipeline die folgende Abfolge von Aktionen und führt sie aus: 1. Holen Sie sich Ihren Code aus dem CodeCommit Repository. 2. Erstellen Sie Ihren Code.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Aktualisieren Sie die Pipeline selbst (`UpdatePipeline`). 4. Führen Sie drei parallel Jobs für Linting-, Sicherheits- und Unit-Test-Checks aus. 5. Im Erfolgsfall verteilt die Pipeline den `Main` Stack von der Entwicklungsumgebung in `./lib/main-stack.ts` die Entwicklungsumgebung. 6. Führen Sie nach der Bereitstellung eine Überprüfung der bereitgestellten Ressourcen durch. Sie können alle CodePipeline Schritte und Ergebnisse in der CodePipeline Konsole verfolgen. 7. Im Erfolgsfall wiederholt die Pipeline die Bereitstellung und Validierung für die Test- und Prod-Umgebungen.	

Testen Sie lokal mit einem Makefile

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den Entwicklungsprozess mithilfe eines Makefiles aus.	Sie können die gesamte Pipeline lokal ausführen, indem Sie den `make` Befehl verwenden, oder Sie können einen einzelnen Schritt ausführen (z. B.`make linting`). Führen Sie die folgenden Aktionen aus`make`, um die Verwendung zu testen: • Implementieren Sie die lokale Pipeline: `make` • Nur Komponententests ausführen: `make unittest` • Auf das Girokonto bereitstellen: `make deploy` • Säubere die Umwelt: `make clean`	App-Entwickler, DevOps Ingenieur

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die AWS-CDK-App-Ressourcen.	Führen Sie den folgenden Befehl aus, um Ihre AWS CDK-App zu bereinigen. `cdk destroy --all`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Beachten Sie, dass die Amazon Simple Storage Service (Amazon S3) - Buckets, die beim Bootstrap ping erstellt werden, nicht automatisch gelöscht werden. Sie benötigen eine Aufbewahr ungsrichtlinie, die das Löschen ermöglicht, oder Sie müssen sie manuell in Ihrem AWS-Konto löschen.	

Fehlerbehebung

Problem	Lösung
Die Vorlage funktioniert nicht wie erwartet.	Wenn etwas schief geht und die Vorlage nicht funktioniert, stellen Sie sicher, dass Sie über Folgendes verfügen: • Die richtigen Versionen der Tools. • Zugriff auf das AWS-Zielkonto (Netzwerk konnektivität). • Genügend Berechtigungen für das AWS-Zielkonto.

Zugehörige Ressourcen

- Beginnen Sie mit den häufigsten Aufgaben im IAM Identity Center
- CodePipeline AWS-Dokumentation
- AWS CDK

Richten Sie mithilfe von Terraform eine zentrale Protokollierung auf Unternehmensebene ein

Erstellt von Aarti Rajput (AWS), Yashwant Patel (AWS) und Nishtha Yadav (AWS)

Übersicht

Die zentralisierte Protokollierung ist für die Cloud-Infrastruktur eines Unternehmens von entscheidender Bedeutung, da sie Einblick in Betrieb, Sicherheit und Compliance bietet. Wenn Ihr Unternehmen seine AWS Umgebung auf mehrere Konten skaliert, wird eine strukturierte Protokollverwaltungsstrategie zur Grundlage für die Durchführung von Sicherheitsoperationen, die Erfüllung von Prüfanforderungen und die Erzielung operativer Exzellenz.

Dieses Muster bietet ein skalierbares, sicheres Framework für die Zentralisierung von Protokollen aus mehreren Diensten AWS-Konten und ermöglicht so ein unternehmensweites Protokollierungsmanagement für komplexe Bereitstellungen. AWS Die Lösung wird mithilfe von Terraform automatisiert, einem IaC-Tool (Infrastructure as Code), das konsistente und wiederholbare Bereitstellungen gewährleistet und HashiCorp die manuelle Konfiguration minimiert. Durch die Kombination von Amazon CloudWatch Logs, Amazon Data Firehose und Amazon Simple Storage Service (Amazon S3) können Sie eine robuste Protokollaggregations- und Analyse-Pipeline implementieren, die Folgendes bietet:

- Zentralisiertes Protokollmanagement in Ihrem gesamten Unternehmen in AWS Organizations
- Automatisierte Protokollerfassung mit integrierten Sicherheitskontrollen
- Skalierbare Protokollverarbeitung und langlebiger Speicher
- Vereinfachte Compliance-Berichterstattung und Audit-Trails
- Betriebliche Einblicke und Überwachung in Echtzeit

Die Lösung sammelt Protokolle von Amazon Elastic Kubernetes Service (Amazon EKS) -Containern, AWS Lambda Funktionen und Amazon Relational Database Service (Amazon RDS) -Datenbank-Instances über Logs. CloudWatch Sie leitet diese Protokolle mithilfe von Abonnementfiltern automatisch an ein spezielles Protokollierungskonto weiter. CloudWatch Firehose verwaltet die Protokoll-Streaming-Pipeline mit hohem Durchsatz zu Amazon S3 zur Langzeitspeicherung. Amazon Simple Queue Service (Amazon SQS) ist so konfiguriert, dass er bei der Objekterstellung Amazon S3 S3-Ereignisbenachrichtigungen empfängt. Dies ermöglicht die Integration mit Analysediensten, einschließlich:

- Amazon OpenSearch Service für Protokollsuche, Visualisierung und Echtzeitanalyse
- Amazon Athena für SQL-basierte Abfragen
- Amazon EMR für die Verarbeitung in großem Maßstab
- Lambda für benutzerdefinierte Transformation
- Amazon QuickSight für Dashboards

Alle Daten werden mit AWS Key Management Service (AWS KMS) verschlüsselt, und die gesamte Infrastruktur wird mithilfe von Terraform bereitgestellt, um eine konsistente Konfiguration in allen Umgebungen zu gewährleisten.

Dieser zentralisierte Protokollierungsansatz ermöglicht es Unternehmen, ihre Sicherheitslage zu verbessern, Compliance-Anforderungen einzuhalten und die betriebliche Effizienz ihrer AWS gesamten Infrastruktur zu optimieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine landing zone für Ihre Organisation, die erstellt wurde mit AWS Control Tower
- Account Factory for Terraform (AFT), bereitgestellt und konfiguriert mit den erforderlichen Konten
- Terraform für die Bereitstellung der Infrastruktur
- AWS Identity and Access Management (IAM) -Rollen und Richtlinien für den kontoübergreifenden Zugriff

Anweisungen zur Einrichtung von AFT AWS Control Tower- und Anwendungskonten finden Sie im Abschnitt Epics.

Erforderliche Konten

Ihre Organisation AWS Organizations sollte die folgenden Konten enthalten:

- Anwendungskonto — Ein oder mehrere Quellkonten, auf denen die AWS-Services (Amazon EKS, Lambda und Amazon RDS) ausgeführt und Protokolle generiert werden
- Log Archive-Konto — Ein spezielles Konto für die zentrale Speicherung und Verwaltung von Protokollen

Produktversionen

- AWS Control Tower Version 3.1 oder höher
- Terraform Version 0.15.0 oder höher

Architektur

Das folgende Diagramm zeigt eine AWS zentralisierte Protokollierungsarchitektur, die eine skalierbare Lösung für das Sammeln, Verarbeiten und Speichern von Protokollen aus mehreren Anwendungskonten in einem speziellen Log Archive-Konto bietet. Diese Architektur verarbeitet effizient Protokolle von AWS-Services, einschließlich Amazon RDS, Amazon EKS und Lambda, und leitet sie über einen optimierten Prozess an regionale S3-Buckets im Log Archive-Konto weiter.

Der Workflow umfasst fünf Prozesse:

1. Log-Flow-Prozess
   - Der Protokollfluss beginnt in den Anwendungskonten, wo verschiedene Arten von Protokollen AWS-Services generiert werden, z. B. allgemeine Protokolle, Fehler-, Prüfprotokolle, langsame Abfrageprotokolle von Amazon RDS, Kontrollebenenprotokolle von Amazon EKS sowie Funktionsausführungs- und Fehlerprotokolle von Lambda.
   - CloudWatch dient als erste Sammelstelle. Es sammelt diese Protokolle auf Protokollgruppenebene innerhalb jedes Anwendungskontos.
   - In CloudWatch bestimmen Abonnementfilter, welche Protokolle an das zentrale Konto weitergeleitet werden sollen. Diese Filter bieten Ihnen eine detaillierte Kontrolle über die Protokollweiterleitung, sodass Sie genaue Protokollmuster oder vollständige Protokollstreams für die Zentralisierung angeben können.
2. Kontoübergreifende Protokollübertragung
   - Protokolle werden in das Log Archive-Konto verschoben. CloudWatch Abonnementfilter erleichtern die kontoübergreifende Übertragung und bewahren den regionalen Kontext.
   - Die Architektur richtet mehrere parallel Streams ein, um verschiedene Protokollquellen effizient zu handhaben und so eine optimale Leistung und Skalierbarkeit zu gewährleisten.
3. Protokollverarbeitung im Log Archive-Konto
   - Im Log Archive-Konto verarbeitet Firehose die eingehenden Protokollstreams.
   - Jede Region unterhält eigene Firehose-Lieferdatenströme, die Protokolle nach Bedarf transformieren, konvertieren oder anreichern können.

- Diese Firehose-Streams liefern die verarbeiteten Protokolle an S3-Buckets im Log Archive-Konto, das sich in derselben Region wie die Quellanwendungskonten (Region A im Diagramm) befindet, um die Anforderungen an die Datenhoheit aufrechtzuerhalten.

4. Benachrichtigungen und zusätzliche Workflows
   - Wenn Protokolle ihre Ziel-S3-Buckets erreichen, implementiert die Architektur mithilfe von Amazon SQS ein Benachrichtigungssystem.
   - Die regionalen SQS-Warteschlangen ermöglichen eine asynchrone Verarbeitung und können auf der Grundlage der gespeicherten Protokolle zusätzliche Workflows, Analyse- oder Warnsysteme auslösen.
5. AWS KMS aus Sicherheitsgründen

   Die Architektur beinhaltet aus AWS KMS Sicherheitsgründen. AWS KMS stellt Verschlüsselungsschlüssel für die S3-Buckets bereit. Dadurch wird sichergestellt, dass alle gespeicherten Protokolle die Verschlüsselung im Ruhezustand beibehalten und gleichzeitig die regionale Verschlüsselung beibehalten wird, um die Anforderungen an die Datenresidenz zu erfüllen.

Tools

AWS-Services

- Amazon CloudWatch ist ein Überwachungs- und Beobachtungsdienst, der Überwachungs- und Betriebsdaten in Form von Protokollen, Metriken und Ereignissen sammelt. Es bietet eine einheitliche Ansicht der AWS Ressourcen, Anwendungen und Services, die auf AWS- und lokalen Servern ausgeführt werden.
- CloudWatch Protokoll-Abonnementfilter sind Ausdrücke, die einem Muster bei eingehenden Protokollereignissen entsprechen und entsprechende Protokollereignisse zur weiteren Verarbeitung oder Analyse an die angegebene AWS Ressource weiterleiten.
- AWS Control Tower Account Factory For Terraform (AFT) richtet eine Terraform-Pipeline ein, mit der Sie Konten bereitstellen und anpassen können. AWS Control Tower AFT bietet eine Terraform-basierte Kontobereitstellung und ermöglicht es Ihnen gleichzeitig, Ihre Konten mit zu verwalten. AWS Control Tower
- Amazon Data Firehose liefert Streaming-Daten in Echtzeit an Ziele wie Amazon S3, Amazon Redshift und Amazon OpenSearch Service. Es passt sich automatisch dem Durchsatz Ihrer Daten an und erfordert keine laufende Verwaltung.

- Amazon Elastic Kubernetes Service (Amazon EKS) ist ein verwalteter Container-Orchestrierungsservice, der die Bereitstellung, Verwaltung und Skalierung containerisierter Anwendungen mithilfe von Kubernetes vereinfacht. Er verwaltet automatisch die Verfügbarkeit und Skalierbarkeit der Knoten der Kubernetes-Steuerebene.
- AWS Key Management Service (AWS KMS) erstellt und kontrolliert Verschlüsselungsschlüssel für die Verschlüsselung Ihrer Daten. AWS KMS integriert sich in andere AWS-Services , um Ihnen zu helfen, die Daten zu schützen, die Sie mit diesen Diensten speichern.
- AWS Lambdaist ein serverloser Rechendienst, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er skaliert Ihre Anwendungen automatisch, indem er Code als Reaktion auf jeden Trigger ausführt, und berechnet nur die Rechenzeit, die Sie tatsächlich nutzen.
- Amazon Relational Database Service (Amazon RDS) ist ein verwalteter relationaler Datenbankservice, der die Einrichtung, den Betrieb und die Skalierung einer relationalen Datenbank in der Cloud vereinfacht. Er bietet kosteneffiziente und anpassbare Kapazität und automatisiert gleichzeitig zeitaufwändige Verwaltungsaufgaben.
- Amazon Simple Queue Service (Amazon SQS) ist ein Nachrichtenwarteschlangen-Service, mit dem Sie Microservices, verteilte Systeme und serverlose Anwendungen entkoppeln und skalieren können. Damit entfällt die Komplexität der Verwaltung und des Betriebs nachrichtenorientierter Middleware.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet. Er kann jede Datenmenge von überall im Internet speichern und abrufen.

Andere Tools

- Terraform ist ein IaC-Tool (Infrastructure as Code) HashiCorp , mit dem Sie Cloud- und lokale Ressourcen erstellen und verwalten können.

Code

Der Code für dieses Muster ist im Centralized Logging Repository verfügbar. GitHub

Bewährte Methoden

- Verwenden Sie mehrere AWS-Konten in einer einzigen Organisation in AWS Organizations. Diese Vorgehensweise ermöglicht eine zentrale Verwaltung und eine standardisierte Protokollierung für alle Konten.
- Konfigurieren Sie S3-Buckets mit Versionierung, Lebenszyklusrichtlinien und regionsübergreifender Replikation. Implementieren Sie Verschlüsselung und Zugriffsprotokollierung für Sicherheit und Compliance.
- Implementieren Sie allgemeine Protokollierungsstandards, indem Sie das JSON-Format mit Standardzeitstempeln und Feldern verwenden. Verwenden Sie eine konsistente Präfixstruktur und Korrelation IDs für eine einfache Nachverfolgung und Analyse.
- Aktivieren Sie Sicherheitskontrollen mit AWS KMS Verschlüsselung und Zugriff mit geringsten Rechten. Sorgen Sie für mehr Sicherheit durch AWS CloudTrail Überwachung und regelmäßige Schlüsselrotation.
- Richten Sie CloudWatch Kennzahlen und Benachrichtigungen für die Sendungsverfolgung ein. Überwachen Sie Kosten und Leistung mit automatisierten Benachrichtigungen.
- Konfigurieren Sie Amazon S3 S3-Aufbewahrungsrichtlinien, um die Compliance-Anforderungen zu erfüllen, und aktivieren Sie die Amazon S3 S3-Serverzugriffsprotokollierung, um alle Anfragen an Ihre S3-Buckets nachzuverfolgen. Pflegen Sie die Dokumentation für S3-Bucket-Richtlinien und Lebenszyklusregeln. Führen Sie regelmäßige Überprüfungen von Zugriffsprotokollen, Bucket-Berechtigungen und Speicherkonfigurationen durch, um die Einhaltung von Vorschriften und bewährten Sicherheitsverfahren sicherzustellen.

Epen

Konten einrichten AWS Control Tower, AFT und Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine AWS Control Tower Umgebung mit AFT ein.	1. Folgen Sie AWS Control Tower bei der Bereitste llung den Anweisungen in der AWS Control Tower Dokumentation. 2. Stellen Sie AFT bereit, indem Sie den Anweisung	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en in der AWS Control Tower Dokumentation folgen.	
Aktivieren Sie die gemeinsame Nutzung von Ressourcen für die Organisation.	1. Konfigurieren Sie AWS Command Line Interface (AWS CLI) mit den Anmeldeinformationen für das Verwaltungskonto, die Administratorberechtigungen für die Verwaltung bereitstellen AWS Control Tower. 2. Führen Sie den folgenden AWS CLI Befehl in einem beliebigen Befehl aus AWS-Region: `aws ram enable-sharing-with-aws-organization` Dies ermöglicht die gemeinsame Nutzung von Ressourcen innerhalb Ihrer Organisation in AWS Organizations allen Regionen, die AWS Resource Access Manager (AWS RAM) unterstützen.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen oder Bereitstellen von Anwendungskonten.	Um neue Anwendungskonten für Ihren Anwendungsfall bereitzustellen, erstellen Sie sie über AFT. Weitere Informationen finden Sie in der AWS Control Tower Dokumentation unter Bereitstellen eines neuen Kontos bei AFT.	AWS-Administrator

Richten Sie Konfigurationsdateien für Anwendungskonten ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopiert `Application_account` den Inhalt des Ordners in das `aft-account-customizations` Repository.	1. Erstellen Sie einen Ordner, der `Application_account` im Stammpfad des `aft-account-customizations` Repositorys benannt ist. Dieses Repository wird automatisch erstellt, wenn Sie AFT einrichten (siehe das vorherige Epos). 2. Navigieren Sie zum Stammverzeichnis des scale-using-terraform Repositorys centralised-logging-at-enterprise—, kopieren Sie den Inhalt des `aft/account` Verzeichnisses und fügen Sie ihn dann in das `Applicati`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	on_account Verzeichnis ein, das Sie in Schritt 1 im aft-account-customizations Repository erstellt haben. 3. Kopieren Sie den Inhalt des Verzeichnisses aus dem Application_account Stammverzeichnis des centralised-logging-at-enterprise-scale-using-terraform Repositorys in das Application_account/terraform Verzeichnis im aft-account-customizations Repository. 4. Vergewissern Sie sich in der aft-account-customizations/Application_account/terraform.tfvars Datei, dass alle Parameter als Argumente in den entsprechenden Terraform-Konfigurationsdateien übergeben wurden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen und bearbeiten Sie die Eingabeparameter für die Einrichtung des Anwendung skontos.	In diesem Schritt richten Sie die Konfigurationsdatei für die Erstellung von Ressourcen in Anwendungskonten ein, einschließlich CloudWatch Protokollgruppen, CloudWatch Abonnementfiltern, IAM-Rollen und -Richtlinien sowie Konfigurationsdetails für Amazon RDS-, Amazon EKS- und Lambda-Funktionen. Konfigurieren Sie in Ihrem `aft-account-customizations` Repository im `Application_account` Ordner die Eingabeparameter in der `terraform.tfvars` Datei entsprechend den Anforderungen Ihrer Organisation: • `environment` : Der Name der Umgebung (z. B.,`prod`,`staging`)`dev`, in der die Ressourcen bereitgestellt werden. • `account_name` : Der Name der AWS-Konto Stelle, in der die Ressourcen erstellt werden. • `log_archive_account_id` : Die AWS-Konto ID, unter der Protokolle archiviert werden.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `admin_role_name` : Der Name der Administratorrolle, die für die Verwaltung von Ressourcen verwendet wird. • `tags`: Eine Zuordnung von Schlüssel-Wert-Paaren, die gemeinsame Tags darstellen, die auf alle Ressourcen angewendet werden sollen. • `rds_config` : Ein Objekt, das Konfigurationsdetails für Amazon RDS-Instances enthält. • `allowed_cidr_blocks` : Eine Liste von CIDR-Blöcken, die auf die Ressourcen zugreifen dürfen. • `destination_name:` Eine Variable, die verwendet wird, um den Amazon-Ressourcennamen (ARN) des CloudWatch Ziels zu erstellen, an das Protokolle gestreamt werden. • `rds_parameters:` Ein Objekt, das Amazon RDS-Parametergruppeneinstellungen enthält. • `vpc_config` : Ein Objekt, das VPC-Konfigurationsdetails enthält.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `eks_config` : Ein Objekt, das Konfigurationsdetails für Amazon EKS-Cluster enthält. • `lambda_config` : Ein Objekt, das Konfigurationsdetails für Lambda-Funktionen enthält. • `restrictive_cidr_range` : Eine Liste restriktiver CIDR-Bereiche für Sicherheitsgruppenregeln. • `target_account_id` : Die AWS-Konto ID des Log Archive-Zielkontos, für das Ressourcen bereitgestellt werden.	

Richten Sie die Konfigurationsdateien für das Log Archive-Konto ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopiert `Log_archive_account` den Inhalt des Ordners in das `aft-account-customizations` Repository.	1. Erstellen Sie einen Ordner mit `Log_archive_account` dem Stammverzeichnis des `aft-account-customizations` Repositorys. Dieses Repository wird automatisch erstellt, wenn Sie AFT einrichten. 2. Navigieren Sie zum Stammverzeichnis des	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`centralised-logging-at-enterprise-scale-using-terraform` Repositorys, kopieren Sie den Inhalt des `aft/account` Verzeichnisses und fügen Sie ihn dann in das `Log_archive_account` Verzeichnis ein, das Sie im vorherigen Schritt im `aft-account-customizations` Repository erstellt haben. 3. Kopieren Sie den Inhalt des Verzeichnisses aus dem `Log_archive_account` Stammverzeichnis des `centralised-logging-at-enterprise-scale-using-terraform` Repositorys in das `Log_archive_account/terraform` Verzeichnis im `aft-account-customizations` Repository. 4. Vergewissern Sie sich in der `aft-account-customizations/Log_archive_account/terraform.tfvars` Datei, dass alle Parameter als Argumente in den entsprechenden	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Terraform-Konfigurationsdateien übergeben wurden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen und bearbeiten Sie die Eingabeparameter für die Einrichtung des Log Archive-Kontos.	In diesem Schritt richten Sie die Konfigurationsdatei für die Erstellung von Ressourcen im Log Archive-Konto ein, einschließlich Firehose-Lieferstreams, S3-Buckets, SQS-Warteschlangen sowie IAM-Rollen und -Richtlinien. Konfigurieren Sie im `Log_archive_account` Ordner Ihres `aft-account-customizations` Repositorys die Eingabeparameter in der `terraform.tfvars` Datei entsprechend den Anforderungen Ihrer Organisation: • `environment` : Der Name der Umgebung (z. B.,`prod`,`staging`)`dev`, in der die Ressourcen bereitgestellt werden. • `destination_name` : Eine Variable, die verwendet wird, um den ARN des CloudWatch Ziels zu erstellen, an das Protokolle gestreamt werden. • `source_account_ids` : Eine Liste von Personen AWS-Konto IDs , die Abonnementfilter auf das	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Protokollziel setzen dürfen. Sie können so viele Konten eingeben, IDs wie Sie für die zentrale Protokollierung aktivieren möchten.	

Führen Sie Terraform-Befehle aus, um Ressourcen bereitzustellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Option 1 — Stellen Sie die Terraform-Konfigurationsdat eien von AFT bereit.	In AFT wird die AFT-Pipel ine ausgelöst, nachdem Sie den Code mit den Konfigura tionsänderungen in das Repository übertragen haben. GitHub `aft-account-customizations` AFT erkennt die Änderungen automatisch und leitet den Prozess der Kontoanpassung ein.
	
	Nachdem Sie Änderunge n an Ihren Terraform (`terraform.tfvars`) -Dateien vorgenommen haben, übertragen Sie Ihre Änderungen und übertrage n Sie sie in Ihr Repository: `aft-account-custom izations`
	
	`$ git add *`
	`$ git commit -m "update message"`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`$ git push origin main` **Note** Wenn du einen anderen Branch (wie`dev`) verwendest, ersetze ihn `main` durch deinen Branch-Namen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Option 2 — Stellen Sie die Terraform-Konfigurationsdatei manuell bereit.	Wenn Sie AFT nicht verwenden oder die Lösung manuell bereitstellen möchten, können Sie die folgenden Terraform-Befehle aus den Ordnern und verwenden: `Application_account` `Log_archive_account`
	1. Klonen Sie das GitHub Repository und konfiguri eren Sie die Eingabepa rameter in der `terraform .tfvars` Datei.
	2. Führen Sie den folgenden Befehl aus:
	`$ terraform init`
	3. Änderungen in der Vorschau anzeigen:
	`$ terraform plan`
	Dieser Befehl wertet die Terraform-Konfiguration aus, um den gewünschten Status der Ressourcen zu ermitteln, und vergleicht ihn mit dem aktuellen Status Ihrer Infrastruktur.
	4. Änderungen übernehmen:
	`$ terraform apply`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Überprüfen Sie die geplanten Änderungen und geben Sie bei der Aufforder ung Ja ein, um mit dem Antrag fortzufahren.	

Ressourcen validieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Abonnementfilter.	Gehen Sie wie folgt vor, um sicherzustellen, dass die Abonnementfilter Protokoll e korrekt von den Protokoll gruppen des Anwendung skontos an das Protokoll archivkonto weiterleiten: 1. Öffnen Sie im Anwendung skonto die CloudWatch Konsole. 2. Wählen Sie im linken Navigationsbereich Log groups (Protokollgruppen) aus. 3. Wählen Sie jede Protokoll gruppe (`/aws/rds`,`/aws/eks`,`/aws/lambda`) aus und klicken Sie auf die Registerkarte Abonnemen tfilter. Sie sollten aktive Abonnementfilter sehen,	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die auf den Ziel-ARN verweisen, basierend auf dem Namen, den Sie in der Terraform-Konfigurationsdatei angegeben haben. 4. Wählen Sie einen beliebigen Abonnementfilter aus, um dessen Konfiguration und Status zu überprüfen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie Firehose-Streams.	So überprüfen Sie, ob die Firehose-Streams im Log Archive-Konto Anwendung sprotokolle erfolgreich verarbeiten: 1. Öffnen Sie im Log Archive-Konto die Firehose-Konsole. 2. Wählen Sie im linken Navigationsbereich Firehose-Streams aus. 3. Wählen Sie einen beliebige n Firehose-Stream aus und überprüfen Sie Folgendes: • Das Ziel zeigt den richtigen S3-Bucket an. • Auf der Registerk arte Überwachung werden Kennzahlen für erfolgreiche Lieferungen angezeigt. • Der Zeitstempel der letzten Lieferung ist aktuell.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die zentralisierten S3-Buckets.	Gehen Sie wie folgt vor, um zu überprüfen, ob die zentralisierten S3-Buckets Protokolle empfangen und ordnungsgemäß organisieren: 1. Öffnen Sie im Log Archive-Konto die Amazon S3 S3-Konsole. 2. Wählen Sie jeden zentralen Logging-Bucket aus. 3. Navigieren Sie durch die Ordnerstruktur: AWSLogs/AccountID/Region/Service. Sie sollten Protokolldateien sehen, die nach timestamp (YYYY/MM/DD/HH) organisiert sind. 4. Wählen Sie eine aktuelle Protokolldatei aus und überprüfen Sie deren Format und Datenintegrität.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die SQS-Warteschlangen.	So überprüfen Sie, ob die SQS-Warteschlangen Benachrichtigungen für neue Protokolldateien erhalten: 1. Öffnen Sie im Log Archive-Konto die Amazon SQS SQS-Konsole. 2. Wählen Sie im linken Navigationsbereich Queues (Wartschlange) aus. 3. Wählen Sie jede konfiguri erte Warteschlange aus und wählen Sie Nachrichten senden und empfangen. Sie sollten Nachrichten sehen, die S3-Ereign isbenachrichtigungen für neue Protokolldateien enthalten. 4. Wählen Sie eine beliebige Nachricht aus, um zu überprüfen, ob sie die richtigen S3-Objektinformati onen enthält.	DevOps Ingenieur

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 1 — Außerbetr iebnahme der Terraform-Konfigurationsdatei von AFT.	Wenn Sie die Terraform -Konfigurationsdateien entfernen und die Änderunge	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	n übertragen, leitet AFT automatisch den Prozess zum Entfernen der Ressourcen ein.
	
	1. Navigieren Sie zum Repository. `aft-account-customizations`
	2. Wechseln Sie zum Verzeichnis `terraform` .
	3. Löschen Sie die folgenden Dateien:
	• `modules`Verzeichnis
	• `iam.tf`
	• `versions.tf`
	• `variables.tf`
	• `outputs.tf`
	• `terraform.tfvars`
	4. Löscht den Inhalt der `main.tf` Datei.
	5. Übertragen Sie Ihre Änderungen in das Repository:
	
	`# Stage all changes`
	`$ git add *`
	
	`# Commit cleanup changes`
	`$ git commit -m "Remove AFT customizations"`
	
	`# Push to repository`
	`$ git push origin main`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Wenn Sie einen anderen Zweig (z. B. `dev`) verwenden, `main` ersetzen Sie ihn durch Ihren Zweignamen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Option 2 — Manuelles Bereinigen der Terraform-Ressourcen.	Wenn Sie AFT nicht verwenden oder Ressourcen manuell bereinigen möchten, verwenden Sie die folgenden Terraform-Befehle aus den Ordnern und: `Application_account` `Log_archive_account`
	
	1. Initialisieren Sie die Terraform-Konfiguration:
	
	`$ terraform init`
	
	Dieser Befehl initialisiert Terraform und stellt den Zugriff auf den aktuellen Status sicher.
	2. Vorschau der Cleanup-Änderungen anzeigen:
	
	`$ terraform destroy`
	
	Dieser Befehl bewertet, welche Ressourcen zerstört werden, und vergleicht den gewünschten Zustand mit dem aktuellen Zustand Ihrer Infrastruktur.
	3. Führen Sie die Bereinigung aus. Wenn Sie dazu aufgefordert werden, geben Sie Ja ein, um den Vernichtungsplan zu
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bestätigen und auszuführen.	

Fehlerbehebung

Problem	Lösung
Das CloudWatch Logs-Ziel wurde nicht erstellt oder ist inaktiv.	Überprüfen Sie Folgendes: 1. Stellen Sie im Log Archive-Konto sicher, dass die Zielrichtlinie Folgendes beinhaltet: • Der richtige Hauptbenutzer des Quellkontos. • Die richtige Aktion (`logs:PutSubscriptionFilter`). • Ein gültiger Ziel-ARN. 2. Vergewissern Sie sich, dass Firehose Firehose-Stream existiert und aktiv ist. 3. Stellen Sie sicher, dass die dem Ziel zugeordnete IAM-Rolle über Berechtigungen für Firehose verfügt.
Der Abonnementfilter ist ausgefallen oder hat den Status „Ausstehend“.	Überprüfen Sie, ob Folgendes der Fall ist: 1. Stellen Sie im Anwendungskonto sicher, dass die IAM-Rolle über Folgendes verfügt: • Berechtigungen zum Anrufen. `PutSubscriptionFilter` • Eine Vertrauensbeziehung mit CloudWatch Logs. 2. Vergewissern Sie sich, dass der Ziel-ARN korrekt ist.

Problem	Lösung
	3. Suchen Sie in den CloudWatch Protokollen nach bestimmten Fehlermeldungen.
Der Firehose-Lieferstream zeigt keine eingehenden Datensätze an.	Überprüfen Sie Folgendes: 1. Vergewissern Sie sich, dass die Firehose-IAM-Rolle Folgendes hat: • Berechtigungen zum Schreiben in Amazon S3. • Zugriff auf den AWS KMS Schlüssel, wenn die Verschlüsselung aktiviert ist. 2. Überprüfen Sie die CloudWatch Kennzahlen für: • `IncomingRecords` • `DeliveryToS3.Records` 3. Überprüfen Sie die Puffereinstellungen und Lieferkonfigurationen.

Zugehörige Ressourcen

- Einrichtung der Terraform-Infrastruktur (Terraform-Dokumentation)
- AWS Control Tower Account Factory für Terraform (AFT) bereitstellen (AWS Control Tower Dokumentation)
- IAM-Tutorial: Delegieren Sie den Zugriff AWS-Konten mithilfe von IAM-Rollen () IAMdocumentation

Richten Sie die end-to-end Verschlüsselung für Anwendungen auf Amazon EKS mithilfe von cert-manager und Let's Encrypt ein

Erstellt von Mahendra Revanasiddappa (AWS) und Vasanth Jeyaraj (AWS)

Übersicht

Die Implementierung von end-to-end Verschlüsselung kann komplex sein und Sie müssen Zertifikate für jedes Asset in Ihrer Microservices-Architektur verwalten. Obwohl Sie die Transport Layer Security (TLS) -Verbindung am Rand des Amazon Web Services (AWS) -Netzwerks mit einem Network Load Balancer oder Amazon API Gateway beenden können, benötigen einige Organisationen end-to-end Verschlüsselung.

Dieses Muster verwendet den NGINX Ingress Controller für den Ingress. Das liegt daran, dass beim Erstellen eines Kubernetes-Ingress die Ingress-Ressource einen Network Load Balancer verwendet. Der Network Load Balancer erlaubt keine Uploads von Client-Zertifikaten. Daher können Sie mit Kubernetes-Ingress kein gegenseitiges TLS erreichen.

Dieses Muster ist für Organisationen gedacht, die eine gegenseitige Authentifizierung zwischen allen Microservices in ihren Anwendungen benötigen. Mutual TLS reduziert den Aufwand für die Verwaltung von Benutzernamen oder Passwörtern und kann auch das schlüsselfertige Sicherheitsframework verwenden. Der Ansatz dieses Musters ist kompatibel, wenn Ihr Unternehmen über eine große Anzahl verbundener Geräte verfügt oder strenge Sicherheitsrichtlinien einhalten muss.

Dieses Muster trägt dazu bei, die Sicherheitslage Ihres Unternehmens zu verbessern, indem es end-to-end Verschlüsselung für Anwendungen implementiert, die auf Amazon Elastic Kubernetes Service (Amazon EKS) ausgeführt werden. Dieses Muster enthält eine Beispielanwendung und einen Code im GitHub End-to-end Encryption on Amazon EKS-Repository, um zu zeigen, wie ein Microservice mit end-to-end Verschlüsselung auf Amazon EKS ausgeführt wird. Der Ansatz des Musters verwendet cert-manager, ein Add-on für Kubernetes, mit Let's Encrypt als Zertifizierungsstelle (CA). Let's Encrypt ist eine kostengünstige Lösung zur Verwaltung von Zertifikaten und bietet kostenlose Zertifikate, die 90 Tage gültig sind. CERT-Manager automatisiert die On-Demand-Bereitstellung und Rotation von Zertifikaten, wenn ein neuer Microservice auf Amazon EKS bereitgestellt wird.

Beabsichtigte Zielgruppe

Dieses Muster wird Benutzern empfohlen, die Erfahrung mit Kubernetes, TLS, Amazon Route 53 und Domain Name System (DNS) haben.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein vorhandener Amazon-EKS-Cluster.
- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 1.7 oder höher, installiert und konfiguriert auf macOS, Linux oder Windows.
- Das `kubectl` Befehlszeilenprogramm, das für den Zugriff auf den Amazon EKS-Cluster installiert und konfiguriert wurde. Weitere Informationen dazu finden Sie unter Installation von kubectl in der Amazon EKS-Dokumentation.
- Ein vorhandener DNS-Name zum Testen der Anwendung. Weitere Informationen dazu finden Sie unter Registrierung von Domainnamen mit Amazon Route 53 in der Amazon Route 53 53-Dokumentation.
- Die neueste Helm-Version, die auf Ihrem lokalen Computer installiert ist. Weitere Informationen dazu finden Sie unter Using Helm with Amazon EKS in der Amazon EKS-Dokumentation und im GitHub Helm-Repository.
- Die GitHub End-to-end Verschlüsselung im Amazon EKS-Repository, auf Ihren lokalen Computer geklont.
- Ersetzen Sie die folgenden Werte in den `trustpolicy.json` Dateien `policy.json` und aus der geklonten GitHub End-to-end Verschlüsselung im Amazon EKS-Repository:
  - `<account number>`— Ersetzen Sie durch die AWS-Konto-ID für das Konto, in dem Sie die Lösung bereitstellen möchten.
  - `<zone id>`— Ersetzen Sie durch die Route 53 53-Zonen-ID des Domainnamens.
  - `<node_group_role>`— Durch den Namen der AWS Identity and Access Management (IAM) -Rolle ersetzen, die den Amazon EKS-Knoten zugeordnet ist.
  - `<namespace>`— Ersetzen Sie durch den Kubernetes-Namespace, in dem Sie den NGINX Ingress Controller und die Beispielanwendung bereitstellen.
  - `<application-domain-name>`— Durch den DNS-Domainnamen von Route 53 ersetzen.

Einschränkungen

- Dieses Muster beschreibt nicht, wie Zertifikate rotiert werden, sondern zeigt nur, wie Zertifikate mit Microservices auf Amazon EKS verwendet werden.

Architektur

Das folgende Diagramm zeigt den Workflow und die Architekturkomponenten für dieses Muster.

Das Diagramm zeigt den folgenden Workflow:

1. Ein Client sendet eine Anfrage für den Zugriff auf die Anwendung an den DNS-Namen.
2. Der Route 53 53-Datensatz ist ein CNAME für den Network Load Balancer.
3. Der Network Load Balancer leitet die Anfrage an den NGINX Ingress Controller weiter, der mit einem TLS-Listener konfiguriert ist. Die Kommunikation zwischen dem NGINX Ingress Controller und dem Network Load Balancer folgt dem HTTPS-Protokoll.
4. Der NGINX Ingress Controller führt auf der Grundlage der Anfrage des Clients an den Anwendungsdienst ein pfadbasiertes Routing durch.
5. Der Anwendungsdienst leitet die Anfrage an den Anwendungs-Pod weiter. Die Anwendung ist so konzipiert, dass sie dasselbe Zertifikat verwendet, indem sie Secrets aufruft.
6. Pods führen die Beispielanwendung mithilfe der Cert-Manager-Zertifikate aus. Die Kommunikation zwischen dem NGINX Ingress Controller und den Pods verwendet HTTPS.

> **Note**
>
> CERT-Manager läuft in einem eigenen Namespace. Es verwendet eine Kubernetes-Clusterrolle, um Zertifikate als Geheimnisse in bestimmten Namespaces bereitzustellen. Sie können diese Namespaces an Anwendungs-Pods und den NGINX Ingress Controller anhängen.

Tools

AWS-Services

- Amazon Elastic Kubernetes Service (Amazon EKS) ist ein verwalteter Service, mit dem Sie Kubernetes auf AWS ausführen können, ohne Ihre eigene Kubernetes-Steuerebene oder Knoten installieren, betreiben und warten zu müssen.
- Elastic Load Balancing verteilt Ihren eingehenden Traffic automatisch auf mehrere Ziele, Container und IP-Adressen.

- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.

Andere Tools

- cert-manager ist ein Add-on für Kubernetes, das Zertifikate anfordert, sie an Kubernetes-Container verteilt und die Zertifikatserneuerung automatisiert.
- NGINX Ingress Controller ist eine Lösung für das Verkehrsmanagement für Cloud-native Apps in Kubernetes und containerisierten Umgebungen.

Epen

Erstellen und konfigurieren Sie eine öffentlich gehostete Zone mit Route 53

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine öffentlich gehostete Zone in Route 53	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon Route 53 53-Konsole, wählen Sie Hosted Zones und dann Create Hosted Zone aus. Erstellen Sie eine öffentlich gehostete Zone und notieren Sie sich die Zonen-ID. Weitere Informationen dazu finden Sie unter Erstellen einer öffentlich gehosteten Zone in der Amazon Route 53 53-Dokumentation. **Note** ACME DNS01 verwendet den DNS-	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anbieter, um eine Aufforderung an den Cert-Manager zur Ausstellung des Zertifikats zu senden. Bei dieser Aufforderung müssen Sie nachweisen, dass Sie den DNS für Ihren Domainnamen kontrollieren, indem Sie einen bestimmten Wert in einen TXT-Eintrag unter diesem Domainnamen eingeben. Nachdem Let's Encrypt Ihrem ACME-Client ein Token gegeben hat, erstellt Ihr Kunde einen TXT-Eintrag, der von diesem Token und Ihrem Kontoschlüssel abgeleitet ist, und platziert diesen Datensatz unter. `_acme-challenge.<YOURDOMAIN>` Dann fragt Let's Encrypt den DNS nach diesem Datensatz ab. Wenn eine Übereinstimmung gefunden wird, können Sie mit der Ausstellu	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ng eines Zertifikats fortfahren.	

Konfigurieren Sie eine IAM-Rolle, damit der Cert-Manager auf die öffentlich gehostete Zone zugreifen kann

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Richtlinie für Cert-Manager.	Eine IAM-Richtlinie ist erforderlich, um dem Cert-Manager die Erlaubnis zu erteilen, zu überprüfen, ob Sie Eigentümer der Route 53 53-Domäne sind. Die `policy.json` Beispiel-IAM-Richtlinie befindet sich im `1-IAMRole` Verzeichnis im Repository für geklonte GitHub End-to-end Verschlüsselung im Amazon EKS-Repository. Geben Sie den folgenden Befehl in der AWS-CLI ein, um die IAM-Richtlinie zu erstellen. `aws iam create-policy \ --policy-name PolicyForCertManager \ --policy-document file://policy.json`	AWS DevOps
Erstellen Sie die IAM-Rolle für cert-manager.	Nachdem Sie die IAM-Richtlinie erstellt haben, müssen Sie eine IAM-Rolle erstellen	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	. Die `trustpolicy.json` IAM-Beispielrolle wird im Verzeichnis bereitgestellt. `1-IAMRole` Geben Sie den folgenden Befehl in der AWS-CLI ein, um die IAM-Rolle zu erstellen. `aws iam create-role \ --role-name RoleForCertManager \ --assume-role-policy-document file://trustpolicy.json`	
Fügen Sie der Rolle die -Richtlinie an.	Geben Sie den folgenden Befehl in der AWS-CLI ein, um die IAM-Richtlinie an die IAM-Rolle anzuhängen. `AWS_ACCOUNT_ID` Ersetzen Sie es durch die ID Ihres AWS-Kontos. `aws iam attach-role-policy \ --policy-arn arn:aws:iam::AWS_ACCOUNT_ID:policy/PolicyForCertManager \ --role-name RoleForCertManager`	AWS DevOps

Den NGINX Ingress Controller in Amazon EKS einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den NGINX Ingress Controller bereit.	Installieren Sie die neueste Version von `nginx-ingress` Using Helm. Sie können die `nginx-ingress` Konfiguration vor der Bereitstellung an Ihre Anforderungen anpassen. Dieses Muster verwendet einen mit Anmerkungen versehenen, nach innen gerichteten Network Load Balancer, der im Verzeichnis verfügbar ist. `5-Nginx-Ingress-Controller` Installieren Sie den NGINX Ingress Controller, indem Sie den folgenden Helm-Befehl aus dem Verzeichnis ausführen. `5-Nginx-Ingress-Controller` `helm install test-nginx nginx-stable/nginx-ingress -f 5-Nginx-Ingress-Controller/values_internal_nlb.yaml`	AWS DevOps
Stellen Sie sicher, dass der NGINX Ingress Controller installiert ist.	Geben Sie den `helm list` -Befehl ein. Die Ausgabe sollte zeigen, dass der NGINX Ingress Controller installiert ist.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Route 53 A-Datensatz.	Der A-Datensatz verweist auf den Network Load Balancer, der vom NGINX Ingress Controller erstellt wurde. 1. Rufen Sie den DNS-Namen des Network Load Balancer. Anweisungen finden Sie unter Den DNS-Namen für einen ELB-Load Balancer abrufen. 2. Wählen Sie auf der Amazon Route 53 53-Konsole Hosted Zones aus. 3. Wählen Sie die öffentlich gehostete Zone aus, in der Sie den Datensatz erstellen möchten, und klicken Sie dann auf Datensatz erstellen. 4. Geben Sie einen Namen für den Datensatz ein. 5. Wählen Sie unter Datensatz typ die Option A — Leitet den Datenverkehr an IPv4 und einige AWS-Resso urcen weiter. 6. Aktivieren Sie Alias. 7. Gehen Sie unter Verkehr weiterleiten nach wie folgt vor: a. Wählen Sie Alias to Network Load Balancer.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	b. Wählen Sie die AWS-Region aus, in der der Network Load Balancer bereitgestellt wird. c. Geben Sie den DNS-Namen des Network Load Balancer ein. 8. Wählen Sie Create records (Datensätze erstellen).	

NGINX VirtualServer auf Amazon EKS einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie NGINX VirtualServer bereit.	Die VirtualServer NGINX-Ressource ist eine Lastenausgleichskonfiguration, die eine Alternative zur Eingangsressource darstellt. Die Konfiguration zum Erstellen der VirtualServer NGINX-Ressource ist in der Datei im `nginx_virtualserver.yaml` Verzeichnis verfügbar. `6-Nginx-Virtual-Server` Geben Sie den folgenden Befehl ein, `kubectl` um die VirtualServer NGINX-Ressource zu erstellen. `kubectl apply -f nginx_virtualserver.yaml`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Important Stellen Sie sicher, dass Sie den Anwendung sdomänennamen, den geheimen Zertifika tsschlüssel und den Namen des Anwendungsdienstes in der `nginx_vir tualserver.yaml` Datei aktualisieren.	
Stellen Sie sicher, dass NGINX erstellt wurde VirtualServer .	Geben Sie den folgenden Befehl ein`kubectl`, um zu überprüfen, ob die VirtualSe rver NGINX-Ressource erfolgreich erstellt wurde. `kubectl get virtualse rver` **Note** Stellen Sie sicher, dass die `Host` Spalte mit dem Domainnam en Ihrer Anwendung übereinstimmt.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den NGINX-Web server mit aktiviertem TLS bereit.	Dieses Muster verwendet einen NGINX-Webserver mit aktiviertem TLS als Anwendung zum Testen der Verschlüsselung. end-to-en d Die für die Bereitstellung der Testanwendung erforderl ichen Konfigurationsdateien sind im `demo-webserver` Verzeichnis verfügbar. Geben Sie den folgenden Befehl ein`kubectl`, um die Testanwendung bereitzus tellen. `kubectl apply -f nginx-tls-ap.yaml`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die Ressourcen für die Testanwendung erstellt wurden.	Geben Sie die folgenden Befehle ein, `kubectl` um zu überprüfen, ob die erforderlichen Ressourcen für die Testanwendung erstellt wurden: • `kubectl get deployments` **Note** Überprüfen Sie die `Ready` Spalte und die `Available` Spalte. • `kubectl get pods | grep -i example-deploy` **Note** Die Pods sollten sich im richtigen `running` Zustand befinden. • `kubectl get configmap` • `kubectl get svc`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Anwendung.	1. Geben Sie den folgenden Befehl ein, indem Sie den `<application-domain-name>` durch den Route53-DNS-Namen ersetzen, den Sie zuvor erstellt haben. `curl --verbose https://<application-domain-name>` 2. Stellen Sie sicher, dass Sie auf die Anwendung zugreifen können.	AWS DevOps

Zugehörige Ressourcen

AWS-Ressourcen

- Erstellen von Datensätzen mithilfe der Amazon Route 53 53-Konsole (Amazon Route 53 53-Dokumentation)
- Verwenden eines Network Load Balancer mit dem NGINX-Ingress-Controller auf Amazon EKS (AWS-Blogbeitrag)

Sonstige Ressourcen

- Route 53 (Cert-Manager-Dokumentation)
- Konfiguration des DNS01 Challenge Providers (Cert-Manager-Dokumentation)
- Lassen Sie uns die DNS-Herausforderung verschlüsseln (Let's Encrypt-Dokumentation)

Vereinfachen Sie die Bereitstellung von Amazon EKS-Anwendungen für mehrere Mandanten mithilfe von Flux

Erstellt von Nadeem Rahaman (AWS), Aditya Ambati (AWS), Aniket Dekate (AWS) und Shrikant Patil (AWS)

Übersicht

AWS CodeCommit Hinweis: ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Bei vielen Unternehmen, die Produkte und Dienstleistungen anbieten, handelt es sich um datenregulierte Branchen, die Datenbarrieren zwischen ihren internen Geschäftsfunktionen aufrechterhalten müssen. Dieses Muster beschreibt, wie Sie die Multi-Tenancy-Funktion in Amazon Elastic Kubernetes Service (Amazon EKS) verwenden können, um eine Datenplattform aufzubauen, die eine logische und physische Isolierung zwischen Mandanten oder Benutzern erreicht, die sich einen einzigen Amazon EKS-Cluster teilen. Das Muster bietet Isolierung durch die folgenden Ansätze:

- Isolierung des Kubernetes-Namespaces
- Rollenbasierte Zugriffskontrolle (RBAC)
- Netzwerkrichtlinien
- Ressourcenkontingente
- AWS Identity and Access Management (IAM) -Rollen für Dienstkonten (IRSA)

Darüber hinaus verwendet diese Lösung Flux, um die Mandantenkonfiguration bei der Bereitstellung von Anwendungen unveränderlich zu halten. Sie können Ihre Mandantenanwendungen bereitstellen, indem Sie in Ihrer Konfiguration das Mandanten-Repository angeben, das die `kustomization.yaml` Flux-Datei enthält.

Dieses Muster implementiert Folgendes:

- Ein AWS CodeCommit Repository, AWS CodeBuild Projekte und eine AWS CodePipeline Pipeline, die durch manuelles Bereitstellen von Terraform-Skripten erstellt werden.
- Netzwerk- und Rechenkomponenten, die für das Hosting der Mandanten erforderlich sind. Diese werden durch CodePipeline und mithilfe CodeBuild von Terraform erstellt.

- Mandanten-Namespaces, Netzwerkrichtlinien und Ressourcenkontingente, die anhand eines Helm-Diagramms konfiguriert werden.
- Anwendungen, die verschiedenen Mandanten gehören und mithilfe von Flux bereitgestellt werden.

Wir empfehlen Ihnen, Ihre eigene Architektur für Mehrmandantenfähigkeit auf der Grundlage Ihrer individuellen Anforderungen und Sicherheitsüberlegungen sorgfältig zu planen und zu erstellen. Dieses Muster bietet einen Ausgangspunkt für Ihre Implementierung.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- AWS Command Line Interface (AWS CLI) Version 2.11.4 oder höher, installiert und konfiguriert
- Terraform Version 0.12 oder höher ist auf Ihrem lokalen Computer installiert
- Terraform AWS Provider Version 3.0.0 oder höher
- Kubernetes Provider Version 2.10 oder höher
- Helm Provider Version 2.8.0 oder höher
- Kubectl Provider Version 1.14 oder höher

Einschränkungen

- Abhängigkeit von manuellen Terraform-Bereitstellungen: Die anfängliche Einrichtung des Workflows, einschließlich der Erstellung von CodeCommit Repositorys, CodeBuild Projekten und CodePipeline Pipelines, basiert auf manuellen Terraform-Bereitstellungen. Dies führt zu potenziellen Einschränkungen in Bezug auf Automatisierung und Skalierbarkeit, da bei Infrastrukturänderungen manuelle Eingriffe erforderlich sind.
- CodeCommit Abhängigkeit von Repositorys: Der Workflow stützt sich auf CodeCommit Repositorien als Lösung für die Quellcodeverwaltung und ist eng mit AWS-Services diesen verknüpft.

Architektur

Zielarchitekturen

Dieses Muster setzt drei Module zum Aufbau der Pipeline-, Netzwerk- und Recheninfrastruktur für eine Datenplattform ein, wie in den folgenden Diagrammen dargestellt.

Pipeline-Architektur:

Netzwerkarchitektur:

Rechenarchitektur:

Tools

AWS-Services

- AWS CodeBuildist ein vollständig verwalteter Build-Service, der Ihnen hilft, Quellcode zu kompilieren, Komponententests durchzuführen und Artefakte zu erstellen, die sofort einsatzbereit sind.
- AWS CodeCommitist ein Versionskontrolldienst, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodePipelinehilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.
- Mit Amazon Elastic Kubernetes Service (Amazon EKS) können Sie Kubernetes ausführen, AWS ohne dass Sie Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten müssen.
- AWS Transit Gatewayist ein zentraler Hub, der virtuelle private Clouds () und lokale Netzwerke verbindet. VPCs
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk bereitzustellen. Dieses virtuelle Netzwerk entspricht einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben würden, mit den Vorteilen der Verwendung der skalierbaren Infrastruktur von AWS.

Andere Tools

- Cilium-Netzwerkrichtlinien unterstützen Kubernetes L3- und L4-Netzwerkrichtlinien. Sie können mit L7-Richtlinien erweitert werden, um Sicherheit auf API-Ebene für HTTP, Kafka und gRPC sowie andere ähnliche Protokolle bereitzustellen.
- Flux ist ein Git-basiertes Continuous Delivery (CD) -Tool, das Anwendungsbereitstellungen auf Kubernetes automatisiert.
- Helm ist ein Open-Source-Paketmanager für Kubernetes, der Sie bei der Installation und Verwaltung von Anwendungen auf Ihrem Kubernetes-Cluster unterstützt.
- Terraform ist ein IaC-Tool (Infrastructure as Code), mit dem Sie Cloud- und lokale HashiCorp Ressourcen erstellen und verwalten können.

Code-Repository

Der Code für dieses Muster ist im GitHub EKS Multi-Tenancy Terraform Solution Repository verfügbar.

Bewährte Methoden

Richtlinien und bewährte Methoden für die Verwendung dieser Implementierung finden Sie im Folgenden:

- Bewährte Methoden für Amazon EKS für mehrere Mandanten
- Flux-Dokumentation

Epen

Erstellen Sie Pipelines für die Phasen Erstellen, Testen und Bereitstellen von Terraform

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Projekt-Repository.	Klonen Sie das GitHub EKS Multi-Tenancy Terraform Solution Repository, indem Sie den folgenden Befehl in einem Terminalfenster ausführen: `git clone https://github.com/aws-samp`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`les/aws-eks-multit enancy-deployment.git`	

Bootstrap für den Terraform S3-Bucket und Amazon DynamoDB.	1. Öffnen Sie in dem `bootstrap` Ordner die `bootstrap.sh` Datei und aktualisieren Sie die Variablenwerte für den S3-Bucket-Namen, den DynamoDB-Tabellennamen und: AWS-Region
	`S3_BUCKET_NAME="<S 3_BUCKET_NAME>" DYNAMODB_TABLE_NA ME="<DYNAMODB_NAME >" REGION="<AWS_REGI ON>"`
	2. Führen Sie das `bootstrap .sh` -Skript aus. Für das Skript ist der erforderlich AWS CLI, den Sie als Teil der Voraussetzungen installiert haben.
	`cd bootstrap ./bootstrap.sh`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisieren Sie die `locals.tf` Dateien `run.sh` und.	1. Nachdem der Bootstrap -Vorgang erfolgreich abgeschlossen wurde, kopieren Sie den Namen des S3-Buckets und der DynamoDB-Tabelle aus dem `variables` Abschnitt des Skripts: `bootstrap.sh`
	`# Variables S3_BUCKET_NAME="< S3_BUCKET_NAME>" DYNAMODB_TABLE_NAME ="<DYNAMODB_NAME"`
	2. Fügen Sie diese Werte in das `run.sh` Skript ein, das sich im Stammverzeichnis des Projekts befindet:
	`BACKEND_BUCKET_ID= "<SAME_NAME_AS_S3_ BUCKET_NAME>" DYNAMODB_ID=" <SAME_NAME_AS_DYNA MODB_NAME>"`
	3. Laden Sie den Projektco de in ein CodeCommi t Repository hoch. Sie können dieses Repository automatisch über Terraform erstellen, indem Sie die folgende Variable `true` in der `demo/pipeline/`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`locals.tf` Datei auf setzen: `create_new_repo = true` 4. Aktualisieren Sie die `locals.tf` Datei gemäß Ihren Anforderungen, um Pipeline-Ressourcen zu erstellen.	

Stellen Sie das Pipeline-Modul bereit.	Führen Sie die folgenden Terraform-Befehle manuell aus, um Pipeline-Ressourcen zu erstellen. Es gibt keine Orchestrierung für die automatische Ausführung dieser Befehle.
	`./run.sh -m pipeline -e demo -r <AWS_REGION> -t init`
	`./run.sh -m pipeline -e demo -r <AWS_REGION> -t plan`
	`./run.sh -m pipeline -e demo -r <AWS_REGION> -t apply`
		AWS DevOps

Erstellen Sie die Netzwerkinfrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Pipeline.	1. Vergewissern Sie sich, dass in dem	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`templates` Ordner für die `buildspec` Dateien die folgende Variable gesetzt ist`network`: `TF_MODULE_TO_BUILD: "network"` 2. Starten Sie in der CodePipeline Konsole auf der Seite mit den Pipeline-Details die Pipeline, indem Sie Änderung veröffent lichen auswählen. Nach dieser ersten Ausführun g wird die Pipeline automatis ch gestartet, wenn Sie eine Änderung an den Hauptzweig des CodeCommit Repositorys übertragen. Die Pipeline umfasst die folgenden Phasen: • `validate`initialisiert Terraform, führt Terraform -Sicherheitsscans mithilfe der Tools checkov und tfsec durch und lädt die Scanberic hte in den S3-Bucket hoch. • `plan` zeigt den Terraform-Plan an und lädt den Plan in den S3-Bucket hoch.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `apply`wendet die Terraform -Planausgabe aus dem S3-Bucket an und erstellt Ressourcen. AWS • `destroy`entfernt die während der Phase erstellte n AWS Ressourcen. `apply` Um diese optionale Phase zu aktivieren, setzen Sie die folgende Variable `true` in der `demo/pipeline/locals.tf` Datei auf: `enable_destroy_stage = true`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die über das Netzwerkmodul erstellten Ressourcen.	Vergewissern Sie sich, dass die folgenden AWS Ressourcen nach der erfolgreichen Bereitstellung der Pipeline erstellt wurden: • Eine Ausgangs-VPC mit drei öffentlichen und drei privaten Subnetzen, einem Internet-Gateway und einem NAT-Gateway. • Eine Amazon EKS-VPC mit drei privaten Subnetzen. • Mandant 1 und Mandant 2 VPCs mit jeweils drei privaten Subnetzen. • Ein Transit-Gateway mit allen VPC-Anhängen und Routen zu jedem privaten Subnetz. • Eine statische Transit-Gateway-Route für die Amazon EKS-Ausgangs-VPC mit einem Ziel-CIDR-Block von. `0.0.0.0/0` Dies ist erforderlich, VPCs um allen den ausgehenden Internetzugang über die Amazon EKS-Ausgangs-VPC zu ermöglichen.	AWS DevOps

Erstellen Sie die Recheninfrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Update`locals.tf` , um den Zugriff des CodeBuild Projekts auf die VPC zu ermöglichen.	Um die Add-Ons für den privaten Amazon EKS-Cluster bereitzustellen, muss das CodeBuild Projekt an die Amazon EKS-VPC angehängt werden.
	1. Öffnen Sie in dem `demo/pipeline` Ordner die `locals.tf` Datei und setzen Sie die `vpc_enabled` Variable auf`true`.
	2. Führen Sie das `run.sh` Skript aus, um die Änderungen auf das Pipeline-Modul anzuwenden:
	`demo/pipeline/locals.tf`
	`./run.sh -m pipeline -env demo -region <AWS_REGION> -tfcmd init`
	`./run.sh -m pipeline -env demo -region <AWS_REGION> -tfcmd plan`
	`./run.sh -m pipeline -env demo -region <AWS_REGION> -tfcmd apply`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die `buildspec` Dateien, um das Rechenmodul zu erstellen.	Setzen `templates` Sie im Ordner in allen `buildspec` YAML-Dateien den Wert der `TF_MODULE_TO_BUILD` Variablen von `network` bis`compute`: `TF_MODULE_TO_BUILD: "compute"`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisieren Sie die `values` Datei für das Helm-Diagramm für die Mandantenverwaltung.	1. Öffnen Sie die `values.yaml` Datei am folgenden Speicherort:
	`cd cfg-terraform/demo/compute/cfg-tenant-mgmt`
	Die Datei sieht wie folgt aus:
	`---`
	`global:`
	`  clusterRoles:`
	`  operator:`
	`  platform-tenant`
	`  flux: flux-tenant-applier`
	`  flux:`
	`  tenantCloneBaseUrl: ${TEANT_BASE_URL}`
	`  repoSecret:`
	`  ${TENANT_REPO_SECRET}`
	`tenants:`
	`  tenant-1:`
	`  quotas:`
	`  limits:`
	`  cpu: 1`
	`  memory: 1Gi`
	`  flux:`
	`  path: overlays/tenant-1`
	`  tenant-2:`
	`  quotas:`
	`  limits:`
	`  cpu: 1`
	`  memory: 2Gi`
	`  flux:`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>path: overlays/
	tenant-2</pre>
	2. Aktualisieren Sie in den `tenants` Abschnitten `global` und die Konfiguration entsprechend Ihren Anforderungen:
	• `tenantCloneBaseUrl` — Pfad zum Repository, das den Code für alle Mandanten hostet (wir verwenden dasselbe Git-Repository für alle Mandanten)
	• `repoSecret` — Kubernetes-Secret, das die SSH-Schlüssel und bekannten Hosts für die Authentifizierung beim globalen Mandanten-Git-Repository enthält
	• `quotas`— Kubernetes-Ressourcenkontingente, die Sie für jeden Mandanten beantragen möchten
	• `flux path`— Pfad zu den YAML-Dateien der Mandantenanwendung im globalen Mandanten-Repository	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Rechenressourcen.	CodePipeline Startet automatisch, nachdem Sie die Dateien in den vorherigen Schritten aktualisiert haben. Vergewissern Sie sich, dass die folgenden AWS Ressourcen für die Recheninfrastruktur erstellt wurden: • Amazon EKS-Cluster mit privatem Endpunkt • Amazon EKS-Worker-Knoten • Amazon EKS-Add-Ons: externe Geheimnisse `aws-loadbalancer-controller` , und `metrics-server` • GitOps Modul, Flux-Helm-Diagramm, Cilium-Helm-Diagramm und Mandantenmanagement-Helm-Diagramm	AWS DevOps

Schauen Sie sich die Mandantenverwaltung und andere Ressourcen an

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Ressourcen zur Mandantenverwaltung in Kubernetes.	Führen Sie die folgenden Befehle aus, um zu überprüfen, ob die Ressourcen für die Mandantenverwaltung erfolgreich mit Hilfe von Helm erstellt wurden.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	1. Mandanten-Namespaces wurden erstellt, wie in: `values.yaml`
	`kubectl get ns -A`
	2. Jedem Mandanten-Namespace werden Kontingente zugewiesen, wie in: `values.yaml`
	`kubectl get quota --namespace=<tenant_namespace>`
	3. Die Angaben zu den Kontingenten sind für jeden Mandanten-Namespace korrekt:
	`kubectl describe quota cpu-memory-resource-quota-limit -n <tenant_namespace>`
	4. Die Cilium-Netzwerkrichtlinien wurden auf jeden Mandanten-Namespace angewendet:
	`kubectl get CiliumNetworkPolicy -A`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Bereitstellungen von Mandantenanwendungen.	Führen Sie die folgenden Befehle aus, um zu überprüfen, ob die Mandantenanwendungen bereitgestellt wurden.
	1. Flux kann eine Verbindung zu dem CodeCommit Repository herstellen, das im GitOps Modul angegeben ist:
	`kubectl get gitrepositories -A`
	2. Der Flux-Kustomization-Controller hat die YAML-Dateien im Repository bereitgestellt: CodeCommit
	`kubectl get kustomizations -A`
	3. Alle Anwendungsressourcen werden in ihren Mandanten-Namespaces bereitgestellt:
	`kubectl get all -n <tenant_namespace>`
	4. Für jeden Mandanten wurde ein Ingress erstellt:
	`kubectl get ingress -n <tenant_namespace>`	

Fehlerbehebung

Problem	Lösung

Sie erhalten eine Fehlermeldung, die der folgenden ähnelt:
 	
`Failed to checkout and determine revision: unable to clone unknown error: You have successfully authenticated over SSH. You can use Git to interact with AWS CodeCommit.`
	Gehen Sie wie folgt vor, um das Problem zu beheben:
	
	1. Überprüfen Sie das Mandantenanwendung s-Repository: Ein leeres oder falsch konfiguriertes Repository könnte den Fehler verursachen. Stellen Sie sicher, dass das Mandantenanwendungs-Repository den erforderlichen Code enthält.
	2. Stellen Sie das `tenant_mgmt` Modul erneut bereit: Suchen Sie in der `tenant_mgmt` Modulkonfigurationsdatei nach dem `app` Block und setzen Sie den `deploy` Parameter auf`0`:
	
	`deploy = 0`
	
	Nachdem Sie den `apply` Terraform-Befehl ausgeführt haben, ändern Sie den `deploy` Parameterwert wieder in: `1`
	
	`deploy = 1`
	
	3. Überprüfen Sie den Status erneut: Nachdem Sie die vorherigen Schritte ausgeführt haben, überprüfen Sie mit dem folgenden Befehl, ob das Problem weiterhin besteht:
	
	`kubectl get gitrepositories -A`
	
	Wenn das Problem weiterhin besteht, sollten Sie sich eingehender mit den Flux-Prot okollen befassen, um weitere Informationen

Problem	Lösung
	zu erhalten, oder lesen Sie den allgemeinen Flux-Leitfaden zur Fehlerbehebung.

Zugehörige Ressourcen

- Amazon EKS Blueprints für Terraform
- Amazon EKS Best Practices-Leitfäden, Abschnitt Mehrmandantenfähigkeit
- Flux-Webseite
- Helm-Webseite

Zusätzliche Informationen

Hier ist ein Beispiel für eine Repository-Struktur für die Bereitstellung von Mandantenanwendungen:

```
applications
sample_tenant_app
### README.md
### base
#   ### configmap.yaml
#   ### deployment.yaml
#   ### ingress.yaml
#   ### kustomization.yaml
#   ### service.yaml
### overlays
    ### tenant-1
    #   ### configmap.yaml
    #   ### deployment.yaml
    #   ### kustomization.yaml
    ### tenant-2
        ### configmap.yaml
        ### kustomization.yaml
```

Abonnieren Sie mithilfe einer benutzerdefinierten Ressource mehrere E-Mail-Endpunkte für ein SNS-Thema

Erstellt von Ricardo Morais (AWS)

Übersicht

Hinweis, August 2022: AWS unterstützt CloudFormation jetzt das Abonnement mehrerer Ressourcen über das AWS::SNS::TopicObjekt und sein Abonnementattribut.

Dieses Muster beschreibt, wie Sie mehrere E-Mail-Adressen abonnieren, um Benachrichtigungen von einem Amazon Simple Notification Service (Amazon SNS) -Thema zu erhalten. Es verwendet eine AWS-Lambda-Funktion als benutzerdefinierte Ressource in einer CloudFormation AWS-Vorlage. Die Lambda-Funktion ist mit einem Eingabeparameter verknüpft, der die E-Mail-Endpunkte für das SNS-Thema angibt.

Derzeit können Sie die CloudFormation AWS-Vorlagenobjekte verwenden AWS::SNS::Topicund AWS::SNS::Subscriptioneinzelne Endpunkte für SNS-Themen abonnieren. Um mehrere Endpunkte zu abonnieren, müssen Sie das Objekt mehrmals aufrufen. Wenn Sie die Lambda-Funktion als benutzerdefinierte Ressource verwenden, können Sie mehrere Endpunkte über einen Eingabeparameter abonnieren. Sie können diese Lambda-Funktion als benutzerdefinierte Ressource in jeder CloudFormation AWS-Vorlage verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein AWS-Profil, das in Ihrer lokalen Umgebung mit einem Zugriffsschlüssel und einem geheimen Schlüssel konfiguriert ist.
- Berechtigungen für Folgendes:
  - Rolle und Richtlinie von AWS Identity and Access Management (IAM)
  - AWS Lambda-Funktion
  - Amazon Simple Storage Service (Amazon S3) zum Hochladen der Lambda-Funktion
  - Thema und Richtlinie von Amazon SNS
  - CloudFormation AWS-Stapel

Einschränkungen

- Der Code unterstützt Linux- und MacOS-Workstations.

Produktversionen

- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 2 oder höher.

Architektur

Zieltechnologie-Stack

- AWS CloudFormation
- Amazon SNS
- AWS Lambda

Tools

Tools

- AWS-CLI Version 2

Code

Der Anhang enthält die folgenden Dateien:

- Lambda-Funktion: `lambda_function.py`
- CloudFormation AWS-Vorlage: `template.yaml`
- Zwei Parameterdateien für die Verwaltung mehrerer oder einzelner E-Mail-Endpunktabonnements: `parameters-multiple-values.json` (wird standardmäßig verwendet) und `parameters-one-value.json`

Um den Stack bereitzustellen, können Sie eine der beiden Parameterdateien verwenden. Um mehrere E-Mail-Endpunkte anzugeben:

```
./deploy.sh -p <YOUR_AWS_PROFILE_NAME> -r <YOUR_AWS_PROFILE_REGION>
```

Um einen einzelnen E-Mail-Endpunkt anzugeben:

```
./deploy.sh -p <YOUR_AWS_PROFILE_NAME> -r <YOUR_AWS_PROFILE_REGION> -f parameters-one-value.json
```

Epen

Option 1 — Stellen Sie ein SNS-Thema mit einem E-Mail-Abonnement bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den E-Mail-Endpunkt für SNS-Theme nabonnements.	Bearbeiten Sie die Datei `parameters-one-value.json` (angehängt) und ändern Sie den Wert des `pSNSNotificationsEmail` Parameters so, dass er der E-Mail-Adresse entspricht, die Sie verwenden möchten, z. B. `someone@example.com`	
Stellen Sie den CloudFormation AWS-Stack bereit, der die Ressourcen und das Abonnement erstellt.	Führen Sie den Befehl deploy.sh mit Ihrem AWS-Profilnamen, Ihrer AWS-Region und der `parameters-one-value.json` Datei aus. `./deploy.sh -p <YOUR_AWS_PROFILE_NAME> -r <YOUR_AWS_PROFILE_REGION> -f parameters-one-value.json`	IAM-Rolle mit den richtigen Berechtigungen

Option 2 — Stellen Sie ein SNS-Thema mit zwei oder mehr E-Mail-Abonnements bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die E-Mail-Endpunkte für SNS-Theme nabonnements.	Bearbeiten Sie die Datei `parameters-multiple-values.json` (angehängt) und ändern Sie den Wert des `pSNSNotificationsEmail` Parameters so, dass er die E-Mail-Adressen wiedergibt, die Sie verwenden möchten, getrennt durch Kommas, wie folgt:. `someone1@example.com, someone2@example.com`	
Stellen Sie den CloudFormation AWS-Stack bereit, der die Ressourcen und das Abonnement erstellt.	Führen Sie den Befehl deploy.sh mit Ihrem AWS-Profilnamen und Ihrer AWS-Region aus. Sie müssen die `parameters-multiple-values.json` Datei nicht angeben, da sie standardmäßig verwendet wird. `./deploy.sh -p <YOUR_AWS_PROFILE_NAME> -r <YOUR_AWS_PROFILE_REGION>`	IAM-Rolle mit den richtigen Berechtigungen

Option 3 — Bereitstellen eines SNS-Themas über eine AWS-Vorlage CloudFormation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein SNS-Thema.	Erstellen Sie ein SNS-Thema über eine CloudForm	IAM-Rolle mit den richtigen Berechtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ation AWS-Vorlage, ohne Abonnementendpunkte im `AWS::SNS::Topic` Vorlagenobjekt anzugeben. Sie können den `template.yaml` Anhang als Ausgangspunkt verwenden.	
Erstellen Sie eine SNS-Themenrichtlinie.	Erstellen Sie eine SNS-Themenrichtlinie in der CloudFormation AWS-Vorlage.	IAM-Rolle mit den richtigen Berechtigungen
Abonnieren Sie die Liste der E-Mail-Endpunkte für das SNS-Thema.	Abonnieren Sie anhand der Liste der E-Mail-Endpunkte (einer oder mehrere) die Endpunkte für das von Ihnen erstellte SNS-Thema.	IAM-Rolle mit den richtigen Berechtigungen

Zugehörige Ressourcen

Referenzen

- CloudFormation Benutzerdefinierte AWS-Ressourcen (AWS-Dokumentation)
- Erstellung CloudFormation benutzerdefinierter AWS-Ressourcen mit Python, AWS Lambda und crhelper (Blogbeitrag)

Erforderliche Tools

- AWS-CLI Version 2

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Koordinieren Sie die Ressourcenabhängigkeit und die Aufgabenausführung mithilfe des AWS Fargate WaitCondition Hook-Konstrukts

Erstellt von Stan Fan (AWS)

Übersicht

Dieses Muster beschreibt das WaitCondition hook (`waitcondition-hook-for-aws-fargate-task`) npm-Paket, eine cloudnative Lösung, die für die Orchestrierung von AWS FargateAufgaben in Amazon Elastic Container Service (Amazon ECS) -Clustern entwickelt wurde.

Der WaitCondition Hook ist ein AWS Cloud Development Kit (AWS CDK) Konstrukt, das speziell auf die Integration mit zugeschnitten ist. AWS CloudFormation Der WaitCondition Hook bietet die folgenden wichtigen Funktionen:

- Dient als Mechanismus für Wartebedingungen und unterbricht die CloudFormation Stack-Ausführung, bis eine bestimmte Fargate-Aufgabe abgeschlossen ist. Dies hilft bei ordnungsgemäßer Bereitstellung und Ressourcenbereitstellung.
- Unterstützt Python TypeScript und ist somit ideal für AWS CDK Projekte.
- Ermöglicht Entwicklern und Architekten die Orchestrierung von Bereitstellungen, indem sie die Ausführung von Aufgaben und das Ressourcenmanagement für containerisierte Anwendungen koordinieren. AWS
- Ermöglicht die Ausführung von Fargate-Aufgaben mit einem oder mehreren Containern, die in einen CloudFormation Lebenszyklus eingebettet sind, und kann Aufgabenausfälle behandeln und den CloudFormation Stack nach einem Aufgabenausfall rückgängig machen.
- Bietet Flexibilität beim Hinzufügen von Abhängigkeiten zwischen Ressourcen und den Ergebnissen der Fargate-Aufgabenausführung, wodurch benutzerdefinierte Aufgaben aktiviert oder andere Endpunkte aufgerufen werden können. Sie können beispielsweise einen CloudFormation Stack anhalten und auf eine Datenbankmigration warten (die durch eine Fargate-Aufgabe durchgeführt wird) und andere Ressourcen bereitstellen, die möglicherweise vom Erfolg der Datenbankmigration abhängen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto.

- AWS Cloud Development Kit (AWS CDK) Die Befehlszeilenschnittstelle (CLI) ist auf einer lokalen Workstation installiert. Weitere Informationen finden Sie in der AWS CDK CLI-Referenz in der AWS CDK Dokumentation.
- Node Package Manager (npm), auf einer lokalen Workstation installiert und für den AWS CDK in TypeScript konfiguriert. Weitere Informationen finden Sie in der npm-Dokumentation unter Node.js und npm herunterladen und installieren.
- Yarn wurde auf einer lokalen Workstation installiert. Weitere Informationen finden Sie unter Installation in der Yarn-Dokumentation.

Einschränkungen

- Diese Lösung wird in einer einzigen Lösung bereitgestellt AWS-Konto.
- Der erwartete Rückgabecode des Containers steht `0` für Erfolg. Jeder andere Rückgabecode weist auf einen Fehler hin, und der CloudFormation Stack wird zurückgesetzt.
- Einige AWS-Services sind nicht in allen verfügbar AWS-Regionen. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie unter Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Architektur

Das folgende Diagramm zeigt die Konstruktarchitektur.

Das Diagramm zeigt den Arbeitsablauf von: `waitcondition-hook-for-aws-fargate-task`

1. `WaitCondition`und `WaitConditionHandler` sind so eingerichtet, dass sie die Antwort der AWS Lambda Funktionen abhören.
2. Je nach Ergebnis der Aufgabe `ErrorHandlerFunction` wird entweder der `CallbackFunction` oder der durch das Ende der Fargate-Aufgabe ausgelöst.
3. Die Lambda-Funktion sendet ein SUCCEED- oder FAILURE-Signal an`WaitConditionHandler`.
4. `WaitConditionHandler`setzt die Bereitstellung der Ressourcen fort, wenn das Ausführungsergebnis der Fargate-Aufgabe erfolgreich ist, oder setzt den Stack zurück, wenn die Aufgabe fehlgeschlagen ist.

Das folgende Diagramm zeigt ein Beispiel für einen Workflow zur Durchführung einer Datenbankmigration.

Der Beispiel-Workflow verwendet das `waitcondition-hook-for-aws-fargate-task` Konstrukt, um eine Datenbankmigration wie folgt durchzuführen:

1. Eine Amazon Relational Database Service (Amazon RDS) -Instance wird bereitgestellt.
2. Das `waitcondition-hook-for-aws-fargate-task` Konstrukt führt die Datenbankmigrationsaufgabe aus und pausiert den Stack als Amazon Elastic Compute Cloud (Amazon EC2) -Instance.
3. Wenn die Migrationsaufgabe erfolgreich abgeschlossen wurde, sendet sie ein Erfolgssignal an CloudFormation. Andernfalls sendet sie ein Fehlersignal an den Stack CloudFormation und führt ein Rollback durch.

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK)ist ein Softwareentwicklungs-Framework, das Ihnen hilft, die Cloud-Infrastruktur im Code zu definieren und diese bereitzustellen AWS CloudFormation.
- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und zu verwalten AWS-Regionen.
- Amazon CloudWatch hilft Ihnen dabei, die Kennzahlen Ihrer AWS Ressourcen und der Anwendungen, auf denen Sie laufen, AWS in Echtzeit zu überwachen.
- Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Beenden und Verwalten von Containern in einem Cluster vereinfacht.
- AWS Fargatehilft Ihnen beim Betrieb von Containern, ohne Server oder EC2 Amazon-Instances verwalten zu müssen. Es wird in Verbindung mit Amazon ECS verwendet.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.

- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Step Functionsist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Funktionen und andere Funktionen kombinieren können, um geschäftskritische AWS-Services Anwendungen zu erstellen.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk bereitzustellen. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, und bietet die Vorteile der Nutzung der skalierbaren Infrastruktur von AWS.

Andere Tools

- npm ist eine Softwareregistrierung, die in einer Node.js -Umgebung ausgeführt wird und verwendet wird, um Pakete gemeinsam zu nutzen oder auszuleihen und die Bereitstellung von privaten Paketen zu verwalten.
- Yarn ist ein Open-Source-Paketmanager, mit dem Sie Abhängigkeiten in JavaScript Projekten verwalten können. Yarn kann Sie bei der Installation, Aktualisierung, Konfiguration und Entfernung von Paketabhängigkeiten unterstützen.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub waitcondition-hook-for-aws-fargate-task verfügbar.

Bewährte Methoden

- Folgen Sie beim Erstellen Ihrer AWS CDK App den Best Practices für die Entwicklung und Bereitstellung der Cloud-Infrastruktur AWS CDK in der v2-Dokumentation. AWS CDK
- Folgen Sie für AWS Fargate diese Aufgabe den Best Practices für Amazon ECS-Container-Images in der Amazon ECS-Dokumentation.

Epen

Richten Sie das ein AWS CDK

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie das AWS CDK.	Führen Sie den folgenden Befehl aus, um den AWS CDK auf Ihrem lokalen Computer oder einer anderen Umgebung zu installieren: `npm install -g aws-cdk@latest`	Cloud-Architekt, App-Entwickler
Bootstrap das AWS CDK.	Bootstrapping ist der Prozess der Vorbereitung einer Umgebung für die Bereitstellung. Führen Sie den folgenden Befehl aus, um Ihr AWS CDK Toolkit für das Ziel AWS-Konto und zu AWS-Region booten: `cdk bootstrap aws://ACCOUNT-NUMBER-1/REGION-1` Dieser Befehl erstellt einen CloudFormation Stack mit dem Namen. `CDKToolkit`	Cloud-Architekt

Führen Sie das Konstrukt WaitCondition Hook for AWS Fargate Tasks aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das CDK-Projekt.	Erstellen Sie ein CDK-Projekt in der Sprache, die Sie bevorzugen. Dieses Muster verwendet TypeScript. Führen Sie den folgenden Befehl aus TypeScript, um ein CDK-Projekt mit zu erstellen: `cdk init app –language typescript`	Cloud-Architekt
Installieren Sie das Paket .	Führen Sie es `npm install` im Root-Pfad Ihres CDK-Projekts aus. Nachdem die CDK-Bibliothek installiert wurde, führen Sie zur Installation den folgenden Befehl aus: `waitcondition-hook-for-aws-fargate-task` `yarn add waitcondition-hook-for-aws-fargate-task`	Cloud-Architekt
Erstellen Sie Ihre CDK-Anwendung und Amazon ECS-Komponenten.	Erstellen Sie Ihr CDK-Projekt. Eine Amazon ECS-Aufgabendefinitionsressource ist erforderlich. Informationen zum Erstellen einer Aufgabendefinition finden Sie unter Amazon ECS-Aufgabendefinitionen in der Amazon ECS-Dokumentation.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Das folgende Beispiel verwendet dieses Konstrukt:
	
	`import * as cdk from 'aws-cdk-lib';`
	`import { Vpc } from 'aws-cdk-lib/aws-ec2';`
	`import * as ecr from 'aws-cdk-lib/aws-ecr';`
	`import * as ecs from 'aws-cdk-lib/aws-ecs';`
	`import { Construct } from 'constructs';`
	`import { FargateRunner } from 'waitcondition-hook-for-aws-fargate-task';`
	`import { Queue } from 'aws-cdk-lib/aws-sqs';`
	
	`export class FargateRunnerStack extends cdk.Stack {`
	`constructor(scope: Construct, id: string, props?: cdk.StackProps) {`
	`super(scope, id, props);`
	`// Define the VPC`
	`const vpc = new Vpc(this, 'MyVpc')`
	`// Define the Fargate Task`
	`const taskDefinition = new ecs.Farga`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	teTaskDefinition(t his, 'MyTask', {}); // Import exiting ecr repo const repo = ecr.Repository.fro mRepositoryName(this, 'MyRepo', 'RepoName'); // Add a container to the task taskDefin ition.addContainer ('MyContainer', { image: ecs.ContainerImage .fromEcrRepository (repo), }); // Create the Fargate runner const myFargate Runner = new FargateRu nner(this, 'MyRunner ', { fargateTa skDef: taskDefinition, timeout: ` ${60 * 5}`, vpc: vpc, }); // Create the SQS queue const myQueue = new Queue(this, 'MyQueue', {}); // Add dependenc y myQueue.n ode.addDependency(myFargateRunner); }	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`}`	

Synchronisieren und starten Sie die CDK-Anwendung.	1. Um die Assets und die CloudFormation Vorlage zu generieren, führen Sie den folgenden Befehl in Ihrem CDK-Root-Pfad aus:
	`cdk synth`
	2. Führen Sie nach erfolgreicher Ausführung des `synth` Befehls den folgenden Befehl aus, um die Ressourcen bereitzustellen:
	`cdk deploy`
	
	Das `waitcondition-hook-for-aws-fargate-task` Konstrukt führt die Fargate-Aufgabe aus.
		Cloud-Architekt

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen von Ressourcen.	Führen Sie den folgenden Befehl aus, um die im vorherigen Schritt bereitgestellten Ressourcen zu bereinigen: `cdk destroy`	Cloud-Architekt

Fehlerbehebung

Problem	Lösung
Allgemeiner CloudFormation Stack-Fehler	Um allgemeine CloudFormation Stack-Fehler zu beheben, fügen Sie das `--no-rollback` Flag hinzu, wie im folgenden Beispiel gezeigt: `cdk deploy --no-rollback` Mit diesem Befehl wird das Rollback des CloudFormation Stacks angehalten, sodass Sie Ressourcen für die Fehlerbehebung zur Verfügung haben. Weitere Informationen finden Sie in der AWS CloudFormation Dokumentation unter Wählen Sie aus, wie mit Fehlern bei der Bereitstellung von Ressourcen umgegangen werden soll.
AWS Step Functions Fehlschlag	Eine AWS Step Functions Zustandsmaschine kann aus verschiedenen Gründen nicht ausgeführt werden. Wenn die `–disable-rollback` Konfiguration abgeschlossen ist, gehen Sie wie folgt vor, um Fehler zu beheben: 1. Melden Sie sich bei der an AWS Management Console, geben Sie Step Functions in das Suchfeld ein und wählen Sie dann den Step Functions Functions-Dienst aus. 2. Wählen Sie im linken Navigationsbereich State Machines und dann den State Machine aus, der vom CloudFormation Stack bereitgestellt wird. 3. Wählen Sie unter Ausführungen den Namen der Ausführung aus, die unerwartet fehlgeschlagen ist.

Problem	Lösung
	4. Wählen Sie in der Ereignisansicht den fehlgeschlagenen Schritt aus. Weitere Informationen finden Sie in der AWS Step Functions Dokumentation unter Problembehandlung in Step Functions und Anzeigen von Ausführungsdetails in der Step Functions Functions-Konsole.
AWS Lambda Funktionsfehler	Dieses Konstrukt stellt zwei Lambda-Funktionen bereit: `CallbackFunction` und`ErrorhandlerFunction` . Sie können aus verschiedenen Gründen fehlschlagen, z. B. aufgrund unbehandelter Ausnahmen. Gehen Sie wie folgt vor, um Fehler zu beheben: 1. Melden Sie sich bei der an AWS Management Console, geben Sie CloudWatch in das Suchfeld ein und wählen Sie dann den CloudWatch Dienst aus. 2. Wählen Sie im linken Navigationsbereich Log groups (Protokollgruppen) aus. 3. Geben Sie im Suchfeld den Namen der Lambda-Funktion ein. 4. Wählen Sie den Namen der Protokollgruppe, der der Lambda-Funktion zugeordnet ist. 5. Um zum Ergebnis der Ausführung der Lambda-Funktion zu gelangen, wählen Sie den neuesten Protokollstream aus. Weitere Informationen finden Sie in der AWS Lambda Dokumentation unter Problembehandlung in Lambda.

Zugehörige Ressourcen

AWS Dokumentation

- AWS CDK API-Referenz erstellen
- Erste Schritte mit dem AWS CDK
- Erfahren Sie, wie Sie Amazon ECS-Ressourcen erstellen und verwenden
- Erfahren Sie, wie Sie mit Step Functions beginnen
- Was ist AWS CDK?

Sonstige Ressourcen

- Waitcondition Hook für die AWS Fargate Aufgabe (npm)
- waitcondition-hook-for-aws-fargate-task 1.0.6 (pypi.org)

Verwenden Sie Git-Quell-Repositorys von Drittanbietern in AWS CodePipeline

Erstellt von Kirankumar Chandrashekar (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Dieses Muster beschreibt, wie AWS CodePipeline mit Git-Quell-Repositorys von Drittanbietern verwendet wird.

AWS CodePipeline ist ein Continuous Delivery Service, der Aufgaben zum Erstellen, Testen und Bereitstellen Ihrer Software automatisiert. Der Service unterstützt derzeit Git-Repositorys GitHub, die von AWS und Atlassian CodeCommit Bitbucket verwaltet werden. Einige Unternehmen verwenden jedoch Git-Repositorys von Drittanbietern, die in ihren Single Sign-On-Dienst (SSO) und Microsoft Active Directory zur Authentifizierung integriert sind. Sie können diese Git-Repositorys von Drittanbietern als Quellen verwenden, CodePipeline indem Sie benutzerdefinierte Aktionen und Webhooks erstellen.

Ein Webhook ist eine HTTP-Benachrichtigung, die Ereignisse in einem anderen Tool, z. B. einem GitHub Repository, erkennt und diese externen Ereignisse mit einer Pipeline verbindet. Wenn Sie einen Webhook in erstellen CodePipeline, gibt der Service eine URL zurück, die Sie in Ihrem Git-Repository-Webhook verwenden können. Wenn Sie Code in einen bestimmten Branch des Git-Repositorys pushen, initiiert der Git-Webhook den CodePipeline Webhook über diese URL und setzt die Quellphase der Pipeline auf In Bearbeitung. Wenn sich die Pipeline in diesem Status befindet, fragt ein Job-Worker CodePipeline nach dem benutzerdefinierten Job ab, führt den Job aus und sendet einen Erfolgs- oder Fehlerstatus an. CodePipeline Da sich die Pipeline in der Quellphase befindet, ruft der Job-Worker in diesem Fall den Inhalt des Git-Repositorys ab, komprimiert den Inhalt und lädt ihn in den Amazon Simple Storage Service (Amazon S3) -Bucket hoch, in dem Artefakte für die Pipeline gespeichert werden. Dabei wird der Objektschlüssel verwendet, der vom abgefragten Job bereitgestellt wird. Sie können auch einen Übergang für die benutzerdefinierte Aktion mit einem Ereignis in Amazon CloudWatch verknüpfen und den Job Worker auf der Grundlage des Ereignisses initiieren. Mit diesem Setup können Sie Git-Repositorys von Drittanbietern, die der Dienst nicht nativ unterstützt, als Quellen verwenden. CodePipeline

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Git-Repository, das Webhooks unterstützt und über das Internet eine Verbindung zu einer CodePipeline Webhook-URL herstellen kann
- Die AWS-Befehlszeilenschnittstelle (AWS CLI) wurde für die Verwendung mit dem AWS-Konto installiert und konfiguriert

Architektur

Das Muster umfasst die folgenden Schritte:

1. Der Benutzer überträgt Code in ein Git-Repository.
2. Der Git-Webhook wird aufgerufen.
3. Der CodePipeline Webhook wird aufgerufen.
4. Die Pipeline ist auf In Bearbeitung gesetzt, und die Quellphase ist auf den Status In Bearbeitung gesetzt.
5. Die Aktion der Quellphase initiiert eine CloudWatch Ereignisregel, die angibt, dass sie gestartet wurde.
6. Das CloudWatch Ereignis initiiert eine Lambda-Funktion.
7. Die Lambda-Funktion ruft die Details des benutzerdefinierten Aktionsauftrags ab.
8. Die Lambda-Funktion initiiert AWS CodeBuild und übergibt ihm alle auftragsbezogenen Informationen.
9. CodeBuild ruft den öffentlichen SSH-Schlüssel oder die Benutzeranmeldeinformationen für den HTTPS-Git-Zugriff von Secrets Manager ab.
10. CodeBuild klont das Git-Repository für einen bestimmten Branch.
11. CodeBuild komprimiert das Archiv und lädt es in den S3-Bucket hoch, der CodePipeline als Artefaktspeicher dient.

Tools

- AWS CodePipeline — AWS CodePipeline ist ein vollständig verwalteter Continuous Delivery Service, der Sie bei der Automatisierung Ihrer Release-Pipelines für schnelle und zuverlässige Anwendungs- und Infrastrukturupdates unterstützt. CodePipeline automatisiert die Erstellungs-, Test- und Bereitstellungsphasen Ihres Release-Prozesses für jede Codeänderung auf der Grundlage des von Ihnen definierten Release-Modells. Auf diese Weise können Sie Funktionen und Updates schnell und zuverlässig bereitstellen. Sie können AWS CodePipeline mit Services von Drittanbietern wie GitHub oder mit Ihrem eigenen benutzerdefinierten Plugin integrieren.
- AWS Lambda — Mit AWS Lambda können Sie Code ausführen, ohne Server bereitzustellen oder zu verwalten. Mit Lambda können Sie Code für praktisch jede Art von Anwendung oder Backend-Service ausführen, ohne dass eine Verwaltung erforderlich ist. Sie laden Ihren Code hoch und Lambda kümmert sich um alles, was für die Ausführung und Skalierung Ihres Codes mit hoher Verfügbarkeit erforderlich ist. Sie können Ihren Code so einrichten, dass er automatisch von anderen AWS-Services aus initiiert wird, oder ihn direkt von einer beliebigen Web- oder mobilen App aus aufrufen.
- AWS CodeBuild — AWS CodeBuild ist ein vollständig verwalteter Continuous Integration Service, der Quellcode kompiliert, Tests durchführt und Softwarepakete produziert, die sofort einsatzbereit sind. Mit CodeBuild müssen Sie Ihre eigenen Build-Server nicht bereitstellen, verwalten und skalieren. CodeBuild skaliert kontinuierlich und verarbeitet mehrere Builds gleichzeitig, sodass Ihre Builds nicht in einer Warteschlange warten müssen. Mit den vorkonfigurierten Build-Umgebungen gelingt der Einstieg leicht. Jedoch können Sie auch benutzerdefinierte Build-Umgebungen mit Ihren eigenen Entwicklungstools erstellen.
- AWS Secrets Manager — AWS Secrets Manager hilft Ihnen beim Schutz von Geheimnissen, die Sie für den Zugriff auf Ihre Anwendungen, Services und IT-Ressourcen benötigen. Mit diesem Service können Sie Datenbankanmeldedaten, API-Schlüssel und andere Geheimnisse während ihres gesamten Lebenszyklus rotieren, verwalten und abrufen. Benutzer und Anwendungen rufen Geheimnisse ab, indem sie Secrets Manager aufrufen APIs, ohne vertrauliche Informationen im Klartext fest codieren zu müssen. Secrets Manager bietet geheime Rotation mit integrierter Integration für Amazon Relational Database Service (Amazon RDS), Amazon Redshift und Amazon DocumentDB. Der Service kann erweitert werden, um andere Arten von Geheimnissen, einschließlich API-Schlüsseln und Tokens, zu unterstützen. OAuth Darüber hinaus können Sie mit Secrets Manager den Zugriff auf geheime Daten mithilfe detaillierter Berechtigungen kontrollieren und die Rotation von Geheimnissen zentral für Ressourcen in der AWS-Cloud, in Diensten von Drittanbietern und in lokalen Umgebungen überprüfen.

- Amazon CloudWatch — Amazon CloudWatch ist ein Überwachungs- und Beobachtungsdienst, der sich an DevOps Ingenieure, Entwickler, Techniker für die Zuverlässigkeit von SREs Standorten () und IT-Manager richtet. CloudWatch bietet Ihnen Daten und umsetzbare Erkenntnisse, um Ihre Anwendungen zu überwachen, auf systemweite Leistungsänderungen zu reagieren, die Ressourcennutzung zu optimieren und einen einheitlichen Überblick über den Betriebsstatus zu erhalten. CloudWatch sammelt Überwachungs- und Betriebsdaten in Form von Protokollen, Metriken und Ereignissen und bietet Ihnen so einen einheitlichen Überblick über AWS-Ressourcen, -Anwendungen und -Services, die auf AWS- und lokalen Servern ausgeführt werden. Sie können CloudWatch damit anomales Verhalten in Ihren Umgebungen erkennen, Alarme einrichten, Protokolle und Metriken nebeneinander visualisieren, automatisierte Maßnahmen ergreifen, Probleme beheben und Erkenntnisse gewinnen, damit Ihre Anwendungen reibungslos funktionieren.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice, mit dem Sie beliebige Datenmengen für eine Reihe von Anwendungsfällen speichern und schützen können, z. B. für Websites, mobile Anwendungen, Sicherung und Wiederherstellung, Archivierung, Unternehmensanwendungen, IoT-Geräte und Big-Data-Analysen. Amazon S3 bietet easy-to-use Verwaltungsfunktionen, mit denen Sie Ihre Daten organisieren und fein abgestimmte Zugriffskontrollen konfigurieren können, um Ihre spezifischen Geschäfts-, Organisations- und Compliance-Anforderungen zu erfüllen.

Epen

Erstellen Sie eine benutzerdefinierte Aktion in CodePipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine benutzerdefinierte Aktion mit AWS CLI oder AWS CloudFormation.	Dieser Schritt beinhaltet die Erstellung einer benutzerdefinierten Quellaktion, die in der Quellphase einer Pipeline in Ihrem AWS-Konto in einer bestimmten Region verwendet werden kann. Sie müssen AWS CLI oder AWS CloudFormation (nicht die Konsole) verwenden, um die	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	benutzerdefinierte Quellaktion zu erstellen. Weitere Informationen zu den in diesem und anderen Epen beschriebenen Befehlen und Schritten finden Sie im Abschnitt „Verwandte Ressourcen“ am Ende dieses Musters. Verwenden Sie in AWS CLI den create-custom-action-type Befehl. Verwenden Sie --configuration-properties, um alle Parameter bereitzustellen, die der Job-Worker verarbeiten muss, wenn er einen Job abfragt. CodePipeline Notieren Sie sich unbedingt die Werte, die für die Optionen --provider und --action-version angegeben wurden, damit Sie dieselben Werte verwenden können, wenn Sie die Pipeline mit diesem benutzerdefinierten Quellschritt erstellen. Sie können die benutzerdefinierte Quellaktion auch in AWS CloudFormation mithilfe des Ressourcentyps erstellen AWS::CodePipeline::CustomActionType.	

Richten Sie die Authentifizierung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein SSH-Schlü sselpaar.	Erstellen Sie ein Secure Shell (SSH) -Schlüsselpaar. Anweisungen finden Sie in der GitHub Dokumentation.	Systeme/ Ingenieur DevOps
Erstellen Sie ein Geheimnis in AWS Secrets Manager.	Kopieren Sie den Inhalt des privaten Schlüssels aus dem SSH-Schlüsselpaar und erstellen Sie ein Geheimnis in AWS Secrets Manager. Dieses Geheimnis wird für die Authentifizierung beim Zugriff auf das Git-Repository verwendet.	Allgemeines AWS
Fügen Sie den öffentlichen Schlüssel zum Git-Repository hinzu.	Fügen Sie den öffentlichen Schlüssel aus dem SSH-Schlü sselpaar zu den Kontoeins tellungen des Git-Repos itorys hinzu, um sich anhand des privaten Schlüssels zu authentifizieren.	Systeme/ Ingenieur DevOps

Erstellen Sie eine Pipeline und einen Webhook

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Pipeline, die die benutzerdefinierte Quellaktion enthält.	Erstellen Sie eine Pipeline in CodePipeline. Wenn Sie die Quellstufe konfigurieren, wählen Sie die benutzerd efinierte Quellaktion aus, die Sie zuvor erstellt haben. Sie	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	können dies in der CodePipeline AWS-Konsole oder in der AWS-CLI tun. CodePipeline fordert Sie zur Eingabe der Konfigurationseigenschaften auf, die Sie für die benutzerdefinierte Aktion festgelegt haben. Diese Informationen sind erforderlich, damit der Job-Worker den Job für die benutzerdefinierte Aktion bearbeiten kann. Folgen Sie dem Assistenten und erstellen Sie die nächste Phase für die Pipeline.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen CodePipeline Webhook.	Erstellen Sie einen Webhook für die Pipeline, die Sie mit der benutzerdefinierten Quellaktion erstellt haben. Sie müssen AWS CLI oder AWS CloudFormation (nicht die Konsole) verwenden, um den Webhook zu erstellen. Führen Sie in der AWS-CLI den Befehl put-webhook aus und geben Sie die entsprechenden Werte für die Webhook-Optionen an. Notieren Sie sich die Webhook-URL, die der Befehl zurückgibt. Wenn Sie AWS verwenden CloudFormation , um den Webhook zu erstellen, verwenden Sie den Ressourcentyp AWS::CodePipeline::Webhook. Stellen Sie sicher, dass Sie die Webhook-URL aus der erstellten Ressource ausgeben, und notieren Sie sich diese.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Lambda-Funktion und ein CodeBuild Lambda-Projekt.	In diesem Schritt verwenden Sie Lambda und CodeBuild erstellen einen Jobworker, der Jobanfragen CodePipeline für die benutzerdefinierte Aktion abfragt, den Job ausführt und das Statusergebnis CodePipeline zurückgibt. Erstellen Sie eine Lambda-Funktion, die durch eine Amazon CloudWatch Events-Regel initiiert wird, wenn die benutzerdefinierte Quellaktionsphase der Pipeline zu „In Bearbeitung“ übergeht. Wenn die Lambda-Funktion initiiert wird, sollte sie die Auftragsdetails der benutzerdefinierten Aktion abrufen, indem sie nach Jobs abfragt. Sie können die PollForJobs API verwenden, um diese Informationen zurückzugeben. Nachdem die abgefragten Auftragsinformationen abgerufen wurden, sollte die Lambda-Funktion eine Bestätigung zurückgeben und die Informationen dann mit den Daten verarbeiten, die sie aus den Konfigurationseigenschaften für die benutzerdefinierte Aktion erhält. Wenn der Worker bereit	Allgemein AWS, Code-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ist, mit dem Git-Repository zu kommunizieren, können Sie ein CodeBuild Projekt initiiere n, da es praktisch ist, Git-Aufgaben mithilfe des SSH-Clients zu erledigen.	

Erstellen Sie ein Ereignis in CloudWatch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CloudWatch Ereignisregel.	Erstellen Sie eine CloudWatch Ereignisregel, die die Lambda-Funktion als Ziel initiiert, wenn die benutzerdefinierte Aktionsphase der Pipeline zu „In Bearbeitung“ übergeht.	Allgemeines AWS

Zugehörige Ressourcen

Erstellen einer benutzerdefinierten Aktion in CodePipeline

- Erstellen Sie eine benutzerdefinierte Aktion und fügen Sie sie hinzu in CodePipeline
- AWS::CodePipeline::CustomActionType Ressource

Authentifizierung einrichten

- Secrets mit AWS Secrets Manager erstellen und verwalten

Eine Pipeline und einen Webhook erstellen

- Erstellen Sie eine Pipeline in CodePipeline
- Put-Webhook-Befehlsreferenz
- AWS::CodePipeline::Webhook Ressource

- PollForJobs API-Referenz
- Erstellen Sie eine benutzerdefinierte Aktion und fügen Sie sie hinzu in CodePipeline
- Erstellen Sie ein Build-Projekt in AWS CodeBuild

Ein Ereignis erstellen

- Mit Amazon CloudWatch Events können Sie Änderungen im Pipeline-Status erkennen und darauf reagieren

Zusätzliche Referenzen

- Arbeiten mit Pipelines in CodePipeline
- AWS Lambda Lambda-Entwicklerhandbuch

Erstellen Sie eine CI/CD-Pipeline zur Validierung von Terraform-Konfigurationen mithilfe von AWS CodePipeline

Erstellt von Aromal Raj Jayarajan (AWS) und Vijesh Vijayakumaran Nair (AWS)

Übersicht

AWS CodeCommit Hinweis: ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Dieses Muster zeigt, wie HashiCorp Terraform-Konfigurationen mithilfe einer von AWS bereitgestellten CI/CD-Pipeline (Continuous Integration and Continuous Delivery) getestet werden. CodePipeline

Terraform ist eine Befehlszeilenschnittstellenanwendung, mit der Sie mithilfe von Code Cloud-Infrastruktur und -Ressourcen bereitstellen und verwalten können. Die in diesem Muster bereitgestellte Lösung erstellt eine CI/CD-Pipeline, mit der Sie die Integrität Ihrer Terraform-Konfigurationen überprüfen können, indem Sie fünf Phasen ausführen: CodePipeline

1. `“checkout”`ruft die Terraform-Konfiguration, die Sie testen, aus einem AWS-Repository ab. CodeCommit
2. `“validate”`führt Tools zur Validierung von Infrastruktur als Code (IaC) aus, einschließlich tfsec, und checkov. TFLint Auf der Stufe werden auch die folgenden Terraform-IaC-Validierungsbefehle ausgeführt: und. `terraform validate` `terraform fmt`
3. `“plan”`zeigt, welche Änderungen auf die Infrastruktur angewendet werden, wenn die Terraform-Konfiguration angewendet wird.
4. `“apply”`verwendet den generierten Plan, um die erforderliche Infrastruktur in einer Testumgebung bereitzustellen.
5. `“destroy”`entfernt die Testinfrastruktur, die während der `“apply”` Phase erstellt wurde.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert

- Git, auf Ihrem lokalen Computer installiert und konfiguriert
- Terraform, auf Ihrem lokalen Computer installiert und konfiguriert

Einschränkungen

- Der Ansatz dieses Musters stellt AWS CodePipeline nur für ein AWS-Konto und eine AWS-Region bereit. Für Bereitstellungen mit mehreren Konten und mehreren Regionen sind Konfigurationsänderungen erforderlich.
- Die AWS Identity and Access Management (IAM) -Rolle, die dieses Muster bereitstellt (codepipeline_iam_role), folgt dem Prinzip der geringsten Rechte. Die Berechtigungen dieser IAM-Rolle müssen auf der Grundlage der spezifischen Ressourcen, die Ihre Pipeline erstellen muss, aktualisiert werden.

Versionen der Produkte

- AWS CLI Version 2.9.15 oder höher
- Terraform Version 1.3.7 oder höher

Architektur

Zieltechnologie-Stack

- AWS CodePipeline
- AWS CodeBuild
- AWS CodeCommit
- AWS IAM
- Amazon Simple Storage Service (Amazon-S3)
- AWS Key Management Service (AWS KMS)
- Terraform

Zielarchitektur

Das folgende Diagramm zeigt ein Beispiel für einen CI/CD-Pipeline-Workflow zum Testen von Terraform-Konfigurationen in. CodePipeline

Das Diagramm zeigt den folgenden Workflow:

1. In CodePipeline initiiert ein AWS-Benutzer die in einem Terraform-Plan vorgeschlagenen Aktionen, indem er den `terraform apply` Befehl in der AWS-CLI ausführt.
2. AWS CodePipeline übernimmt eine IAM-Servicerolle, die die für den Zugriff auf CodeCommit CodeBuild, AWS KMS und Amazon S3 erforderlichen Richtlinien umfasst.
3. CodePipeline führt die `“checkout”` Pipeline-Phase aus, um die Terraform-Konfiguration zum Testen aus einem CodeCommit AWS-Repository abzurufen.
4. CodePipeline führt die `“validate”` Phase zum Testen der Terraform-Konfiguration aus, indem IaC-Validierungstools und Terraform-IaC-Validierungsbefehle in einem Projekt ausgeführt werden. CodeBuild
5. CodePipeline führt die `“plan”` Phase aus, um einen Plan im CodeBuild Projekt auf der Grundlage der Terraform-Konfiguration zu erstellen. Der AWS-Benutzer kann diesen Plan überprüfen, bevor die Änderungen auf die Testumgebung angewendet werden.
6. Code Pipeline führt die `“apply”` Phase zur Implementierung des Plans durch, indem das CodeBuild Projekt zur Bereitstellung der erforderlichen Infrastruktur in der Testumgebung verwendet wird.
7. CodePipeline führt die `“destroy”` Phase aus, in der die Testinfrastruktur entfernt wird, die während der `“apply”` Phase erstellt wurde. CodeBuild
8. Ein Amazon S3 S3-Bucket speichert Pipeline-Artefakte, die mithilfe eines vom Kunden verwalteten AWS KMS KMS-Schlüssels ver- und entschlüsselt werden.

Tools

Tools

AWS-Services

- AWS CodePipeline hilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.
- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Komponententests ausführen und bereitstellungsbereite Artefakte erstellen können.
- AWS CodeCommit ist ein Versionskontrollservice, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.

- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Key Management Service (AWS KMS) unterstützt Sie bei der Erstellung und Kontrolle kryptografischer Schlüssel, um Ihre Daten zu schützen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere Dienste

- HashiCorp Terraform ist eine Befehlszeilenschnittstellenanwendung, mit der Sie mithilfe von Code Cloud-Infrastruktur und -Ressourcen bereitstellen und verwalten können.

Code

Der Code für dieses Muster ist im Repository verfügbar. GitHub aws-codepipeline-terraform-cicdsamples Das Repository enthält die Terraform-Konfigurationen, die zur Erstellung der in diesem Muster beschriebenen Zielarchitektur erforderlich sind.

Epen

Stellen Sie die Lösungskomponenten bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	Klonen Sie das GitHub aws-codepipeline-terraform-cicdsamplesRepository, indem Sie den folgenden Befehl in einem Terminalfenster ausführen: `git clone https://github.com/aws-samples/aws-codepipeline-terraform-cicd-samples.git`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie in der GitHub Dokumentation unter Ein Repository klonen.	
Erstellen Sie eine Terraform-Variablendefinitionsdatei.	Erstellen Sie eine `terraform.tfvars` Datei, die auf Ihren Anwendungsfallanforderungen basiert. Sie können die Variablen in der `examples/terraform.tfvars` Datei aktualisieren, die sich im geklonten Repository befindet. Weitere Informationen finden Sie unter Zuweisen von Werten zu Stammmodulvariablen in der Terraform-Dokumentation. **Note** Die `Readme.md` Datei des Repositorys enthält weitere Informationen zu den erforderlichen Variablen.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie AWS als Terraform-Anbieter.	1. Öffnen Sie in einem Code-Editor die Datei des geklonten Repositorys. `main.tf` 2. Fügen Sie die erforderl ichen Konfigurationen hinzu, um die Konnektiv ität zum AWS-Zielkonto herzustellen. Weitere Informationen finden Sie unter AWS-Anbieter in der Terraform-Dokumentation.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Terraform-Anbieterkonfiguration für die Erstellung des Amazon S3 S3-Replikationsbuckets.	1. Öffnen Sie das `S3` Verzeichnis des Repositorys, indem Sie den folgenden Befehl ausführen: `cd ./modules/s3` 2. Aktualisieren Sie die Terraform-Anbieterkonfiguration für die Erstellung des Amazon S3 S3-Replikationsbuckets, indem Sie den `region` Wert in der `tf` Datei aktualisieren. Stellen Sie sicher, dass Sie die Region eingeben, in die Amazon S3 Objekte replizieren soll. 3. (Optional) Standardmäßig verwendet Terraform lokale Statusdateien für die Statusverwaltung. Wenn Sie Amazon S3 als Remote-Backend hinzufügen möchten, müssen Sie die Terraform-Konfiguration aktualisieren. Weitere Informationen finden Sie unter Backend-Konfiguration in der Terraform-Dokumentation.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Die Replikation aktiviert das automatische, asynchrone Kopieren von Objekten zwischen Amazon S3 S3-Buckets.	
Initialisieren Sie die Terraform-Konfiguration.	Um Ihr Arbeitsverzeichnis zu initialisieren, das die Terraform-Konfigurationsdateien enthält, führen Sie den folgenden Befehl im Stammordner des geklonten Repositorys aus: `terraform init`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Terraform-Plan.	Um einen Terraform-Plan zu erstellen, führen Sie den folgenden Befehl im Stammordner des geklonten Repositorys aus: `terraform plan --var-file=terraform.tfvars -out=tfplan` **Note** Terraform wertet die Konfigurationsdateien aus, um den Zielstatus für die deklarierten Ressourcen zu ermitteln. Anschließend wird der Zielstatus mit dem aktuellen Status verglichen und ein Plan erstellt.	DevOps Ingenieur
Überprüfen Sie den Terraform-Plan.	Überprüfen Sie den Terraform-Plan und stellen Sie sicher, dass er die erforderliche Architektur in Ihrem AWS-Zielkonto konfiguriert.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Lösung bereit.	1. Um den Terraform-Plan anzuwenden, führen Sie den folgenden Befehl im Stammordner des geklonten Repositorys aus: `terraform apply "tfplan"` 2. Geben Sie Ja ein, um zu bestätigen, dass Sie die Ressourcen bereitstellen möchten. **Note** Terraform erstellt, aktualisiert oder zerstört die Infrastruktur, um den in den Konfigurationsdateien angegebenen Zielstatus zu erreichen.	DevOps Ingenieur

Validieren Sie Terraform-Konfigurationen, indem Sie die Pipeline ausführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie das Quellcode-Repository ein.	1. Rufen Sie aus der Terraform-Ausgabe die Quell-Repository-Details für das Repository ab, das die Terraform-Konfigurationen	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	enthält, die Sie validieren möchten. 2. Melden Sie sich bei der AWS-Managementkonsole an. Öffnen Sie dann die Konsole. CodeCommit 3. Erstellen Sie einen neuen Zweig im Quell-Repository mit dem Namen`main`. Anweisungen finden Sie in der CodeCommit Dokumentation unter Erstellen einer Filiale CodeCommit in AWS. 4. Klonen Sie den `main` Zweig des Quell-Repositorys auf Ihre lokale Workstation. Anweisungen finden Sie in der Dokumentation unter Einrichtungsschritte für HTTPS-Verbindungen zu CodeCommit AWS-Repositorys unter Windows mit dem AWS CLI Credential Helper. CodeCommit 5. Kopieren Sie den **`templates`** Ordner aus dem GitHub aws-codepipeline-terraform-cicdsamplesRepository, indem Sie den folgenden Befehl ausführen:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cp -r templates $YOUR_CODECOMMIT_REPO_ROOT` **Note** Der `templates` Ordner enthält die Build-Spezifikationsdateien und das Überprüfungsskript für das Stammverzeichnis des Quell-Repositorys. 6. Fügen Sie Ihre erforderlichen Terraform IaC-Konfigurationen zum Stammordner des Quell-Repositorys hinzu. 7. Fügen Sie die Details für das Remote-Backend in die Terraform-Konfiguration Ihres Projekts ein. Weitere Informationen finden Sie unter S3 in der Terraform-Dokumentation. 8. (Optional) Aktualisieren Sie die Variablen im `templates` Ordner, um die vorkonfigurierten Scans und Tool-Change-Versionen entweder zu aktivieren oder zu deaktivie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ren und Ihr Verzeichn is in benutzerdefinierten Skriptdateien anzugeben . Weitere Informationen finden Sie im Abschnitt Zusätzliche Informationen dieses Musters. 9. Übertragen Sie die Änderungen in den `main` Zweig des Quell-Rep ositorys.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Pipeline-Phasen.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CodePipeline -Konsole. 2. Suchen Sie in der Ausgabe, die mit dem `terraform apply "tfplan"` Befehl im vorherigen Epic-Abschnitt generiert wurde, den Namen des generierten Befehls CodePipeline. 3. Öffnen Sie die Pipeline in der CodePipeline Konsole und wählen Sie Änderung veröffentlichen. 4. Überprüfen Sie jede Pipeline-Phase und vergewissern Sie sich, dass sie wie erwartet funktioniert. Weitere Informationen finden Sie unter Pipeline-Details und Verlauf anzeigen (Konsole) im CodePipeline AWS-Benutzerhandbuch. ⚠ Important Wenn eine Änderung in den Hauptzweig des Quell-Repositorys übernommen wird,	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wird die Testpipeline automatisch aktiviert.	
Überprüfen Sie die Berichtsausgabe.	1. Wählen Sie auf der CodePipeline Konsole im linken Navigationsbereich Build aus. Wählen Sie dann Verlauf melden aus. 2. Überprüfen Sie die TFSEC- und Checkov-Scan-Berichte, die die Pipeline generiert. Diese Berichte können Ihnen helfen, Probleme anhand von Visualisierungen und grafischen Darstellungen zu identifizieren. **Note** Das `<project_name>-validate` CodeBuild Projekt generiert während der Phase Berichte über Sicherheitslücken für Ihren Code. `“validate”`	DevOps Ingenieur

Bereinigen Ihrer Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Säubern Sie die Pipeline und die zugehörigen Ressourcen.	Um die Testressourcen aus Ihrem AWS-Konto zu löschen, führen Sie den folgenden Befehl im Stammordner des geklonten Repositorys aus: `terraform destroy --var-file=terraform.tfvars`	DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Sie erhalten während der “`apply`” Phase eine AccessDenied Fehlermeldung.	1. Überprüfen Sie die Ausführungsprotokolle des CodeBuild Projekts, das der “`apply`” Phase zugeordnet ist, um etwaige fehlende IAM-Berechtigungen zu ermitteln. Weitere Informationen finden Sie im CodeBuild AWS-Benutzerhandbuch unter Build-Details CodeBuild in AWS anzeigen. 2. Öffnen Sie in einem Code-Editor den `modules` Ordner des geklonten Repository. Navigieren Sie dann zu dem `iam-role` Ordner und öffnen Sie die `main.tf` Datei, die sich in diesem Ordner befindet. 3. Fügen Sie in der `codepipeline_policy` Erklärung die IAM-Richtlinien hinzu, die für die Bereitstellung von Ressourcen in Ihrem AWS-Konto erforderlich sind.

Zugehörige Ressourcen

- Modulblöcke (Terraform-Dokumentation)
- So verwenden Sie CI/CD zur Bereitstellung und Konfiguration von AWS-Sicherheitsservices mit Terraform (AWS-Blogbeitrag)
- Verwenden von serviceverknüpften Rollen (IAM-Dokumentation)
- Pipeline erstellen (AWS-CLI-Dokumentation)
- Serverseitige Verschlüsselung für in Amazon S3 gespeicherte Artefakte konfigurieren für CodePipeline (CodePipeline AWS-Dokumentation)
- Kontingente für AWS CodeBuild (CodeBuild AWS-Dokumentation)
- Datenschutz in AWS CodePipeline (CodePipeline AWS-Dokumentation)

Zusätzliche Informationen

Benutzerdefinierte Terraform-Module

Im Folgenden finden Sie eine Liste der benutzerdefinierten Terraform-Module, die in diesem Muster verwendet werden:

- `codebuild_terraform`erstellt die CodeBuild Projekte, die jede Phase der Pipeline bilden.
- `codecommit_infrastructure_source_repo`erfasst und erstellt das CodeCommit Quell-Repository.
- `codepipeline_iam_role`erstellt die erforderlichen IAM-Rollen für die Pipeline.
- `codepipeline_kms`erstellt den erforderlichen AWS-KMS-Schlüssel für die Amazon S3 S3-Objektverschlüsselung und -entschlüsselung.
- `codepipeline_terraform`erstellt die Testpipeline für das CodeCommit Quell-Repository.
- `s3_artifacts_bucket`erstellt einen Amazon S3 S3-Bucket zur Verwaltung von Pipeline-Artefakten.

Spezifikationsdateien erstellen

Im Folgenden finden Sie eine Liste von Build-Spezifikationsdateien (Buildspec), die dieses Muster verwendet, um jede Pipeline-Phase auszuführen:

- `buildspec_validate.yml`führt die Phase aus. `“validate”`

- `buildspec_plan.yml`leitet die “`plan`” Bühne.
- `buildspec_apply.yml`leitet die “`apply`” Bühne.
- `buildspec_destroy.yml`leitet die “`destroy`” Bühne.

Variablen in der Spezifikationsdatei erstellen

Jede Buildspec-Datei verwendet die folgenden Variablen, um unterschiedliche buildspezifische Einstellungen zu aktivieren:

Variable	Standardwert	Beschreibung
`CODE_SRC_DIR`	"."	CodeCommit Definiert das Quellverzeichnis
`TF_VERSION`	„1.3.7"	Definiert die Terraform-Version für die Build-Umgebung

Die `buildspec_validate.yml` Datei unterstützt auch die folgenden Variablen, um verschiedene Build-spezifische Einstellungen zu aktivieren:

Variable	Standardwert	Beschreibung
`SCRIPT_DIR`	“. /Vorlagen/Skripte“	Definiert das Skriptverzeichnis
`ENVIRONMENT`	„dev“	Definiert den Namen der Umgebung
`SKIPVALIDATIONFAIL URE`	„Y“	Überspringt die Validierung bei Fehlern
`ENABLE_TFVALIDATE`	„Y“	Aktiviert Terraform Validate
`ENABLE_TFFORMAT`	„Y“	Aktiviert das Terraform-Format
`ENABLE_TFCHECKOV`	„Y“	Aktiviert den Checkov-Scan
`ENABLE_TFSEC`	„Y“	Aktiviert den TFSec-Scan

TFSEC_VERSION	„v1.28.1"	Definiert die TFSec-Version

Mehr Muster

- Greifen Sie mit AWS PrivateLink und einem Network Load Balancer privat auf Container-Anwendungen auf Amazon EKS zu
- Verknüpfen Sie ein AWS CodeCommit Repository in einem AWS-Konto mit Amazon SageMaker AI Studio Classic in einem anderen Konto
- Automatisieren Sie die Kontoerstellung mit dem Landing Zone Accelerator auf AWS
- Automatisieren Sie das Hinzufügen oder Aktualisieren von Windows-Registrierungseinträgen mit AWS Systems Manager
- Automatisieren Sie Backups für Amazon RDS for PostgreSQL PostgreSQL-DB-Instances mithilfe von AWS Batch
- Automatisieren Sie die Bereitstellung verschachtelter Anwendungen mit AWS SAM
- Automatisieren Sie die Bereitstellung von Node Termination Handler in Amazon EKS mithilfe einer CI/CD-Pipeline
- Automatisieren Sie die RabbitMQ-Konfiguration in Amazon MQ
- Automatisieren Sie die Replikation von Amazon RDS-Instances auf AWS-Konten
- Automatisches Erstellen und Bereitstellen einer Java-Anwendung auf Amazon EKS mithilfe einer CI/CD-Pipeline
- Automatisches Generieren eines PynamoDB-Modells und CRUD-Funktionen für Amazon DynamoDB mithilfe einer Python-Anwendung
- Automatische Validierung und Bereitstellung von IAM-Richtlinien und -Rollen in einem AWS-Konto mithilfe CodePipeline von IAM Access Analyzer und AWS-Makros CloudFormation
- Sun SPARC-Server im Stromasys Charon-SSP-Emulator in der AWS-Cloud sichern
- Erstellen Sie mit dem AWS DataOps Development Kit eine Datenpipeline, um Google Analytics-Daten aufzunehmen, zu transformieren und zu analysieren
- Erstellen Sie ein Micro Focus Enterprise Server PAC mit Amazon EC2 Auto Scaling und Systems Manager
- Erstellen Sie mit EC2 Image Builder und Terraform eine Pipeline für gehärtete Container-Images
- Erstellen Sie einen MLOps Workflow mithilfe von Amazon SageMaker AI und Azure DevOps
- Zentralisieren Sie die DNS-Auflösung mithilfe von AWS Managed Microsoft AD und vor Ort von Microsoft Active Directory
- Verketten Sie AWS-Services mithilfe eines serverlosen Ansatzes

- Bereinigen Sie die Ressourcen von AWS Account Factory for Terraform (AFT) nach dem Verlust von Statusdateien sicher
- Konfigurieren Sie die Protokollierung für .NET-Anwendungen in Amazon CloudWatch Logs mithilfe von NLog
- Kontinuierliche Bereitstellung einer modernen AWS Amplify Amplify-Webanwendung aus einem AWS-Repository CodeCommit
- Erstellen Sie ein benutzerdefiniertes Docker-Container-Image für SageMaker und verwenden Sie es für Modelltrainings in AWS Step Functions
- Erstellen Sie eine Pipeline in AWS-Regionen, die AWS nicht unterstützen CodePipeline
- Erstellen Sie mithilfe der CloudWatch Amazon-Anomalieerkennung Alarme für benutzerdefinierte Metriken
- Passen Sie Standardrollennamen mithilfe von AWS CDK Aspekten und Escape-Schraffuren an
- Stellen Sie eine Pipeline bereit, die Sicherheitsprobleme in mehreren Codeergebnissen gleichzeitig erkennt
- Bereitstellen und verwalten Sie einen serverlosen Data Lake in der AWS-Cloud, indem Sie Infrastruktur als Code verwenden
- Stellen Sie Kubernetes-Ressourcen und -Pakete mithilfe von Amazon EKS und einem Helm-Chart-Repository in Amazon S3 bereit
- Stellen Sie Anwendungen mit mehreren Stacks mithilfe von AWS CDK bereit mit TypeScript
- Stellen Sie mithilfe von Terraform SQL Server-Failover-Cluster-Instances auf Amazon EC2 und Amazon FSx bereit
- Stellen Sie die Security Automations for AWS WAF Solution mithilfe von Terraform bereit
- Entwickeln Sie mithilfe von RAG und Prompting fortschrittliche, auf KI basierende Chat-Assistenten ReAct
- Aktivieren Sie Amazon GuardDuty unter bestimmten Bedingungen mithilfe von Vorlagen AWS CloudFormation
- Richten Sie ereignisgesteuertes Auto Scaling in Amazon EKS mithilfe von Amazon EKS Pod Identity und KEDA ein
- Generieren Sie mit Amazon Personalize personalisierte und neu eingestufte Empfehlungen
- Erhalten Sie Amazon SNS SNS-Benachrichtigungen, wenn sich der Schlüsselstatus eines AWS KMS KMS-Schlüssels ändert
- Automatische Identifizierung doppelter Container-Images bei der Migration zu einem Amazon ECR-Repository

- Implementieren Sie eine pfadbasierte API-Versionierung mithilfe benutzerdefinierter Domains in Amazon API Gateway
- Verbessern Sie die Betriebsleistung, indem Sie Amazon DevOps Guru in mehreren AWS-Regionen, Konten und OUs mit dem AWS CDK aktivieren
- Installieren Sie SSM Agent mithilfe von Kubernetes auf Amazon EKS-Worker-Knoten DaemonSet
- Integrieren Sie den Stonebranch Universal Controller in die AWS-Mainframe-Modernisierung
- Mainframe-Modernisierung: DevOps Weiter AWS mit Rocket Software Enterprise Suite
- Verwalten Sie AWS IAM Identity Center Berechtigungssätze als Code, indem Sie AWS CodePipeline
- Verwalten Sie lokale Containeranwendungen, indem Sie Amazon ECS Anywhere mit dem AWS CDK einrichten
- AWS Organizations Richtlinien mithilfe AWS CodePipeline von Amazon Bedrock als Code verwalten
- Massenmigrieren von DNS-Einträgen in eine private gehostete Zone von Amazon Route 53
- Migrieren Sie ML-Workloads zum Erstellen, Trainieren und Bereitstellen zu Amazon SageMaker mithilfe der AWS-Entwicklertools
- Überwachen Sie die Nutzung eines gemeinsam genutzten Amazon Machine Image über mehrere AWS-Konten
- Optimieren Sie die von AWS App2Container generierten Docker-Images
- Orchestrieren Sie eine ETL-Pipeline mit Validierung, Transformation und Partitionierung mithilfe von AWS Step Functions
- Automatisieren Sie blaue/grüne Bereitstellungen globaler Amazon Aurora Aurora-Datenbanken mithilfe von IaC-Prinzipien
- Beibehaltung von routingfähigem IP-Speicherplatz in VPC-Designs mit mehreren Konten für Subnetze ohne Arbeitslast
- Stellen Sie ein Terraform-Produkt AWS Service Catalog mithilfe eines Code-Repositorys bereit
- Replizieren Sie gefilterte Amazon ECR-Container-Images über Konten oder Regionen hinweg
- Datenbankanmeldedaten rotieren, ohne Container neu zu starten
- Führen Sie AWS Systems Manager Automation Automation-Aufgaben synchron über AWS Step Functions aus
- Richten Sie mithilfe von AWS CDK eine CI/CD-Pipeline für Hybrid-Workloads auf Amazon ECS Anywhere ein und GitLab

- Richten Sie mithilfe von Terraform eine CI/CD-Pipeline für die Datenbankmigration ein
- Richten Sie mithilfe von Amazon eine Multi-AZ-Infrastruktur für einen SQL Server Always On FCI ein FSx
- Richten Sie mithilfe EC2 von AWS automatisch UiPath RPA-Bots auf Amazon ein CloudFormation
- Vereinfachen Sie die Anwendungsauthentifizierung mit gegenseitigem TLS in Amazon ECS mithilfe von Application Load Balancer
- Mandanten-Onboarding in der SaaS-Architektur für das Silomodell mit C# und AWS CDK
- Verwenden Sie Terraform, um Amazon automatisch GuardDuty für eine Organisation zu aktivieren
- Verwenden Sie Amazon Bedrock-Agenten, um die Erstellung von Zugriffskontrollen in Amazon EKS durch textbasierte Eingabeaufforderungen zu automatisieren
- Validieren Sie den Account Factory for Terraform (AFT) -Code lokal
- Visualisieren Sie KI/ML-Modellergebnisse mit Flask und AWS Elastic Beanstalk

Infrastruktur

Themen

- Greifen Sie mithilfe von Session Manager und Amazon EC2 Instance Connect auf einen Bastion-Host zu
- Zentralisieren Sie die DNS-Auflösung mithilfe von AWS Managed Microsoft AD und vor Ort von Microsoft Active Directory
- Zentralisieren Sie die Überwachung mithilfe von Amazon CloudWatch Observability Access Manager
- EC2 Instances beim Start auf obligatorische Tags überprüfen
- Bereinigen Sie die Ressourcen von AWS Account Factory for Terraform (AFT) nach dem Verlust von Statusdateien sicher
- Stellen Sie mithilfe von Session Manager eine Connect zu einer EC2 Amazon-Instance her
- Erstellen Sie eine Pipeline in AWS-Regionen, die AWS nicht unterstützen CodePipeline
- Passen Sie Standardrollennamen mithilfe von AWS CDK Aspekten und Escape-Schraffuren an
- Stellen Sie einen Cassandra-Cluster auf Amazon EC2 mit Private Static bereit, um ein IPs Rebalancing zu vermeiden
- Mit AWS Transit Gateway Connect auf AWS erweitern VRFs
- Erhalten Sie Amazon SNS SNS-Benachrichtigungen, wenn sich der Schlüsselstatus eines AWS KMS KMS-Schlüssels ändert
- Beibehaltung von routingfähigem IP-Speicherplatz in VPC-Designs mit mehreren Konten für Subnetze ohne Arbeitslast
- Stellen Sie ein Terraform-Produkt AWS Service Catalog mithilfe eines Code-Repositorys bereit
- Registrieren Sie mehrere AWS-Konten mit einer einzigen E-Mail-Adresse mithilfe von Amazon SES
- Richten Sie die DNS-Auflösung für Hybridnetzwerke in einer AWS-Umgebung mit einem Konto ein
- Richten Sie mithilfe EC2 von AWS automatisch UiPath RPA-Bots auf Amazon ein CloudFormation
- Richten Sie eine hochverfügbare PeopleSoft Architektur auf AWS ein
- Richten Sie die Notfallwiederherstellung für Oracle JD Edwards EnterpriseOne mit AWS Elastic Disaster Recovery ein
- Richten Sie die AWS CloudFormation Drifterkennung in einer Organisation mit mehreren Regionen und mehreren Konten ein
- Erfolgreicher Import eines S3-Buckets als CloudFormation AWS-Stack

- Synchronisieren Sie Daten zwischen Amazon EFS-Dateisystemen in verschiedenen AWS-Regionen mithilfe von AWS DataSync
- Testen Sie die AWS Infrastruktur mithilfe LocalStack von Terraform-Tests
- Aktualisieren Sie SAP Pacemaker-Cluster von ENSA1 auf ENSA2
- Verwenden Sie konsistente Availability Zones VPCs für verschiedene AWS-Konten
- Verwenden Sie Benutzer IDs in IAM-Richtlinien für Zugriffskontrolle und Automatisierung
- Validieren Sie den Account Factory for Terraform (AFT) -Code lokal
- Mehr Muster

Greifen Sie mithilfe von Session Manager und Amazon EC2 Instance Connect auf einen Bastion-Host zu

Erstellt von Piotr Chotkowski (AWS) und Witold Kowalik (AWS)

Übersicht

Ein Bastion-Host, manchmal auch Jumpbox genannt, ist ein Server, der einen zentralen Zugriffspunkt von einem externen Netzwerk auf die Ressourcen in einem privaten Netzwerk bietet. Ein Server, der einem externen öffentlichen Netzwerk wie dem Internet ausgesetzt ist, stellt ein potenzielles Sicherheitsrisiko für unbefugten Zugriff dar. Es ist wichtig, den Zugriff auf diese Server zu sichern und zu kontrollieren.

Dieses Muster beschreibt, wie Sie Session Manager und Amazon EC2 Instance Connect verwenden können, um eine sichere Verbindung zu einem Amazon Elastic Compute Cloud (Amazon EC2) - Bastion-Host herzustellen, der in Ihrem AWS-Konto bereitgestellt wird. Session Manager ist eine Funktion von. AWS Systems Manager Zu den Vorteilen dieses Musters gehören:

- Der bereitgestellte Bastion-Host hat keine offenen, eingehenden Ports, die mit dem öffentlichen Internet verbunden sind. Dadurch wird die potenzielle Angriffsfläche reduziert.
- Sie müssen keine langfristigen Secure Shell (SSH) -Schlüssel in Ihrem AWS-Konto speichern und verwalten. Stattdessen generiert jeder Benutzer jedes Mal, wenn er sich mit dem Bastion-Host verbindet, ein neues SSH-Schlüsselpaar. AWS Identity and Access Management (IAM) - Richtlinien, die an die AWS Anmeldeinformationen des Benutzers angehängt sind, steuern den Zugriff auf den Bastion-Host.

Beabsichtigte Zielgruppe

Dieses Muster richtet sich an Leser, die Erfahrung mit grundlegenden Kenntnissen von Amazon EC2, Amazon Virtual Private Cloud (Amazon VPC) und Hashicorp Terraform haben.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- AWS Command Line Interface (AWS CLI) Version 2, installiert und konfiguriert
- Session Manager-Plugin für das AWS CLI, installiert

- Terraform CLI, installiert
- Speicher für den Terraform-Status, z. B. ein Amazon Simple Storage Service (Amazon S3) -Bucket und eine Amazon DynamoDB-Tabelle, die als Remote-Backend zum Speichern des Terraform-Status dienen. Weitere Informationen zur Verwendung von Remote-Backends für den Terraform-Status finden Sie unter Amazon S3 S3-Backends (Terraform-Dokumentation). Ein Codebeispiel, das die Remote-Statusverwaltung mit einem Amazon S3 S3-Backend einrichtet, finden Sie unter remote-state-s3-backend (Terraform Registry). Beachten Sie die folgenden Voraussetzungen:
  - Der Amazon S3 S3-Bucket und die DynamoDB-Tabelle müssen sich im selben Raum befinden. AWS-Region
  - Beim Erstellen der DynamoDB-Tabelle müssen der Partitionsschlüssel `LockID` (Groß- und Kleinschreibung beachten) und der Partitionsschlüsseltyp muss angegeben werden. `String` Für alle anderen Tabelleneinstellungen müssen die Standardwerte verwendet werden. Weitere Informationen finden Sie unter Über Primärschlüssel und Erstellen einer Tabelle in der DynamoDB-Dokumentation.
- Ein SSH-Client, installiert

Einschränkungen

- Dieses Muster ist als Machbarkeitsnachweis (PoC) oder als Grundlage für die weitere Entwicklung gedacht. Es sollte in seiner derzeitigen Form nicht in Produktionsumgebungen verwendet werden. Passen Sie vor der Bereitstellung den Beispielcode im Repository an Ihre Anforderungen und Ihren Anwendungsfall an.
- Dieses Muster geht davon aus, dass der Ziel-Bastion-Host Amazon Linux 2 als Betriebssystem verwendet. Es ist zwar möglich, andere Amazon Machine Images (AMIs) zu verwenden, andere Betriebssysteme fallen jedoch nicht in den Anwendungsbereich dieses Musters.

> **Note**
>
> Amazon Linux 2 nähert sich dem Ende der Unterstützung. Weitere Informationen finden Sie unter Amazon Linux FAQs 2.

- In diesem Muster befindet sich der Bastion-Host in einem privaten Subnetz ohne NAT-Gateway und Internet-Gateway. Dieses Design isoliert die EC2 Amazon-Instance vom öffentlichen Internet. Sie können eine bestimmte Netzwerkkonfiguration hinzufügen, die es ihr ermöglicht, mit dem Internet zu kommunizieren. Weitere Informationen finden Sie unter Connect Ihrer Virtual Private Cloud (VPC) mit anderen Netzwerken in der Amazon VPC-Dokumentation. Entsprechend dem

Prinzip der geringsten Rechte hat der Bastion-Host keinen Zugriff auf andere Ressourcen in Ihrem, AWS-Konto sofern Sie nicht ausdrücklich die entsprechenden Berechtigungen erteilen. Weitere Informationen finden Sie in der IAM-Dokumentation unter Ressourcenbasierte Richtlinien.

Produktversionen

- AWS-CLI Version 2
- Terraform-Version 1.3.9

Architektur

Zieltechnologie-Stack

- Eine VPC mit einem einzigen privaten Subnetz
- Die folgenden Schnittstellen-VPC-Endpunkte:
  - `amazonaws.<region>.ssm`— Der Endpunkt für den AWS Systems Manager Service.
  - `amazonaws.<region>.ec2messages`— Systems Manager verwendet diesen Endpunkt, um Anrufe vom SSM-Agent an den Systems Manager Manager-Dienst zu tätigen.
  - `amazonaws.<region>.ssmmessages`— Session Manager verwendet diesen Endpunkt, um über einen sicheren Datenkanal eine Verbindung zu Ihrer EC2 Amazon-Instance herzustellen.
- Eine `t3.nano` EC2 Amazon-Instance, auf der Amazon Linux 2 ausgeführt wird
- IAM-Rolle und Instanzprofil
- Amazon VPC-Sicherheitsgruppen und Sicherheitsgruppenregeln für die Endgeräte und die Amazon-Instance EC2

Zielarchitektur

Das Diagramm zeigt den folgenden Prozess:

1. Der Benutzer nimmt eine IAM-Rolle an, die über die folgenden Berechtigungen verfügt:
   - Authentifizieren, autorisieren und eine Verbindung zur Amazon-Instance herstellen EC2
   - Starten Sie eine Sitzung mit Session Manager
2. Der Benutzer initiiert eine SSH-Sitzung über den Sitzungsmanager.

3. Session Manager authentifiziert den Benutzer, überprüft die Berechtigungen in den zugehörigen IAM-Richtlinien, überprüft die Konfigurationseinstellungen und sendet eine Nachricht an den SSM-Agenten, um eine bidirektionale Verbindung herzustellen.
4. Der Benutzer überträgt den öffentlichen SSH-Schlüssel über Amazon-Metadaten an den Bastion-Host. EC2 Dies muss vor jeder Verbindung erfolgen. Der öffentliche SSH-Schlüssel bleibt 60 Sekunden lang verfügbar.
5. Der Bastion-Host kommuniziert mit den VPC-Endpunkten der Schnittstelle für Systems Manager und Amazon. EC2
6. Der Benutzer greift über Session Manager auf den Bastion-Host zu, indem er einen mit TLS 1.2 verschlüsselten bidirektionalen Kommunikationskanal verwendet.

Automatisierung und Skalierung

Die folgenden Optionen sind verfügbar, um die Bereitstellung zu automatisieren oder diese Architektur zu skalieren:

- Sie können die Architektur über eine CI/CD-Pipeline (Continuous Integration and Continuous Delivery) bereitstellen.
- Sie können den Code ändern, um den Instanztyp des Bastion-Hosts zu ändern.
- Sie können den Code ändern, um mehrere Bastion-Hosts bereitzustellen. Fügen Sie in der `bastion-host/main.tf` Datei im `aws_instance` Ressourcenblock das `count` Metaargument hinzu. Weitere Informationen finden Sie in der Terraform-Dokumentation.

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie AWS-Services über Befehle in Ihrer Befehlszeilen-Shell interagieren können.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.

- AWS Systems Managerhilft Ihnen bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der ausgeführt werden. AWS Cloud Es vereinfacht das Anwendungs- und Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme und hilft Ihnen, Ihre AWS Ressourcen sicher und in großem Umfang zu verwalten. Dieses Muster verwendet Session Manager, eine Funktion von Systems Manager.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk bereitzustellen. Dieses virtuelle Netzwerk entspricht einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben würden, mit den Vorteilen der Verwendung der skalierbaren Infrastruktur von AWS.

Andere Tools

- HashiCorp Terraform ist ein Infrastructure-as-Code-Tool (IaC), mit dem Sie mithilfe von Code Cloud-Infrastruktur und -Ressourcen bereitstellen und verwalten können. Dieses Muster verwendet Terraform CLI.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub Access a Bastion Host mithilfe von Session Manager und Amazon EC2 Instance Connect verfügbar.

Bewährte Methoden

- Wir empfehlen die Verwendung automatisierter Tools zum Scannen von Code, um die Sicherheit und Qualität des Codes zu verbessern. Dieses Muster wurde mit Checkov, einem statischen Codeanalyse-Tool für IaC, gescannt. Wir empfehlen Ihnen, mindestens grundlegende Validierungs- und Formatierungsprüfungen mithilfe der `terraform validate` Befehle und Terraform durchzuführen. `terraform fmt -check -recursive`
- Es empfiehlt sich, automatisierte Tests für IaC hinzuzufügen. Weitere Informationen zu den verschiedenen Ansätzen zum Testen von Terraform-Code finden Sie unter Terraform testen (HashiCorp Terraform-Blogbeitrag).
- Während der Bereitstellung verwendet Terraform jedes Mal, wenn eine neue Version des Amazon Linux 2-AMI erkannt wird, die EC2 Amazon-Instance ersetzt. Dadurch wird die neue Version des Betriebssystems einschließlich Patches und Upgrades bereitgestellt. Wenn der Bereitstellungszeitplan selten ist, kann dies ein Sicherheitsrisiko darstellen, da die Instanz nicht über die neuesten Patches verfügt. Es ist wichtig, regelmäßig Sicherheitspatches zu aktualisieren

und auf bereitgestellte EC2 Amazon-Instances anzuwenden. Weitere Informationen finden Sie unter Update-Verwaltung in Amazon EC2.

- Da es sich bei diesem Muster um einen Machbarkeitsnachweis handelt, AWS werden verwaltete Richtlinien verwendet, wie `AmazonSSMManagedInstanceCore` z. AWS verwaltete Richtlinien decken allgemeine Anwendungsfälle ab, gewähren jedoch keine Berechtigungen mit den geringsten Rechten. Je nach Bedarf für Ihren Anwendungsfall empfehlen wir Ihnen, benutzerdefinierte Richtlinien zu erstellen, die Berechtigungen mit den geringsten Rechten für die in dieser Architektur bereitgestellten Ressourcen gewähren. Weitere Informationen finden Sie unter Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten.
- Verwenden Sie ein Passwort, um den Zugriff auf SSH-Schlüssel zu schützen und Schlüssel an einem sicheren Ort zu speichern.
- Richten Sie die Protokollierung und Überwachung für den Bastion-Host ein. Protokollierung und Überwachung sind wichtige Bestandteile der Wartung von Systemen, sowohl aus betrieblicher als auch aus sicherheitstechnischer Sicht. Es gibt mehrere Möglichkeiten, Verbindungen und Aktivitäten auf Ihrem Bastion-Host zu überwachen. Weitere Informationen finden Sie in den folgenden Themen in der Systems Manager Manager-Dokumentation:
  - Überwachung AWS Systems Manager
  - Anmeldung und Überwachung AWS Systems Manager
  - Überwachung der Sitzungsaktivität
  - Protokollieren von Sitzungsaktivitäten

Epen

Stellen Sie die Ressourcen bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Code-Repo sitory.	1. Ändern Sie in einer Befehlszeilenschnittstelle Ihr Arbeitsverzeichnis in das Verzeichnis, in dem Sie die Beispieldateien speichern möchten.	DevOps Ingenieur, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Geben Sie den folgenden Befehl ein. `git clone https://github.com/aws-samples/secured-bastion-host-terraform.git`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Initialisieren Sie das Terraform -Arbeitsverzeichnis.	Dieser Schritt ist nur für die erste Bereitstellung erforderl ich. Wenn Sie das Muster erneut bereitstellen, fahren Sie mit dem nächsten Schritt fort.
	
	Geben Sie im Stammverz eichnis des geklonten Repositorys den folgenden Befehl ein, wobei:
	
	• `$S3_STATE_BUCKET` ist der Name des Amazon S3 S3-Buckets, der den Terraform-Status enthält
	• `$PATH_TO_STATE_FIL E` ist der Schlüssel zur Terraform-Statusdatei, wie zum Beispiel `infra/bas tion-host/tetfstat e`
	• `$AWS_REGION` ist die Region, in der der Amazon S3 S3-Bucket bereitgestellt wird
	
	`terraform init \`
	`  -backend-config="b ucket=$S3_STATE_BU CKET" \`
	`  -backend-config="k ey=$PATH_TO_STATE_ FILE" \`
	`  -backend-config="r egion=$AWS_REGION`
		DevOps Ingenieur, Entwickler, Terraform

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Alternativ können Sie die Datei config.tf öffnen und in dem `terraform` Abschnitt diese Werte manuell angeben.	
Stellen Sie die Ressourcen bereit.	1. Geben Sie im Stammverzeichnis des geklonten Repositorys den folgenden Befehl ein. `terraform apply -var-file="dev.tfvars"` 2. Sehen Sie sich die Liste aller Änderungen an, die auf Ihr System angewendet werden AWS-Konto, und bestätigen Sie dann die Bereitstellung. 3. Warten Sie, bis alle Ressourcen bereitgestellt sind.	DevOps Ingenieur, Entwickler, Terraform

Richten Sie die lokale Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die SSH-Verbindung.	Aktualisieren Sie die SSH-Konfigurationsdatei, um SSH-Verbindungen über den	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sitzungsmanager zuzulasse n. Anweisungen finden Sie unter Zulassen von SSH-Verbi ndungen für Session Manager. Auf diese Weise können autorisierte Benutzer einen Proxybefehl eingeben, der eine Session Manager-Sitzung startet und alle Daten über eine bidirektionale Verbindung überträgt.	
Generieren Sie die SSH-Schlü ssel.	Geben Sie den folgenden Befehl ein, um ein lokales privates und öffentliches SSH-Schlüsselpaar zu generiere n. Sie verwenden dieses key pair, um eine Verbindung zum Bastion-Host herzustellen. `ssh-keygen -t rsa -f my_key`	DevOps Ingenieur, Entwickler

Stellen Sie mithilfe von Session Manager eine Connect zum Bastion-Host her

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Holen Sie sich die Instanz-ID.	1. Um eine Verbindung zum bereitgestellten Bastion-Host herzustellen, benötigen Sie die ID der EC2 Amazon-Instance. Gehen Sie wie folgt vor, um die ID zu finden:	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	• Öffnen Sie die EC2 Amazon-Konsole. Wählen Sie im Navigationsbereich Instances aus. Suchen Sie die Bastion-Host-Instance.
	• Geben Sie in AWS CLI der den folgenden Befehl ein.
	`aws ec2 describe-instances`
	Um die Ergebnisse zu filtern, geben Sie den folgenden Befehl ein. Dabei `$BASTION_HOST_TAG` handelt es sich um das Tag, das Sie dem Bastion-Host zugewiesen haben. Der Standardwert für dieses Tag ist `sandbox-dev-bastion-host` .
	`aws ec2 describe-instances \ --filters "Name=tag:Name,Values=$BASTION_HOST_TAG" \ --output text \ --query 'Reservations[*].Instances[*].InstanceId' \`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>--output text</pre> 2. Kopieren Sie die ID der EC2 Amazon-Instance. Sie verwenden diese ID später.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie den öffentlichen SSH-Schlüssel.	**Note** In diesem Abschnitt laden Sie den öffentlichen Schlüssel in die Instanz-Metadaten des Bastion-Hosts hoch. Nachdem der Schlüssel hochgeladen wurde, haben Sie 60 Sekunden Zeit, um eine Verbindung mit dem Bastion-Host herzustellen. Nach 60 Sekunden wird der öffentliche Schlüssel entfernt. Weitere Informationen finden Sie im Abschnitt zur Fehlerbehebung dieses Musters. Führen Sie die nächsten Schritte schnell durch, um zu verhindern, dass der Schlüssel entfernt wird, bevor Sie eine Verbindung zum Bastion-Host herstellen. 1. Senden Sie den SSH-Schlüssel mithilfe von Amazon	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	EC2 Instance Connect an den Bastion-Host. Geben Sie den folgenden Befehl ein, wobei: • `$INSTANCE_ID` ist die ID der EC2 Amazon-Instance • `$PUBLIC_KEY_FILE` ist der Pfad zu Ihrer öffentlichen Schlüsseldatei, z. B. `my_key.pub` **Important** Achten Sie darauf, den öffentlichen Schlüssel und nicht den privaten Schlüssel zu verwenden. `aws ec2-instance-connect send-ssh-public-key \ --instance-id $INSTANCE_ID \ --instance-os-user ec2-user \ --ssh-public-key file://$PUBLIC_KEY_FILE` 2. Warten Sie, bis Sie eine Meldung erhalten, dass der Schlüssel erfolgreich	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	hochgeladen wurde. Fahren Sie sofort mit dem nächsten Schritt fort.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Connect zum Bastion-Host her.	1. Geben Sie den folgenden Befehl ein, um über Session Manager eine Verbindung zum Bastion-Host herzustellen. Dabei gilt: • `$PRIVATE_KEY_FILE` ist der Pfad zu Ihrem privaten Schlüssel, z. B. `my_key` • `$INSTANCE_ID` ist die ID der EC2 Amazon-Instance `ssh -i $PRIVATE_KEY_FILE ec2-user@$INSTANCE_ID` 2. Bestätigen Sie die Verbindung, indem Sie eingeben `yes`. Dadurch wird mithilfe des Sitzungsmanagers eine SSH-Verbindung geöffnet. **Note** Es gibt andere Optionen zum Öffnen einer SSH-Verbindung mit dem Bastion-Host. Weitere Informationen finden Sie unter Alternative Ansätze zum Herstellen einer SSH-Verbindung mit	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dem Bastion-Host im Abschnitt Zusätzliche Informationen dieses Musters.	

(Optional) Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die bereitgestellten Ressourcen.	1. Um alle bereitgestellten Ressourcen zu entfernen, führen Sie den folgenden Befehl im Stammverzeichnis des geklonten Repositorys aus. `terraform destroy -var-file="dev.tfvars"` 2. Bestätigen Sie das Entfernen der Ressourcen.	DevOps Ingenieur, Entwickler, Terraform

Fehlerbehebung

Problem	Lösung
`TargetNotConnected` Fehler beim Versuch, eine Verbindung zum Bastion-Host herzustellen	1. Starten Sie den Bastion-Host gemäß den Anweisungen unter Reboot your Instance in der EC2 Amazon-Dokumentation neu. 2. Nachdem die Instance erfolgreich neu gestartet wurde, senden Sie den öffentlichen Schlüssel erneut an den Bastion-Host

Problem	Lösung
	und versuchen Sie erneut, die Verbindung herzustellen.
`Permission denied` Fehler beim Versuch, eine Verbindung zum Bastion-Host herzustellen	Nachdem der öffentliche Schlüssel auf den Bastion-Host hochgeladen wurde, haben Sie nur 60 Sekunden Zeit, um die Verbindung herzustellen. Nach 60 Sekunden wird der Schlüssel automatisch entfernt und Sie können ihn nicht verwenden, um eine Verbindung mit der Instanz herzustellen. In diesem Fall können Sie den Schritt wiederholen, um den Schlüssel erneut an die Instanz zu senden.

Zugehörige Ressourcen

AWS Dokumentation

- AWS Systems Manager Session Manager(Systems Manager Manager-Dokumentation)
- Installieren Sie das Session Manager-Plug-In für AWS CLI (Systems Manager Manager-Dokumentation)
- Zulassen von SSH-Verbindungen für Session Manager (Systems Manager Manager-Dokumentation)
- Über die Verwendung von EC2 Instance Connect (EC2 Amazon-Dokumentation)
- Stellen Sie mithilfe von EC2 Instance Connect eine Verbindung her (EC2 Amazon-Dokumentation)
- Identitäts- und Zugriffsmanagement für Amazon EC2 (EC2 Amazon-Dokumentation)
- Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden (IAM-Dokumentation)
- Bewährte Sicherheitsmethoden in IAM (IAM-Dokumentation)
- Steuern Sie den Datenverkehr zu Ressourcen mithilfe von Sicherheitsgruppen (Amazon VPC-Dokumentation)

Sonstige Ressourcen

- Terraform-Webseite für Entwickler
- Befehl: validate (Terraform-Dokumentation)
- Befehl: fmt (Terraform-Dokumentation)
- HashiCorp Terraform testen (Blogbeitrag) HashiCorp
- Checkov-Webseite

Zusätzliche Informationen

Alternative Ansätze zum Herstellen einer SSH-Verbindung mit dem Bastion-Host

Port-Weiterleitung

Sie können die `-D 8888` Option verwenden, um eine SSH-Verbindung mit dynamischer Portweiterleitung zu öffnen. Weitere Informationen finden Sie in den Anweisungen auf explainshell.com. Im Folgenden finden Sie ein Beispiel für einen Befehl zum Öffnen einer SSH-Verbindung mithilfe von Portweiterleitung.

```
ssh -i $PRIVATE_KEY_FILE -D 8888 ec2-user@$INSTANCE_ID
```

Diese Art von Verbindung öffnet einen SOCKS-Proxy, der den Datenverkehr von Ihrem lokalen Browser über den Bastion-Host weiterleiten kann. Wenn Sie Linux oder macOS verwenden, geben Sie ein, um alle Optionen anzuzeigen`man ssh`. Dadurch wird das SSH-Referenzhandbuch angezeigt.

Unter Verwendung des bereitgestellten Skripts

Anstatt die unter Connect zum Bastion-Host mithilfe des Sitzungsmanagers im Abschnitt Epics beschriebenen Schritte manuell auszuführen, können Sie das Skript connect.sh verwenden, das im Code-Repository enthalten ist. Dieses Skript generiert das SSH-Schlüsselpaar, überträgt den öffentlichen Schlüssel an die EC2 Amazon-Instance und initiiert eine Verbindung mit dem Bastion-Host. Wenn Sie das Skript ausführen, übergeben Sie das Tag und den Schlüsselnamen als Argumente. Im Folgenden finden Sie ein Beispiel für den Befehl zum Ausführen des Skripts.

```
./connect.sh sandbox-dev-bastion-host my_key
```

Zentralisieren Sie die DNS-Auflösung mithilfe von AWS Managed Microsoft AD und vor Ort von Microsoft Active Directory

Erstellt von Brian Westmoreland (AWS)

Übersicht

Dieses Muster bietet Anleitungen für die Zentralisierung der DNS-Auflösung in einer Umgebung mit AWS mehreren Konten, indem sowohl AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) als auch Amazon Route 53 verwendet werden. In diesem Muster ist der AWS DNS-Namespace eine Unterdomäne des lokalen DNS-Namespace. Dieses Muster enthält auch Anleitungen zur Konfiguration der lokalen DNS-Server für die Weiterleitung von Abfragen, AWS wenn die lokale DNS-Lösung Microsoft Active Directory verwendet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Umgebung AWS mit mehreren Konten, eingerichtet mit. AWS Organizations
- Netzwerkkonnektivität wurde hergestellt zwischen AWS-Konten.
- Netzwerkkonnektivität, die zwischen AWS und der lokalen Umgebung hergestellt wurde (mithilfe einer VPN-Verbindung AWS Direct Connect oder einer beliebigen Art von VPN-Verbindung).
- AWS Command Line Interface (AWS CLI) auf einer lokalen Arbeitsstation konfiguriert.
- AWS Resource Access Manager (AWS RAM) wird verwendet, um Route 53-Regeln zwischen Konten gemeinsam zu nutzen. Daher muss die gemeinsame Nutzung innerhalb der AWS Organizations Umgebung aktiviert sein, wie im Abschnitt Epics beschrieben.

Einschränkungen

- AWS Managed Microsoft AD Die Standard Edition hat ein Limit von 5 Shares.
- AWS Managed Microsoft AD Die Enterprise Edition hat ein Limit von 125 Aktien.
- Die Lösung in diesem Muster ist auf AWS-Regionen die gemeinsame Nutzung des Supports beschränkt AWS RAM.

Produktversionen

- Microsoft Active Directory wird auf Windows Server 2008, 2012, 2012 R2 oder 2016 ausgeführt.

Architektur

Zielarchitektur

In diesem Design AWS Managed Microsoft AD ist es in den Shared Services installiert AWS-Konto. Obwohl dies keine Anforderung ist, geht dieses Muster von dieser Konfiguration aus. Wenn Sie eine andere Konfiguration AWS Managed Microsoft AD verwenden AWS-Konto, müssen Sie möglicherweise die Schritte im Abschnitt Epics entsprechend ändern.

Dieses Design verwendet Route 53-Resolver, um die Namensauflösung mithilfe von Route 53-Regeln zu unterstützen. Wenn die lokale DNS-Lösung Microsoft DNS verwendet, ist die Erstellung einer bedingten Weiterleitungsregel für den AWS-Namespace (`aws.company.com`), der eine Unterdomäne des Unternehmens-DNS-Namespace (`company.com`) ist, nicht einfach. Wenn Sie versuchen, eine herkömmliche bedingte Weiterleitung zu erstellen, führt dies zu einem Fehler. Dies liegt daran, dass Microsoft Active Directory bereits für jede Subdomain von als maßgeblich angesehen wird. `company.com` Um diesen Fehler zu umgehen, müssen Sie zunächst eine Delegierung erstellen, um die Autorität für diesen `aws.company.com` Namespace zu delegieren. Anschließend können Sie die bedingte Weiterleitung erstellen.

Die Virtual Private Cloud (VPC) für jedes Spoke-Konto kann einen eigenen eindeutigen DNS-Namespace haben, der auf dem AWS Root-Namespace basiert. In diesem Design hängt jedes Spoke-Konto eine Abkürzung des Kontonamens an den AWS-Basisnamespace an. Nachdem die privaten Hosting-Zonen im Spoke-Konto erstellt wurden, werden die Zonen der lokalen VPC im Spoke-Konto sowie der VPC im zentralen AWS Netzwerkkonto zugeordnet. Dadurch kann das zentrale AWS Netzwerkkonto DNS-Anfragen beantworten, die sich auf die Spoke-Konten beziehen. Auf diese Weise teilen sich Route 53 und Route 53 AWS Managed Microsoft AD gemeinsam die Verantwortung für die Verwaltung des AWS Namespaces (`aws.company.com`).

Automatisierung und Skalierung

Dieses Design verwendet Route 53 Resolver-Endpunkte, um DNS-Abfragen zwischen AWS und Ihrer lokalen Umgebung zu skalieren. Jeder Route 53 Resolver-Endpunkt besteht aus mehreren elastischen Netzwerkschnittstellen (verteilt auf mehrere Availability Zones), und jede Netzwerkschnittstelle kann bis zu 10.000 Abfragen pro Sekunde verarbeiten. Route 53 Resolver unterstützt bis zu 6 IP-Adressen pro Endpunkt. Insgesamt unterstützt dieses Design also bis zu 60.000 DNS-Abfragen pro Sekunde, die über mehrere Availability Zones verteilt sind, um eine hohe Verfügbarkeit zu gewährleisten.

Darüber hinaus berücksichtigt dieses Muster automatisch das future Wachstum innerhalb AWS. Die vor Ort konfigurierten DNS-Weiterleitungsregeln müssen nicht geändert werden, um neue VPCs und die zugehörigen privaten Hosting-Zonen zu unterstützen, die hinzugefügt werden AWS.

Tools

AWS-Services

- AWS Directory Service for Microsoft Active Directoryermöglicht Ihren verzeichnissensitiven Workloads und AWS Ressourcen die Verwendung von Microsoft Active Directory in der. AWS Cloud
- AWS Organizationsist ein Kontoverwaltungsdienst, der Ihnen hilft, mehrere Konten AWS-Konten in einer Organisation zu konsolidieren, die Sie erstellen und zentral verwalten.
- AWS Resource Access Manager (AWS RAM) hilft Ihnen dabei, Ihre Ressourcen sicher gemeinsam zu nutzen AWS-Konten , um den betrieblichen Aufwand zu reduzieren und für Transparenz und Überprüfbarkeit zu sorgen.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.

Tools

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie AWS-Services über Befehle in Ihrer Befehlszeilen-Shell interagieren können. In diesem Muster AWS CLI wird der verwendet, um Route 53-Autorisierungen zu konfigurieren.

Epen

Ein AWS Managed Microsoft AD Verzeichnis erstellen und teilen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereitstellen AWS Managed Microsoft AD.	1. Erstellen und konfigurieren Sie ein neues Verzeichnis. Eine ausführliche Anleitung finden Sie unter Erstellen Ihres AWS Managed Microsoft AD im AWS	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Directory Service Administrator handbuch. 2. Notieren Sie sich die IP-Adressen der AWS Managed Microsoft AD Domänencontroller. Auf diese wird in einem späteren Schritt verwiesen.	
Teilen Sie das Verzeichnis.	Nachdem das Verzeichnis erstellt wurde, können Sie es mit anderen Mitgliedern AWS-Konten der AWS Organisation teilen. Anweisungen dazu finden Sie im AWS Directory Service Administratorhandbuch unter Verzeichnis teilen. **Note** AWS Managed Microsoft AD Die Standard Edition hat ein Limit von 5 Shares. Die Enterprise Edition hat ein Limit von 125 Aktien.	AWS-Administrator

Route 53 konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Route 53-Resolver.	Route 53-Resolver erleichtern die Auflösung von DNS-Abfra	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	gen zwischen AWS und dem lokalen Rechenzentrum. 1. Installieren Sie Route 53 Resolver, indem Sie den Anweisungen im Route 53 Developer Guide folgen. 2. Konfigurieren Sie Route 53-Resolver in privaten Subnetzen in mindesten s zwei Availability Zones innerhalb der zentralen AWS Netzwerkkonto-VPC für hohe Verfügbarkeit. **Note** Die Verwendung des zentralen AWS Netzwerkkontos VPC ist zwar nicht erforderlich, bei den verbleibenden Schritten wird jedoch von dieser Konfigura tion ausgegangen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie Route 53-Regeln .	Ihr spezieller Anwendungsfall erfordert möglicherweise eine große Anzahl von Route 53-Regeln, aber Sie müssen die folgenden Regeln als Grundlage konfigurieren:
	• Eine ausgehende Regel für den lokalen Namespace (`company.com`) unter Verwendung der ausgehenden Route 53-Resolver des zentralen Netzwerkkontos. Die Ziel-IP-Adressen sind die lokalen DNS-Server.
	  • Ordnen Sie diese Regel dem zentralen Netzwerkkonto VPC zu.
	• Eine ausgehende Regel für den AWS Namespace (`aws.company.com`) unter Verwendung der ausgehenden Route 53-Resolver des zentralen Netzwerkkontos. Die Ziel-IP-Adressen sind die eingehenden Route 53-Resolver-IP-Adressen des zentralen Netzwerkkontos.
	  • Ordnen Sie diese Regel nicht dem zentralen AWS Netzwerkkonto VPC zu (in dem sich die Route 53-Resolver befinden).
		AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	• Eine zweite ausgehend e Regel für den AWS Namespace (`aws.compa ny.com`), die auf die AWS Managed Microsoft AD Domänencontroller verweist (verwenden Sie die IPs aus dem vorherigen Epic).
	  • Ordnen Sie diese Regel dem zentralen AWS Netzwerkkonto VPC zu (in dem sich die Route 53-Resolver befinden).
	  • Teilen Sie diese Regel nicht mit anderen und verknüpfen Sie sie nicht mit anderen. AWS-Konten
	
	Weitere Informationen finden Sie im Route 53 Developer Guide unter Managing Forwarding Rules.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie ein Route 53-Profil.	Ein Route 53-Profil wird verwendet, um die Regeln mit Spoke-Konten zu teilen. 1. Erstellen Sie ein neues Route 53-Profil im zentralen Netzwerkkonto, indem Sie den Anweisungen im Route 53-Entwicklerhandbuch folgen. 2. Fügen Sie dem Profil die Regel für den lokalen Namespace (`company.com`) hinzu. 3. Fügen Sie dem Profil die erste Regel für den AWS Namespace (`aws.company.com`) hinzu, der auf die IP-Adressen der Route 53-Inbound-Resolver abzielt. 4. Geben Sie das Route 53-Profil für die Organisation frei. AWS 5. Akzeptieren Sie die Ressourcenfreigabe für das Route 53-Profil in jedem Spoke-Konto. 6. Ordnen Sie das Route 53-Profil jeder Spoke-Konto-VPC zu.	AWS-Administrator

Konfigurieren Sie das lokale Active Directory-DNS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Delegation.	Verwenden Sie das Microsoft DNS-Snap-In (`dnsmgmt.msc`), um eine neue Delegierung für den `company.com` Namespace in Active Directory zu erstellen. Der Name der delegierten Domäne sollte lauten. `aws` Dies ist der vollqualifizierte Domänenname (FQDN) der Delegation. `aws.company.com` Verwenden Sie die IP-Adressen der AWS Managed Microsoft AD Domänencontroller für die IP-Werte des Nameservers und verwenden Sie sie `server.aws.company.com` für den Namen. (Diese Delegierung dient nur der Redundanz, da für diesen Namespace eine bedingte Weiterleitung erstellt wird, die Vorrang vor der Delegierung hat.)	Active Directory
Erstellen Sie die bedingte Weiterleitung.	Verwenden Sie das Microsoft DNS-Snap-In (`dnsmgmt.msc`), um eine neue bedingte Weiterleitung für zu erstellen. `aws.company.com` Verwenden Sie die IP-Adressen der AWS eingehend	Active Directory

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en Route 53-Resolver im zentralen DNS AWS-Konto für das Ziel der bedingten Weiterleitung.	

Erstellen Sie private, gehostete Route 53-Zonen für Spoke AWS-Konten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die privaten Hosting-Zonen von Route 53.	Erstellen Sie in jedem Spoke-Konto eine private gehostete Route 53-Zone. Ordnen Sie diese privat gehostete Zone der Spoke-Konto-VPC zu. Eine ausführliche Anleitung finden Sie unter Creating a private hosted zone im Route 53 Developer Guide.	AWS-Administrator
Autorisierungen erstellen.	Verwenden Sie die AWS CLI , um eine Autorisierung für das zentrale AWS Netzwerkkonto VPC zu erstellen. Führen Sie diesen Befehl im Kontext der einzelnen AWS-Konto Spokes aus: `aws route53 create-vpc-association-authorization --hosted-zone-id <hosted-zone-id> \ --vpc VPCRegion=<region>,VPCId=<vpc-id>`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wobei: • `<hosted-zone-id>` ist die privat gehostete Route 53-Zone im Spoke-Konto. • `<region>`und `<vpc-id>` sind die AWS-Region und VPC-ID des zentralen AWS Netzwerkkontos VPC.	
Verknüpfungen erstellen.	Erstellen Sie die Route 53-Zuordnung für die private gehostete Zone für die zentrale AWS Netzwerkkonto-VPC mithilfe von. AWS CLI Führen Sie diesen Befehl im Kontext des zentralen AWS Netzwerkkontos aus: `aws route53 associate -vpc-with-hosted-z one --hosted-zone-id <hosted-zone-id> \ --vpc VPCRegion =<region>,VPCId=<vpc-id>` Wobei: • `<hosted-zone-id>` ist die private gehostete Route 53-Zone im Spoke-Konto. • `<region>`und `<vpc-id>` sind die AWS-Region und VPC-ID des zentralen AWS Netzwerkkontos.	AWS-Administrator

Zugehörige Ressourcen

- Vereinfachen Sie die DNS-Verwaltung in einer Umgebung mit mehreren Konten mit Route 53 Resolver (AWS Blogbeitrag)
- Erstellen Sie Ihre AWS Managed Microsoft AD (Dokumentation)AWS Directory Service
- Ein AWS Managed Microsoft AD Verzeichnis teilen (AWS Directory Service Dokumentation)
- Was ist Amazon Route 53 Resolver? (Dokumentation zu Amazon Route 53)
- Eine private gehostete Zone erstellen (Amazon Route 53-Dokumentation)
- Was sind Amazon Route 53 53-Profile? (Dokumentation zu Amazon Route 53)

Zentralisieren Sie die Überwachung mithilfe von Amazon CloudWatch Observability Access Manager

Erstellt von Anand Krishna Varanasi (AWS), Jimmy Morgan (AWS), Ashish Kumar (AWS), Balaji Vedagiri (AWS), JAGDISH KOMAKULA (AWS), Sarat Chandra Pothula (AWS) und Vivek Thangamuthu (AWS)

Übersicht

Beobachtbarkeit ist entscheidend für die Überwachung, das Verständnis und die Fehlerbehebung von Anwendungen. Anwendungen, die sich über mehrere Konten erstrecken, wie bei Implementierungen AWS Control Tower oder landing zone Zone-Implementierungen, generieren eine große Anzahl von Protokollen und Trace-Daten. Um Probleme schnell zu beheben oder Benutzeranalysen oder Geschäftsanalysen zu verstehen, benötigen Sie eine gemeinsame Observability-Plattform für alle Konten. Mit dem Amazon CloudWatch Observability Access Manager können Sie von einem zentralen Ort aus auf mehrere Kontoprotokolle zugreifen und diese kontrollieren.

Sie können den Observability Access Manager verwenden, um Observability-Datenprotokolle anzuzeigen und zu verwalten, die von Quellkonten generiert wurden. Quellkonten sind Einzelpersonen AWS-Konten , die Observability-Daten für ihre Ressourcen generieren. Observabilitätsdaten werden zwischen Quellkonten und Monitoring-Konten gemeinsam genutzt. Die gemeinsam genutzten Observability-Daten können Metriken in Amazon CloudWatch, Logs in Amazon CloudWatch Logs und Traces in AWS X-Ray beinhalten. Weitere Informationen finden Sie in der Dokumentation zu Observability Access Manager.

Dieses Muster ist für Benutzer gedacht, die über Anwendungen oder Infrastrukturen verfügen, die in mehreren ausgeführt werden AWS-Konten und die einen gemeinsamen Ort zum Einsehen von Protokollen benötigen. Es erklärt, wie Sie Observability Access Manager mithilfe von Terraform einrichten können, um den Status und den Zustand dieser Anwendungen oder Infrastrukturen zu überwachen. Sie können diese Lösung auf verschiedene Arten installieren:

- Als eigenständiges Terraform-Modul, das Sie manuell einrichten
- Durch die Verwendung einer Pipeline für kontinuierliche Integration und kontinuierliche Lieferung (CI/CD)
- Durch die Integration mit anderen Lösungen wie AWS Control Tower Account Factory for Terraform (AFT)

Die Anweisungen im Abschnitt Epics behandeln die manuelle Implementierung. Die Schritte zur AFT-Installation finden Sie in der README-Datei für das GitHub Observability Access Manager-Repository.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Terraform ist in Ihrem System oder in automatisierten Pipelines installiert oder referenziert. (Wir empfehlen Ihnen, die neueste Version zu verwenden.)
- Ein Konto, das Sie als zentrales Überwachungskonto verwenden können. Andere Konten erstellen Links zum zentralen Überwachungskonto, um Protokolle einzusehen.
- (Optional) Ein Quellcode-Repository wie GitHub, AWS CodeCommit, Atlassian Bitbucket oder ein ähnliches System. Ein Quellcode-Repository ist nicht erforderlich, wenn du automatisierte CI/CD-Pipelines verwendest.
- (Optional) Berechtigungen zum Erstellen von Pull-Requests (PRs) für Code-Reviews und Code-Zusammenarbeit in. GitHub

Einschränkungen

Observability Access Manager hat die folgenden Dienstkontingente, die nicht geändert werden können. Berücksichtigen Sie diese Kontingente, bevor Sie diese Funktion bereitstellen. Weitere Informationen finden Sie in der CloudWatch Dokumentation unter CloudWatch Servicekontingenten.

- Links zu Quellkonten: Sie können jedes Quellkonto mit maximal fünf Überwachungskonten verknüpfen.
- Senken: Sie können mehrere Senken für ein Konto erstellen, pro Konto AWS-Region ist jedoch nur eine Senke zulässig.

Darüber hinaus gilt:

- Senken und Links müssen im selben System erstellt werden. Sie können nicht regionsübergreifend sein AWS-Region.

Regions- und kontenübergreifende Überwachung

Für die regionsübergreifende, kontenübergreifende Überwachung können Sie eine der folgenden Optionen wählen:

- Erstellen Sie konto- und regionsübergreifende CloudWatch Dashboards für Alarme und Messwerte. Diese Option unterstützt keine Logs und Traces.
- Implementieren Sie die zentralisierte Protokollierung mithilfe von Amazon OpenSearch Service.
- Erstellen Sie eine Senke pro Region aus allen Mandantenkonten, übertragen Sie Metriken an ein zentrales Überwachungskonto (wie in diesem Muster beschrieben) und verwenden Sie dann CloudWatch Metrik-Streams, um die Daten an ein gemeinsames externes Ziel oder an Monitoring-Produkte von Drittanbietern wie Datadog, Dynatrace, Sumo Logic, Splunk oder New Relic zu senden.

Architektur

Komponenten

CloudWatch Observability Access Manager besteht aus zwei Hauptkomponenten, die eine kontenübergreifende Observability ermöglichen:

- Eine Senke bietet Quellkonten die Möglichkeit, Observabilitätsdaten an das zentrale Monitoring-Konto zu senden. Eine Senke stellt im Grunde eine Gateway-Verbindung dar, mit der Quellkonten eine Verbindung herstellen können. Es kann nur ein Senken-Gateway oder eine Senkenverbindung geben, und mehrere Konten können eine Verbindung zu diesem herstellen.
- Jedes Quellkonto hat einen Link zum Sink-Gateway-Junction, und Observability-Daten werden über diesen Link gesendet. Sie müssen eine Senke erstellen, bevor Sie Links von jedem Quellkonto aus erstellen können.

Architektur

Das folgende Diagramm veranschaulicht Observability Access Manager und seine Komponenten.

Tools

AWS-Services

- Amazon CloudWatch hilft Ihnen dabei, die Kennzahlen Ihrer AWS Ressourcen und der Anwendungen, auf denen Sie laufen, AWS in Echtzeit zu überwachen.

- AWS Organizationsist ein Kontoverwaltungsservice, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie erstellen und zentral verwalten.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.

Tools

- Terraform ist ein IaC-Tool (Infrastructure as Code) HashiCorp , mit dem Sie Cloud- und lokale Ressourcen erstellen und verwalten können.
- AWS Control Tower Account Factory for Terraform (AFT) richtet eine Terraform-Pipeline ein, mit der Sie Konten bereitstellen und anpassen können. AWS Control Tower Sie können AFT optional verwenden, um Observability Access Manager skalierbar für mehrere Konten einzurichten.

Code-Repository

Der Code für dieses Muster ist im GitHub Observability Access Manager-Repository verfügbar.

Bewährte Methoden

- Markieren Sie in AWS Control Tower Umgebungen das Protokollierungskonto als zentrales Überwachungskonto (Senke).
- Wenn Sie mehrere Organisationen mit mehreren Konten haben AWS Organizations, empfehlen wir, dass Sie die Organisationen und nicht einzelne Konten in die Konfigurationsrichtlinie aufnehmen. Wenn Sie nur über eine geringe Anzahl von Konten verfügen oder wenn die Konten nicht Teil einer Organisation sind, die in der Konfigurationsrichtlinie aufgeführt ist, können Sie sich dafür entscheiden, stattdessen einzelne Konten einzubeziehen.

Epen

Richten Sie das Spülmodul ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Klonen Sie das GitHub Observability Access Manager-Repository:	AWS DevOps, Cloud-Adm inistrator, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`git clone https://github.com/aws-samples/cloudwatch-observability-access-manager-terraform`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie Eigenschaftswerte für das Sink-Modul an.	Geben Sie in der `main.tf` Datei (im `deployments/aft-account-customizations/LOGGING/terraform/` Ordner des Repositorys) Werte für die folgenden Eigenschaften an: • `sink_name` : Der Name der CloudWatch Senke. • `allowed_oam_resource_types` : Observability Access Manager unterstützt derzeit CloudWatch Metriken, Protokollgruppen und AWS X-Ray Traces. • `allowed_source_accounts` : Die Quellkonten, die Protokolle an das zentrale CloudWatch Senkenkonto senden dürfen. • `allowed_source_organizations` : Die AWS Control Tower Quellorganisationen, die Protokolle an das Central-Senk-Konto CloudWatch senden dürfen. Weitere Informationen finden Sie AWS::Oam::Sink in der AWS CloudFormation Dokumentation.	AWS DevOps, Cloud-Administrator, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie das Sink-Modul.	Exportieren Sie die Anmeldeinformationen des Kontos AWS-Konto , das Sie als Überwachungskonto ausgewählt haben, und installieren Sie das Observability Access Manager-Senkmodul:
	`Terraform Init`
	`Terrafom Plan`
	`Terraform Apply`
		AWS DevOps, Cloud-Administrator, AWS-Administrator

Richten Sie das Link-Modul ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Geben Sie Eigenschaftswerte für das Linkmodul an.	Geben Sie in der `main.tf` Datei (im `deployments/aft-account-customizations/LOGGING/terraform/` Ordner des Repositorys) Werte für die folgenden Eigenschaften an:
	• `account_label` : Verwenden Sie einen der folgenden Werte:
	  • `$AccountName` : Der Name des Kontos.
	  • `$AccountEmail` : Eine weltweit eindeutige E-Mail-Adresse, zu der auch die E-Mail-Domain
		AWS DevOps, Cloud-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	gehört (z. B.`hello@example.com`) • `$AccountEmailNoDomain` : Eine E-Mail-Adresse ohne den Domainnamen. • `allowed_oam_resource_types` : Observability Access Manager unterstützt derzeit CloudWatch Metriken, Protokollgruppen und AWS X-Ray Traces. Weitere Informationen finden Sie AWS::Oam::Link in der AWS CloudFormation Dokumentation.	

Installieren Sie das Link-Modul für einzelne Konten.	Exportieren Sie die Anmeldeinformationen einzelner Konten und installieren Sie das Observability Access Manager-Linkmodul:
	
	`Terraform Plan`
	`Terraform Apply`
	
	Sie können das Linkmodul für jedes Konto einzeln einrichten oder AFT verwenden, um dieses Modul automatisch für eine große Anzahl von Konten zu installieren.
		AWS DevOps, Cloud-Administrator, Cloud-Architekt

sink-to-linkVerbindungen genehmigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Statusmeldung.	1. Melden Sie sich beim Überwachungskonto an. 2. Öffnen Sie die CloudWatch -Konsole. 3. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus. Auf der rechten Seite sollte die Statusmeldung Das Überwachungskonto aktiviert mit einem grünen Häkchen angezeigt werden. Das bedeutet, dass das Überwachungskonto über eine Observability Access Manager-Senke verfügt, zu der die Links anderer Konten eine Verbindung herstellen.	
Genehmigen Sie die link-to-sink Verbindungen.	1. Wählen Sie unter der Statusmeldung die Option Ressourcen zum Verknüpfen von Konten aus. Die Information bestätigt, dass es sich um das Überwachungskonto handelt, listet die Daten auf, die von den Quellkonten des Mandanten gemeinsam genutzt wurden (Logs, Metrics, Traces), und	AWS DevOps, Cloud-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zeigt die Kontobezeichnung $ anAccountName. Dieser Bildschirm bietet zwei Optionen für die Verknüpfung von Mandantenkonten mit dem Überwachu ngskonto: Genehmigung auf Organisationsebene oder Genehmigung auf Kontoebene. Für jede Option können Sie wählen, ob Sie eine AWS CloudFormation Vorlage für die Genehmigung herunterladen oder jedes Konto einzeln genehmigen möchten. 2. Der Einfachheit halber wählen Sie „Beliebiges Konto“, um es auf jeder Kontoebene zu genehmige n. Diese Option stellt einen Genehmigungslink für das Konto bereit. 3. Wählen Sie URL kopieren, um den Link zu kopieren. 4. Melden Sie sich bei jedem Quellkonto an. 5. Fügen Sie den Link in einem Browserfenster ein und wählen Sie Link	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	genehmigen, Verbindung zur Senke herstellen. 6. Wiederholen Sie den Vorgang für weitere Quellkonten. Weitere Informationen finden Sie in der CloudWatch Dokumentation unter Monitoring-Konten mit Quellkonten verknüpfen.	

Überprüfen Sie kontoübergreifende Beobachtbarkeitsdaten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kontoübergreifende Daten anzeigen.	1. Melden Sie sich beim zentralen Überwachungskonto an. 2. Öffnen Sie die CloudWatch-Konsole. 3. Wählen Sie im linken Navigationsbereich Optionen aus, um kontoübergreifende Logs, Metriken und Traces anzuzeigen.	AWS DevOps, Cloud-Administrator, Cloud-Architekt

(Optional) Aktivieren Sie Quellkonten, damit sie dem Überwachungskonto vertrauen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich Metriken, Dashboards, Protokolle, Widgets und Alarme von anderen Konten an.	Als zusätzliche Funktion können Sie die CloudWatch Metriken, Dashboards, Protokolle, Widgets und Alarme mit anderen Konten teilen. Jedes Konto verwendet eine IAM-Rolle namens CloudWatch- CrossAccountSharingRole , um Zugriff auf diese Daten zu erhalten. Quellkonten, die eine Vertrauensbeziehung mit dem zentralen Überwachungskonto haben, können diese Rolle übernehmen und Daten aus dem Überwachungskonto einsehen. CloudWatch stellt ein CloudFormation Beispielskript zum Erstellen der Rolle bereit. Wählen Sie „Rolle in IAM verwalten“ und führen Sie dieses Skript in den Konten aus, in denen Sie Daten anzeigen möchten. `{ "Version": "2012-10-17", "Statement": [ {`	AWS DevOps, Cloud-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"Effect": "Allow", "Principal": { "AWS": ["arn:aws:iam::XXXXXXXXXX:root", "arn:aws:iam::XXXXXXXXXX:root", "arn:aws:iam::XXXXXXXXXX:root", "arn:aws:iam::XXXXXXXXXX:root"] }, "Action": "sts:AssumeRole" }] }</pre> Weitere Informationen finden Sie in CloudWatch der Dokumentation unter Aktivieren der CloudWatch kontoübergreifenden Funktionalität.	

(Optional) Kontenübergreifendes Abrufen regionsübergreifender Daten vom Monitoring-Konto aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie einen konto- und regionsübergreifenden Zugriff ein.	Im zentralen Überwachungskonto können Sie optional eine Kontoauswahl hinzufüge	AWS DevOps, Cloud-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	n, um einfach zwischen Konten zu wechseln und deren Daten einzusehen, ohne sich authentifizieren zu müssen. 1. Melden Sie sich beim zentralen Überwachu ngskonto an. 2. Öffnen Sie die CloudWatch -Konsole. 3. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus. 4. Wählen Sie im Abschnitt Kontoübergreifendes regionsübergreifendes anzeigen die Option Konfigurieren aus. 5. Wählen Sie Aktivieren und aktivieren Sie dann das Kontrollkästchen Auswahl in der Konsole anzeigen. 6. Wählen Sie eine dieser Optionen aus: • Eingabe der Konto-ID: Diese Option fordert Sie auf, die Konto-ID manuell einzugeben, wenn Sie Konten ändern möchten, um kontoübergreifende Daten anzuzeigen. • AWS-Kontoauswahl für Organisationen:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wenn Sie CloudWatch mit integriert haben AWS Organizations, bietet diese Option eine Dropdownauswahl mit einer vollständigen Liste der Konten in der Organisation. • Benutzerdefinierter Kontoauswahldialog: Mit dieser Option können Sie manuell eine Liste von Konten eingeben, IDs um die Kontoauswahl auszufüllen. 7. Wählen Sie Änderungen speichern aus. Weitere Informationen finden Sie in der Dokumentation unter Kontoübergreifende regionsübergreifende Konsole CloudWatch . CloudWatch	

Zugehörige Ressourcen

- CloudWatch kontoübergreifende Beobachtbarkeit (CloudWatch Amazon-Dokumentation)
- Amazon CloudWatch Observability Access Manager API-Referenz (CloudWatch Amazon-Dokumentation)
- Ressource: aws_oam_sink (Terraform-Dokumentation)
- Datenquelle: aws_oam_link (Terraform-Dokumentation)
- CloudWatchObservabilityAccessManagerAWS (Boto3-Dokumentation)

EC2 Instances beim Start auf obligatorische Tags überprüfen

Erstellt von Susanne Kangnoh (AWS) und Archit Mathur (AWS)

Übersicht

Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der Amazon Web Services (AWS) Cloud. EC2 Durch die Nutzung von Amazon müssen Sie nicht im Voraus in Hardware investieren, sodass Sie Anwendungen schneller entwickeln und bereitstellen können.

Sie können Tagging verwenden, um Ihre AWS-Ressourcen auf unterschiedliche Weise zu kategorisieren. EC2 Instance-Tagging ist nützlich, wenn Sie viele Ressourcen in Ihrem Konto haben und Sie anhand der Tags schnell eine bestimmte Ressource identifizieren möchten. Mithilfe von Tags können Sie Ihren EC2 Instanzen benutzerdefinierte Metadaten zuweisen. Ein Tag besteht aus einem benutzerdefinierten Schlüssel und Wert. Wir empfehlen Ihnen, einen konsistenten Satz von Stichwörtern zu erstellen, um die Anforderungen Ihrer Organisation zu erfüllen.

Dieses Muster bietet eine CloudFormation AWS-Vorlage, mit der Sie EC2 Instances auf bestimmte Tags überwachen können. Die Vorlage erstellt ein Amazon CloudWatch Events-Ereignis, das nach AWS CloudTrail TagResourceoder UntagResourceEreignissen Ausschau hält, um zu erkennen, ob neue EC2 Instances markiert oder Tags entfernt wurden. Wenn ein vordefiniertes Tag fehlt, ruft es eine AWS-Lambda-Funktion auf, die mithilfe von Amazon Simple Notification Service (Amazon SNS) eine Meldung über einen Verstoß an eine von Ihnen angegebene E-Mail-Adresse sendet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket zum Hochladen des bereitgestellten Lambda-Codes.
- Eine E-Mail-Adresse, an die Sie Benachrichtigungen über Verstöße erhalten möchten.

Einschränkungen

- Diese Lösung unterstützt CloudTrail TagResourceunsere UntagResourceEreignisse. Es werden keine Benachrichtigungen für andere Ereignisse erstellt.
- Diese Lösung sucht nur nach Tag-Schlüsseln. Schlüsselwerte werden nicht überwacht.

Architektur

Workflow-Architektur

Automatisierung und Skalierung

- Sie können die CloudFormation AWS-Vorlage mehrfach für verschiedene AWS-Regionen und Konten verwenden. Sie müssen die Vorlage in jeder Region oder jedem Konto nur einmal ausführen.

Tools

AWS-Services

- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) ist ein Webservice, der sichere, anpassbare Rechenkapazität in der Cloud bietet. Er wurde entwickelt, um Entwicklern Cloud-Computing im Web-Scale-Maßstab zu erleichtern.
- AWS CloudTrail — CloudTrail ist ein AWS-Service, der Sie bei der Steuerung, Einhaltung von Vorschriften sowie der Betriebs- und Risikoprüfung Ihres AWS-Kontos unterstützt. Aktionen, die von einem Benutzer, einer Rolle oder einem AWS-Service ausgeführt werden, werden als Ereignisse in aufgezeichnet CloudTrail.
- Amazon CloudWatch Events — Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit. CloudWatch Events wird sofort auf betriebliche Änderungen aufmerksam und ergreift bei Bedarf Korrekturmaßnahmen, indem es Nachrichten sendet, um auf die Umgebung zu reagieren, Funktionen aktiviert, Änderungen vornimmt und Statusinformationen erfasst.
- AWS Lambda — Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne dass Server bereitgestellt oder verwaltet werden müssen. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice, der für eine Vielzahl von Speicherlösungen verwendet werden kann, darunter Websites, mobile Anwendungen, Backups und Data Lakes.

- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) ist ein Webservice, der es Anwendungen, Endbenutzern und Geräten ermöglicht, sofort Benachrichtigungen aus der Cloud zu senden und zu empfangen.

Code

Dieses Muster beinhaltet einen Anhang mit zwei Dateien:

- `index.zip`ist eine komprimierte Datei, die den Lambda-Code für dieses Muster enthält.
- `ec2-require-tags.yaml`list eine CloudFormation Vorlage, die den Lambda-Code bereitstellt.

Informationen zur Verwendung dieser Dateien finden Sie im Abschnitt Epics.

Epen

Stellen Sie den Lambda-Code bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Code in einen S3-Bucket hoch.	Erstellen Sie einen neuen S3-Bucket oder verwenden Sie einen vorhandenen S3-Bucket, um die angehängte `index.zip` Datei hochzuladen (Lambda-Code). Dieser Bucket muss sich in derselben AWS-Region befinden wie die Ressourcen (EC2 Instances), die Sie überwachen möchten.	Cloud-Architekt
Stellen Sie die CloudFormation Vorlage bereit.	Öffnen Sie die Cloudformation-Konsole in derselben AWS-Region wie der S3-Bucket und stellen Sie die `ec2-require-tags.yaml` Datei bereit, die im Anhang bereitgestellt wird. Geben Sie im nächsten Epic	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Werte für die Vorlagenp arameter an.	

Vervollständigen Sie die Parameter in der CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den S3-Bucket-Namen an.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epic erstellt oder ausgewählt haben. Dieser S3-Bucket enthält die ZIP-Datei für den Lambda-Code und muss sich in derselben AWS-Region befinden wie die CloudFormation Vorlage und die EC2 Instances, die Sie überwachen möchten.	Cloud-Architekt
Geben Sie den S3-Schlüssel an.	Geben Sie den Speicherort der Lambda-Code-ZIP-Datei in Ihrem S3-Bucket an, ohne vorangestellte Schrägstriche (z. B. `index.zip` oder). `controls/index.zip`	Cloud-Architekt
Geben Sie eine E-Mail-Ad resse an.	Geben Sie eine aktive E-Mail-Adresse an, unter der Sie Benachrichtigungen über Verstöße erhalten möchten.	Cloud-Architekt
Definieren Sie eine Protokoll ierungsebene.	Geben Sie die Protokoll ierungsebene und die Ausführlichkeit an. `Info`bezeichnet detaillie	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	rte Informationsmeldungen über den Fortschritt der Anwendung und sollte nur zum Debuggen verwendet werden. `Error`bezeichne t Fehlerereignisse, die es der Anwendung dennoch ermöglichen könnten, weiter zu laufen. `Warning`bezeichnet potenziell schädliche Situation en.	
Geben Sie die erforderlichen Tag-Schlüssel ein.	Geben Sie die Tag-Schlü ssel ein, nach denen Sie suchen möchten. Wenn Sie mehrere Schlüssel angeben möchten, trennen Sie sie durch Kommas ohne Leerzeichen. (`Applicati onId,CreatedBy,Env ironment,Organizat ion` Sucht beispielsweise nach vier Schlüsseln.) Das Ereignis CloudWatch Ereignisse sucht nach diesen Tag-Schlüsseln und sendet eine Benachrichtigung, wenn sie nicht gefunden werden.	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das E-Mail-Abonnement.	Wenn die CloudFormation Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail-Nachricht an die von Ihnen angegebene E-Mail-Adresse. Um Benachrichtigungen zu erhalten, müssen Sie dieses E-Mail-Abonnement bestätigen.	Cloud-Architekt

Zugehörige Ressourcen

- Einen Bucket erstellen (Amazon S3 S3-Dokumentation)
- Objekte hochladen (Amazon S3 S3-Dokumentation)
- Kennzeichnen Sie Ihre EC2 Amazon-Ressourcen (EC2 Amazon-Dokumentation)
- Erstellen einer CloudWatch Ereignisregel, die bei einem AWS-API-Aufruf mithilfe von AWS ausgelöst wird CloudTrail (CloudWatch Amazon-Dokumentation)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Bereinigen Sie die Ressourcen von AWS Account Factory for Terraform (AFT) nach dem Verlust von Statusdateien sicher

Erstellt von Gokendra Malviya (AWS)

Übersicht

Wenn Sie AWS Account Factory for Terraform (AFT) zur Verwaltung Ihrer AWS Control Tower Umgebung verwenden, generiert AFT eine Terraform-Statusdatei, um den Status und die Konfiguration der von Terraform erstellten Ressourcen zu verfolgen. Der Verlust der Terraform-Statusdatei kann zu erheblichen Herausforderungen für das Ressourcenmanagement und die Bereinigung führen. Dieses Muster bietet einen systematischen Ansatz zur sicheren Identifizierung und Entfernung von AFT-bezogenen Ressourcen bei gleichzeitiger Wahrung der Integrität Ihrer Umgebung. AWS Control Tower

Das Verfahren ist so konzipiert, dass sichergestellt ist, dass alle AFT-Komponenten ordnungsgemäß entfernt werden, auch wenn der ursprüngliche Verweis auf die Statusdatei nicht vorhanden ist. Dieser Prozess bietet einen klaren Weg zur erfolgreichen Wiederherstellung und Neukonfiguration von AFT in Ihrer Umgebung, um sicherzustellen, dass Ihr AWS Control Tower Betrieb nur minimal unterbrochen wird.

Weitere Informationen zu AFT finden Sie in der AWS Control Tower Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein gründliches Verständnis der AFT-Architektur.
- Administratorzugriff auf die folgenden Konten:
  - AFT-Verwaltungskonto
  - AWS Control Tower Verwaltungskonto
  - Konto protokollieren und archivieren
  - Prüfungskonto
- Überprüfung, dass keine Dienststeuerungsrichtlinien (SCPs) Einschränkungen oder Beschränkungen enthalten, die das Löschen von AFT-bezogenen Ressourcen verhindern würden.

Einschränkungen

- Durch diesen Vorgang können Ressourcen effektiv bereinigt werden, verloren gegangene Statusdateien können jedoch nicht wiederhergestellt werden, und einige Ressourcen müssen möglicherweise manuell identifiziert werden.
- Die Dauer des Bereinigungsvorgangs hängt von der Komplexität Ihrer Umgebung ab und kann mehrere Stunden dauern.
- Dieses Muster wurde mit AFT Version 1.12.2 getestet und löscht die folgenden Ressourcen. Wenn Sie eine andere Version von AFT verwenden, müssen Sie möglicherweise zusätzliche Ressourcen löschen.

Name des Dienstes	Anzahl der Ressourcen
AWS CodeBuild	6
AWS CodeCommit	4
AWS CodePipeline	4
Amazon-DynamoDB	5
Amazon Elastic Compute Cloud (Amazon EC2)	16
Amazon EventBridge	4
AWS Identity and Access Management (IAM) - Rollen	40
AWS Key Management Service (AWS KMS)	2
AWS Lambda	17
Amazon Simple Storage Service (Amazon-S3)	2
Amazon-Simple-Notification-Service (Amazon-SNS)	2
Amazon-Simple-Queue-Service (Amazon SQS)	2
AWS Systems Manager	62

AWS Step Functions	4

> **Important**
>
> Die Ressourcen, die durch die Schritte in diesem Muster gelöscht werden, können nicht wiederhergestellt werden. Bevor Sie diese Schritte ausführen, überprüfen Sie die Ressourcennamen sorgfältig und stellen Sie sicher, dass sie von AFT erstellt wurden.

Architektur

Das folgende Diagramm zeigt die AFT-Komponenten und den Arbeitsablauf auf hoher Ebene. AFT richtet eine Terraform-Pipeline ein, mit der Sie Ihre Konten bereitstellen und anpassen können. AWS Control Tower AFT folgt einem GitOps Modell zur Automatisierung der Prozesse der Kontobereitstellung in. AWS Control Tower Sie erstellen eine Terraform-Datei für eine Kontoanfrage und übertragen sie in ein Repository, das die Eingabe bereitstellt, die den AFT-Workflow für die Kontobereitstellung auslöst. Nach Abschluss der Kontobereitstellung kann AFT weitere Anpassungsschritte automatisch ausführen.

In dieser Architektur:

- AWS Control Tower Das Verwaltungskonto ist ein Konto AWS-Konto , das dem AWS Control Tower Dienst gewidmet ist. Dies wird in der Regel auch als AWS Zahlerkonto oder AWS Organizations Verwaltungskonto bezeichnet.
- Das AFT-Verwaltungskonto AWS-Konto ist für AFT-Verwaltungsvorgänge vorgesehen. Dies unterscheidet sich vom Verwaltungskonto Ihrer Organisation.
- Ein Verkäuferkonto ist ein Konto AWS-Konto , das alle von Ihnen ausgewählten Basiskomponenten und Steuerelemente enthält. AFT wird verwendet AWS Control Tower , um ein neues Konto zu verkaufen.

Weitere Informationen zu dieser Architektur finden Sie im AWS Control Tower Workshop unter Einführung in AFT.

Tools

AWS-Services

- AWS Control Towerhilft Ihnen bei der Einrichtung und Verwaltung einer Umgebung AWS mit mehreren Konten und folgt dabei den vorgeschriebenen Best Practices.
- AWS Account Factory for Terraform (AFT) richtet eine Terraform-Pipeline ein, mit der Sie Konten und Ressourcen bereitstellen und anpassen können. AWS Control Tower
- AWS Organizationshilft Ihnen dabei, Ihre Umgebung zentral zu verwalten und zu steuern, während Sie Ihre Ressourcen erweitern und skalieren. AWS Mithilfe von Organizations können Sie Konten erstellen und Ressourcen zuweisen, Konten gruppieren, um Ihre Workflows zu organisieren, Richtlinien für die Unternehmensführung anwenden und die Abrechnung vereinfachen, indem Sie eine einzige Zahlungsmethode für alle Ihre Konten verwenden.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem es kontrolliert, wer authentifiziert und zu deren Nutzung autorisiert ist. Für dieses Muster sind IAM-Rollen und -Berechtigungen erforderlich.

Andere Tools

- Terraform ist ein IaC-Tool (Infrastructure as Code) HashiCorp , mit dem Sie Cloud- und lokale Ressourcen erstellen und verwalten können.

Bewährte Methoden

- Weitere AWS Control Tower Informationen finden Sie in der Dokumentation unter Bewährte Methoden für AWS Control Tower Administratoren. AWS Control Tower
- Informationen zu IAM finden Sie in der IAM-Dokumentation unter Bewährte Sicherheitsmethoden.

Epen

Löschen Sie AFT-Ressourcen im AFT-Management-Konto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie Ressourcen, die durch das AFT-Tag identifiziert werden.	1. Melden Sie sich mit Administratorrechten beim AFT-Verwaltungskonto an. 2. Öffnen Sie die AWS Resource Groups -Konsole.	AWS-Administrator, AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie die Region aus, in der der Einsatz durchgeführt AWS Control Tower wurde. 4. Wählen Sie im Navigationsbereich Tag Editor aus. 5. Wählen Sie für Ressourcentypen die Option Alle unterstützten Ressourcentypen aus. 6. Geben Sie für Tags managed_by als Tag-Schlüssel und AFT als Tag-Wert ein. 7. Wählen Sie Ressourcen durchsuchen aus. Bei dieser Suche werden alle Ressourcen angezeigt, die von AFT erstellt wurden. 8. Identifizieren Sie die Ressourcennamen und löschen Sie sie mithilfe der entsprechenden Servicekonsolen. Um beispielsweise Parameter Store-Ressourcen zu löschen: a. Öffnen Sie die AWS Systems Manager - Konsole. b. Wählen Sie im Navigationsbereich Parameter Store (Parameterspeicher) aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	c. Klicken Sie im Suchfeld, um die Dropdownliste anzuzeigen, wählen Sie Name, wählen Sie ist gleich und geben Sie dann /aft ein. d. Löschen Sie die Parameter in Stapeln von 10 Stück. (Dies ist die maximale Anzahl, die Sie gleichzeitig löschen können.) Für AFT Version 1.12.2 müssen ungefähr 62 Parameter Store-Ressourcen gelöscht werden. Alle Parameter namen beginnen mit /aft. Es können jedoch nicht alle Ressourcen durch AWS Resource Groups identifiziert werden. In den folgenden Schritten werden Sie die verbleibe nden Ressourcen finden und löschen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie IAM-Rollen.	1. Melden Sie sich mit Administratorrechten beim AFT-Verwaltungskonto an. 2. Öffnen Sie die IAM-Konsole. 3. Löschen Sie diese Rollen in der angegebenen Reihenfolge (die Reihenfolge ist aufgrund der Abhängigkeiten wichtig): • `aft-*` • `AWSAFTAdmin` • `AWSAFTExecution` • `AWSAFTService` • `codebuild_trigger_role`	AWS-Administrator, AWS DevOps, DevOps Ingenieur
Löschen Sie den AWS Backup Backup-Tresor.	1. Öffnen Sie die AWS Backup-Konsole. 2. Suchen Sie den Backup-Tresor mit dem Namen `aws_backup_vault` . 3. Vergewissern Sie sich, dass der Tresor keine aktiven Backups enthält. 4. Löschen `aws_backup_vault` .	AWS-Administrator, AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie CloudWatch Amazon-Ressourcen.	1. Öffnen Sie die CloudWatch -Konsole. 2. Löschen Sie die folgenden Ressourcen in der angegebenen Reihenfolge: a. Event-Bus: Löschen`aws_cloudwatch_event_bus` . b. Protokolle: Suchen Sie nach dem Präfix AFT und löschen Sie alle zugehörigen Protokollgruppen. c. Abfragedefinitionen: Löschen Sie die folgenden Abfragen: • `Customization Logs by Account ID` • `Customization Logs by Customization Request ID`	AWS-Administrator, AWS DevOps, DevOps Ingenieur
AWS KMS Ressourcen löschen.	1. Wechseln Sie zur sekundären Region, die als Backend für die Statusverfolgung des eigenen Zustands von AFT dient. 2. Öffnen Sie die AWS KMS -Konsole. 3. Löschen Sie den Alias AFT.	AWS-Administrator, AWS DevOps, DevOps Ingenieur

Löschen Sie AFT-Ressourcen im Log Archive-Konto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie S3-Buckets.	1. Melden Sie sich mit Administratorrechten beim Log Archive-Konto an. 2. Öffnen Sie die Amazon S3-Konsole. 3. Leeren Sie die folgenden Buckets: • `aws-aft-logs-471112509802-us-east-1` • `aws-aft-s3-access-logs-471112509802-us-east-1` (Ersetzen Sie es `111122223333` durch Ihre Konto-ID.) 4. Löschen Sie die beiden Buckets.	AWS-Administrator, AWS DevOps, DevOps Ingenieur
Löschen Sie IAM-Rollen.	1. Öffnen Sie die IAM-Konsole. 2. Stellen Sie sicher, dass die folgenden Rollen von keinem aktiven Dienst verwendet werden: • `AWSAFTService` • `AWSAFTExecution` 3. Löschen Sie die beiden Rollen.	AWS-Administrator, AWS DevOps, DevOps Ingenieur

Löschen Sie AFT-Ressourcen im Audit-Konto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie IAM-Rollen.	1. Melden Sie sich mit Administratorrechten beim Audit-Konto an. 2. Öffnen Sie die IAM-Konsole. 3. Stellen Sie sicher, dass die folgenden Rollen von keinem aktiven Dienst verwendet werden: • `AWSAFTService` • `AWSAFTExecution` 4. Löschen Sie die beiden Rollen.	AWS-Administrator, AWS DevOps, DevOps Ingenieur

Löschen Sie AFT-Ressourcen im AWS Control Tower Verwaltungskonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie IAM-Rollen.	1. Melden Sie sich mit Administratorrechten beim AWS Control Tower Verwaltungskonto an. 2. Öffnen Sie die IAM-Konsole. 3. Stellen Sie sicher, dass die folgenden Rollen von keinem aktiven Dienst verwendet werden: • `AWSAFTService` • `AWSAFTExecution`	AWS-Administrator, AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `aft-control-tower-events-rule` 4. Löschen Sie die drei Rollen.	
EventBridge Regeln löschen.	1. Öffnen Sie die EventBridge Amazon-Konsole. 2. Wählen Sie im linken Navigationsbereich Rules (Regeln) aus. 3. Suchen Sie die genannte Regel und wählen Sie sie aus`aft-capture-ct-events` . 4. Wählen Sie Löschen und bestätigen Sie den Löschvorgang, wenn Sie dazu aufgefordert werden.	AWS-Administrator, AWS DevOps, DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Das Trennen des Internet-Gateways war nicht erfolgreich.	Wenn Sie Ressourcen löschen, die durch das AFT-Tag identifiziert wurden, und dieses Problem beim Trennen oder Löschen des Internet-Gateways auftritt, müssen Sie zuerst VPC-Endpunkte löschen: 1. Melden Sie sich beim AFT-Management-Konto an und öffnen Sie dann die Amazon VPC-Konsole.

Problem	Lösung
	2. Wählen Sie im Navigationsbereich in der Liste Nach VPC filtern die benannte VPC aus. aft-management-vpc 3. Wählen Sie im Navigationsbereich Endpunkte aus. 4. Wählen Sie die Endpoints aus, die der aft-management-vpcVPC zugeordnet sind. • Überprüfen Sie vor dem Löschen noch einmal die VPC-ID-Spalte, um zu vermeiden, dass die falschen Endpoints entfernt werden. • Achten Sie darauf, nur die Endpoints zu löschen, die der AFT-VPC zugeordnet sind. 5. Wählen Sie Actions (Aktionen), Delete VPC Endpoint (VPC-Endpunkte löschen). 6. Geben Sie im Bestätigungsdialogfeld Löschen ein und wählen Sie dann Löschen aus. 7. Warten Sie, bis sich der Endpunktstatus auf Gelöscht ändert. Der Löschvorgang kann einige Minuten dauern.

Problem	Lösung
Sie können die angegebenen CloudWatch Abfragen nicht finden.	Wenn Sie die von AFT erstellten CloudWatch Abfragen nicht finden können, gehen Sie wie folgt vor: 1. Melden Sie sich beim AFT-Management-Konto an und öffnen Sie dann die CloudWatch Konsole. 2. Wählen Sie im Navigationsbereich unter Logs die Option Logs Insights aus. 3. Wählen Sie in der oberen rechten Ecke das Symbol Gespeicherte Abfragen und Beispielabfragen aus. Sie sollten jetzt AFT-Abfragen sehen können. Einen Screenshot finden Sie im Abschnitt Zusätzliche Informationen. 4. Wählen Sie die folgenden Abfragen aus und wählen Sie dann Aktionen, Löschen, um sie zu entfernen. • `Customization Logs by Account ID` • `Customization Logs by Customization Request ID`

Zugehörige Ressourcen

- HINTEN:
  - GitHub Repository
  - Werkstatt
  - Dokumentation
- AWS Control Tower Dokumentation

Zusätzliche Informationen

Um AFT-Abfragen im CloudWatch Logs Insights-Dashboard anzuzeigen, wählen Sie in der oberen rechten Ecke das Symbol Gespeicherte Abfragen und Beispielabfragen aus, wie im folgenden Screenshot dargestellt:

Stellen Sie mithilfe von Session Manager eine Connect zu einer EC2 Amazon-Instance her

Erstellt von Jason Cornick (AWS), Abhishek Bastikoppa (AWS) und Yaniv Ron (AWS)

Übersicht

Dieses Muster beschreibt, wie Sie mithilfe des Session Managers, einer Funktion von AWS Systems Manager, eine Verbindung zu einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance herstellen. Mithilfe dieses Musters können Sie Bash-Befehle auf einer EC2 Instance über einen Webbrowser ausführen. Session Manager erfordert nicht, dass Sie eingehende Ports öffnen, und es sind keine öffentlichen IP-Adressen für EC2 Instanzen erforderlich. Darüber hinaus entfällt die Notwendigkeit, Bastion-Hosts mit unterschiedlichen Secure Shell (SSH) -Schlüsseln zu verwalten. Sie können den Zugriff auf Session Manager mit AWS Identity and Access Management (IAM) -Richtlinien steuern und die Protokollierung konfigurieren, in der wichtige Informationen wie Instance-Zugriff und Aktionen aufgezeichnet werden.

In diesem Muster konfigurieren Sie eine IAM-Rolle und ordnen sie einer EC2 Linux-Instance zu, die Sie mithilfe eines Amazon Machine Image (AMI) bereitstellen. Anschließend konfigurieren Sie die Protokollierung in Amazon CloudWatch Logs und verwenden Session Manager, um eine Sitzung mit der Instance zu starten.

Dieses Muster stellt zwar eine Verbindung zu einer EC2 Linux-Instance in der Amazon Web Services (AWS) -Cloud her, aber Sie könnten diesen Ansatz verwenden, um Session Manager für Verbindungen mit anderen Servern wie lokalen Servern oder anderen virtuellen Maschinen zu verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Berechtigungen für den Zugriff auf den verwalteten Knoten. Anweisungen finden Sie unter Steuern des Zugriffs von Benutzersitzungen auf verwaltete Knoten.
- VPC-Endpunkte für`ssm`,, `ec2` `ec2messages`ss`smmessages`, und. `s3` Anweisungen finden Sie in der Systems Manager Manager-Dokumentation unter VPC-Endpoints erstellen.

Architektur

Zieltechnologie-Stack

- Session Manager
- Amazon EC2
- CloudWatch Logs

Zielarchitektur

1. Der Benutzer authentifiziert seine Identität und seine Anmeldeinformationen über IAM.
2. Der Benutzer initiiert eine SSH-Sitzung über den Sitzungsmanager und sendet API-Aufrufe an die Instanz. EC2
3. Der AWS Systems Manager SSM Agent, der auf der EC2 Instance installiert ist, stellt eine Verbindung mit Session Manager her und führt die Befehle aus.
4. Zu Prüf- und Überwachungszwecken sendet Session Manager die Protokolldaten an CloudWatch Logs. Alternativ können Sie Protokolldaten an einen Amazon Simple Storage Service (Amazon S3) -Bucket senden. Weitere Informationen finden Sie unter Protokollieren von Sitzungsdaten mit Amazon S3 (Systems Manager Manager-Dokumentation).

Tools

AWS-Services

- Amazon CloudWatch Logs hilft Ihnen dabei, die Protokolle all Ihrer Systeme, Anwendungen und AWS-Services zu zentralisieren, sodass Sie sie überwachen und sicher archivieren können.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren. Dieses Muster verwendet ein Amazon Machine Image (AMI) zur Bereitstellung einer EC2 Linux-Instance.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Systems Manager unterstützt Sie bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der AWS-Cloud ausgeführt werden. Es vereinfacht das Anwendungs- und

Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme und hilft Ihnen, Ihre AWS-Ressourcen sicher und skalierbar zu verwalten. Dieses Muster verwendet Session Manager, eine Funktion von Systems Manager.

Bewährte Methoden

Wir empfehlen Ihnen, mehr über die Sicherheitssäule des AWS Well-Architected Framework zu lesen und die Verschlüsselungsoptionen zu erkunden und die Sicherheitsempfehlungen unter Setting up Session Manager (Systems Manager Manager-Dokumentation) anzuwenden.

Epen

Richten Sie die Infrastruktur ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Rolle.	Erstellen Sie die IAM-Rolle für den SSM-Agenten. Folgen Sie den Anweisungen unter Eine Rolle für einen AWS-Service erstellen (IAM-Dokumentation) und beachten Sie Folgendes: 1. Wählen Sie für den AWS-Service EC2. 2. Wählen Sie für Richtlinien für Berechtigungen die Option `AmazonSSMManagedInstanceCore` . 3. Geben Sie im Feld Rollenname den Wert ein `EC2_SSM_Role` .	AWS-Systemadministrator
Erstellen Sie die EC2 Instanz.	1. Erstellen Sie die EC2 Instanz. Folgen Sie den Anweisungen unter Launch an Instance (EC2 Amazon-	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dokumentation) und beachten Sie Folgendes: a. Wählen Sie im Abschnitt Name und Tags die Option Zusätzliche Tags hinzufügen aus. Geben Sie unter Key (Schlüssel) „`Name`“ ein, und geben Sie in Value (Wert) „`Productio n_Server_One` “ ein. b. Wählen Sie ein Amazon Linux AMI aus, auf dem der SSM-Agent vorinstal liert ist. Eine vollständ ige Liste finden Sie unter AMIsMit vorinstalliertem SSM-Agent (Systems Manager Manager-D okumentation). c. Wählen Sie im Abschnitt Erweiterte Details im IAM-Instanzprofil die Option _SSM_Role aus. EC2 2. Öffnen Sie die Systems Manager Manager-Konsole unter https://console.a ws.amazon.com/systems-manager/. 3. Wählen Sie im Navigatio nsbereich Fleet Manager aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Stellen Sie sicher, dass die Instanz in der Liste der verwalteten Knoten erscheint.	
Richten Sie die Protokollierung ein.	1. Erstellen Sie eine Protokollgruppe in CloudWatch Logs. Folgen Sie den Anweisungen unter Protokollgruppe erstellen (Dokumentation zu CloudWatch Protokollen). Geben Sie der neuen Protokollgruppe einen Namen `SessionManager`. 2. Konfigurieren Sie die Protokollierung für Session Manager. Folgen Sie den Anweisungen unter Sitzungsdaten mithilfe von Amazon CloudWatch Logs protokollieren (Systems Manager Manager-Dokumentation) und beachten Sie Folgendes: a. Wählen Sie nicht Nur verschlüsselte CloudWatch Protokollgruppen zulassen aus. b. Wählen Sie unter Wählen Sie eine Protokollgruppe aus der Liste die Option aus SessionManager.	AWS-Systemadministrator

Eine Verbindung zur Instance herstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Connect zur EC2 Instanz her.	1. Starten Sie eine Sitzung in der Systems Manager Manager-Konsole. Anweisungen finden Sie unter Starten einer Sitzung (Systems Manager Manager-Dokumentation). Wählen Sie für Target-In stanzen das Optionsfeld links neben der Productio n_Server_One-Instanz. 2. Nachdem die Verbindung hergestellt wurde, führen Sie mehrere Bash-Befehle aus. 3. Beenden Sie die Sitzung in der Systems Manager Manager-Konsole. Anweisungen finden Sie unter Sitzung beenden (Systems Manager Manager-Dokumentation).	AWS-Systemadministrator
Überprüfen Sie die Protokoll ierung.	1. Öffnen Sie unter CloudWatc h Logs den Log-Stream für die Protokollgruppe. Anweisungen finden Sie unter Protokolldaten anzeigen (CloudWatch Protokolldokumentation). 2. Vergewissern Sie sich, dass die Befehle, die Sie in	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der vorherigen Geschicht e ausgeführt haben, in den Protokolldaten aufgeführt sind.	

Fehlerbehebung

Problem	Lösung
IAM-Probleme	Support finden Sie unter Problembehandlung (IAM-Dokumentation).

Zugehörige Ressourcen

- Vollständige Voraussetzungen für Session Manager (Systems Manager Manager-Dokumentation)
- Entwerfen und Implementieren von Protokollierung und Überwachung mit Amazon CloudWatch (AWS Prescriptive Guidance)

Erstellen Sie eine Pipeline in AWS-Regionen, die AWS nicht unterstützen CodePipeline

Erstellt von Anand Krishna Varanasi (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

AWS CodePipeline ist ein Orchestrierungsservice für Continuous Delivery (CD), der Teil einer Reihe von DevOps Tools von Amazon Web Services (AWS) ist. Es lässt sich in eine Vielzahl von Quellen (wie Versionskontrollsysteme und Speicherlösungen), Produkte und Services für kontinuierliche Integration (CI) von AWS und AWS-Partnern sowie Open-Source-Produkte integrieren, um einen end-to-end Workflow-Service für schnelle Anwendungs- und Infrastrukturbereitstellungen bereitzustellen.

Wird jedoch CodePipeline nicht in allen AWS-Regionen unterstützt, und es ist nützlich, einen unsichtbaren Orchestrator zu haben, der CI/CD services. This pattern describes how to implement an end-to-end workflow pipeline in AWS Regions where CodePipeline isn’t yet supported by using AWS CI/CD AWS-Services wie AWS CodeCommit CodeBuild, AWS und AWS CodeDeploy verbindet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS Cloud Development Kit (AWS CDK) CLI Version 2.28 oder höher

Architektur

Zieltechnologie-Stack

Das folgende Diagramm zeigt eine Pipeline, die in einer Region erstellt wurde, die nicht unterstützt wird CodePipeline, z. B. in der Region Afrika (Kapstadt). Ein Entwickler überträgt die CodeDeploy Konfigurationsdateien (auch als Deployment-Lifecycle-Hook-Skripte bezeichnet) in das Git-Repository, das von CodeCommit gehostet wird. (Sehen Sie sich das GitHub Repository an, das mit diesem Muster bereitgestellt wird.) Eine EventBridge Amazon-Regel wird automatisch initiiert. CodeBuild

Die CodeDeploy Konfigurationsdateien werden CodeCommit als Teil der Quellphase der Pipeline abgerufen und an diese übertragen. CodeBuild

CodeBuild Führt in der nächsten Phase die folgenden Aufgaben aus:

1. Lädt die TAR-Datei mit dem Quellcode der Anwendung herunter. Sie können den Namen dieser Datei mithilfe von Parameter Store, einer Funktion von AWS Systems Manager, konfigurieren.
2. Lädt die CodeDeploy Konfigurationsdateien herunter.
3. Erstellt ein kombiniertes Archiv aus Anwendungsquellcode und CodeDeploy Konfigurationsdateien, die für den Anwendungstyp spezifisch sind.
4. Initiiert die CodeDeploy Bereitstellung auf einer Amazon Elastic Compute Cloud (Amazon EC2) - Instance mithilfe des kombinierten Archivs.

Tools

AWS-Services

- AWS CodeBuild ist ein vollständig verwalteter Build-Service, mit dem Sie Quellcode kompilieren, Komponententests ausführen und bereitstellungsbereite Artefakte erstellen können.
- AWS CodeCommit ist ein Versionskontrollservice, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodeDeploy automatisiert Bereitstellungen auf Amazon EC2 - oder lokalen Instances, AWS Lambda Lambda-Funktionen oder Amazon Elastic Container Service (Amazon ECS) -Services.
- AWS CodePipeline hilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.
- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.

Code

Der Code für dieses Muster ist im Repository „ GitHub CodePipeline Nicht unterstützte Regionen“ verfügbar.

Epen

Richten Sie Ihre Entwickler-Workstation ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die AWS CDK CLI.	Anweisungen finden Sie in der AWS-CDK-Dokumentation.	AWS DevOps
Installieren Sie einen Git-Client.	Um Commits zu erstellen, kannst du einen Git-Client verwenden, der auf deinem lokalen Computer installiert ist, und deine Commits dann in das CodeCommit Repository übertragen. Informationen zur Einrichtung CodeCommit mit deinem Git-Client findest du in der CodeCommit Dokumentation.	AWS DevOps
Installieren Sie "npm".	Installieren Sie den npm-Paketmanager. Weitere Informationen finden Sie in der npm-Dokumentation.	AWS DevOps

Richten Sie die Pipeline ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Code-Repository.	Klonen Sie das Repository „ GitHub CodePipeline Nicht unterstützte Regionen“ auf Ihren lokalen Computer, indem Sie den folgenden Befehl ausführen.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`git clone https://github.com/aws-samples/invisible-codepipeline-unsupported-regions`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Parameter in cdk.json ein.	Öffnen Sie die `cdk.json` Datei und geben Sie Werte für die folgenden Parameter an: `"pipeline_account" :"XXXXXXXXXXXX", "pipeline_region":" us-west-2", "repo_name": "app-dev- repo", "ec2_tag_key": "test- vm", "configName" : "cbdeployconfig", "deploymentGroupNa me": "cbdeploygroup", "applicationName" : "cbdeployapplicati on", "projectName" : "CodeBuildProject"` Wobei: • `pipeline_account` ist das AWS-Konto, auf dem die Pipeline erstellt wird. • `pipeline_region` ist die AWS-Region, in der die Pipeline gebaut wird. • `repo_name` ist der Name des CodeCommit Repositor ys. • `ec2_tag_key` ist das Tag, das an die EC2 Instanz angehängt ist, für die Sie	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den Code bereitstellen möchten. • `configName` ist der Name der CodeDeploy Konfigura tionsdatei. • `deploymentGroupNam e` ist der Name der CodeDeploy Bereitste llungsgruppe. • `applicationName` ist der Name der CodeDeploy Anwendung. • `projectName` ist der CodeBuild Projektname.	

Richten Sie die AWS-CDK-K onstruktbibliothek ein.	Verwenden Sie im geklonten GitHub Repository die folgenden Befehle, um die AWS-CDK-Konstruktionsbiblio thek zu installieren, Ihre Anwendung zu erstellen und zu synthetisieren, um die CloudFormation AWS-Vorla ge für die Anwendung zu generieren.
	`npm i aws-cdk-lib`
	`npm run build`
	`cdk synth`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die AWS-CDK-B eispielanwendung bereit.	Stellen Sie den Code bereit, indem Sie den folgenden Befehl in einer Region ausführen, die nicht unterstützt wird (z. B.`af-south-1`). `cdk deploy`	AWS DevOps

Richten Sie das CodeCommit Repository ein für CodeDeploy

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie CI/CD für die Anwendung ein.	Klonen Sie das CodeCommi t Repository, das Sie in der `cdk.json` Datei angegeben haben (dies wird `app-dev-repo` standardmäßig aufgerufen), um die CI/CD-Pipeline für die Anwendung einzurichten. `git clone https://g it-codecommit.us-w est-2.amazonaws.com/ v1/repos/app-dev-repo` wobei der Repository-Name und die Region von den Werten abhängen, die Sie in der `cdk.json` Datei angegeben haben.	AWS DevOps

Testen Sie die Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Pipeline anhand von Bereitste llungsanweisungen.	Der `CodeDeploy_Files` Ordner des Repositorys „ GitHub CodePipeline Nicht unterstützte Regionen“ enthält Beispieldateien mit Anweisungen CodeDeplo y zur Bereitstellung der Anwendung. Die `appspec.y ml` Datei ist eine CodeDeplo y Konfigurationsdatei, die Hooks zur Steuerung des Ablaufs der Anwendung sbereitstellung enthält. Sie können die Beispield ateien`index.html` ,, und verwenden `start_ser ver.sh stop_server.sh` , um eine Website `install_d ependencies.sh` zu aktualisieren, die auf Apache gehostet wird. Dies sind Beispiele — Sie können den Code im GitHub Repositor y verwenden, um jede Art von Anwendung bereitzus tellen. Wenn die Dateien in das CodeCommit Repositor y übertragen werden, wird die unsichtbare Pipeline automatisch initiiert. Die Ergebnisse der Bereitstellung finden Sie in den Ergebniss en der einzelnen Phasen in	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den CodeDeploy Konsolen CodeBuild und.	

Zugehörige Ressourcen

- Erste Schritte (AWS CDK-Dokumentation)
- Einführung in das Cloud Development Kit (CDK) (AWS Workshop Studio)
- AWS-CDK-Workshop

Passen Sie Standardrollennamen mithilfe von AWS CDK Aspekten und Escape-Schraffuren an

Erstellt von SANDEEP SINGH (AWS) und James Jacob (AWS)

Übersicht

Dieses Muster zeigt, wie Sie die Standardnamen von Rollen anpassen können, die durch AWS Cloud Development Kit (AWS CDK) Konstrukte erstellt werden. Das Anpassen von Rollennamen ist häufig erforderlich, wenn in Ihrer Organisation bestimmte Einschränkungen gelten, die auf Namenskonventionen basieren. Beispielsweise kann Ihre Organisation AWS Identity and Access Management (IAM) Berechtigungsgrenzen oder Dienststeuerungsrichtlinien (SCPs) festlegen, die ein bestimmtes Präfix in Rollennamen erfordern. In solchen Fällen entsprechen die durch AWS CDK Konstrukte generierten Standardrollennamen möglicherweise nicht diesen Konventionen und müssen möglicherweise geändert werden. Dieses Muster erfüllt diese Anforderungen durch die Verwendung von Notluken und Aspekten in der. AWS CDK Sie verwenden Schraffuren, um benutzerdefinierte Rollennamen zu definieren, und Aspekte, um allen Rollen einen benutzerdefinierten Namen zuzuweisen, um sicherzustellen, dass die Richtlinien und Einschränkungen Ihrer Organisation eingehalten werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- In der AWS CDK Dokumentation angegebene Voraussetzungen

Einschränkungen

- Aspekte filtern Ressourcen nach Ressourcentypen, sodass alle Rollen dasselbe Präfix verwenden. Wenn Sie unterschiedliche Rollenpräfixe für verschiedene Rollen benötigen, ist eine zusätzliche Filterung auf der Grundlage anderer Eigenschaften erforderlich. Um beispielsweise Rollen, die mit AWS Lambda Funktionen verknüpft sind, unterschiedliche Präfixe zuzuweisen, könnten Sie nach bestimmten Rollenattributen oder Tags filtern und ein Präfix für Lambda-bezogene Rollen und ein anderes Präfix für andere Rollen anwenden.
- IAM-Rollennamen haben eine maximale Länge von 64 Zeichen. Daher müssen modifizierte Rollennamen gekürzt werden, um diese Einschränkung zu erfüllen.

- Einige AWS-Services sind nicht in allen verfügbar. AWS-Regionen Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie auf der Seite Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Architektur

Zieltechnologie-Stack

- AWS CDK
- AWS CloudFormation

Zielarchitektur

- Eine AWS CDK App besteht aus einem oder mehreren AWS CloudFormation Stacks, die synthetisiert und zur Verwaltung von Ressourcen bereitgestellt werden. AWS
- Um eine Eigenschaft einer AWS CDK verwalteten Ressource zu ändern, die nicht durch ein Layer-2-Konstrukt (L2) offengelegt wird, verwenden Sie eine Escape-Hatch, um die zugrunde liegenden CloudFormation Eigenschaften (in diesem Fall den Rollennamen) zu überschreiben, und einen Aspekt, um die Rolle während der Stack-Synthese auf alle Ressourcen in der AWS CDK App anzuwenden. AWS CDK

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK)ist ein Softwareentwicklungs-Framework, das Ihnen hilft, AWS Cloud Infrastruktur im Code zu definieren und bereitzustellen.
- AWS CDK Die Befehlszeilenschnittstelle (AWS CDK CLI) (auch als AWS CDK Toolkit bezeichnet) ist ein Befehlszeilen-Cloud-Entwicklungskit, mit dem Sie mit Ihrer AWS CDK App interagieren können. Der `cdk` CLI-Befehl ist das wichtigste Tool für die Interaktion mit Ihrer AWS CDK App. Er führt Ihre App aus, fragt das von Ihnen definierte Anwendungsmodell ab und erstellt und stellt die CloudFormation Vorlagen bereit, die von der generiert werden. AWS CDK

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend AWS-Konten zu verwalten.

Code-Repository

Der Quellcode und die Vorlagen für dieses Muster sind im GitHub CDK Aspects Override-Repository verfügbar.

Bewährte Methoden

Weitere Informationen finden Sie auf der Website AWS Prescriptive Guidance unter Bewährte Methoden für die Verwendung von AWS CDK in TypeScript zur Erstellung von IaC-Projekten.

Epen

Installieren Sie die AWS CDK CLI

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die AWS CDK CLI.	Führen Sie den folgenden Befehl aus, um die AWS CDK CLI global zu installieren: `npm install -g aws-cdk`	AWS DevOps
Überprüfen Sie die Version.	Führen Sie den Befehl aus: `cdk --version` Vergewissern Sie sich, dass Sie Version 2 der AWS CDK CLI verwenden.	AWS DevOps
Bootstrapping für die AWS CDK Umgebung.	Bevor Sie die AWS CloudFormation Vorlagen bereitstellen, bereiten Sie das Konto vor AWS-Region ,	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	das Sie verwenden möchten. Führen Sie den Befehl aus: `cdk bootstrap <account>/<Region>` Weitere Informationen finden Sie in der AWS CDK Dokumentation unter Bootstrapping. AWS	

Stellen Sie die AWS CDK App bereit, um die Verwendung von Aspekten zu demonstrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie das Projekt ein.	1. Klonen Sie das GitHub Repository für dieses Muster auf Ihren lokalen Computer:
	`git clone https://github.com/aws-samples/cdk-aspects-override`
	2. Navigieren Sie zum Projektverzeichnis auf Ihrem lokalen Computer.
	3. Installieren Sie die Projektabhängigkeiten:
	`npm ci`
		AWS DevOps

Stellen Sie Stacks mit Standardrollennamen bereit,	Stellen Sie zwei CloudFormation Stacks (`ExampleSt`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
die AWS CDK von der zugewiesen wurden.	`ack1` und `ExampleStack2`) bereit, die die Lambda-Fu nktionen und die zugehörigen Rollen enthalten: `npm run deploy:Ex ampleAppWithoutAsp ects` Der Code übergibt Rolleneig enschaften nicht explizit, sodass die Rollennamen von erstellt werden. AWS CDK Ein Beispiel für die Ausgabe finden Sie im Abschnitt Zusätzliche Informationen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie Stacks mit Aspekten bereit.	In diesem Schritt wenden Sie einen Aspekt an, der eine Konvention für Rollennam en erzwingt, indem Sie allen IAM-Rollen, die im Projekt bereitgestellt werden, ein Präfix hinzufügen. AWS CDK Der Aspekt ist in der `lib/ aspects.ts` Datei definiert . Der Aspekt verwendet eine Escape-Schraffur, um den Rollennamen durch Hinzufüge n eines Präfixes zu überschre iben. Der Aspekt wird auf die Stapel in der `bin/app-w ith-aspects.ts` Datei angewendet. Das in diesem Beispiel verwendete Präfix für den Rollennamen lautet`dev- unicorn` .
	
	1. Bearbeiten Sie die `bin/ app-with-aspec ts.ts` -Datei.
	2. Aktualisieren Sie in der Datei die Variable `ROLE_NAME_PREFIX` mit dem Präfix`dev-unicorn` :
	
	`const app = new cdk.App();`
	
	`// Define a prefix for the role names`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>const ROLE_NAME
	_PREFIX = 'dev-unic
	orn';
	
	// Instantiate the
	 RoleNamingConventi
	onAspect with the
	 desired prefix
	const roleNamin
	gConventionAspect
	 = new RoleNamin
	gConventionAspect(
	ROLE_NAME_PREFIX);</pre>
	3. Stellen Sie die AWS CDK App mit folgenden Aspekten bereit:
	<pre>npm run deploy:Ex
	ampleAppWithAspects</pre>
	Ein Beispiel für die Ausgabe finden Sie im Abschnitt Zusätzliche Informationen.	

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Lösche deine AWS CloudFormation Stapel.	Wenn Sie dieses Muster nicht mehr verwenden, führen Sie den folgenden Befehl aus, um Ressourcen zu bereinige n und zusätzliche Kosten zu vermeiden:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cdk destroy --all -f && cdk --app npx ts-node bin/app-with-aspects.ts' destroy --all -f`	

Fehlerbehebung

Problem	Lösung
Sie stoßen auf Probleme mit der AWS CDK.	Weitere Informationen finden Sie in der AWS CDK Dokumentation unter Behebung häufig auftretender AWS CDK Probleme.

Zugehörige Ressourcen

- AWS Cloud Development Kit (AWS CDK)
- AWS CDK Dokumentation
- AWS CDK auf GitHub
- Fluchtluken
- Aspekte und die AWS CDK

Zusätzliche Informationen

Rollennamen, die von AWS CloudFormation Without Aspects erstellt wurden

```
Outputs:
ExampleStack1WithoutAspects.Function1RoleName = example-stack1-without-as-
Function1LambdaFunctionSe-y7FYTY6FXJXA
ExampleStack1WithoutAspects.Function2RoleName = example-stack1-without-as-
Function2LambdaFunctionSe-dDZV4rkWqWnI
...

Outputs:
```

```
ExampleStack2WithoutAspects.Function3RoleName = example-stack2-without-as-
Function3LambdaFunctionSe-ygMv49iTyMq0
```

Rollennamen, die von AWS CloudFormation with aspects erstellt wurden

```
Outputs:
ExampleStack1WithAspects.Function1RoleName = dev-unicorn-
Function1LambdaFunctionServiceRole783660DC
ExampleStack1WithAspects.Function2RoleName = dev-unicorn-
Function2LambdaFunctionServiceRole2C391181
...

Outputs:
ExampleStack2WithAspects.Function3RoleName = dev-unicorn-
Function3LambdaFunctionServiceRole4CAA721C
```

Stellen Sie einen Cassandra-Cluster auf Amazon EC2 mit Private Static bereit, um ein IPs Rebalancing zu vermeiden

Erstellt von Dipin Jain (AWS)

Übersicht

Die private IP einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance wird während ihres gesamten Lebenszyklus beibehalten. Die private IP kann sich jedoch während eines geplanten oder ungeplanten Systemabsturzes ändern, z. B. während eines Amazon Machine Image (AMI) -Upgrades. In einigen Szenarien kann die Beibehaltung einer privaten statischen IP die Leistung und die Wiederherstellungszeit von Workloads verbessern. Durch die Verwendung einer statischen IP für einen Apache Cassandra-Seed-Node wird beispielsweise verhindert, dass für den Cluster ein Overhead beim Rebalancing anfällt.

Dieses Muster beschreibt, wie eine sekundäre elastic network interface an EC2 Instances angehängt wird, um die IP während des Rehostings statisch zu halten. Das Muster konzentriert sich auf Cassandra-Cluster, aber Sie können diese Implementierung für jede Architektur verwenden, die von Private Static profitiert. IPs

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Service (AWS) -Konto

Produktversionen

- DataStax Version 5.11.1
- Betriebssystem: Ubuntu 16.04.6 LTS

Architektur

Quellarchitektur

Die Quelle könnte ein Cassandra-Cluster auf einer lokalen virtuellen Maschine (VM) oder auf EC2 Instanzen in der AWS-Cloud sein. Das folgende Diagramm veranschaulicht das zweite Szenario. Dieses Beispiel umfasst vier Clusterknoten: drei Seed-Knoten und einen Management-Knoten. In der Quellarchitektur ist an jeden Knoten eine einzige Netzwerkschnittstelle angeschlossen.

Zielarchitektur

Der Zielcluster wird auf EC2 Instances gehostet, an die an jeden Knoten eine sekundäre elastic network interface angeschlossen ist, wie in der folgenden Abbildung dargestellt.

Automatisierung und Skalierung

Sie können auch das Anhängen einer zweiten elastic network interface an eine EC2 Auto Scaling Scaling-Gruppe automatisieren, wie in einem AWS Knowledge Center-Video beschrieben.

Epen

Einen Cassandra-Cluster bei Amazon konfigurieren EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie EC2 Knoten, um einen Cassandra-Cluster zu hosten.	Starten Sie auf der EC2 Amazon-Konsole vier EC2 Instances für Ihre Ubuntu-Knoten in Ihrem AWS-Konto. Drei (Seed-) Knoten werden für den Cassandra-Cluster verwendet, und der vierte Knoten fungiert als Cluster-Management-Knoten, auf dem Sie DataStax Enterprise (DSE) OpsCenter installieren. Anweisungen finden Sie in der EC2 Amazon-Dokumentation.	Cloud-Ingenieur
Bestätigen Sie die Knotenkommunikation.	Stellen Sie sicher, dass die vier Knoten über die Datenbank- und Clustermanagement-Ports miteinander kommunizieren können.	Netzwerkingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie DSE OpsCenter auf dem Verwaltungsknoten.	Installieren Sie DSE OpsCenter 6.1 aus dem Debian-Paket auf dem Management-Knoten. Anweisungen finden Sie in der DataStax Dokumentation.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine sekundäre Netzwerkschnittstelle.	Cassandra generiert einen Universal Unique Identifier (UUID) für jeden Knoten, der auf der IP-Adresse der EC2 Instanz für diesen Knoten basiert. Diese UUID wird für die Verteilung virtuelle r Knoten (Vnodes) auf dem Ring verwendet. Wenn Cassandra auf EC2 Instanzen bereitgestellt wird, werden den Instanzen bei ihrer Erstellun g automatisch IP-Adressen zugewiesen. Im Falle eines geplanten oder ungeplant en Ausfalls ändert sich die IP-Adresse für die neue EC2 Instanz, die Datenvert eilung ändert sich und der gesamte Ring muss neu gewichtet werden. Das ist nicht wünschenswert. Um die zugewiesene IP-Adress e beizubehalten, verwenden Sie eine sekundäre elastic network interface mit einer festen IP-Adresse. 1. Wählen Sie auf der EC2 Amazon-Konsole Netzwerkschnittstellen, Netzwerkschnittstelle erstellen aus. 2. Wählen Sie unter Subnetz das Subnetz aus, in dem	Cloud-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie die EC2 Instance erstellt haben. 3. Wählen Sie für Private IPv4 Adresse die Option Automatisch zuweisen aus. 4. Wählen Sie für Sicherhei tsgruppen eine Sicherhei tsgruppe aus und klicken Sie dann auf Netzwerks chnittstelle erstellen. Weitere Informationen zum Erstellen einer Netzwerks chnittstelle finden Sie in der EC2 Amazon-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verbinden Sie die sekundäre Netzwerkschnittstelle mit den Clusterknoten.	1. Wählen Sie auf der EC2 Amazon-Konsole Instances aus. 2. Aktivieren Sie das Kontrollk ästchen für die EC2 Instance, die Sie zuvor erstellt haben. 3. Wählen Sie Aktionen, Netzwerk, Netzwerks chnittstelle, anhängen. 4. Wählen Sie die Netzwerks chnittstelle aus, die Sie im vorherigen Schritt erstellt haben, und wählen Sie dann Attach aus. Weitere Informationen zum Anschließen einer Netzwerks chnittstelle finden Sie in der EC2 Amazon-Dokumentation.	Cloud-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Routen in Amazon hinzu EC2 , um asymmetri sches Routing zu beheben.	Wenn Sie die zweite Netzwerkschnittstelle anschließen, führt das Netzwerk sehr wahrschei nlich asymmetrisches Routing durch. Um dies zu vermeiden , können Sie Routen für die neuen Netzwerkschnittstellen hinzufügen. Eine ausführliche Erklärung und Behebung von asymmetri schem Routing finden Sie im AWS Knowledge Center-Video oder Overcoming Asymmetri c Routing on Multi-Home Servers (Artikel im Linux Journal von Patrick McManus, 5. April 2004).	Netzwerkingenieur
Aktualisieren Sie die DNS-Einträge so, dass sie auf die IP der sekundären Netzwerks chnittstelle verweisen.	Verweisen Sie den vollquali fizierten Domänennamen (FQDN) des Knotens auf die IP der sekundären Netzwerks chnittstelle.	Netzwerkingenieur
Installieren und konfigurieren Sie den Cassandra-Cluster mithilfe von DSE OpsCenter.	Wenn die Clusterknoten mit den sekundären Netzwerks chnittstellen bereit sind, können Sie den Cassandra -Cluster installieren und konfigurieren.	DBA

Cluster nach einem Knotenausfall wiederherstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein AMI für den Cluster-Seed-Knoten.	Erstellen Sie eine Sicherungskopie der Knoten, damit Sie sie im Falle eines Knotenausfalls mit Datenbank-Binärdateien wiederherstellen können. Anweisungen finden Sie in der EC2 Amazon-Dokumentation unter Create an AMI.	Backup-Administrator
Wiederherstellung nach einem Knotenausfall.	Ersetzen Sie den ausgefallenen Knoten durch eine neue EC2 Instance, die über das AMI gestartet wurde, und fügen Sie die sekundäre Netzwerkschnittstelle des ausgefallenen Knotens hinzu.	Backup-Administrator
Stellen Sie sicher, dass der Cassandra-Cluster fehlerfrei ist.	Wenn der Ersatzknoten aktiv ist, überprüfen Sie den Zustand des Clusters in DSE OpsCenter.	DBA

Zugehörige Ressourcen

- Installation von DSE OpsCenter 6.1 aus dem Debian-Paket (DataStax Dokumentation)
- So sorgen Sie dafür, dass eine sekundäre Netzwerkschnittstelle in einer EC2 Ubuntu-Instanz funktioniert (AWS Knowledge Center-Video)
- Bewährte Methoden für die Ausführung von Apache Cassandra auf Amazon EC2 (AWS-Blogbeitrag)

Mit AWS Transit Gateway Connect auf AWS erweitern VRFs

Erstellt von Adam Till (AWS), Yashar Araghi (AWS), Vikas Dewangan (AWS) und Mohideen (AWS) HajaMohideen

Übersicht

Virtuelles Routing und Forwarding (VRF) ist ein Merkmal herkömmlicher Netzwerke. Es verwendet isolierte logische Routingdomänen in Form von Routingtabellen, um den Netzwerkverkehr innerhalb derselben physischen Infrastruktur zu trennen. Sie können AWS Transit Gateway so konfigurieren, dass es die VRF-Isolierung unterstützt, wenn Sie Ihr lokales Netzwerk mit AWS verbinden. Dieses Muster verwendet eine Beispielarchitektur, um eine lokale Verbindung VRFs zu verschiedenen Routentabellen für Transit-Gateways herzustellen.

Dieses Muster verwendet virtuelle Transitschnittstellen (VIFs) in AWS Direct Connect- und Transit Gateway Connect-Anhängen, um die zu erweitern VRFs. Eine Transit-VIF wird für den Zugriff auf ein oder mehrere Amazon VPC-Transit-Gateways verwendet, die Direct Connect-Gateways zugeordnet sind. Ein Transit Gateway Connect-Anhang verbindet ein Transit-Gateway mit einer virtuellen Appliance eines Drittanbieters, die in einer VPC ausgeführt wird. Ein Transit Gateway Connect-Anhang unterstützt das GRE (Generic Routing Encapsulation) -Tunnelprotokoll für hohe Leistung und unterstützt das Border Gateway Protocol (BGP) für dynamisches Routing.

Der in diesem Muster beschriebene Ansatz bietet die folgenden Vorteile:

- Mit Transit Gateway Connect können Sie dem Transit Gateway Connect-Peer bis zu 1.000 Routen ankündigen und bis zu 5.000 Routen von diesem empfangen. Die Verwendung der Direct Connect-Transit-VIF-Funktion ohne Transit Gateway Connect ist auf 20 Präfixe pro Transit-Gateway beschränkt.
- Sie können die Isolierung des Datenverkehrs aufrechterhalten und Transit Gateway Connect verwenden, um gehostete Dienste auf AWS bereitzustellen, unabhängig davon, welche IP-Adressschemas Ihre Kunden verwenden.
- Der VRF-Verkehr muss keine öffentliche virtuelle Schnittstelle passieren. Dies erleichtert die Einhaltung der Compliance- und Sicherheitsanforderungen in vielen Organisationen.
- Jeder GRE-Tunnel unterstützt bis zu 5 Gbit/s, und Sie können bis zu vier GRE-Tunnel pro Transit Gateway Connect-Anhang haben. Dies ist schneller als viele andere Verbindungstypen, wie z. B. Site-to-Site AWS-VPN-Verbindungen, die bis zu 1,25 Gbit/s unterstützen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Die erforderlichen AWS-Konten wurden erstellt (Einzelheiten finden Sie in der Architektur)
- Berechtigungen zur Übernahme einer AWS Identity and Access Management (IAM) -Rolle in jedem Konto.
- Die IAM-Rollen in jedem Konto müssen über Berechtigungen zur Bereitstellung von AWS Transit Gateway- und AWS Direct Connect Connect-Ressourcen verfügen. Weitere Informationen finden Sie unter Authentifizierung und Zugriffskontrolle für Ihre Transit-Gateways und unter Identitäts- und Zugriffsmanagement für Direct Connect.
- Die Direct Connect-Verbindungen wurden erfolgreich erstellt. Weitere Informationen finden Sie unter Erstellen einer Verbindung mit dem Verbindungsassistenten.

Einschränkungen

- Es gibt Beschränkungen für Transit-Gateway-Anlagen VPCs in den Konten Produktion, Qualitätssicherung und Entwicklung. Weitere Informationen finden Sie unter Transit-Gateway-Anlagen zu einer VPC.
- Bei der Erstellung und Verwendung von Direct Connect-Gateways gibt es Grenzen. Weitere Informationen finden Sie unter AWS Direct Connect Connect-Kontingente.

Architektur

Zielarchitektur

Die folgende Beispielarchitektur bietet eine wiederverwendbare Lösung für die Bereitstellung von Transit VIFs mit Transit Gateway Connect-Anhängen. Diese Architektur bietet Ausfallsicherheit durch die Verwendung mehrerer Direct Connect-Standorte. Weitere Informationen finden Sie unter Maximale Ausfallsicherheit in der Direct Connect-Dokumentation. Das lokale Netzwerk verfügt über Produktion, Qualitätssicherung und Entwicklung, VRFs die auf AWS ausgedehnt und mithilfe von dedizierten Routing-Tabellen isoliert werden.

In der AWS-Umgebung sind zwei Konten für die Erweiterung vorgesehen VRFs: ein Direct Connect-Konto und ein Netzwerk-Hub-Konto. Das Direct Connect-Konto enthält die Verbindung und den Transit VIFs für jeden Router. Sie erstellen die Übertragung VIFs über das Direct Connect-Konto,

stellen sie jedoch auf dem Netzwerk-Hub-Konto bereit, sodass Sie sie dem Direct Connect-Gateway im Netzwerk-Hub-Konto zuordnen können. Das Netzwerk-Hub-Konto enthält das Direct Connect-Gateway und das Transit-Gateway. Die AWS-Ressourcen sind wie folgt verbunden:

1. Transit VIFs verbindet die Router an den Direct Connect-Standorten mit AWS Direct Connect im Direct Connect-Konto.
2. Eine Transit-VIF verbindet Direct Connect mit dem Direct Connect-Gateway im Netzwerk-Hub-Konto.
3. Eine Transit-Gateway-Zuordnung verbindet das Direct Connect-Gateway mit dem Transit-Gateway im Netzwerk-Hub-Konto.
4. Transit Gateway Connect-Anlagen verbinden das Transit-Gateway mit den Konten VPCs in den Bereichen Produktion, Qualitätssicherung und Entwicklung.

Transit VIF-Architektur

Das folgende Diagramm zeigt die Konfigurationsdetails für den Transit VIFs. Diese Beispielarchitektur verwendet ein VLAN für die Tunnelquelle, Sie könnten aber auch ein Loopback verwenden.

Im Folgenden finden Sie die Konfigurationsdetails, wie z. B. autonome Systemnummern (ASNs), für den Transit. VIFs

Ressource	Item	Detail
Router-01	ASN	65534
Router-02	ASN	65534
Router-03	ASN	65534
Router-04	ASN	65534
Direct-Connect-Gateway	ASN	64601
Transit Gateway	ASN	64600
	CIDR-Block	10,100,254,0/24

Transit Gateway Connect-Architektur

Das folgende Diagramm und die folgenden Tabellen beschreiben, wie ein einzelnes VRF über einen Transit Gateway Connect-Anhang konfiguriert wird. Weisen Sie zusätzlich eindeutige Tunnel VRFs - IDs, TRANSIT-Gateway-GRE-IP-Adressen und BGP innerhalb von CIDR-Blöcken zu. Die Peer-GRE-IP-Adresse entspricht der Router-Peer-IP-Adresse aus der Transit-VIF.

Die folgende Tabelle enthält Details zur Router-Konfiguration.

Router	Tunnel	IP-Adresse	Quelle	Ziel
Router-01	Tunnel 1	169,254.101,17	VLAN 60	10.100,254,1
			169,254,100,1	
Router-02	Tunnel 11	169,254.101,81	VLAN 61	10,100,254,11
			169,254,100,5	
Router-03	Tunnel 21	169,254.101.145	VLAN 62	10,100,254,21
			169,254,100,9	
Router-04	Tunnel 31	169.254.101.209	VLAN 63	10,100,254,31
			169,254.100,13	

Die folgende Tabelle enthält Einzelheiten zur Konfiguration des Transit-Gateways.

Tunnel	GRE-IP-Adresse des Transit-Gateways	Peer-GRE-IP-Adresse	BGP innerhalb von CIDR-Blöcken
Tunnel 1	10.100.254.1	VLAN 60	169,254,101,16/29
		169,254,100,1	
Tunnel 11	10.100.254.11	VLAN 61	169,254,101,80/29
		169,254,100,5	

Tunnel 21	10.100.254.21	VLAN 62 169,254,100,9	169,254,101,144/29
Tunnel 31	10.100.254.31	VLAN 63 169,254.100,13	169,254,101,208/29

Bereitstellung

Im Abschnitt Epics wird beschrieben, wie Sie eine Beispielkonfiguration für eine einzelne VRF auf mehreren Kundenroutern bereitstellen. Nachdem die Schritte 1—5 abgeschlossen sind, können Sie neue Transit Gateway Connect-Anlagen erstellen, indem Sie die Schritte 6—7 für jedes neue VRF, das Sie auf AWS erweitern, ausführen:

1. Erstellen Sie das Transit-Gateway.
2. Erstellen Sie eine Transit Gateway Gateway-Routentabelle für jedes VRF.
3. Erstellen Sie die virtuellen Transitschnittstellen.
4. Erstellen Sie das Direct Connect-Gateway.
5. Erstellen Sie die virtuelle Direct Connect-Gateway-Schnittstelle und die Gateway-Zuordnungen mit zulässigen Präfixen.
6. Erstellen Sie den Transit Gateway Connect-Anhang.
7. Erstellen Sie die Transit Gateway Connect-Peers.
8. Ordnen Sie den Transit Gateway Connect-Anhang der Routentabelle zu.
9. Kündigen Sie Routen zu den Routern an.

Tools

AWS-Services

- AWS Direct Connect verbindet Ihr internes Netzwerk über ein Standard-Ethernet-Glasfaserkabel mit einem Direct Connect-Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt zu öffentlichen AWS-Services erstellen und dabei Internetdienstanbieter in Ihrem Netzwerkpfad umgehen.
- AWS Transit Gateway ist ein zentraler Hub, der virtuelle private Clouds (VPCs) und lokale Netzwerke verbindet.

- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.

Epen

Plane die Architektur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie benutzerdefinierte Architekturdiagramme.	1. Laden Sie im Bereich Anlagen die Schemavorlage herunter. 2. Öffnen Sie das angehängte Diagramm in Microsoft Office PowerPoint. 3. Passen Sie auf der Folie mit der Architekturübersicht das Architekturdiagramm an Ihre Umgebung an. Identifizieren Sie die lokalen Standorte VRFs , die auf Ihre AWS-Umgebung ausgedehnt werden müssen. 4. Passen Sie auf der Folie Transit VIF das Architekturdiagramm an. Identifizieren Sie die AS-Nummern der Router, des Direct Connect-Gateways und des Transit-Gateways. Identifizieren Sie die IP-Adressen an jedem Ende der Transit-VIF.	Cloud-Architekt, Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Passen Sie auf der Folie Transit Gateway Connect ein Architekturdiagramm für jedes VRF an. Identifizieren Sie alle erforderlichen IP-Adressen, die für die Konfiguration der Router und der Transit Gateway Connect-Peers erforderlich sind.	

Erstellen Sie die Transit Gateway Gateway-Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Transit-Gateway.	1. Melden Sie sich beim Netzwerk-Hub-Konto an. 2. Folgen Sie den Anweisungen unter Ein Transit-Gateway erstellen. Beachten Sie für dieses Muster Folgendes: • Geben Sie für Amazon Side Autonomous System Number (ASN) eine eindeutige ASN ein. Für die Zwecke dieses Beispiels lautet die ASN. `64600` • Wählen Sie DNS-Unterstützung aus. • Für diese Beispielarchitektur sind VPN-	Netzwerkadministrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ECMP-Unterstützung, Standardroutentabellenzuweisung, Standardroutentabellenverlängerung und Multicast-Unterstützung nicht erforderlich. • Geben Sie für CIDR-Blöcke des Transit-Gateways die IPv4 CIDR-Blöcke für Ihr Transit-Gateway ein. Für die Zwecke dieses Beispiels lautet der CIDR-Block. `10.100.254.0/24`	
Erstellen Sie die Routentabelle des Transit-Gateways.	Folgen Sie den Anweisungen unter Erstellen einer Transit-Gateway-Routentabelle. Beachten Sie für dieses Muster Folgendes: • Geben Sie im Feld Name Tag einen Namen für die Transit-Gateway-Routentabelle ein. Wir empfehlen, einen Namen zu verwenden, der dem VRF entspricht, z. B. `routetable-dev-vrf` • Wählen Sie als Transit-Gateway-ID das Transit-Gateway aus, das Sie zuvor erstellt haben.	Cloud-Architekt, Netzwerkadministrator

Erstellen Sie die virtuellen Transitschnittstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die virtuellen Transitschnittstellen.	1. Melden Sie sich beim Direct Connect-Konto an. 2. Folgen Sie den Anweisungen unter Erstellen einer virtuellen Transitschnittstelle zum Direct Connect-Gateway. Beachten Sie Folgendes für dieses Muster: • Geben Sie unter Name der virtuellen Schnittstelle einen Namen für die Transit-VIF ein. Wir empfehlen, einen Namen zu verwenden, der dem Router entspricht, z. B. `transit-vif-router01` • Wählen Sie unter Verbindung den Router aus, z. B. `router-01`. • Geben Sie für Besitzer der virtuellen Schnittstelle die Konto-ID des Netzwerk-Hub-Kontos ein. Anweisungen finden Sie unter Ihre AWS-Konto-ID anzeigen. • Treffen Sie für Direct Connect Gateway keine Auswahl. In einem nachfolgenden Schritt	Cloud-Architekt, Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	fügen Sie das Direct Connect-Gateway hinzu.
	• Geben Sie für VLAN das VLAN des Routers ein, z. B. `60`
	• Geben Sie für BGP ASN die ASN des Routers ein, z. B. `65534`
	• Gehen Sie unter Additional Settings (Weitere Einstellungen) wie folgt vor:
	  • Wählen Sie IPv4.
	  • Geben Sie für Ihre Router-Peer-IP die Router-Peer-IP-Adresse ein, z. B. `169.254.100.1`
	  • Geben Sie für Amazon-Router-Peer-IP die Amazon-Router-Peer-IP ein, z. `169.254.100.2` B.
	  • Für den BGP-Authentifizierungsschlüssel ist ein Passwort erforderlich. Wenn dieses Feld leer gelassen wird, erstellt AWS einen Schlüssel, auf den nur in diesem Konto zugegriffen werden kann.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wiederholen Sie diese Anweisungen, um den gesamten Transit VIFs für die VRF zu erstellen.	

Erstellen Sie die Direct Connect-Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Direct Connect-Gateway.	1. Melden Sie sich beim Netzwerk-Hub-Konto an. 2. Folgen Sie den Anweisungen unter Erstellen eines Direct Connect-Gateways. Beachten Sie für dieses Muster Folgendes: • Geben Sie für ASN auf Amazon-Seite die ASN des Direct Connect-Gateways ein, z. B. `64601` • Wählen Sie kein virtuelles privates Gateway.	Cloud-Architekt, Netzwerkadministrator
Schließen Sie das Direct Connect-Gateway an den Transit an VIFs.	1. Öffnen Sie im Netzwerk-Hub-Konto die AWS Direct Connect Connect-Konsole auf https://console.aws.amazon.com/directconnect/v2/. 2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.	Cloud-Architekt, Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie eine neue Transit-VIF aus und klicken Sie dann auf Akzeptieren. 4. Wählen Sie das von Ihnen erstellte Direct Connect-Gateway aus. 5. Wiederholen Sie diese Anweisungen für jedes Transit-VIF.	
Erstellen Sie die Direct Connect-Gateway-Verknüpfungen mit zulässigen Präfixen.	Folgen Sie im Netzwerk-Hub-Konto den Anweisungen unter So ordnen Sie ein Transit-Gateway zu. Beachten Sie für dieses Muster Folgendes: • Wählen Sie für Gateways das Transit-Gateway aus, das Sie zuvor erstellt haben. • Geben Sie unter Zulässige Präfixe den CIDR-Block ein, der dem Transit-Gateway zugewiesen ist, z. B. **`10.100.254.0/24`** Durch das Erstellen dieser Zuordnung wird automatisch ein Transit Gateway Gateway-Anhang mit einem Direct Connect Gateway-Ressourcentyp erstellt. Dieser Anhang muss keiner Transit-Gateway-Routentabelle zugeordnet werden.	Cloud-Architekt, Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Transit Gateway Connect-Anhang.	1. Öffnen Sie im Netzwerk-Hub-Konto die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/. 2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhänge). 3. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus. 4. Geben Sie unter Namenstag einen Namen für den Anhang ein. Wir empfehlen, einen Namen zu verwenden, der dem VRF entspricht, z. B. `PROD-VRF` 5. Wählen Sie als Transit-Gateway-ID das Transit-Gateway aus, das Sie zuvor erstellt haben. 6. Wählen Sie bei Attachment type (Anhangstyp) die Option Connect aus. 7. Wählen Sie für Transport Attachment ID das Direct Connect-Gateway aus, das Sie zuvor erstellt haben. 8. Wählen Sie Create Transit Gateway Attachment	Cloud-Architekt, Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(Transit-Gateway-Anhang erstellen) aus. 9. Wiederholen Sie diesen Schritt für jedes VRF, das Sie erweitern möchten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Transit Gateway Connect-Peers.	1. Folgen Sie im Netzwerk-Hub-Konto den Anweisungen unter Erstellen eines Transit Gateway Connect-Peers (GRE-Tunnel). Beachten Sie Folgendes für dieses Muster: • Geben Sie unter Namenstag einen Namen für den Transit Gateway Connect-Peer ein. Wir empfehlen, einen Namen zu verwenden, der dem Router entspricht, z. B. `connectpeer-router01` • Geben Sie für die GRE-Adresse des Transit-Gateways die zugewiesene IP-Adresse aus dem CIDR-Block des Transit-Gateways ein, z. B. `10.100.254.1` • Geben Sie als Peer-GRE-Adresse die IP-Adresse ein, die dem VLAN zugewiesen ist, das auf dem Router für die Transit-VIF erstellt wurde, z. B. `169.254.100.1` Vorausgesetzt, dass AWS die IP-Adresse erreichen kann, können Sie eine beliebige	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Schnittstelle wie VLAN oder Loopback für die Peer-GRE-Adresse verwenden. • Geben Sie für BGP Inside CIDR Blocks (IPv4) die IP-Adresse des BGP inside CIDR-Blocks ein, z. B. `169.254.101.16/29` • Geben Sie für Peer ASN die ASN des Routers ein, z. B. `65534` 2. Wiederholen Sie diese Anweisungen, um für jeden Router einen GRE-Tunnel zu erstellen.	

Kündigen Sie Routen zu den Routern an

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Werben Sie für die Routen.	Ordnen Sie den neuen Transit Gateway Connect-Anhang der Routentabelle zu, die Sie zuvor für diese VRF erstellt haben. Ordnen Sie beispielsweise den Connect-Anhang des Production Transit Gateway der `Production-VRF` Routentabelle zu.	Netzwerkadministrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Erstellen Sie eine statische Route für das Präfix, das den Routern angekündigt wird. 1. Melden Sie sich beim Netzwerk-Hub-Konto an. 2. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/. 3. Wählen Sie im Navigationsbereich unter Transit Gateways die Option Transit Gateway-Routentabellen aus. 4. Wählen Sie die `Production-VRF` -Routing-Tabelle aus. 5. Wählen Sie im Menü Aktionen die Option Statische Route erstellen aus. 6. Geben Sie für CIDR den CIDR-Block für die angekündigte Route zum Transit-Gateway-Anhang in der Ziel-VPC ein, z. B. `10.100.1.0/24` 7. Wählen Sie für Choose Attachment den entsprechenden Transit Gateway Connect-Anhang aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Wählen Sie Create static route (Statische Route erstellen) aus.	

Zugehörige Ressourcen

AWS-Dokumentation

- Direct Connect-Dokumentation
  - Working with Direct Connect gateways
  - Verknüpfungen zwischen Transit-Gateways
  - Virtuelle Schnittstellen von AWS Direct Connect
- Transit Gateway Gateway-Dokumentation
  - Arbeiten mit Transit-Gateways
  - Transit-Gateway-Anlagen an ein Direct Connect-Gateway
  - Transit Gateway Connect-Anlagen und Transit Gateway Connect-Peers
  - Einen Transit Gateway Connect-Anhang erstellen

AWS-Blogbeiträge

- Segmentierung hybrider Netzwerke mit AWS Transit Gateway Connect
- Verwenden von AWS Transit Gateway Connect zur Erweiterung VRFs und Erhöhung der IP-Präfix-Advertising

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Erhalten Sie Amazon SNS SNS-Benachrichtigungen, wenn sich der Schlüsselstatus eines AWS KMS KMS-Schlüssels ändert

Erstellt von Shubham Harsora (AWS), Aromal Raj Jayarajan (AWS) und Navdeep Pareek (AWS)

Übersicht

Die mit einem AWS Key Management Service (AWS KMS) -Schlüssel verknüpften Daten und Metadaten gehen verloren, wenn dieser Schlüssel gelöscht wird. Das Löschen ist irreversibel und Sie können verlorene Daten (einschließlich verschlüsselter Daten) nicht wiederherstellen. Sie können Datenverlust verhindern, indem Sie ein Benachrichtigungssystem einrichten, das Sie über Statusänderungen der wichtigsten Status Ihrer AWS KMS KMS-Schlüssel informiert.

Dieses Muster zeigt Ihnen, wie Sie Statusänderungen an AWS-KMS-Schlüsseln überwachen können, indem Sie Amazon EventBridge und Amazon Simple Notification Service (Amazon SNS) verwenden, um automatische Benachrichtigungen auszugeben, wenn sich der Schlüsselstatus eines AWS KMS KMS-Schlüssels auf `Disabled` oder `PendingDeletion` ändert. Wenn ein Benutzer beispielsweise versucht, einen AWS KMS KMS-Schlüssel zu deaktivieren oder zu löschen, erhalten Sie eine E-Mail-Benachrichtigung mit Einzelheiten zur versuchten Statusänderung. Sie können dieses Muster auch verwenden, um das Löschen von AWS-KMS-Schlüsseln zu planen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit einem AWS Identity and Access Management (IAM) -Benutzer
- Ein AWS-KMS-Schlüssel

Architektur

Technologie-Stack

- Amazon EventBridge
- AWS Key Management Service (AWS KMS)
- Amazon-Simple-Notification-Service (Amazon-SNS)

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur für den Aufbau eines automatisierten Überwachungs- und Benachrichtigungsprozesses zur Erkennung von Änderungen am Status eines AWS-KMS-Schlüssels.

Das Diagramm zeigt den folgenden Workflow:

1. Ein Benutzer deaktiviert oder plant das Löschen eines AWS-KMS-Schlüssels.
2. Eine EventBridge Regel bewertet das geplante Ereignis `Disabled` oder `PendingDeletion` Ereignis.
3. Die EventBridge Regel ruft das Amazon SNS SNS-Thema auf.
4. Amazon SNS sendet eine E-Mail-Benachrichtigung an die Benutzer.

> **Note**
>
> Sie können die E-Mail-Nachricht an die Bedürfnisse Ihres Unternehmens anpassen. Wir empfehlen, Informationen über die Entitäten anzugeben, in denen der AWS-KMS-Schlüssel verwendet wird. Dies kann Benutzern helfen, die Auswirkungen des Löschens des AWS-KMS-Schlüssels zu verstehen. Sie können auch eine Erinnerungs-E-Mail-Benachrichtigung planen, die ein oder zwei Tage vor dem Löschen des AWS-KMS-Schlüssels gesendet wird.

Automatisierung und Skalierung

Der CloudFormation AWS-Stack stellt alle erforderlichen Ressourcen und Dienste bereit, damit dieses Muster funktioniert. Sie können das Muster unabhängig in einem einzigen Konto implementieren oder indem Sie AWS CloudFormation StackSets für mehrere unabhängige Konten oder Organisationseinheiten in AWS Organizations verwenden.

Tools

- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und AWS-Regionen hinweg zu verwalten. Die CloudFormation Vorlage für dieses Muster beschreibt alle AWS-Ressourcen, die Sie benötigen, und stellt CloudFormation diese Ressourcen für Sie bereit und konfiguriert sie.

- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. EventBridge liefert einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen und AWS-Services und leitet diese Daten an Ziele wie AWS Lambda weiter. EventBridge vereinfacht den Prozess der Erstellung ereignisgesteuerter Architekturen.
- AWS Key Management Service (AWS KMS) unterstützt Sie bei der Erstellung und Kontrolle kryptografischer Schlüssel, um Ihre Daten zu schützen.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.

Code

Der Code für dieses Muster ist im Repository GitHub Monitor AWS KMS Keys Disable and Scheduled Deletion verfügbar.

Epen

Stellen Sie die Vorlage CloudFormation bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Klonen Sie das Repository GitHub Monitor AWS KMS Keys Disable and Scheduled Deletion auf Ihren lokalen Computer, indem Sie den folgenden Befehl ausführen: `git clone https://github.com/aws-samples/aws-kms-deletion-notification`	AWS-Administrator, Cloud-Architekt
Aktualisieren Sie die Parameter der Vorlage.	Öffnen Sie in einem Code-Editor die `Alerting-KMS-Events.yaml` CloudFormation Vorlage, die Sie aus dem	AWS-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Repository geklont haben, und aktualisieren Sie dann die folgenden Parameter: • Geben Sie für `DestinationEmailAddress` eine aktive E-Mail-Adresse ein, die Sie für den Empfang der SNS-Benachrichtigung verwenden möchten. • Geben Sie für `SNSTopicName` einen Namen für Ihr SNS-Thema ein.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation Vorlage bereit.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudFormation -Konsole. 2. Wählen Sie im Navigationsbereich Stapel erstellen und dann Mit neuen Ressourcen (Standard) aus. 3. Wählen Sie auf der Seite Ressourcen identifizieren die Option Weiter aus. 4. Wählen Sie auf der Seite Vorlage angeben für Vorlagenquelle die Option Vorlagendatei hochladen aus. 5. Wählen Sie Datei auswählen, wählen Sie die `Alerting-KMS-Events.yaml` Datei aus Ihrem geklonten GitHub Repository aus und klicken Sie dann auf Weiter. 6. Geben Sie unter Stackname Ihren Stack-Namen ein. 7. Wählen Sie Absenden aus.	AWS-Administrator, Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie die Abonnement-E-Mail.	Nachdem die CloudFormation Vorlage erfolgreich bereitgestellt wurde, sendet Amazon SNS eine Bestätigungsnachricht für das Abonnement an die E-Mail-Adresse, die Sie in der CloudFormation Vorlage angegeben haben. Um Benachrichtigungen zu erhalten, müssen Sie dieses E-Mail-Abonnement bestätigen. Weitere Informationen finden Sie unter Bestätigen des Abonnements im Amazon SNS Developer Guide.	AWS-Administrator, Cloud-Architekt

Testen Sie die Abonnementbenachrichtigung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Deaktivieren Sie die AWS-KMS-Schlüssel.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS-KMS-Konsole. 2. Um die Region zu ändern, wählen Sie den Namen der aktuell angezeigten Region und dann die Region aus, zu der Sie wechseln möchten.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Klicken Sie im Navigation sbereich auf Kundenverwaltete Schlüssel. 4. Aktivieren Sie das Kontrollkästchen für den AWS KMS KMS-Schlüssel, den Sie aktivieren oder deaktivieren möchten. 5. Um den AWS KMS KMS-Schlüssel zu deaktivieren, wählen Sie Key Actions und dann Disable aus.	
Bestätigen Sie das Abonnement.	Bestätigen Sie, dass Sie die Amazon SNS SNS-Benachrichtigungs-E-Mail erhalten haben.	AWS-Administrator

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie den CloudFormation Stapel.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudFormation -Konsole. 2. Klicken Sie im Navigation sbereich auf Stacks. 3. Wählen Sie den Stapel aus, den Sie zuvor erstellt haben, und klicken Sie dann auf Löschen.	AWS-Administrator

Zugehörige Ressourcen

- AWS CloudFormation (AWS-Dokumentation)
- Einen Stack auf der CloudFormation AWS-Konsole erstellen (CloudFormation AWS-Dokumentation)
- Aufbau ereignisgesteuerter Architekturen auf AWS (AWS Workshop Studio-Dokumentation)
- Bewährte Methoden für den AWS Key Management Service (AWS-Whitepaper)
- Bewährte Sicherheitsmethoden für AWS Key Management Service (AWS KMS Developer Guide)

Zusätzliche Informationen

Amazon SNS bietet standardmäßig Verschlüsselung bei der Übertragung. Um den bewährten Sicherheitsmethoden zu entsprechen, können Sie auch die serverseitige Verschlüsselung für Amazon SNS aktivieren, indem Sie einen vom Kunden verwalteten AWS KMS KMS-Schlüssel verwenden.

Beibehaltung von routingfähigem IP-Speicherplatz in VPC-Designs mit mehreren Konten für Subnetze ohne Arbeitslast

Erstellt von Adam Spicer (AWS)

Übersicht

Amazon Web Services (AWS) hat bewährte Methoden veröffentlicht, die die Verwendung von dedizierten Subnetzen in einer Virtual Private Cloud (VPC) sowohl für Transit-Gateway-Anhänge als auch für Gateway Load Balancer-Endpunkte (zur Unterstützung von AWS Network Firewall oder Appliances von Drittanbietern) empfehlen. Diese Subnetze werden verwendet, um elastische Netzwerkschnittstellen für diese Services zu enthalten. Wenn Sie sowohl AWS Transit Gateway als auch einen Gateway Load Balancer verwenden, werden in jeder Availability Zone zwei Subnetze für die VPC erstellt. Aufgrund der Art und Weise, wie sie konzipiert VPCs sind, dürfen diese zusätzlichen Subnetze nicht kleiner als eine /28-Maske sein und können wertvollen routingfähigen IP-Speicherplatz beanspruchen, der andernfalls für routingfähige Workloads verwendet werden könnte. Dieses Muster zeigt, wie Sie für diese dedizierten Subnetze einen sekundären, nicht routbaren CIDR-Bereich (Classless Inter-Domain Routing) verwenden können, um routingfähigen IP-Bereich zu erhalten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Multi-VPC-Strategie für routingfähigen IP-Bereich
- Ein nicht routbarer CIDR-Bereich für die Dienste, die Sie verwenden (Transit-Gateway-Anhänge und GatewayLoad Balancer - oder Network Firewall Firewall-Endpunkte)

Architektur

Zielarchitektur

Dieses Muster umfasst zwei Referenzarchitekturen: Eine Architektur hat Subnetze für Transit Gateway (TGW) -Anlagen und einen Gateway Load Balancer-Endpunkt (GWLBe), und die zweite Architektur hat Subnetze nur für TGW-Anlagen.

Architektur 1 – TGW-verbundene VPC mit Eingangs-Routing zu einer Appliance

Das folgende Diagramm stellt eine Referenzarchitektur für eine VPC dar, die sich über zwei Availability Zones erstreckt. Beim Eingang verwendet die VPC ein Ingress-Routing-Muster, um den für das öffentliche Subnetz bestimmten Datenverkehr zur Firewall-Inspektion an eine bump-in-the-wire Appliance weiterzuleiten. Ein TGW-Anhang unterstützt den Ausgang von privaten Subnetzen zu einer separaten VPC.

Dieses Muster verwendet einen CIDR-Bereich, der nicht routbar ist, für das TGW-Anhangs-Subnetz und das Subnetz. GWLBe In der TGW-Routingtabelle ist dieser nicht routbare CIDR mit einer (statischen) Blackhole-Route konfiguriert, wobei eine Reihe speziellerer Routen verwendet wird. Wenn die Routen an die TGW-Routingtabelle weitergegeben würden, würden diese spezifischeren Blackhole-Routen gelten.

In diesem Beispiel ist das routbare CIDR /23 aufgeteilt und vollständig routingfähigen Subnetzen zugewiesen.

Architektur 2 — TGW-angeschlossene VPC

Das folgende Diagramm stellt eine weitere Referenzarchitektur für eine VPC dar, die sich über zwei Availability Zones erstreckt. Ein TGW-Anhang unterstützt ausgehenden Datenverkehr (Egress) von den privaten Subnetzen zu einer separaten VPC. Es verwendet einen CIDR-Bereich, der nicht routbar ist, nur für das TGW-Anhangs-Subnetz. In der TGW-Routingtabelle ist dieser nicht routbare CIDR mit einer Blackhole-Route konfiguriert, wobei eine Reihe speziellerer Routen verwendet wird. Wenn die Routen an die TGW-Routingtabelle weitergegeben würden, würden diese spezifischeren Blackhole-Routen gelten.

In diesem Beispiel ist das routbare CIDR /23 aufgeteilt und vollständig routingfähigen Subnetzen zugewiesen.

Tools

AWS-Services und -Ressourcen

- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS. In diesem Muster CIDRs werden sekundäre VPCs verwendet, um routingfähigen IP-Speicherplatz während der Arbeitslast beizubehalten. CIDRs

- Internet-Gateway-Ingress-Routing (Edge-Zuordnungen) kann zusammen mit Gateway Load Balancer-Endpunkten für dedizierte, nicht routbare Subnetze verwendet werden.
- AWS Transit Gateway ist ein zentraler Knotenpunkt, der lokale Netzwerke verbindet VPCs . Bei diesem Muster VPCs sind sie zentral an ein Transit-Gateway angeschlossen, und die Transit-Gateway-Anlagen befinden sich in einem speziellen, nicht routbaren Subnetz.
- Gateway-Load Balancer ermöglichen Ihnen die Bereitstellung, Skalierung und Verwaltung virtueller Geräte, wie Firewalls, Systeme zur Angriffserkennung und -Abwehr und Deep-Packet-Inspection-Systeme. Das Gateway dient als einziger Eingangs- und Ausgangspunkt für den gesamten Verkehr. In diesem Muster können Endpunkte für einen Gateway Load Balancer in einem dedizierten, nicht routbaren Subnetz verwendet werden.
- Die AWS Network Firewall ist ein zustandsbehafteter, verwalteter Netzwerk-Firewall sowie Service zur Erkennung und Verhinderung von Eindringlingen VPCs in der AWS-Cloud. Bei diesem Muster können Endpunkte für eine Firewall in einem dedizierten, nicht routbaren Subnetz verwendet werden.

Code-Repository

Ein Runbook und CloudFormation AWS-Vorlagen für dieses Muster sind im Repository GitHub Non-Routable Secondary CIDR Patterns verfügbar. Sie können die Beispieldateien verwenden, um ein funktionierendes Labor in Ihrer Umgebung einzurichten.

Bewährte Methoden

AWS Transit Gateway

- Verwenden Sie für jeden Transit-Gateway-VPC-Anhang ein separates Subnetz.
- Weisen Sie den Transit-Gateway-Anhangssubnetzen ein /28-Subnetz aus dem sekundären, nicht routbaren CIDR-Bereich zu.
- Fügen Sie in jeder Transit-Gateway-Routingtabelle eine statische, spezifischere Route für den nicht routbaren CIDR-Bereich als schwarzes Loch hinzu.

Gateway Load Balancer und Ingress-Routing

- Verwenden Sie Ingress-Routing, um den Datenverkehr vom Internet zu den Gateway Load Balancer-Endpunkten weiterzuleiten.
- Verwenden Sie für jeden Gateway Load Balancer-Endpunkt ein separates Subnetz.

- Weisen Sie den Gateway Load Balancer-Endpunktsubnetzen ein /28-Subnetz aus dem sekundären, nicht routbaren CIDR-Bereich zu.

Epen

Erschaffen VPCs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie den CIDR-Bere ich, der nicht routbar ist.	Ermitteln Sie einen nicht routbaren CIDR-Bereich, der für das Transit-Gateway-An hangssubnetz und (optional) für alle Gateway Load Balancer- oder Network Firewall Firewall-Endpunkts ubnetze verwendet wird. Dieser CIDR-Bereich wird als sekundärer CIDR für die VPC verwendet. Er darf nicht vom primären CIDR-Bereich der VPC oder dem größeren Netzwerk aus routbar sein.	Cloud-Architekt
Ermitteln Sie routingfähige CIDR-Bereiche für. VPCs	Ermitteln Sie eine Reihe routingfähiger CIDR-Bereiche, die für Ihre verwendet werden. VPCs Dieser CIDR-Bereich wird als primärer CIDR-Bere ich für Sie verwendet. VPCs	Cloud-Architekt
Erstellen VPCs.	Erstellen Sie Ihre VPCs und hängen Sie sie an das Transit-Gateway an. Jede VPC sollte einen primären CIDR-Bereich haben, der routbar ist, und einen sekundäre	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	n CIDR-Bereich, der nicht routbar ist, basierend auf den Bereichen, die Sie in den beiden vorherigen Schritten festgelegt haben.	

Blackhole-Routen für Transit Gateway konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie spezifischere, nicht routingfähige schwarze Löcher CIDRs .	Für jede Routingtabelle eines Transit-Gateways muss eine Reihe von Blackhole-Routen für die nicht routbaren Routen erstellt werden. CIDRs Diese sind so konfiguriert, dass sichergestellt ist, dass jeglicher Datenverkehr vom sekundären VPC-CIDR nicht routbar bleibt und nicht in das größere Netzwerk gelangt. Diese Routen sollten spezifisc her sein als das nicht routbare CIDR, das auf der VPC als sekundäres CIDR festgeleg t ist. Wenn das sekundäre, nicht routbare CIDR beispiels weise 100.64.0.0/26 ist, sollten die Blackhole-Routen in der Transit-Gateway-Ro utingtabelle 100.64.0.0/27 und 100.64.0.32/27 lauten.	Cloud-Architekt

Zugehörige Ressourcen

- Best practices for deploying Gateway Load Balancer
- Verteilte Inspektionsarchitekturen mit Gateway Load Balancer
- Networking Immersion Day – Internet to VPC Firewall Lab
- Bewährte Methoden für das Transit-Gateway-Design

Zusätzliche Informationen

Der sekundäre CIDR-Bereich, der nicht routbar ist, kann auch nützlich sein, wenn Sie mit größeren skalierten Container-Bereitstellungen arbeiten, die eine große Anzahl von IP-Adressen erfordern. Sie können dieses Muster mit einem privaten NAT-Gateway verwenden, um ein nicht routbares Subnetz zum Hosten Ihrer Container-Bereitstellungen zu verwenden. Weitere Informationen finden Sie im Blogbeitrag So lösen Sie die Erschöpfung privater IP-Adressen mit Private NAT Solution.

Stellen Sie ein Terraform-Produkt AWS Service Catalog mithilfe eines Code-Repositorys bereit

Erstellt von Dr. Rahul Sharad Gaikwad (AWS) und Tamilselvan P (AWS)

Übersicht

AWS Service Catalog unterstützt Self-Service-Bereitstellung mit Steuerung für Ihre Terraform-Konfigurationen. HashiCorp Wenn Sie Terraform verwenden, können Sie Service Catalog als einziges Tool verwenden, um Ihre Terraform-Konfigurationen innerhalb eines großen Maßstabs zu organisieren, zu verwalten und zu verteilen. AWS Sie können auf die wichtigsten Funktionen von Service Catalog zugreifen, darunter die Katalogisierung standardisierter und vorab genehmigter IaC-Vorlagen (Infrastructure as Code), Zugriffskontrolle, Bereitstellung von Cloud-Ressourcen mit geringsten Zugriffsrechten, Versionierung, gemeinsame Nutzung für Tausende von Benutzern und Tagging. AWS-Konten Endbenutzern wie Technikern, Datenbankadministratoren und Datenwissenschaftlern wird eine Liste der Produkte und Versionen angezeigt, auf die sie Zugriff haben, und sie können diese mit einer einzigen Aktion bereitstellen.

Dieses Muster hilft Ihnen bei der Bereitstellung von AWS Ressourcen mithilfe von Terraform-Code. Auf den Terraform-Code im GitHub Repository wird über Service Catalog zugegriffen. Mit diesem Ansatz integrieren Sie die Produkte in Ihre bestehenden Terraform-Workflows. Administratoren können mithilfe von Terraform Service Catalog-Portfolios erstellen und ihnen AWS Launch Wizard Produkte hinzufügen.

Im Folgenden sind die Vorteile dieser Lösung aufgeführt:

- Aufgrund der Rollback-Funktion in Service Catalog können Sie das Produkt auf eine frühere Version zurücksetzen, wenn während der Bereitstellung Probleme auftreten.
- Sie können die Unterschiede zwischen den Produktversionen leicht erkennen. Dies hilft Ihnen, Probleme bei der Bereitstellung zu lösen.
- Sie können im Service Catalog eine Repository-Verbindung konfigurieren, z. B. zu GitHub oder GitLab. Sie können Produktänderungen direkt über das Repository vornehmen.

Informationen zu den allgemeinen Vorteilen von finden Sie AWS Service Catalog unter Was ist Service Catalog.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto.
- Ein GitHub, BitBucket, oder ein anderes Repository, das Terraform-Konfigurationsdateien im ZIP-Format enthält.
- AWS Serverless Application Model Befehlszeilenschnittstelle (AWS SAM CLI), installiert.
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert.
- Los, installiert.
- Python-Version 3.9, installiert. AWS SAM CLI benötigt diese Version von Python.
- Berechtigungen zum Schreiben und Ausführen von AWS Lambda Funktionen sowie Berechtigungen für den Zugriff auf und die Verwaltung von Service Catalog-Produkten und -Portfolios.

Architektur

Das Diagramm zeigt den folgenden Workflow:

1. Wenn eine Terraform-Konfiguration fertig ist, erstellt ein Entwickler eine ZIP-Datei, die den gesamten Terraform-Code enthält. Der Entwickler lädt die ZIP-Datei in das Code-Repository hoch, das mit Service Catalog verbunden ist.
2. Ein Administrator ordnet das Terraform-Produkt einem Portfolio im Service Catalog zu. Der Administrator erstellt außerdem eine Startbeschränkung, die es Endbenutzern ermöglicht, das Produkt bereitzustellen.
3. In Service Catalog starten Endbenutzer AWS Ressourcen mithilfe der Terraform-Konfiguration. Sie können wählen, welche Produktversion bereitgestellt werden soll.

Tools

AWS-Services

- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.

- AWS Service Catalog hilft Ihnen dabei, Kataloge von IT-Services, für AWS die eine Genehmigung erteilt wurde, zentral zu verwalten. Endbenutzer können schnell nur die jeweils benötigten genehmigten IT-Services bereitstellen, wobei die Einschränkungen Ihrer Organisation berücksichtigt werden.

Andere Dienste

- Go ist eine Open-Source-Programmiersprache, die Google unterstützt.
- Python ist eine Allzweck-Computerprogrammiersprache.

Code-Repository

Wenn Sie Terraform-Beispielkonfigurationen benötigen, die Sie über Service Catalog bereitstellen können, können Sie die Konfigurationen im GitHub Amazon Macie Organization Setup Using Terraform Repository verwenden. Die Verwendung der Codebeispiele in diesem Repository ist nicht erforderlich.

Bewährte Methoden

- Anstatt die Werte für Variablen in der Terraform-Konfigurationsdatei (`terraform.tfvars`) bereitzustellen, konfigurieren Sie Variablenwerte, wenn Sie das Produkt über Service Catalog starten.
- Gewähren Sie nur bestimmten Benutzern oder Administratoren Zugriff auf das Portfolio.
- Folgen Sie dem Prinzip der geringsten Rechte und gewähren Sie die für die Ausführung einer Aufgabe erforderlichen Mindestberechtigungen. Weitere Informationen finden Sie in der AWS Identity and Access Management (IAM-) Dokumentation unter Gewährung der geringsten Rechte und bewährte Methoden zur Sicherheit.

Epen

Richten Sie Ihre lokale Workstation ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Installieren Sie Docker.	Wenn Sie die AWS Lambda Funktionen in Ihrer Entwicklungsumgebung ausführen	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	möchten, installieren Sie Docker. Weitere Informationen finden Sie unter Installieren der Docker-Engine in der Docker-Dokumentation.	

Installieren Sie die AWS Service Catalog Engine für Terraform.	1. Geben Sie den folgenden Befehl ein, um das AWS Service Catalog Engine for Terraform-Repository zu klonen.
	`git clone https://github.com/aws-samples/service-catalog-engine-for-terraform-os.git`
	2. Navigieren Sie zum Stammverzeichnis des geklonten Repositorys.
	3. Geben Sie den folgenden Befehl ein. Dadurch wird die Engine installiert.
	`run ./bin/bash/deploy-tre.sh -r`
	Der in Ihrem Standardprofil AWS-Region eingestellte Wert wird bei der automatisierten Installation nicht verwendet. Stattdessen geben Sie die Region an, wenn Sie diesen Befehl ausführen.
		DevOps Ingenieur, AWS-Administrator

Connect das GitHub Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie eine Verbindung zum GitHub Repository her.	1. Melden Sie sich bei der AWS Management Console an und öffnen Sie dann die Developer Tools-Konsole. Sie können auf die Developer Tools-Konsole zugreifen, indem Sie einen Dienst wie AWS CodePipeline oder auswählen AWS CodeDeploy. 2. Wählen Sie im linken Navigationsbereich Einstellungen und dann Verbindungen aus. 3. Wählen Sie Create Connection (Verbindung erstellen) aus. 4. Wählen Sie das Repository aus, in dem Sie den Terraform-Quellcode verwalten. Sie können beispielsweise Bitbucket oder GitHub Enterprise Server GitHubwählen. 5. Geben Sie einen Namen für die Verbindung ein, und wählen Sie dann Connect. 6. Wenn Sie dazu aufgefordert werden, authentifizieren Sie das Repository.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Nach Abschluss der Authentifizierung wird die Verbindung hergestellt und der Status wechselt zu aktiv.	

Erstellen Sie ein Terraform-Produkt im Service Catalog

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Service Catalog-Produkt.	1. Öffnen Sie die AWS Service Catalog -Konsole. 2. Navigieren Sie zum Abschnitt Administration und wählen Sie dann Produktliste aus. 3. Wählen Sie Produkt erstellen. 4. Wählen Sie auf der Seite Produkt erstellen im Abschnitt Produktdetails den externen Produktty p aus. Service Catalog verwendet diesen Produktty p zur Unterstützung von Terraform Community Edition-Produkten. 5. Geben Sie einen Namen und Besitzer für das Service Catalog-Produkt ein. 6. Wählen Sie Geben Sie Ihr Code-Repository mithilfe	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eines CodeStar Anbieters an. 7. Geben Sie die folgenden Informationen für Ihr Repository ein: • Connect zu Ihrem Anbieter her über AWS CodeConnections — Wählen Sie die Verbindung aus, die Sie zuvor erstellt haben. • Repository — Wählen Sie das Repository aus. • Zweig — Wählen Sie den Zweig aus. • Pfad der Vorlagendatei — Wählen Sie den Pfad, in dem die Codevorla gendatei gespeichert ist. Der Dateiname sollte mit enden `tar.gz`. 8. Geben Sie unter Versionsn ame und Beschreib ung Informationen zur Produktversion an. 9. Wählen Sie Produkt erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Portfolio.	1. Öffnen Sie die AWS Service Catalog -Konsole. 2. Navigieren Sie zum Abschnitt Administration und wählen Sie dann Portfolios aus. 3. Wählen Sie Portfolio erstellen. 4. Geben Sie die folgenden Werte ein: • Portfolio-Name – `Sample terraform` • Beschreibung des Portfolios — `Sample portfolio for Terraform configurations` • Eigentümer — Ihre Kontaktinformationen, z. B. eine E-Mail-Adresse 5. Wählen Sie Erstellen aus.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie das Terraform-Produkt dem Portfolio hinzu.	1. Öffnen Sie die AWS Service Catalog -Konsole. 2. Navigieren Sie zum Abschnitt Administration und wählen Sie dann Produktliste aus. 3. Wählen Sie das Terraform-Produkt aus, das Sie zuvor erstellt haben. 4. Wählen Sie Aktionen und dann Produkt zum Portfolio hinzufügen. 5. Wählen Sie das `Sample terraform` Portfolio aus. 6. Wählen Sie Produkt zum Portfolio hinzufügen.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Zugriffsr ichtlinie.	1. Öffnen Sie die AWS Identity and Access Management (IAM-) Konsole. 2. Wählen Sie im Navigatio nsbereich Policies. 3. Wählen Sie im Inhaltsbe reich die Option Create policy (Richtlinie erstellen). 4. Wählen Sie die JSON-Opti on. 5. Geben Sie die JSON-Beis pielrichtlinie unter Zugriffsr ichtlinie im Abschnitt Zusätzliche Informationen dieses Musters ein. 6. Wählen Sie Weiter aus. 7. Geben Sie auf der Seite Überprüfen und erstellen im Feld Richtlinienname den Text ein `TerraformResourceCreationAndArtifactAccessPolicy` . 8. Wählen Sie Richtlinie erstellen aus.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine benutzerdefinierte Vertrauensrichtlinie.	1. Öffnen Sie die IAM-Konsole. 2. Wählen Sie im Navigationsbereich Roles aus. 3. Wählen Sie Create role (Rolle erstellen) aus. 4. Wählen Sie unter Vertrauenswürdiger Entitätstyp die Option Benutzerdefinierte Vertrauensrichtlinie aus. 5. Geben Sie im JSON-Richtlinieneditor die JSON-Beispielrichtlinie unter Vertrauensrichtlinie im Abschnitt Zusätzliche Informationen dieses Musters ein. 6. Wählen Sie Weiter aus. 7. Wählen Sie unter Berechtigungsrichtlinien die aus`TerraformResourceCreationAndArtifactAccessPolicy` , die Sie zuvor erstellt haben. 8. Wählen Sie Weiter aus. 9. Geben Sie unter Rollendetails in das Feld Rollenname den Text ein`SCLaunch-product` .	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Important Der Rollenname muss mit beginnen `SCLaunch`. 10. Wählen Sie Rolle erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie dem Service Catalog-Produkt eine Startbeschränkung hinzu.	1. Melden Sie sich AWS Management Console als Benutzer mit Administr atorrechten bei der an. 2. Öffnen Sie die AWS Service Catalog -Konsole. 3. Wählen Sie im Navigatio nsbereich Portfolios aus. 4. Wählen Sie das Portfolio aus, das Sie zuvor erstellt haben. 5. Wählen Sie auf der Seite mit den Portfoliodetails die Registerkarte Einschrän kungen und dann Einschrän kung erstellen aus. 6. Wählen Sie unter Produkt das Terraform-Produkt aus, das Sie zuvor erstellt haben. 7. Wählen Sie unter Startbesc hränkung für Methode die Option Rollennamen eingeben aus. 8. Geben Sie in das Feld Rollenname den Text ein`SCLaunch-product` . 9. Wählen Sie Erstellen aus.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gewähren Sie Zugriff auf das Produkt.	1. Öffnen Sie die AWS Service Catalog -Konsole. 2. Wählen Sie im Navigationsbereich Portfolios aus. 3. Wählen Sie das Portfolio aus, das Sie zuvor erstellt haben. 4. Wählen Sie die Registerkarte Zugriff und anschließend Zugriff gewähren aus. 5. Wählen Sie die Registerkarte Rollen und dann die Rolle aus, die Zugriff auf die Bereitstellung dieses Produkts haben soll. 6. Wählen Sie Zugriff gewähren.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie das Produkt.	1. Melden Sie sich AWS Management Console als Benutzer mit Berechtigungen zur Bereitstellung des Service Catalog-Produkts an. 2. Öffnen Sie die AWS Service Catalog -Konsole. 3. Wählen Sie im Navigationsbereich Produkte aus. 4. Wählen Sie das Produkt aus, das Sie zuvor erstellt haben, und klicken Sie dann auf Produkt starten. 5. Geben Sie einen Produktnamen ein und definieren Sie alle erforderlichen Parameter. 6. Wählen Sie Produkt starten.	DevOps Ingenieur

Überprüfen der Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Bereitstellung.	Es gibt zwei AWS Step Functions Zustandsmaschinen für den Service Catalog-Bereitstellungsworkflow: • `ManageProvisionedProductStateMachine` — Service Catalog ruft diese Zustandsmaschine	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	auf, wenn ein neues Terraform-Produkt bereitgestellt wird und wenn ein vorhandenes von Terraform bereitgestelltes Produkt aktualisiert wird. • `TerminateProvisionedProductStateMachine` — Service Catalog ruft diese Zustandsmaschine auf, wenn ein vorhandenes, von Terraform bereitgestelltes Produkt beendet wird. Sie überprüfen die Protokolle für den `ManageProvisionedProductStateMachine` State Machine, um zu bestätigen, dass das Produkt bereitgestellt wurde. 1. Melden Sie sich bei der AWS Management Console an und öffnen Sie dann die AWS Step Functions Konsole. 2. Wählen Sie im linken Navigationsbereich State Machines aus. 3. `ManageProvisionedProductStateMachine`. 4. Geben Sie in der Liste Ausführungen die bereitges	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	tellte Produkt-ID ein, um nach der Ausführung zu suchen. **Note** Die Namen der Backend-Buckets für die Statusdat ei beginnen mit. `sc-terraform-engine-state-` 5. Stellen Sie sicher, dass alle erforderlichen Ressourcen im Konto erstellt wurden.	

Infrastruktur aufräumen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie bereitgestellte Produkte.	1. Melden Sie sich AWS Management Console als Benutzer mit Berechtig ungen zur Bereitstellung des Service Catalog-P rodukts an. 2. Öffnen Sie die AWS Service Catalog -Konsole. 3. Wählen Sie im linken Navigationsbereich die Option Bereitgestellte Produkte aus.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie das von Ihnen erstellte Produkt aus. 5. Wählen Sie in der Liste Aktionen die Option Beenden aus. 6. Geben Sie `terminate` in das Bestätigungsfeld den Text ein und wählen Sie dann Bereitgestelltes Produkt beenden aus. 7. Wiederholen Sie diese Schritte, um alle bereitgestellten Produkte zu beenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entferne die AWS Service Catalog Engine für Terraform.	1. Melden Sie sich AWS Management Console als Benutzer mit Administr atorrechten bei der an. 2. Öffnen Sie die Amazon Simple Storage Service (Amazon S3) -Konsole. 3. Wählen Sie im Navigatio nsbereich die Option Buckets aus. 4. Wählen Sie den `sc-terraform-engine-logging-XXXX` Bucket aus. 5. Wählen Sie Leer. 6. Wiederholen Sie die Schritte 4—5 für die folgenden Buckets: • `sc-terraform-engine-state-XXXX` • `terraform-engine-bootstrap-XXXX` 7. Öffnen Sie die AWS CloudFormation Konsole und überprüfen Sie dann, ob Sie sich im richtigen Modus befinden. AWS-Region 8. Wählen Sie in der linken Navigationsleiste Stacks aus.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	9. Wählen Sie `SAM-TRE` und wählen Sie dann Löschen. Warten Sie, bis der Stapel gelöscht wurde. 10. Wählen Sie `Bootstrap-TRE` und wählen Sie dann Löschen. Warten Sie, bis der Stapel gelöscht wurde.	

Zugehörige Ressourcen

AWS Dokumentation

- Erste Schritte mit einem Terraform-Produkt

Terraform-Dokumentation

- Terraform-Installation
- Terraform-Backend-Konfiguration
- Terraform Provider-Dokumentation AWS

Zusätzliche Informationen

Richtlinie für den Zugriff

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
```

```
                }
            }
        },
        {
            "Action": [
                "s3:CreateBucket*",
                "s3:DeleteBucket*",
                "s3:Get*",
                "s3:List*",
                "s3:PutBucketTagging"
            ],
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "resource-groups:CreateGroup",
                "resource-groups:ListGroupResources",
                "resource-groups:DeleteGroup",
                "resource-groups:Tag"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "tag:GetResources",
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Vertrauensrichtlinie

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "GivePermissionsToServiceCatalog",
            "Effect": "Allow",
            "Principal": {
                "Service": "servicecatalog.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account_id:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::accounti_id:role/TerraformEngine/
TerraformExecutionRole*",
                        "arn:aws:iam::accounti_id:role/TerraformEngine/
ServiceCatalogExternalParameterParserRole*",
                        "arn:aws:iam::accounti_id:role/TerraformEngine/
ServiceCatalogTerraformOSParameterParserRole*"
                    ]
                }
            }
        }
    ]
}
```

Registrieren Sie mehrere AWS-Konten mit einer einzigen E-Mail-Adresse mithilfe von Amazon SES

Erstellt von Joe Wozniak (AWS) und Shubhangi Vishwakarma (AWS)

Übersicht

Dieses Muster beschreibt, wie Sie echte E-Mail-Adressen von der E-Mail-Adresse entkoppeln können, die mit einer verknüpft ist. AWS-Konto AWS-Konten erfordern, dass bei der Kontoerstellung eine eindeutige E-Mail-Adresse angegeben wird. In einigen Organisationen AWS-Konten muss das verwaltende Team die Last der Verwaltung vieler eindeutiger E-Mail-Adressen mit seinem Messaging-Team übernehmen. Dies kann für große Organisationen, die viele verwalten, schwierig sein AWS-Konten. Wenn Ihr E-Mail-System die Plus- oder Unteradressierung nicht zulässt, wie in Sieve Email Filtering: Subaddress Extension (RFC 5233) definiert, kann `admin+123456789123@example.com` dieses Muster außerdem helfen, diese Einschränkung zu umgehen, indem Sie am Ende des lokalen Teils der E-Mail-Adresse ein Pluszeichen (+) und eine Kennung hinzufügen, z. B.

Dieses Muster bietet eine einzigartige Lösung für den Verkauf von E-Mail-Adressen, mit der AWS-Konto Eigentümer eine E-Mail-Adresse mehreren zuordnen können. AWS-Konten Die echten E-Mail-Adressen der AWS-Konto Eigentümer werden dann diesen generierten E-Mail-Adressen in einer Tabelle zugeordnet. Die Lösung verarbeitet alle eingehenden E-Mails für die einzelnen E-Mail-Konten, sucht nach dem Besitzer jedes Kontos und leitet dann alle empfangenen Nachrichten an den Eigentümer weiter.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Administrativer Zugriff auf ein AWS-Konto.
- Zugriff auf eine Entwicklungsumgebung.
- (Optional) Wenn Sie mit AWS Cloud Development Kit (AWS CDK) Workflows und der Programmiersprache Python vertraut sind, können Sie Probleme beheben oder Änderungen vornehmen.

Einschränkungen

- Die Gesamtlänge der verkauften E-Mail-Adresse beträgt 64 Zeichen. Einzelheiten finden Sie CreateAccountin der AWS Organizations API-Referenz.

Produktversionen

- Node.js Version 12.7.0 oder höher
- Python 3.9 oder höher
- Python-Pakete pip und virtualenv
- AWS CDK Version 2.23.0 oder höher
- Docker 20.10.x oder höher

Architektur

Zieltechnologie-Stack

- AWS CloudFormation stapeln
- AWS Lambda Funktionen
- Regel und Regelsatz für Amazon Simple Email Service (Amazon SES)
- AWS Identity and Access Management (IAM) -Rollen und -Richtlinien
- Bucket- und Bucket-Richtlinie für Amazon Simple Storage Service (Amazon S3)
- AWS Key Management Service (AWS KMS) Schlüssel und wichtige Richtlinie
- Thema und Themenrichtlinie für Amazon Simple Notification Service (Amazon SNS)
- Amazon-DynamoDB-Tabelle.

Zielarchitektur

Dieses Diagramm zeigt zwei Abläufe:

- Ablauf des Verkaufs von E-Mail-Adressen: Im Diagramm beginnt der Ablauf des Verkaufs von E-Mail-Adressen (unterer Abschnitt) in der Regel mit einer Kontoverkaufslösung oder einer externen Automatisierung oder wird manuell aufgerufen. In der Anfrage wird eine Lambda-Funktion mit einer Nutzlast aufgerufen, die die benötigten Metadaten enthält. Die Funktion verwendet diese Informationen, um einen eindeutigen Kontonamen und eine E-Mail-Adresse zu generieren, sie in

einer DynamoDB-Datenbank zu speichern und die Werte an den Aufrufer zurückzugeben. Diese Werte können dann verwendet werden, um eine neue zu erstellen AWS-Konto (normalerweise mithilfe von). AWS Organizations

- Ablauf der E-Mail-Weiterleitung: Dieser Ablauf ist im oberen Abschnitt des vorherigen Diagramms dargestellt. Wenn ein mithilfe der Konto-E-Mail erstellt AWS-Konto wird, die aus dem E-Mail-Verkaufsablauf generiert wurde, AWS werden verschiedene E-Mails, wie z. B. die Bestätigung der Kontoregistrierung und regelmäßige Benachrichtigungen, an diese E-Mail-Adresse gesendet. Indem Sie die Schritte in diesem Muster befolgen, konfigurieren Sie Ihr System AWS-Konto mit Amazon SES für den Empfang von E-Mails für die gesamte Domain. Diese Lösung konfiguriert Weiterleitungsregeln, die es Lambda ermöglichen, alle eingehenden E-Mails zu verarbeiten, zu überprüfen, ob sich die T0 Adresse in der DynamoDB-Tabelle befindet, und die Nachricht stattdessen an die E-Mail-Adresse des Kontoinhabers weiterzuleiten. Mithilfe dieses Verfahrens haben Kontoinhaber die Möglichkeit, mehrere Konten mit einer E-Mail-Adresse zu verknüpfen.

Automatisierung und Skalierung

Dieses Muster verwendet die AWS CDK , um die Bereitstellung vollständig zu automatisieren. Die Lösung verwendet AWS verwaltete Dienste, die automatisch skaliert werden (oder so konfiguriert werden können), dass sie Ihren Anforderungen entsprechen. Die Lambda-Funktionen erfordern möglicherweise eine zusätzliche Konfiguration, um Ihre Skalierungsanforderungen zu erfüllen. Weitere Informationen finden Sie in der Lambda-Dokumentation unter Grundlegendes zur Lambda-Funktionsskalierung.

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend AWS-Konten zu verwalten.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.

- AWS Key Management Service (AWS KMS) hilft Ihnen dabei, kryptografische Schlüssel zu erstellen und zu kontrollieren, um Ihre Daten zu schützen.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Email Service (Amazon SES) unterstützt Sie beim Senden und Empfangen von E-Mails mithilfe Ihrer eigenen E-Mail-Adressen und Domains.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Für die Bereitstellung benötigte Tools

- Entwicklungsumgebung mit AWS CLI und IAM-Zugriff auf Ihre AWS-Konto. Einzelheiten finden Sie unter den Links im Abschnitt Verwandte Ressourcen.
- Installieren Sie auf Ihrem Entwicklungssystem Folgendes:
  - Git-Befehlszeilentool, verfügbar auf der Git-Download-Website.
  - Das AWS CLI , um die Zugangsdaten für die zu konfigurieren AWS CDK. Weitere Informationen finden Sie in der AWS CLI -Dokumentation.
  - Python-Version 3.9 oder höher, erhältlich auf der Python-Download-Website.
  - Python-Pakete pip und virtualenv. Installationsanweisungen finden Sie in der Pip-Dokumentation und in der Virtualenv-Dokumentation.
  - Node.js Version 12.7.0 oder höher. Installationsanweisungen finden Sie in der Dokumentation zu Node.js.
  - AWS CDK Version 2.23.0 oder höher. Installationsanweisungen finden Sie in der AWS CDK Dokumentation.
  - Docker-Version 20.10.x oder höher. Installationsanweisungen finden Sie in der Docker-Dokumentation.

Code

Der Code für dieses Muster ist im GitHub AWS-Konto werkseitigen E-Mail-Repository verfügbar.

Epen

Ordnen Sie eine Zielbereitstellungsumgebung zu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren oder erstellen Sie eine AWS-Konto.	Identifizieren Sie ein vorhandenes oder neues, AWS-Konto auf das Sie vollen Administratorzugriff haben, um die E-Mail-Lösung bereitzustellen.	AWS-Administrator, Cloud-Administrator
Richten Sie eine Bereitstellungsumgebung ein.	Konfigurieren Sie eine benutzerfreundliche Bereitstellungsumgebung und richten Sie Abhängigkeiten ein, indem Sie die folgenden Schritte ausführen: 1. Richten Sie Ihre Entwicklungsumgebung mit den im Abschnitt Tools aufgeführten Tools ein. 2. Klonen Sie die GitHub AWS-Konto werkseitige E-Mail-Repository-Codebasis mit dem folgenden Befehl in Ihre Entwicklungsumgebung: `git clone https://github.com/aws-samples/aws-account-factory-email` 3. Aktualisieren Sie in der `requirements.txt`	AWS DevOps, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Datei (im Stammverzeichnis des Repositorys) die Zeile, die mit beginnt, sodass `aws-cdk-lib==` sie der Version entspricht AWS CDK , die in Ihrer Umgebung ausgeführt wird. Verwenden Sie den `cdk --version` Befehl, um die Version zu identifizieren.	

Richten Sie eine verifizierte Domain ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren und weisen Sie eine Domain zu.	Für die E-Mail-Weiterleitungsfunktion ist eine dedizierte Domain erforderlich. Identifizieren und weisen Sie eine Domain oder Subdomain zu, die Sie mit Amazon SES verifizieren können. Diese Domain sollte für den Empfang eingehender E-Mails in dem Land verfügbar sein, in AWS-Konto dem die E-Mail-Weiterleitungslösung eingesetzt wird. Anforderungen an die Domain: • Die Domain sollte eine Standarddomain oder Subdomain sein.	Cloud-Administrator, Netzwerkadministrator, DNS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Die Domain sollte extern per DNS auflösbar sein, da sie für den Empfang von E-Mails von außerhalb der Organisation verwendet wird.	
Überprüfen Sie die Domain.	Stellen Sie sicher, dass die identifizierte Domain verwendet werden kann, um eingehende E-Mails zu akzeptieren. Folgen Sie den Anweisungen unter Verifizieren Ihrer Domain für den E-Mail-Empfang von Amazon SES in der Amazon SES SES-Dokumentation. Dies erfordert eine Abstimmung mit der Person oder dem Team, die für die DNS-Einträge der Domain verantwortlich ist.	App-Entwickler, AWS DevOps
Richten Sie MX-Einträge ein.	Richten Sie Ihre Domain mit MX-Einträgen ein, die auf die Amazon SES SES-Endpunkte in Ihrer Region AWS-Konto und Ihrer Region verweisen. Weitere Informationen finden Sie unter Veröffentlichen eines MX-Eintrags für den Amazon SES SES-E-Mail-Empfang in der Amazon SES SES-Dokumentation.	Cloud-Administrator, Netzwerkadministrator, DNS-Administrator

Stellen Sie die Lösung für den Verkauf und die Weiterleitung von E-Mails bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Standardwerte in`cdk.json`.	Bearbeiten Sie einige der Standardwerte in der `cdk.json` Datei (im Stammverzeichnis des Repositorys), sodass die Lösung nach der Bereitstellung ordnungsgemäß funktioniert. 1. Ändern Sie den `SES_DOMAIN_NAME` Wert so, dass er dem Domainnamen entspricht, den Sie zuvor verifiziert haben. 2. Ändern Sie den `ADDRESS_FROM` Wert so, dass er dieselbe Domain enthält wie in`SES_DOMAIN_NAME` . Der lokale Teil der Adresse sollte von Ihrem Cloud-Team festgelegt werden. Diese Adresse wird zur `FROM` Adresse für jede E-Mail, die über die Lösung weitergeleitet wird. 3. Ändern Sie den `ADDRESS_ADMIN` Wert so, dass er mit der E-Mail-Adresse übereinstimmt, an die alle nicht passenden eingehenden Nachricht	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en weitergeleitet werden. Bei diesem Wert muss es sich um eine gültige und funktionierende E-Mail-Adresse handeln.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die Lösung für den Verkauf und die Weiterleitung von E-Mails bereit.	1. Erstellen Sie eine virtuelle Python-Umgebung:
	`python -m venv .venv`
	2. Aktivieren Sie die virtuelle Python-Umgebung:
	`source .venv/bin/activate`
	Oder verwenden Sie auf der Windows-Plattform:
	`% .venv\Scripts\activate.bat`
	3. Installieren Sie alle Python-Anforderungen ohne Fehler:
	`pip install -r requirements.txt`
	4. Synthetisieren Sie die CloudFormation Vorlage:
	`cdk synth`
	Vergewissern Sie sich, dass keine Fehler vorliegen und dass die vollständige CloudFormation Vorlage die erwartete Ausgabe enthält.
	5. (Optional) Wenn Sie den AWS CDK Code zum ersten Mal in der aktuellen
		App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Version AWS-Konto oder Region bereitstellen, starten Sie die Umgebung. Weitere Informationen finden Sie in der Dokumentation unter AWS CDK Bootstrapping. AWS CDK
	`cdk bootstrap aws://AWS-ACCOUNT-NUMBER/REGION`
	Ersetzen Sie `AWS-ACCOUNT-NUMBER` und `REGION` durch tatsächliche Werte.
	6. Stellen Sie die Lösung bereit:
	`cdk bootstrap`
	`cdk deploy`
	Die Befehle sollten ohne Fehler abgeschlossen werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die Lösung bereitgestellt wurde.	Stellen Sie sicher, dass die Lösung erfolgreich bereitgestellt wurde, bevor Sie mit dem Testen beginnen: 1. Öffnen Sie die AWS CloudFormation Konsole und suchen Sie nach einem CloudFormation Stack, der den Namen enthält`AwsMailFwdStack` . 2. Vergewissern Sie sich, dass dieser `AwsMailFwdStack` Stack über die folgenden Ressourcen verfügt: • Lambda-Funktionen • Amazon SES SES-Regel und Regelsatz • IAM-Rollen und -Richtlinien • Amazon S3 S3-Bucket- und Bucket-Richtlinie • AWS KMS Schlüssel und wichtige Richtlinie • Amazon SNS SNS-Thema und Themenrichtlinie • DynamoDB-Tabelle	App-Entwickler, AWS DevOps

Stellen Sie sicher, dass der Verkauf und die Weiterleitung von E-Mails erwartungsgemäß funktionieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die API funktioniert.	In diesem Schritt senden Sie Testdaten an die API der Lösung und bestätigen, dass die Lösung die erwartete Ausgabe erzeugt und dass die Backend-Operationen wie erwartet ausgeführt wurden. Führen Sie die Lambda-Funktion von Vend Email mithilfe der Testeingabe manuell aus. (Ein Beispiel finden Sie in der Datei sample_vend_request.json.) Verwenden Sie für eine gültige E-Mail-Adresse `0wnerAddress` . Die API sollte einen Kontonamen und eine Konto-E-Mail-Adresse mit den erwarteten Werten zurückgeben.	App-Entwickler, AWS DevOps
Stellen Sie sicher, dass die E-Mail weitergeleitet wird.	In diesem Schritt senden Sie eine Test-E-Mail über das System und überprüfen, ob die E-Mail an den erwarteten Empfänger weitergeleitet wurde. 1. Rufen Sie die Konto-E-Mail aus dem letzten Schritt ab. 2. Senden Sie eine E-Mail mit einer Testperson und einem	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Nachrichtentext an diese Adresse. 3. Bestätigen Sie, dass Sie die E-Mail an die E-Mail-Adresse des Kontoinhabers erhalten haben. 4. Vergewissern Sie sich, dass die E-Mail, die Sie erhalten haben, eine `FROM` Adresse hat, die der `ADDRESS_FROM` Einstellung unter entsprichtcdk.json. 5. Vergewissern Sie sich, dass Betreff und Text der empfangenen E-Mail mit der ursprünglich gesendeten Nachricht übereinstimmen.	

Fehlerbehebung

Problem	Lösung
Das System leitet E-Mails nicht wie erwartet weiter.	Vergewissern Sie sich, dass Ihre Einrichtung korrekt ist: 1. Sie sollten den Amazon SES SES-Verifizierungsprozess für Ihre Domain abgeschlossen haben. 2. Ihre Domain sollte ordnungsgemäß eingerichtet sein, sodass MX-Einträge auf die Amazon SES SES-Endpunkte in Ihrer Region AWS-Konto und Ihrer Region verweisen. Weitere Informationen finden Sie unter Veröffent

Problem	Lösung
	lichen eines MX-Eintrags für den Amazon SES SES-E-Mail-Empfang in der Amazon SES SES-Dokumentation. Gehen Sie wie folgt vor, nachdem Sie Ihre Domain-Einrichtung verifiziert haben: 1. Öffnen Sie die CloudWatch Amazon-Konsole für das Konto und die Region, in der Sie die Lösung bereitgestellt haben, und navigieren Sie im Navigationsbereich zu CloudWatch Protokollgruppen. 2. Suchen Sie in der Liste der Protokollgruppen nach `SesMailForwardLogGroup` . 3. Untersuchen Sie die Protokolle in dieser Gruppe, um festzustellen, ob beim Verkauf und Weiterleiten von E-Mails Fehler aufgetreten sind.

Problem	Lösung
Wenn Sie versuchen, den AWS CDK Stack bereitzustellen, erhalten Sie eine Fehlermeldung, die der folgenden ähnelt: „Fehler im Vorlagenformat: Unbekannte Ressourcentypen“	In den meisten Fällen bedeutet diese Fehlermeldung, dass die Region, auf die Sie abzielen, nicht über alle verfügbaren AWS-Services verfügt. Wenn Sie eine EC2 Amazon-Instance für die Bereitstellung der Lösung verwenden, zielen Sie möglicherweise auf eine Region ab, die sich von der Region unterscheidet, in der die Instance ausgeführt wird. **Note** Standardmäßig erfolgt die AWS CDK Bereitstellung in der Region und dem Konto, die Sie in der AWS CLI konfiguriert haben. Mögliche Lösungen: 1. Prüfen Sie anhand der AWS-Services nach Regionen, ob alle für diese Lösung benötigten Services (siehe den Abschnitt Target-Technologie-Stack weiter oben in diesem Muster) in dem Bereich enthalten sind, auf den AWS-Region Sie abzielen. 2. Wenn Sie eine EC2 Instance verwenden und auf eine Region abzielen, die sich von der Region unterscheidet, in der Ihre Instance ausgeführt wird, stellen Sie sicher, dass Sie die `AWS_DEFAULT_REGION` Umgebungsvariable oder eine Region mit der festlegen, AWS CLI bevor Sie die Lösung bereitstellen. Weitere Informationen finden Sie AWS CLI in der AWS CLI Dokumentation unter Konfiguration von Umgebungsvariablen für. Alternativ

Problem	Lösung
	können Sie die `app.py` Datei im Stammverz eichnis des Repositorys so ändern, dass sie eine fest codierte Konto-ID und Region enthält, indem Sie den Anweisungen in der AWS CDK Dokumentation für Umgebungen folgen.
Wenn Sie die Lösung bereitstellen, erhalten Sie die folgende Fehlermeldung: „Die Bereitstellung ist fehlgeschlagen: Fehler AwsMailFwdStack: SSM wurde parameter /cdk-bootstrap/hnb659fds/version nicht gefunden. Wurde für die Umgebung ein Bootstrapping durchgeführt? Bitte führe 'cdk bootstrap' aus	Wenn Sie noch nie AWS CDK Ressourcen für die AWS-Konto Zielregion bereitgestellt haben, müssen Sie zuerst den `cdk bootstrap` Befehl ausführen, wie der Fehler darauf hinweist. Wenn Sie diesen Fehler weiterhin erhalten, nachdem Sie den Bootstrapping-Befe hl ausgeführt haben, versuchen Sie möglicher weise, die Lösung in einer Region bereitzus tellen, die sich von der Region unterscheidet, in der Ihre Entwicklungsumgebung ausgeführt wird. Um dieses Problem zu lösen, legen Sie die `AWS_DEFAULT_REGION` Umgebungsvariable oder eine Region mit fest, AWS CLI bevor Sie die Lösung bereitstellen. Alternativ können Sie die `app.py` Datei im Stammverzeichnis des Repositorys so ändern, dass sie eine fest codierte Konto-ID und Region enthält, indem Sie den Anweisungen in der AWS CDK Dokumentation für Umgebungen folgen.

Zugehörige Ressourcen

- Hilfe bei der AWS CLI Installation von finden Sie unter Installation oder Aktualisierung auf die neueste Version von. AWS CLI
- Hilfe beim Einrichten von AWS CLI mit IAM-Zugangsdaten finden Sie unter Konfiguration der AWS CLI Einstellungen für.

- Hilfe zu dem finden Sie AWS CDK unter Erste Schritte mit dem AWS CDK.

Zusätzliche Informationen

Kosten

Wenn Sie diese Lösung einsetzen, können dem AWS-Konto Inhaber Kosten entstehen, die mit der Nutzung der folgenden Dienste verbunden sind. Es ist wichtig, dass Sie wissen, wie diese Dienste in Rechnung gestellt werden, damit Sie sich über mögliche Gebühren im Klaren sind. Preisinformationen finden Sie auf den folgenden Seiten:

- Amazon SES — Preisgestaltung
- Amazon S3 S3-Preise
- AWS KMS Preisgestaltung
- AWS Lambda Preisgestaltung
- Amazon DynamoDB — Preise

Richten Sie die DNS-Auflösung für Hybridnetzwerke in einer AWS-Umgebung mit einem Konto ein

Erstellt von Abdullahi Olaoye (AWS)

Übersicht

Dieses Muster beschreibt, wie eine vollständig hybride DNS-Architektur (Domain Name System) eingerichtet wird, die die end-to-end DNS-Auflösung von lokalen Ressourcen, AWS-Ressourcen und Internet-DNS-Abfragen ohne Verwaltungsaufwand ermöglicht. Das Muster beschreibt, wie Amazon Route 53 Resolver Resolver-Weiterleitungsregeln eingerichtet werden, die anhand des Domainnamens festlegen, wohin eine von AWS stammende DNS-Anfrage gesendet werden soll. DNS-Abfragen für lokale Ressourcen werden an lokale DNS-Resolver weitergeleitet. DNS-Abfragen für AWS-Ressourcen und Internet-DNS-Abfragen werden vom Route 53 Resolver gelöst.

Dieses Muster deckt die hybride DNS-Auflösung in einer AWS-Einzelkonto-Umgebung ab. Informationen zur Einrichtung ausgehender DNS-Abfragen in einer AWS-Umgebung mit mehreren Konten finden Sie im Muster DNS-Auflösung für Hybridnetzwerke in einer AWS-Umgebung mit mehreren Konten einrichten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein AWS-Konto
- Eine virtuelle private Cloud (VPC) in Ihrem AWS-Konto
- Eine Netzwerkverbindung zwischen der lokalen Umgebung und Ihrer VPC über AWS Virtual Private Network (AWS VPN) oder AWS Direct Connect
- IP-Adressen Ihrer lokalen DNS-Resolver (von Ihrer VPC aus erreichbar)
- Domain-/Subdomänenname, der an lokale Resolver weitergeleitet werden soll (z. B. onprem.mydc.com)
- Domain-/Subdomainname für die private gehostete AWS-Zone (z. B. myvpc.cloud.com)

Architektur

Zieltechnologie-Stack

- Private gehostete Zone von Amazon Route 53

- Amazon Route 53 Resolver
- Amazon VPC
- AWS VPN oder Direct Connect

Zielarchitektur

Tools

- Amazon Route 53 Resolver erleichtert Unternehmenskunden die Hybrid-Cloud, indem es eine nahtlose DNS-Abfrageauflösung in Ihrer gesamten Hybrid-Cloud ermöglicht. Sie können DNS-Endpunkte und Regeln für bedingte Weiterleitungen erstellen, um DNS-Namespaces zwischen Ihrem lokalen Rechenzentrum und Ihrem aufzulösen. VPCs
- Die private gehostete Zone von Amazon Route 53 ist ein Container, der Informationen darüber enthält, wie Route 53 auf DNS-Anfragen für eine Domain und deren Subdomains innerhalb einer oder mehrerer VPCs , die Sie mit dem Amazon VPC-Service erstellen, reagieren soll.

Epen

Konfigurieren Sie eine private gehostete Zone

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine private gehostete Route 53 53-Zone für einen reservierten AWS-Domainnamen wie myvpc.cloud.com.	Diese Zone enthält die DNS-Einträge für AWS-Ressourcen, die in der lokalen Umgebung aufgelöst werden sollten. Anweisungen finden Sie unter Erstellen einer privaten gehosteten Zone in der Route 53 53-Dokumentation.	Netzwerkadministrator, Systemadministrator
Ordnen Sie die privat gehostete Zone Ihrer VPC zu.	Damit Ressourcen in Ihrer VPC DNS-Einträge in dieser privaten Hosting-Zone auflösen können, müssen	Netzwerkadministrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie Ihre VPC der Hosting-Z one zuordnen. Anweisungen finden Sie unter Erstellen einer privaten gehosteten Zone in der Route 53 53-Dokume ntation.	

Route 53 Resolver-Endpunkte einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Endpunkt für eingehenden Datenverk ehr.	Route 53 Resolver verwendet den eingehenden Endpunkt, um DNS-Abfragen von lokalen DNS-Resolvern zu empfangen . Anweisungen finden Sie in der Route 53 53-Dokume ntation unter Weiterleiten eingehender DNS-Abfra gen an Ihre VPCs. Notieren Sie sich die IP-Adresse des eingehenden Endpunkts.	Netzwerkadministrator, Systemadministrator
Erstellen Sie einen ausgehend en Endpunkt.	Route 53 Resolver verwendet den ausgehenden Endpunkt, um DNS-Abfragen an lokale DNS-Resolver zu senden. Anweisungen finden Sie in der Route 53 53-Dokume ntation unter Weiterleiten ausgehender DNS-Abfragen an Ihr Netzwerk. Notieren Sie sich die ID des Ausgabeen dpunkts.	Netzwerkadministrator, Systemadministrator

Richten Sie eine Weiterleitungsregel ein und verknüpfen Sie sie mit Ihrer VPC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Weiterleitungsregel für die lokale Domain.	Diese Regel weist Route 53 Resolver an, alle DNS-Abfragen für lokale Domänen (wie onprem.mydc.com) an lokale DNS-Resolver weiterzuleiten. Um diese Regel zu erstellen, benötigen Sie die IP-Adressen der lokalen DNS-Resolver und die ausgehende Endpunkt-ID für Route 53 Resolver. Anweisungen finden Sie in der Route 53 53-Dokumentation unter Verwalten von Weiterleitungsregeln.	Netzwerkadministrator, Systemadministrator
Ordnen Sie die Weiterleitungsregel Ihrer VPC zu.	Damit die Weiterleitungsregel wirksam wird, müssen Sie die Regel mit Ihrer VPC verknüpfen. Route 53 Resolver berücksichtigt die Regel dann bei der Auflösung einer Domain. Anweisungen finden Sie in der Route 53 53-Dokumentation unter Verwalten von Weiterleitungsregeln.	Netzwerkadministrator, Systemadministrator

Konfigurieren Sie lokale DNS-Resolver

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die bedingte Weiterleitung in den lokalen DNS-Resolvern.	Damit DNS-Abfragen aus der lokalen Umgebung an die private Hosting-Zone Route 53 gesendet werden können, müssen Sie die bedingte Weiterleitung in den lokalen DNS-Resolvern konfigurieren. Dadurch werden die DNS-Resolver angewiesen, alle DNS-Abfragen für die AWS-Domäne (z. B. für myvpc.cloud.com) an die eingehende Endpunkt-IP-Adresse für Route 53 Resolver weiterzuleiten.	Netzwerkadministrator, Systemadministrator

Testen Sie die end-to-end DNS-Auflösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die DNS-Auflösung von AWS in der lokalen Umgebung.	Führen Sie von einem Server in der VPC aus eine DNS-Abfrage für eine lokale Domäne aus (z. B. server1.onprem.mydc.com).	Netzwerkadministrator, Systemadministrator
Testen Sie die DNS-Auflösung von der lokalen Umgebung zu AWS.	Führen Sie von einem lokalen Server aus die DNS-Auflösung für eine AWS-Domain durch (z. B. server1.myvpc.cloud.com).	Netzwerkadministrator, Systemadministrator

Zugehörige Ressourcen

- Zentralisiertes DNS-Management der Hybrid Cloud mit Amazon Route 53 und AWS Transit Gateway (Blog AWS Networking & Content Delivery)
- Vereinfachen Sie das DNS-Management in einer Umgebung mit mehreren Konten mit Route 53 Resolver (AWS-Sicherheitsblog)
- Arbeiten mit privaten Hosting-Zonen (Route 53 53-Dokumentation)
- Erste Schritte mit Route 53 Resolver (Route 53 53-Dokumentation)

Richten Sie mithilfe EC2 von AWS automatisch UiPath RPA-Bots auf Amazon ein CloudFormation

Erstellt von Dr. Rahul Sharad Gaikwad (AWS) und Tamilselvan P (AWS)

Übersicht

Dieses Muster erklärt, wie Sie Robotic Process Automation (RPA) -Bots auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances bereitstellen können. Es verwendet eine EC2 Image Builder Builder-Pipeline, um ein benutzerdefiniertes Amazon Machine Image (AMI) zu erstellen. Ein AMI ist ein vorkonfiguriertes Image einer virtuellen Maschine (VM), das das Betriebssystem (OS) und die vorinstallierte Software zur Bereitstellung EC2 von Instanzen enthält. Dieses Muster verwendet CloudFormation AWS-Vorlagen, um die UiPath Studio Community Edition auf dem benutzerdefinierten AMI zu installieren. UiPath ist ein RPA-Tool, mit dem Sie Roboter einrichten können, um Ihre Aufgaben zu automatisieren.

Im Rahmen dieser Lösung werden EC2 Windows-Instances mithilfe des Basis-AMI gestartet, und die UiPath Studio-Anwendung wird auf den Instances installiert. Das Muster verwendet das Microsoft System Preparation (Sysprep) -Tool, um die benutzerdefinierte Windows-Installation zu duplizieren. Danach werden die Host-Informationen entfernt und ein endgültiges AMI aus der Instance erstellt. Sie können die Instances dann bei Bedarf starten, indem Sie das endgültige AMI mit Ihren eigenen Benennungskonventionen und Ihrem eigenen Monitoring-Setup verwenden.

> **Note**
>
> Dieses Muster enthält keine Informationen zur Verwendung von RPA-Bots. Diese Informationen finden Sie in der UiPath Dokumentation. Sie können dieses Muster auch verwenden, um andere RPA-Bot-Anwendungen einzurichten, indem Sie die Installationsschritte an Ihre Anforderungen anpassen.

Dieses Muster bietet die folgenden Automatisierungen und Vorteile:

- Bereitstellung und gemeinsame Nutzung von Anwendungen: Sie können Amazon EC2 AMIs für die Anwendungsbereitstellung erstellen und diese über eine EC2 Image Builder Builder-Pipeline, die CloudFormation AWS-Vorlagen als Infrastructure-as-Code-Skripts (IaC) verwendet, für mehrere Konten gemeinsam nutzen.

- EC2 Bereitstellung und Skalierung durch Amazon: CloudFormation IaC-Vorlagen bieten benutzerdefinierte Computernamenssequenzen und die Automatisierung von Active Directory-Verknüpfungen.
- Beobachtbarkeit und Überwachung: Das Muster richtet CloudWatch Amazon-Dashboards ein, mit denen Sie EC2 Amazon-Metriken (wie CPU- und Festplattennutzung) überwachen können.
- Vorteile von RPA für Ihr Unternehmen: RPA verbessert die Genauigkeit, da Roboter zugewiesene Aufgaben automatisch und konsistent ausführen können. RPA erhöht auch die Geschwindigkeit und Produktivität, da Abläufe, die keinen Mehrwert bieten, wegfallen und sich wiederholende Aktivitäten erledigt werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS Identity and Access Management (IAM) -Berechtigungen für die Bereitstellung von Vorlagen CloudFormation
- IAM-Richtlinien zur Einrichtung einer kontenübergreifenden AMI-Verteilung mit Image Builder EC2

Architektur

1. Der Administrator stellt das Basis-Windows-AMI in der `ec2-image-builder.yaml` Datei bereit und stellt den Stack in der CloudFormation Konsole bereit.
2. Der CloudFormation Stack stellt die EC2 Image Builder Builder-Pipeline bereit, die die folgenden Ressourcen umfasst:
   - `Ec2ImageInfraConfiguration`
   - `Ec2ImageComponent`
   - `Ec2ImageRecipe`
   - `Ec2AMI`
3. Die EC2 Image Builder Builder-Pipeline startet mithilfe des Basis-AMI eine temporäre EC2 Windows-Instanz und installiert die erforderlichen Komponenten (in diesem Fall UiPath Studio).
4. Der EC2 Image Builder entfernt alle Hostinformationen und erstellt ein AMI von Windows Server.

5. Sie aktualisieren die `ec2-provisioning yaml` Datei mit dem benutzerdefinierten AMI und starten eine Reihe von EC2 Instances, die Ihren Anforderungen entsprechen.
6. Sie stellen das Count-Makro mithilfe einer CloudFormation Vorlage bereit. Dieses Makro stellt eine Count-Eigenschaft für CloudFormation Ressourcen bereit, sodass Sie auf einfache Weise mehrere Ressourcen desselben Typs angeben können.
7. Sie aktualisieren den Namen des Makros in der CloudFormation `ec2-provisioning.yaml` Datei und stellen den Stapel bereit.
8. Der Administrator aktualisiert die `ec2-provisioning.yaml` Datei je nach Bedarf und startet den Stack.
9. Die Vorlage stellt EC2 Instanzen mit der UiPath Studio-Anwendung bereit.

Tools

AWS-Services

- AWS CloudFormation unterstützt Sie bei der automatisierten und sicheren Modellierung und Verwaltung von Infrastrukturressourcen.
- Amazon CloudWatch unterstützt Sie bei der Beobachtung und Überwachung von Ressourcen und Anwendungen auf AWS, vor Ort und in anderen Clouds.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet sichere und anpassbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- EC2 Image Builder vereinfacht das Erstellen, Testen und Bereitstellen von virtuellen Maschinen und Container-Images für die Verwendung auf AWS oder vor Ort.
- Amazon EventBridge unterstützt Sie bei der Entwicklung ereignisgesteuerter Anwendungen in großem Umfang für AWS, bestehende Systeme oder Software-as-a-Service (SaaS) - Anwendungen.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf AWS-Ressourcen sicher kontrollieren. Mit IAM können Sie Berechtigungen zentral verwalten, die steuern, auf welche AWS-Ressourcen Benutzer zugreifen können. Sie verwenden IAM, um zu steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzt) ist, Ressourcen zu nutzen.
- AWS Lambda ist ein serverloser, ereignisgesteuerter Rechenservice, mit dem Sie Code für praktisch jede Art von Anwendung oder Backend-Service ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Sie können Lambda-Funktionen von über 200 AWS-Services und SaaS-Anwendungen aus aufrufen und zahlen nur für das, was Sie tatsächlich nutzen.

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, mit dem Sie beliebige Datenmengen speichern, schützen und abrufen können.
- AWS Systems Manager Agent (SSM Agent) unterstützt Systems Manager bei der Aktualisierung, Verwaltung und Konfiguration von EC2 Instances, Edge-Geräten, lokalen Servern und virtuellen Maschinen ()VMs.

Code-Repositorys

Der Code für dieses Muster ist im GitHub UiPath RPA-Bot-Setup unter Verwendung CloudFormation des Repositorys verfügbar. Das Muster verwendet auch ein Makro, das im CloudFormation AWS-Macros-Repository verfügbar ist.

Bewährte Methoden

- AWS veröffentlicht AMIs jeden Monat ein neues Windows. Diese enthalten die neuesten Betriebssystem-Patches, Treiber und Start-Agents. Wir empfehlen, dass Sie das neueste AMI verwenden, wenn Sie neue Instances starten oder wenn Sie Ihre eigenen benutzerdefinierten Images erstellen.
- Wenden Sie bei der Image-Erstellung alle verfügbaren Windows- oder Linux-Sicherheitspatches an.

Epen

Stellen Sie eine Image-Pipeline für das Basis-Image bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine EC2 Image Builder Builder-Pipeline ein.	1. Klonen Sie das UiPath RPA-Bot-Setup mithilfe des CloudFormation Repositorys, oder laden Sie die `ec2-image-builder.yaml` Vorlage aus dem Repository herunter. 2. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CloudFormation AWS-Konsole. 3. Wählen Sie Stack erstellen aus. 4. Wählen Sie im Abschnitt Specify template (Vorlage angeben) die Option Upload a template file (Vorlagen datei hochladen) aus. 5. Suchen Sie die `ec2-image-builder.yaml` Vorlage, laden Sie sie von Ihrem Computer hoch und wählen Sie dann Weiter. 6. Geben Sie Eingabepa rameter für Ihren Stack ein oder akzeptieren Sie die Standardwerte. Wählen Sie Weiter aus. **Note** Die Anzahl und die Werte der Parameter können je nach Ihren Eingabewerten variieren. 7. Konfigurieren Sie optional die Stack-Optionen und wählen Sie dann Weiter. 8. Überprüfen Sie Ihre Stack-Details.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	9. Aktivieren Sie am Ende des Bildschirms das Kontrollk ästchen, um die Funktione n zu bestätigen, und klicken Sie dann auf Absenden. 10. Überwachen Sie den Fortschritt des Stacks. Wenn der Status lautet `CREATE_COMPLETE` , ist die Bereitstellung bereit.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
EC2 Image Builder Builder-E instellungen anzeigen.	Die EC2 Image Builder Builder-Einstellungen umfassen die Infrastrukturkonfiguration, die Verteilungseinstellungen und die Einstellungen für Sicherheitsscans. So zeigen Sie die Einstellungen an: 1. Öffnen Sie die EC2 Image Builder Builder-Konsole. 2. Navigieren Sie im Navigationsbereich zu verschiedenen Image Builder Builder-E instellungen. **Note** Es hat sich bewährt, dass Sie alle Aktualisierungen von EC2 Image Builder nur über die CloudFormation Vorlage vornehmen sollten.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich die Image-Pipeline an.	So zeigen Sie die bereitgestellte Image-Pipeline an: 1. Wählen Sie in der EC2 Image Builder Builder-Konsole im Navigationsbereich Image-Pipelines aus. 2. Wählen Sie die Image-Pipeline aus, die Sie erstellt haben. 3. Sehen Sie sich die Konfigurationsdetails der Ausgabebilder, das Image-Rezept, die Infrastrukturkonfiguration, die Vertriebseinstellungen, EventBridge Amazon-Regeln und Tags an.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Image Builder Builder-P rotokolle anzeigen.	EC2 Image Builder Builder-Protokolle werden in CloudWatch Protokollgruppen zusammengefasst. So zeigen Sie die Protokolle an in CloudWatch: 1. Öffnen Sie die CloudWatch -Konsole. 2. Wählen Sie im Navigatio nsbereich Logs (Protokol le), Log groups (Protokol lgruppen) aus. 3. Wählen Sie den Namen der Protokollgruppe. EC2 Image Builder Builder-P rotokolle werden in der Protokollgruppe `/aws/imagebuilder/XXX` zusammengefasst. 4. Überprüfen Sie die neuesten Protokolle im jeweiligen Protokollstream auf Fehler, die beim Ausführen der Image-Pip eline aufgetreten sind. EC2 Image Builder Builder-Protokolle werden auch in einem S3-Bucket gespeichert. So zeigen Sie die Protokolle im Bucket an:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Öffnen Sie die Amazon S3-Konsole. 2. Wählen Sie in der Liste Buckets den Namen des Buckets aus. Die Protokolle werden im S3-Bucket `<stack-name>-XXXXXX` zusammengefasst.	
Laden Sie die UiPath Datei in einen S3-Bucket hoch.	1. Laden Sie die `.msi` Datei für UiPath Studio vom Speicherort https://download.uipath.com/UiPathStudioCommunity/.msi herunter. 2. Laden Sie die Datei zu einem S3-Bucket hoch. 3. Aktualisieren Sie den Bucket-Namen und den `ec2-image-builder.yaml` Dateischlüssel in der Vorlage im Bereich Benutzerdaten, Zeile 310.	AWS DevOps

Stellen Sie das Count-Makro bereit und testen Sie es

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie das Count-Makro bereit.	1. Klonen Sie das CloudFormation Count-Makro oder laden Sie es herunter. 2. Navigieren Sie zum Verzeichnis `Count`.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	3. Sie benötigen einen S3-Bucket, um die CloudFormation Artefakte zu speichern. Wenn Sie noch keinen S3-Bucket haben, erstellen Sie einen mit dem Namen `aws s3 mb s3://<bucket name>`.
	4. Package Sie die Count Makrovorlage. Die Vorlage verwendet das AWS Serverless Application Model (SAM), sodass sie transformiert werden muss, bevor Sie sie bereitstellen können.
	`aws cloudformation package \ --template-file template.yaml \ --s3-bucket <your bucket name here> \ --output-template-file packaged.yaml`
	Zum Beispiel:
	`aws cloudformation package \ --template-file template.yaml \ --s3-bucket count-macro-ec2 \`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>--output-
	template-file
	packaged.yaml</pre>
	5. Stellen Sie die verpackte Vorlage bereit, um einen CloudFormation Stack zu erstellen.
	<pre>aws cloudformation
	deploy \
	--stack-name
	Count-macro \
	--template-file
	packaged.yaml \
	--capabilities
	CAPABILITY_IAM</pre>
	Wenn du die Konsole verwenden möchtest, befolge die Anweisungen im vorherigen Epic oder in der CloudFormation Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie das Count-Makro.	Um die Funktionen des Makros zu testen, versuchen Sie, die Beispielvorlage zu starten, die im Lieferumfang des Makros enthalten ist. `aws cloudformation deploy \ --stack-name Count-test \ --template-file test.yaml \ --capabilities CAPABILITY_IAM`	DevOps Ingenieur

Stellen Sie den CloudFormation Stack bereit, um Instanzen mit dem benutzerdefinierten Image bereitzustellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die EC2 Amazon-Bereitstellungsvorlage bereit.	So stellen Sie EC2 Image Pipeline bereit, indem Sie CloudFormation: 1. Laden Sie die `ec2-provisioning.yaml` Vorlage aus dem GitHub Repository herunter, oder suchen Sie sie auf Ihrem Computer, falls Sie das Repository geklont haben. 2. Öffnen Sie die CloudFormation -Konsole. 3. Wiederhole die Schritte aus dem ersten Epic (oder	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	folge den Anweisungen in der CloudFormation Dokumentation), um es bereitzustellen`ec2-provisioning.yaml` .	
EC2 Amazon-Einstellungen anzeigen.	Zu den EC2 Amazon-Einstellungen gehören Sicherheits-, Netzwerk-, Speicher-, Statusprüfungen, Überwachung und Tag-Konfigurationen. So sehen Sie sich diese Konfigurationen an: 1. Öffnen Sie die EC2 Amazon-Konsole. 2. Wählen Sie im Navigationsbereich Instances und dann die EC2 Instance aus, die mit der EC2 Amazon-Bereitstellungsvorlage erstellt wurde. 3. Wählen Sie in der Instanzübersicht die Tabs aus, um die entsprechenden EC2 Amazon-Einstellungen anzuzeigen.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich das CloudWatch Dashboard an.	1. Öffnen Sie die CloudWatch -Konsole. 2. Wählen Sie im Navigationsbereich Dashboards aus. 3. Wählen Sie das Dashboard mit Ihrem Stack-Namen. **Note** Nachdem Sie den Stack bereitgestellt haben, dauert es einige Zeit, bis das Dashboard mit Metriken gefüllt ist. Das Dashboard bietet die folgenden Metriken:`CPUUtilization` ,`DiskUtilization` ,`MemoryUtilization` ,`NetworkIn` ,`NetworkOut` ,`StatusCheckFailed` .	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Zeigen Sie benutzerdefinierte Messwerte für die Speicher- und Festplattennutzung an.	1. Wählen Sie auf der CloudWatch Konsole Dashboards aus. 2. Wählen Sie im Navigationsbereich Metrics (Metriken) All metrics (Alle Metriken) aus. 3. Wählen Sie Benutzerdefinierte Namespaces,. CWAgent	AWS DevOps
Alarme zur Speicher- und Festplattennutzung anzeigen.	1. Wählen Sie auf der CloudWatch Konsole im Navigationsbereich Dashboards aus. 2. Wählen Sie All alarms (Alle Warnungen) aus.	AWS DevOps
Überprüfen Sie die Snapshot-Lebenszyklusregel.	1. Öffnen Sie die EC2 Amazon-Konsole. 2. Wählen Sie im Navigationsbereich Lifecycle Manager aus. 3. Überprüfen Sie die Einstellungen für den AMI-Lebenszyklus.	AWS DevOps

Löschen Sie die Umgebung (optional)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Lösche die Stapel.	Wenn Ihr PoC- oder Pilotprojekt abgeschlossen ist, empfehlen wir Ihnen, die von	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ihnen erstellten Stacks zu löschen, um sicherzustellen, dass Ihnen diese Ressourcen nicht in Rechnung gestellt werden. 1. Öffnen Sie die CloudFormation AWS-Konsole. 2. Wählen Sie im Navigationsbereich Stacks und dann einen oder beide Stacks aus, die Sie zuvor erstellt haben und die Sie löschen möchten. Der Stack muss aktuell ausgeführt werden. 3. Wählen Sie im Stack-Detailbereich Delete (Löschen) aus. 4. Wählen Sie bei Aufforderung Delete stack (Stack löschen) aus. ⚠ Important Der Vorgang zum Löschen des Stapels kann nicht gestoppt werden, nachdem er begonnen hat. Der Stack wird in den Status `DELETE_IN_PROGRESS` versetzt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Schlägt das Löschen fehl, befindet sich der Stapel im `DELETE_FAILED` Status. Lösungen finden Sie unter Fehler beim Löschen des Stacks in der AWS-Dokumentation CloudFormation zur Fehlerbehebung. Informationen zum Schutz von Stacks vor versehentlichem Löschen finden Sie in der CloudFormation AWS-Dokumentation unter Schützen eines Stacks vor dem Löschen.	

Fehlerbehebung

Problem	Lösung
Wenn Sie die EC2 Amazon-Bereitstellungsvorlage bereitstellen, erhalten Sie die folgende Fehlermeldung: Falsch formatierte Antwort von der Transformation 123xxxx: :Count erhalten.	Dies ist ein bekanntes Problem. (Weitere Informationen zur benutzerdefinierten Lösung und PR finden Sie im CloudFormation AWS-Makros-Repository.) Um dieses Problem zu beheben, öffnen Sie die AWS Lambda Lambda-Konsole und aktualisieren Sie `index.py` mit den Inhalten aus dem GitHub Repository.

Zugehörige Ressourcen

GitHub Repositorys

- UiPath RPA-Bot-Setup mit CloudFormation

- Makro zählen CloudFormation

AWS-Referenzen

- Einen Stack auf der CloudFormation AWS-Konsole erstellen (CloudFormation Dokumentation)
- Fehlerbehebung CloudFormation (CloudFormation Dokumentation)
- Speicher- und Festplattenmetriken für EC2 Amazon-Instances überwachen (EC2 Amazon-Dokumentation)
- Wie kann ich den CloudWatch Agenten verwenden, um Metriken für Performance Monitor auf einem Windows-Server anzuzeigen? (Artikel AWS re:POST)

Zusätzliche Referenzen

- UiPath Dokumentation
- Den Hostnamen in einem SysPreped AMI festlegen (Blogbeitrag von Brian Beach)
- Wie lasse ich Cloudformation eine Vorlage mithilfe eines Makros erneut verarbeiten, wenn sich die Parameter ändern? (Stack Overflow)

Richten Sie eine hochverfügbare PeopleSoft Architektur auf AWS ein

Erstellt von Ramanathan Muralidhar (AWS)

Übersicht

Wenn Sie Ihre PeopleSoft Workloads zu AWS migrieren, ist Resilienz ein wichtiges Ziel. Es stellt sicher, dass Ihre PeopleSoft Anwendung immer hochverfügbar ist und nach Ausfällen schnell wiederhergestellt werden kann.

Dieses Muster bietet eine Architektur für Ihre PeopleSoft Anwendungen auf AWS, um Hochverfügbarkeit (HA) auf Netzwerk-, Anwendungs- und Datenbankebene sicherzustellen. Es verwendet eine Amazon Relational Database Service (Amazon RDS) für Oracle- oder Amazon RDS for SQL Server Server-Datenbank für die Datenbankebene. Diese Architektur umfasst auch AWS-Services wie Amazon Route 53, Amazon Elastic Compute Cloud (Amazon EC2) Linux-Instances, Amazon Elastic Block Storage (Amazon EBS), Amazon Elastic File System (Amazon EFS) und einen Application Load Balancer und ist skalierbar.

Oracle PeopleSoft bietet eine Reihe von Tools und Anwendungen für das Personalmanagement und andere Geschäftsabläufe.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine PeopleSoft Umgebung mit den erforderlichen Lizenzen für die Einrichtung auf AWS
- Eine in Ihrem AWS-Konto eingerichtete Virtual Private Cloud (VPC) mit den folgenden Ressourcen:
  - Mindestens zwei Availability Zones
  - Ein öffentliches Subnetz und drei private Subnetze in jeder Availability Zone
  - Ein NAT-Gateway und ein Internet-Gateway
  - Routing-Tabellen für jedes Subnetz zur Weiterleitung des Datenverkehrs
  - Netzwerkzugriffskontrolllisten (Netzwerk ACLs) und Sicherheitsgruppen, die so definiert wurden, dass die Sicherheit der PeopleSoft Anwendung gemäß den Standards Ihres Unternehmens gewährleistet ist

Einschränkungen

- Dieses Muster bietet eine Hochverfügbarkeitslösung (HA). Es unterstützt keine Notfallwiederherstellungsszenarien (DR). In dem seltenen Fall, dass die gesamte AWS-Region für die HA-Implementierung ausfällt, ist die Anwendung nicht mehr verfügbar.

Produktversionen

- PeopleSoft Anwendungen, auf denen PeopleTools 8.52 und höher ausgeführt wird

Architektur

Zielarchitektur

Ausfallzeiten oder Ausfälle Ihrer PeopleSoft Produktionsanwendung wirken sich auf die Verfügbarkeit der Anwendung aus und führen zu erheblichen Störungen Ihres Geschäftsbetriebs.

Wir empfehlen Ihnen, Ihre PeopleSoft Produktionsanwendung so zu gestalten, dass sie stets hochverfügbar ist. Sie können dies erreichen, indem Sie einzelne Fehlerquellen eliminieren, zuverlässige Crossover- oder Failover-Points hinzufügen und Fehler erkennen. Das folgende Diagramm zeigt eine HA-Architektur für PeopleSoft auf AWS.

Diese Architekturbereitstellung verwendet Amazon RDS for Oracle als PeopleSoft Datenbank und EC2 Instances, die auf Red Hat Enterprise Linux (RHEL) ausgeführt werden. Sie können Amazon RDS for SQL Server auch als Peoplesoft-Datenbank verwenden.

Diese Architektur enthält die folgenden Komponenten:

- Amazon Route 53 wird als Domain Name Server (DNS) für die Weiterleitung von Anfragen aus dem Internet an die PeopleSoft Anwendung verwendet.
- AWS WAF schützt Sie vor gängigen Web-Exploits und Bots, die die Verfügbarkeit beeinträchtigen, die Sicherheit gefährden oder übermäßig viele Ressourcen verbrauchen können. AWS Shield Advanced (nicht abgebildet) bietet einen viel umfassenderen Schutz.
- Ein Application Load Balancer verteilt den HTTP- und HTTPS-Verkehr mit erweitertem Anforderungsrouting, das auf die Webserver ausgerichtet ist.
- Die Webserver, Anwendungsserver, Process Scheduler-Server und Elasticsearch-Server, die die PeopleSoft Anwendung unterstützen, werden in mehreren Availability Zones ausgeführt und verwenden Amazon EC2 Auto Scaling.

- Die von der PeopleSoft Anwendung verwendete Datenbank läuft auf Amazon RDS in einer Multi-AZ-Konfiguration.
- Die von der PeopleSoft Anwendung verwendete Dateifreigabe ist in Amazon EFS konfiguriert und wird für den instanzübergreifenden Zugriff auf Dateien verwendet.
- Amazon Machine Images (AMI) werden von Amazon EC2 Auto Scaling verwendet, um sicherzustellen, dass PeopleSoft Komponenten bei Bedarf schnell geklont werden.
- Die NAT-Gateways verbinden Instances in einem privaten Subnetz mit Diensten außerhalb Ihrer VPC und stellen sicher, dass externe Dienste keine Verbindung mit diesen Instances initiieren können.
- Das Internet-Gateway ist eine horizontal skalierte, redundante und hochverfügbare VPC-Komponente, die die Kommunikation zwischen Ihrer VPC und dem Internet ermöglicht.
- Die Bastion-Hosts im öffentlichen Subnetz ermöglichen den Zugriff auf die Server im privaten Subnetz über ein externes Netzwerk, z. B. das Internet oder ein lokales Netzwerk. Die Bastion-Hosts bieten kontrollierten und sicheren Zugriff auf die Server in den privaten Subnetzen.

Einzelheiten zur Architektur

Die PeopleSoft Datenbank befindet sich in einer Amazon RDS-Datenbank für Oracle (oder Amazon RDS for SQL Server) in einer Multi-AZ-Konfiguration. Die Amazon RDS Multi-AZ-Funktion repliziert Datenbankaktualisierungen in zwei Availability Zones, um die Haltbarkeit und Verfügbarkeit zu erhöhen. Amazon RDS führt bei geplanten Wartungsarbeiten und ungeplanten Störungen automatisch einen Failover zur Standby-Datenbank durch.

Das PeopleSoft Web und die Middle Tier sind auf EC2 Instances installiert. Diese Instances sind über mehrere Availability Zones verteilt und durch eine Auto Scaling Scaling-Gruppe verknüpft. Dadurch wird sichergestellt, dass diese Komponenten immer hochverfügbar sind. Es wird eine Mindestanzahl erforderlicher Instanzen verwaltet, um sicherzustellen, dass die Anwendung immer verfügbar ist und bei Bedarf skaliert werden kann.

Wir empfehlen, dass Sie für die EC2 OEM-Instances einen EC2 Instance-Typ der aktuellen Generation verwenden. Instance-Typen der aktuellen Generation, wie Instances, die auf dem AWS Nitro System basieren, unterstützen virtuelle Hardware-Maschinen (HVMs). Die HVM AMIs sind erforderlich, um die Vorteile erweiterter Netzwerke nutzen zu können, und sie bieten auch mehr Sicherheit. Die EC2 Instances, die Teil jeder Auto Scaling Scaling-Gruppe sind, verwenden ihr eigenes AMI, wenn sie Instances ersetzen oder hochskalieren. Wir empfehlen, dass Sie die EC2 Instance-Typen auf der Grundlage der Last, die Ihre PeopleSoft Anwendung bewältigen soll, und der von Oracle empfohlenen Mindestwerte für Ihre PeopleSoft Anwendung und PeopleTools Version

auswählen. Weitere Informationen zu den Hardware- und Softwareanforderungen finden Sie auf der Oracle-Support-Website.

PeopleSoft Web und Middle Tier teilen sich einen Amazon EFS-Mount, um Berichte, Datendateien und (falls erforderlich) das `PS_HOME` Verzeichnis gemeinsam zu nutzen. Amazon EFS ist aus Leistungs- und Kostengründen mit Mount-Zielen in jeder Availability Zone konfiguriert.

Ein Application Load Balancer wird bereitgestellt, um den Datenverkehr zu unterstützen, der auf die PeopleSoft Anwendung zugreift, und für den Lastenausgleich des Datenverkehrs zwischen den Webservern in verschiedenen Availability Zones. Ein Application Load Balancer ist ein Netzwerkgerät, das HA in mindestens zwei Availability Zones bereitstellt. Die Webserver verteilen den Datenverkehr mithilfe einer Lastenausgleichskonfiguration auf verschiedene Anwendungsserver. Der Lastenausgleich zwischen dem Webserver und dem Anwendungsserver stellt sicher, dass die Last gleichmäßig auf die Instanzen verteilt wird, und trägt dazu bei, Engpässe und Serviceunterbrechungen aufgrund überlasteter Instanzen zu vermeiden.

Amazon Route 53 wird als DNS-Service verwendet, um den Datenverkehr aus dem Internet an den Application Load Balancer weiterzuleiten. Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.

HA-Einzelheiten

- Datenbanken: Die Multi-AZ-Funktion von Amazon RDS betreibt zwei Datenbanken in mehreren Availability Zones mit synchroner Replikation. Dadurch entsteht eine hochverfügbare Umgebung mit automatischem Failover. Amazon RDS verfügt über eine Erkennung von Failover-Ereignissen und leitet ein automatisches Failover ein, wenn diese Ereignisse auftreten. Sie können auch ein manuelles Failover über die Amazon RDS-API einleiten. Eine ausführliche Erklärung finden Sie im Blogbeitrag Amazon RDS Under The Hood: Multi-AZ. Der Failover ist nahtlos und die Anwendung stellt in diesem Fall automatisch wieder eine Verbindung zur Datenbank her. Alle Process Scheduler-Jobs während des Failovers erzeugen jedoch Fehler und müssen erneut eingereicht werden.
- PeopleSoft Anwendungsserver: Die Anwendungsserver sind auf mehrere Availability Zones verteilt und für sie wurde eine Auto Scaling Scaling-Gruppe definiert. Wenn eine Instance ausfällt, ersetzt die Auto Scaling Scaling-Gruppe sie sofort durch eine fehlerfreie Instance, die aus dem AMI der Anwendungsservervorlage geklont wurde. Insbesondere ist Jolt-Pooling aktiviert. Wenn also eine Anwendungsserver-Instance ausfällt, werden die Sitzungen automatisch auf einen anderen Anwendungsserver umgeleitet, und die Auto Scaling Scaling-Gruppe startet automatisch eine weitere Instance, startet den Anwendungsserver und registriert ihn im Amazon EFS-

Mount. Der neu erstellte Anwendungsserver wird mithilfe des `PSSTRSETUP.SH` Skripts auf den Webservern automatisch zu den Webservern hinzugefügt. Dadurch wird sichergestellt, dass der Anwendungsserver immer hochverfügbar ist und sich nach einem Ausfall schnell erholt.

- Prozessplaner: Die Process Scheduler-Server sind auf mehrere Availability Zones verteilt und für sie wurde eine Auto Scaling-Gruppe definiert. Wenn eine Instance ausfällt, ersetzt die Auto Scaling Scaling-Gruppe sie sofort durch eine fehlerfreie Instance, die aus dem AMI der Process Scheduler-Servervorlage geklont wurde. Insbesondere wenn eine Prozessplaner-Instanz ausfällt, startet die Auto Scaling Scaling-Gruppe automatisch eine weitere Instanz und startet den Prozessplaner. Alle Jobs, die ausgeführt wurden, als die Instanz ausfiel, müssen erneut eingereicht werden. Dadurch wird sichergestellt, dass der Prozessplaner immer hochverfügbar ist und sich nach einem Ausfall schnell erholt.
- Elasticsearch-Server: Für die Elasticsearch-Server wurde eine Auto Scaling Scaling-Gruppe definiert. Wenn eine Instance ausfällt, ersetzt die Auto Scaling Scaling-Gruppe sie sofort durch eine fehlerfreie Instance, die aus dem AMI der Elasticsearch-Servervorlage geklont wird. Insbesondere wenn eine Elasticsearch-Instance ausfällt, erkennt der Application Load Balancer, der Anfragen an sie sendet, den Fehler und sendet keinen Traffic mehr an sie. Die Auto Scaling Scaling-Gruppe startet automatisch eine weitere Instance und ruft die Elasticsearch-Instance auf. Wenn die Elasticsearch-Instance wieder verfügbar ist, erkennt der Application Load Balancer, dass sie fehlerfrei ist, und sendet erneut Anfragen an sie. Dadurch wird sichergestellt, dass der Elasticsearch-Server immer hochverfügbar ist und sich nach einem Ausfall schnell erholt.
- Webserver: Für die Webserver ist eine Auto Scaling Scaling-Gruppe definiert. Wenn eine Instance ausfällt, ersetzt die Auto Scaling Scaling-Gruppe sie sofort durch eine fehlerfreie Instance, die aus dem AMI der Webservervorlage geklont wurde. Insbesondere wenn eine Webserver-Instance ausfällt, erkennt der Application Load Balancer, der Anfragen an sie weiterleitet, den Fehler und beendet das Senden von Datenverkehr an sie. Die Auto Scaling Scaling-Gruppe startet automatisch eine weitere Instance und ruft die Webserver-Instance auf. Wenn die Webserver-Instance wieder verfügbar ist, erkennt der Application Load Balancer, dass sie fehlerfrei ist, und sendet erneut Anfragen an sie. Dadurch wird sichergestellt, dass der Webserver immer hochverfügbar ist und sich nach einem Ausfall schnell erholt.

Tools

AWS-Services

- Application Load Balancer verteilen den eingehenden Anwendungsdatenverkehr auf mehrere Ziele, z. B. EC2 Instances, in mehreren Availability Zones.

- Amazon Elastic Block Store (Amazon EBS) bietet Speichervolumes auf Blockebene zur Verwendung mit Amazon Elastic Compute Cloud (Amazon EC2) -Instances.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Elastic File System (Amazon EFS) unterstützt Sie bei der Erstellung und Konfiguration gemeinsam genutzter Dateisysteme in der AWS-Cloud.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der AWS-Cloud.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.

Bewährte Methoden

Bewährte Methoden für den Betrieb

- Wenn Sie PeopleSoft auf AWS arbeiten, verwenden Sie Route 53, um den Datenverkehr aus dem Internet und lokal weiterzuleiten. Verwenden Sie die Failover-Option, um den Datenverkehr zur Disaster Recovery (DR) -Site umzuleiten, falls die primäre DB-Instance nicht verfügbar ist.
- Verwenden Sie immer einen Application Load Balancer vor der PeopleSoft Umgebung. Dadurch wird sichergestellt, dass der Datenverkehr auf sichere Weise auf die Webserver verteilt wird.
- Stellen Sie in den Zielgruppeneinstellungen des Application Load Balancer sicher, dass Stickiness mit einem vom Load Balancer generierten Cookie aktiviert ist.

> **Note**
>
> Möglicherweise müssen Sie ein anwendungsbasiertes Cookie verwenden, wenn Sie externes Single Sign-On (SSO) verwenden. Dadurch wird sichergestellt, dass die Verbindungen zwischen den Webservern und Anwendungsservern konsistent sind.

- Für eine PeopleSoft Produktionsanwendung muss das Leerlauf-Timeout des Application Load Balancer mit den Einstellungen in dem von Ihnen verwendeten Webprofil übereinstimmen. Dadurch wird verhindert, dass Benutzersitzungen auf der Load Balancer-Ebene ablaufen.
- Legen Sie für eine PeopleSoft Produktionsanwendung den Wert für die Anzahl der Wiederverwendungsvorgänge auf dem Anwendungsserver auf einen Wert fest, der Speicherlecks minimiert.

- Wenn Sie eine Amazon RDS-Datenbank für Ihre PeopleSoft Produktionsanwendung verwenden, wie in diesem Muster beschrieben, führen Sie sie für hohe Verfügbarkeit im Multi-AZ-Format aus.
- Wenn Ihre Datenbank auf einer EC2 Instance für Ihre PeopleSoft Produktionsanwendung läuft, stellen Sie sicher, dass eine Standby-Datenbank in einer anderen Availability Zone läuft, um hohe Verfügbarkeit zu gewährleisten.
- Stellen Sie für DR sicher, dass Ihre Amazon RDS-Datenbank oder EC2 -Instance über einen Standby-Modus verfügt, der in einer anderen AWS-Region als der Produktionsdatenbank konfiguriert ist. Dadurch wird sichergestellt, dass Sie im Falle eines Notfalls in der Region die Anwendung auf eine andere Region umstellen können.
- Verwenden Sie für DR Amazon Elastic Disaster Recovery, um Komponenten auf Anwendungsebene in einer von den Produktionskomponenten getrennten Region einzurichten. Dadurch wird sichergestellt, dass Sie bei einem Notfall in der Region die Anwendung auf eine andere Region umstellen können.
- Verwenden Sie Amazon EFS (für moderate I/O-Anforderungen) oder Amazon FSx (für hohe I/O-Anforderungen), um Ihre PeopleSoft Berichte, Anlagen und Datendateien zu speichern. Dadurch wird sichergestellt, dass der Inhalt an einem zentralen Ort gespeichert wird und von überall innerhalb der Infrastruktur abgerufen werden kann.
- Verwenden Sie Amazon CloudWatch (einfach und detailliert), um die AWS-Cloud-Ressourcen, die Ihre PeopleSoft Anwendung verwendet, nahezu in Echtzeit zu überwachen. Dadurch wird sichergestellt, dass Sie sofort über Probleme informiert werden und diese schnell beheben können, bevor sie die Verfügbarkeit der Umgebung beeinträchtigen.
- Wenn Sie eine Amazon RDS-Datenbank als Datenbank verwenden, verwenden Sie Enhanced Monitoring. PeopleSoft Diese Funktion bietet Zugriff auf über 50 Messwerte, darunter CPU, Arbeitsspeicher, Dateisystem-I/O und Festplatten-I/O.
- Verwenden Sie AWS CloudTrail, um API-Aufrufe auf den AWS-Ressourcen zu überwachen, die Ihre PeopleSoft Anwendung verwendet. Dies hilft Ihnen bei der Durchführung von Sicherheitsanalysen, der Nachverfolgung von Ressourcenänderungen und der Überprüfung der Einhaltung von Vorschriften.

Bewährte Methoden für die Gewährleistung der Sicherheit

- Verwenden Sie AWS WAF, um Ihre PeopleSoft Anwendung vor häufigen Exploits wie SQL-Injection oder Cross-Site Scripting (XSS) zu schützen. Erwägen Sie die Nutzung von AWS Shield Advanced für maßgeschneiderte Erkennungs- und Schadensbegrenzungsservices.

- Fügen Sie dem Application Load Balancer eine Regel hinzu, um den Datenverkehr automatisch von HTTP zu HTTPS umzuleiten, um Ihre PeopleSoft Anwendung zu schützen.
- Richten Sie eine separate Sicherheitsgruppe für den Application Load Balancer ein. Diese Sicherheitsgruppe sollte nur eingehenden HTTPS/HTTP-Verkehr und keinen ausgehenden Datenverkehr zulassen. Dadurch wird sichergestellt, dass nur beabsichtigter Datenverkehr zulässig ist, und trägt zur Sicherheit Ihrer Anwendung bei.
- Verwenden Sie private Subnetze für die Anwendungsserver, Webserver und die Datenbank und verwenden Sie NAT-Gateways für ausgehenden Internetverkehr. Dadurch wird sichergestellt, dass die Server, die die Anwendung unterstützen, nicht öffentlich erreichbar sind, und gleichzeitig wird der öffentliche Zugriff nur den Servern gewährt, die ihn benötigen.
- Verwenden Sie verschiedene Optionen VPCs für den Betrieb Ihrer PeopleSoft Produktions- und Nichtproduktionsumgebungen. Verwenden Sie AWS Transit Gateway, VPC-Peering ACLs, Netzwerk und Sicherheitsgruppen, um den Datenfluss zwischen den VPC und, falls erforderlich, Ihrem lokalen Rechenzentrum zu steuern.
- Folgen Sie dem Prinzip der geringsten Rechte. Gewähren Sie den Zugriff auf die von der PeopleSoft Anwendung verwendeten AWS-Ressourcen nur Benutzern, die ihn unbedingt benötigen. Gewähren Sie nur die Mindestberechtigungen, die zur Ausführung einer Aufgabe erforderlich sind. Weitere Informationen finden Sie in der Sicherheitssäule des AWS Well-Architected Framework.
- Verwenden Sie nach Möglichkeit AWS Systems Manager, um auf die EC2 Instances zuzugreifen, die die PeopleSoft Anwendung verwendet.

Bewährte Methoden zur Zuverlässigkeit

- Wenn Sie einen Application Load Balancer verwenden, registrieren Sie ein einzelnes Ziel für jede aktivierte Availability Zone. Dadurch ist der Load Balancer am effektivsten.
- Wir empfehlen, dass Sie URLs für jede PeopleSoft Produktionsumgebung drei unterschiedliche URLs verwenden: eine URL für den Zugriff auf die Anwendung, eine für den Integration Broker und eine für die Anzeige von Berichten. Wenn möglich, sollte jede URL über eigene dedizierte Webserver und Anwendungsserver verfügen. Dieses Design trägt dazu bei, Ihre PeopleSoft Anwendung sicherer zu machen, da jede URL über eine eigene Funktionalität und einen kontrollierten Zugriff verfügt. Es minimiert auch den Umfang der Auswirkungen, wenn die zugrunde liegenden Dienste ausfallen.
- Wir empfehlen Ihnen, Integritätsprüfungen für die Load Balancer-Zielgruppen für Ihre PeopleSoft Anwendung zu konfigurieren. Die Integritätsprüfungen sollten auf den Webservern und nicht auf

den EC2 Instanzen durchgeführt werden, auf denen diese Server ausgeführt werden. Dadurch wird sichergestellt, dass der Application Load Balancer diese Informationen korrekt wiedergibt, wenn der Webserver abstürzt oder die EC2 Instanz, die den Webserver hostet, ausfällt.

- Für eine PeopleSoft Produktionsanwendung empfehlen wir, die Webserver auf mindestens drei Availability Zones zu verteilen. Dadurch wird sichergestellt, dass die PeopleSoft Anwendung immer hochverfügbar ist, auch wenn eine der Availability Zones ausfällt.
- Für eine PeopleSoft Produktionsanwendung aktivieren Sie Jolt Pooling ()`joltPooling=true`. Dadurch wird sichergestellt, dass Ihre Anwendung ein Failover auf einen anderen Anwendungsserver durchführt, falls ein Server zu Patching-Zwecken oder aufgrund eines VM-Fehlers ausgefallen ist.
- Legen Sie für eine PeopleSoft Produktionsanwendung den Wert 1 fest`DynamicConfigReload` . Diese Einstellung wird in PeopleTools Version 8.52 und höher unterstützt. Sie fügt dem Webserver dynamisch neue Anwendungsserver hinzu, ohne die Server neu zu starten.
- Um Ausfallzeiten bei der Installation von PeopleTools Patches zu minimieren, verwenden Sie die blaue/grüne Bereitstellungsmethode für Ihre Auto Scaling Scaling-Gruppenstartkonfigurationen für die Web- und Anwendungsserver. Weitere Informationen finden Sie im AWS-Whitepaper „Überblick über Bereitstellungsoptionen“.
- Verwenden Sie AWS Backup, um Ihre PeopleSoft Anwendung auf AWS zu sichern. AWS Backup ist ein kostengünstiger, vollständig verwalteter und richtlinienbasierter Service, der den Datenschutz in großem Maßstab vereinfacht.

Bewährte Methoden zur Leistung

- Beenden Sie das SSL am Application Load Balancer, um eine optimale Leistung der PeopleSoft Umgebung zu erzielen, es sei denn, Ihr Unternehmen benötigt verschlüsselten Datenverkehr in der gesamten Umgebung.
- Erstellen Sie VPC-Endpunkte mit Schnittstellen für AWS-Services wie Amazon Simple Notification Service (Amazon SNS), CloudWatchsodass der Datenverkehr immer intern ist. Das ist kostengünstig und trägt zur Sicherheit Ihrer Anwendung bei.

Bewährte Methoden zur Kostenoptimierung

- Kennzeichnen Sie alle Ressourcen, die von Ihrer PeopleSoft Umgebung verwendet werden, und aktivieren Sie Tags zur Kostenzuweisung. Diese Tags helfen Ihnen dabei, Ihre Ressourcenkosten einzusehen und zu verwalten.

- Richten Sie für eine PeopleSoft Produktionsanwendung Auto Scaling Scaling-Gruppen für die Webserver und die Anwendungsserver ein. Dadurch wird eine minimale Anzahl von Web- und Anwendungsservern zur Unterstützung Ihrer Anwendung bereitgestellt. Sie können Auto Scaling Scaling-Gruppenrichtlinien verwenden, um die Server nach Bedarf hoch- und herunterzuskalieren.
- Verwenden Sie Fakturierungsalarme, um Benachrichtigungen zu erhalten, wenn die Kosten einen von Ihnen angegebenen Budgetschwellenwert überschreiten.

Bewährte Praktiken im Bereich Nachhaltigkeit

- Verwenden Sie Infrastructure as Code (IaC) zur Wartung Ihrer PeopleSoft Umgebungen. Auf diese Weise können Sie konsistente Umgebungen aufbauen und die Kontrolle über Änderungen behalten.

Epen

Migrieren Sie Ihre PeopleSoft Datenbank zu Amazon RDS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine DB-Subnetzgruppe.	Wählen Sie in der Amazon RDS-Konsole im Navigationsbereich Subnetzgruppen aus und erstellen Sie dann eine Amazon RDS-DB-Subnetzgruppe mit Subnetzen in mehreren Availability Zones. Dies ist erforderlich, damit die Amazon RDS-Datenbank in einer Multi-AZ-Konfiguration ausgeführt werden kann.	Cloud-Administrator
Erstellen Sie die Amazon RDS-Datenbank.	Erstellen Sie eine Amazon RDS-Datenbank in einer Availability Zone der AWS-Region, die Sie für die PeopleSoft HA-Umgebung ausgewählt haben. Achten Sie	Cloud-Administrator, Oracle-Datenbankadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	beim Erstellen der Amazon RDS-Datenbank darauf, die Multi-AZ-Option (Standby-Instance erstellen) und die Datenbank-Subnetzgruppe auszuwählen, die Sie im vorherigen Schritt erstellt haben. Weitere Informationen finden Sie in der Dokumentation zu Amazon RDS.	
Migrieren Sie Ihre PeopleSoft Datenbank zu Amazon RDS.	Migrieren Sie Ihre bestehende PeopleSoft Datenbank mithilfe des AWS Database Migration Service (AWS DMS) in die Amazon RDS-Datenbank. Weitere Informationen finden Sie in der AWS-DMS-Dokumentation und im AWS-Blogbeitrag Migration von Oracle-Datenbanken mit nahezu null Ausfallzeiten mithilfe von AWS DMS.	Cloud-Administrator PeopleSoft , DBA

Richten Sie Ihr Amazon EFS-Dateisystem ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen eines Dateisystems.	Erstellen Sie auf der Amazon EFS-Konsole ein Dateisystem und mounten Sie Ziele für jede Availability Zone. Anweisungen finden Sie in der Amazon EFS-Dokumentation. Wenn das Dateisyst	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	em erstellt wurde, notieren Sie sich seinen DNS-Namen . Sie werden diese Informati onen verwenden, wenn Sie das Dateisystem mounten.	

Richten Sie Ihre PeopleSoft Anwendung und Ihr Dateisystem ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie eine EC2 Instanz.	Starten Sie eine EC2 Instanz für Ihre PeopleSof t Anwendung. Anweisung en finden Sie in der EC2 Amazon-Dokumentation. • Geben Sie unter Name `APP_TEMPLATE` ein. • Wählen Sie für Betriebss ystem-Images Red Hat. • Wählen Sie unter Instanzty p den Instanztyp aus, der für Ihre PeopleSoft Anwendung geeignet ist. Weitere Informationen finden Sie unter Architekturdetails im Abschnitt Architektur.	Cloud-Administrator, PeopleSoft Administrator
PeopleSoft Auf der Instanz installieren.	Installieren Sie Ihre PeopleSof t Anwendung und PeopleToo ls auf der von Ihnen erstellte n EC2 Instanz. Anweisungen finden Sie in der Oracle-Do kumentation.	Cloud-Administrator, PeopleSoft Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Anwendungsserver.	Erstellen Sie den Anwendungsserver für die AMI-Vorlage und stellen Sie sicher, dass er erfolgreich eine Verbindung zur Amazon RDS-Datenbank herstellt.	Cloud-Administrator, PeopleSoft Administrator

Mounten Sie das Amazon-EFS-Dateisystem ein.	Melden Sie sich als Root-Benutzer bei der EC2 Instance an und führen Sie die folgenden Befehle aus, um das Amazon EFS-Dateisystem in einem Ordner namens `PSFTMNT` auf dem Server zu mounten.
	`sudo su -`
	`mkdir /psftmnt`
	`cat /etc/fstab`
	Hängen Sie die folgende Zeile an die `/etc/fstab` Datei an. Verwenden Sie den DNS-Namen, den Sie sich bei der Erstellung des Dateisystems notiert haben.
	`fs-09e064308f11453 88.efs.us-east-1.a mazonaws.com:/ / psftmnt nfs4 nfsvers=4 .1,rsize=1048576,w size=1048576,hard, timeo=600,retrans= 2,noresvport,_netdev 0 0`
	`mount -a`
		Cloud-Administrator, PeopleSoft Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Berechtigungen.	Stellen Sie sicher, dass der `PSFTMNT` Ordner über die richtigen Berechtigungen verfügt, damit der PeopleSoft Benutzer ordnungsgemäß darauf zugreifen kann.	Cloud-Administrator, PeopleSoft Administrator
Erstellen Sie zusätzliche Instanzen.	Wiederhole die vorherigen Schritte in diesem Epos, um Template-Instances für den Process Scheduler, den Webserver und den Elasticsearch-Server zu erstellen. Nennen Sie diese Instanzen `PRCS_TEMPLATE` , `WEB_TEMPLATE` , und. `SRCH_TEMPLATE` Legen Sie für den Webserver `joltPooling=true` und festDynamicConfigReload=1 .	Cloud-Administrator, PeopleSoft Administrator

Erstellen Sie Skripts zum Einrichten von Servern

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Skript zur Installation des Anwendungsservers.	Erstellen Sie in der EC2 `APP_TEMPLATE` Amazon-Instance als PeopleSoft Benutzer das folgende Skript. Benennen Sie es `appstart.sh` und platzieren Sie es im `PS_HOME` Verzeichnis. Sie verwenden dieses	PeopleSoft Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Skript, um den Anwendungsserver aufzurufen und den Servernamen auf dem Amazon EFS-Mount aufzuzeichnen.
	
	`#!/bin/ksh`
	`. /usr/homes/hcmdemo/.profile.`
	`psadmin -c configure -d HCMDEMO`
	`psadmin -c parallelboot -d HCMDEMO`
	`touch /psftmnt/`echo $HOSTNAME`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie ein Skript zur Installation des Process Scheduler-Servers.	Erstellen Sie in der EC2 `PRCS_TEMPLATE` Amazon-Instance als PeopleSoft Benutzer das folgende Skript. Benennen Sie es `prcsstart.sh` und platzieren Sie es im `PS_HOME` Verzeichnis. Sie werden dieses Skript verwenden, um den Process Scheduler-Server aufzurufen.
	`#!/bin/ksh`
	`. /usr/homes/hcmdemo/.profile`
	`/* The following line ensures that the process scheduler always has a unique name during replacement or scaling activity. */`
	`sed -i "s/.*PrcsServerName.*/`hostname -I | awk -F. '{print "PrcsServerName=PSUNX"$3$4}'`/" $HOME/appserv/prcs/*/psprcs.cfg`
	`psadmin -p configure -d HCMDEMO`
	`psadmin -p start -d HCMDEMO`
		PeopleSoft Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie ein Skript zur Installation des Elasticsearch-Servers.	Erstellen Sie in der EC2 `SRCH_TEMPLATE` Amazon-Instance als Elasticsearch-Benutzer das folgende Skript. Benennen Sie es `srchstart.sh` und platzieren Sie es im `HOME` Verzeichnis.
	`#!/bin/ksh`
	`/* The following line ensures that the correct IP is indicated in the elasticsearch.yaml file. */`
	`sed -i "s/.*network.host.*/`hostname -I
		awk '{print "host:"$0}'`/" $ES_HOME_DIR/config/elasticsearch.yaml`
		`nohup $ES_HOME_DIR/bin/elasticsearch &`
			PeopleSoft Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Skript zur Installation des Webservers.	Erstellen Sie in der EC2 `WEB_TEMPLATE` Amazon-Instance als Webserver-Benutzer die folgenden Skripts im `HOME` Verzeichnis. `renip.sh`: Dieses Skript stellt sicher, dass der Webserver die richtige IP hat, wenn er aus dem AMI geklont wird. `#!/bin/ksh` `hn=`hostname`` `/* On the following` ` line, change the IP` ` with the hostname with` ` the hostname of the web` ` template. */` `for text_file in `find` ` * -type f -exec grep` ` -l '<hostname-of-the-` `web-template>' {} \;` `do` `sed -e 's/<hostn` `ame-of-the-web-tem` `plate>/'$hn'/g'` ` $text_file > temp` `mv -f temp $text_file` `done`  `psstrsetup.sh` : Dieses Skript stellt sicher, dass der Webserver den richtigen Anwendungsserver verwendet IPs , der derzeit ausgeführ t wird. Es versucht, eine Verbindung zu jedem Anwendungsserver am Jolt-	PeopleSoft Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Port herzustellen und fügt ihn der Konfigurationsdatei hinzu. `#!/bin/ksh` `c2=""` `for ctr in `ls -1 /psftmnt/*.internal`` `do` `c1=`echo $ctr | awk -F "/" '{print $3}'`` `/* In the following lines, 9000 is the jolt port. Change it if necessary. */` `if nc -z $c1 9000 2> /dev/null; then` `if [[ $c2 = "" ]]; then` `c2="psserver="`echo $c1`":9000"` `else` `c2=`echo $c2`","`echo $c1`":9000"` `fi` `fi` `done` `webstart.sh` : Dieses Skript führt die beiden vorherigen Skripten aus und startet die Webserver. `#!/bin/ksh` `/* Change the path in the following if necessary. */` `cd /usr/homes/hcmdemo` `./renip.sh` `./psstrsetup.sh`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`webserv/peoplesoft/bin/startPIA.sh`	
Fügen Sie einen Crontab-E intrag hinzu.	Fügen Sie in der EC2 `WEB_TEMPLATE` Amazon-Instance als Webserver-Benutzer die folgende Zeile zu crontab hinzu. Ändern Sie die Zeit und den Pfad, um die benötigten Werte widerzuspiegeln. Dieser Eintrag stellt sicher, dass Ihr Webserver immer die richtigen Anwendungsserver-Einträge in der `configuration.properties` Datei hat. `* * * * * /usr/homes/hcmdemo/psstrsetup.sh`	PeopleSoft Administrator

Gruppenvorlagen erstellen AMIs und Auto Scaling

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein AMI für die Anwendungsservervorlage.	Erstellen Sie auf der EC2 Amazon-Konsole ein AMI-Image der EC2 `APP_TEMPLATE` Amazon-Instance. Nennen Sie das `AMIPSAPPSRV-SCG-VER1` . Anweisungen finden Sie in der EC2 Amazon-Dokumentation.	Cloud-Administrator, PeopleSoft Administrator
AMIs Für die anderen Server erstellen.	Wiederholen Sie den vorherigen Schritt, um AMIs	Cloud-Administrator, Administrator PeopleSoft

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	für den Prozessplaner, den Elasticsearch-Server und den Webserver etwas zu erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine Startvorlage für die Auto Scaling Scaling-Gruppe des Anwendung sservers.	Erstellen Sie eine Startvorlage für die Auto Scaling Scaling-Gruppe des Anwendung sservers. Benennen Sie die Vorlage Wählen Sie `PSAPPSRV_TEMPLATE.` in der Vorlage das AMI aus, das Sie für die `APP_TEMPL ATE` Instance erstellt haben. Anweisungen finden Sie in der EC2 Amazon-Dokumentation.
	• Wählen Sie in der Startvorl age den Instance-Typ entsprechend Ihren Anforderungen aus.
	• Fügen Sie im Feld Benutzerdaten des Abschnitts Erweiterte Details die folgenden Einträge hinzu. Stellen Sie sicher, dass der Pfad und die Benutzerinformationen korrekt sind. Sie haben das `appstart.sh` Skript in einem vorherigen Schritt erstellt.
	`#! /bin/ksh`
	`su -c “/usr/homes/ hcmdemo/appstart.sh”`
	`- hcmdemo`
		Cloud-Administrator, PeopleSoft Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine Startvorlage für die Auto Scaling Scaling-Gruppe des Process Scheduler-Servers.	Wiederholen Sie den vorherigen Schritt, um eine Startvorlage für die Auto Scaling Scaling-Gruppe des Process Scheduler-Servers zu erstellen. Benennen Sie die Vorlage`PSPRCS_TEMPLATE` . Wählen Sie in der Vorlage das AMI aus, das Sie für den Prozessplaner erstellt haben.
	• Fügen Sie im Feld Benutzerdaten des Abschnitts Erweiterte Details die folgenden Einträge hinzu. Stellen Sie sicher, dass der Pfad und die Benutzerinformationen korrekt sind. Sie haben das `prcsstart.sh` Skript in einem vorherigen Schritt erstellt.
	`#! /bin/ksh`
	`su -c “/usr/hom`
	`es/hcmdemo/prcssta`
	`rt.sh” - hcmdemo`
		Cloud-Administrator, PeopleSoft Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine Startvorlage für die Auto Scaling Scaling-Gruppe des Elasticsearch-Servers.	Wiederholen Sie die vorherigen Schritte, um eine Startvorlage für die Auto Scaling Scaling-Gruppe des Elasticsearch-Servers zu erstellen. Benennen Sie die Vorlage`SRCH_TEMPLATE` . Wählen Sie in der Vorlage das AMI aus, das Sie für den Suchserver erstellt haben.
	• Fügen Sie im Feld Benutzerdaten des Abschnitts Erweiterte Details die folgenden Einträge hinzu. Stellen Sie sicher, dass der Pfad und die Benutzerinformationen korrekt sind. Sie haben das `srchstart.sh` Skript in einem vorherigen Schritt erstellt.
	`#! /bin/ksh`
	`su -c “/usr/hom`
	`es/essearch/srchst`
	`art.sh” - essearch`
		Cloud-Administrator, PeopleSoft Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine Startvorlage für die Auto Scaling Scaling-G ruppe des Webservers.	Wiederholen Sie die vorherigen Schritte, um eine Startvorlage für die Auto Scaling Scaling-G ruppe des Webservers zu erstellen. Benennen Sie die Vorlage`WEB_TEMPLATE` . Wählen Sie in der Vorlage das AMI aus, das Sie für den Webserver erstellt haben.
	• Fügen Sie im Feld Benutzerdaten des Abschnitts Erweiterte Details die folgenden Einträge hinzu. Stellen Sie sicher, dass der Pfad und die Benutzerinformationen korrekt sind. Sie haben das `webstart.sh` Skript in einem vorherigen Schritt erstellt.
	`#! /bin/ksh`
	`su -c “/usr/homes/`
	`hcmdemo/webstart.sh”`
	`- hcmdemo`
		Cloud-Administrator, PeopleSoft Administrator

Auto Scaling Scaling-Gruppen erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Auto Scaling Scaling-Gruppe für den Anwendungsserver.	Erstellen Sie auf der EC2 Amazon-Konsole mithilfe der `PSAPPSRV_TEMPLATE` Vorlage eine Auto Scaling Scaling-Gruppe, die `PSAPPSRV_ASG` für den Anwendungsserver aufgerufen wird. Anweisungen finden Sie in der EC2 Amazon-Dokumentation. • Wählen Sie auf der Seite Instance-Startoptionen auswählen die richtige VPC aus und wählen Sie dann mehrere Subnetze aus verschiedenen Availability Zones aus. • Wählen Sie auf der Seite Erweiterte Optionen konfigurieren keinen Load Balancer aus. • Wählen Sie auf der Seite Gruppengröße und Skalierungsrichtlinien konfigurieren Einstellungen aus, je nachdem, für wie viel Last Sie Ihr System einrichten möchten und ob Sie eine Skalierungsrichtlinie verwenden möchten. Es wird empfohlen, die gewünschte Kapazität	Cloud-Administrator, PeopleSoft Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und Mindestkapazität auf mindestens 2 festzulegen, sodass zu jedem Zeitpunkt mindestens eine Instanz für den Datenverkehr verfügbar ist. Weitere Informationen zu Auto Scaling Scaling-R ichtlinien finden Sie in der EC2 Amazon-Dokumentati on.	
Erstellen Sie Auto Scaling Scaling-Gruppen für die anderen Server.	Wiederholen Sie den vorherigen Schritt, um Auto Scaling Scaling-Gruppen für den Prozessplaner, den Elasticsearch-Server und den Webserver zu erstellen.	Cloud-Administrator, Administr ator PeopleSoft

Zielgruppen erstellen und konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Zielgruppe für den Webserver.	Erstellen Sie auf der EC2 Amazon-Konsole eine Zielgruppe für den Webserver . Anweisungen finden Sie in der Elastic Load Balancing Balancing-Dokumentation. Stellen Sie den Port auf den Port ein, den der Webserver abhört.	Cloud-Administrator
Konfigurieren Sie Integritä tsprüfungen.	Vergewissern Sie sich, dass die Zustandsprüfungen die richtigen Werte haben, um	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ihre Geschäftsanforderungen widerzuspiegeln. Weitere Informationen finden Sie im Elastic Load Balancing-Benutzerhandbuch.	
Erstellen Sie eine Zielgruppe für den Elasticsearch-Server.	Wiederholen Sie die vorherigen Schritte, um eine Zielgruppe mit dem Namen `PSFTSRCH` Elasticsearch-Server zu erstellen, und legen Sie den richtigen Elasticsearch-Port fest.	Cloud-Administrator
Fügen Sie Zielgruppen zu Auto Scaling Scaling-Gruppen hinzu.	Öffnen Sie die Auto Scaling Scaling-Gruppe des Webservers mit dem Namen`PSPIA_ASG` , die Sie zuvor erstellt haben. Wählen Sie auf der Registerkarte Load Balancing die Option Bearbeiten aus und fügen Sie die `PSFTWEB` Zielgruppe dann der Auto Scaling Scaling-Gruppe hinzu. Wiederholen Sie diesen Schritt für die Elasticsearch Auto Scaling Scaling-Gruppe`PSSRCH_ASG` , um die zuvor `PSFTSRCH` erstellte Zielgruppe hinzuzufügen.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie die Dauer der Sitzung fest.	Wählen Sie in der Zielgrupp e `PSFTWEB` die Registerkarte Attribute und dann Bearbeite n aus und legen Sie die Sitzungsbindung fest. Wählen Sie für den Typ „Stickiness“ die Option Load Balancer generated cookie aus und legen Sie die Dauer auf 1 fest. Weitere Informationen finden Sie im Elastic Load Balancing-Benutzerhandbuch. Wiederholen Sie diesen Schritt für die Zielgruppe. `PSFTSRCH`	Cloud-Administrator

Erstellen und konfigurieren Sie Load Balancer für Anwendungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Load Balancer für die Webserver.	Erstellen Sie einen Applicati on Load Balancer mit dem Namen `PSFTLB` für den Lastenausgleich des Datenverkehrs zu den Webservern. Anweisung en finden Sie in der Elastic Load Balancing Balancing-Dokumentation. • Geben Sie den Namen des Load Balancers an. • Für Scheme, wählen Sie Internet-facing.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wählen Sie im Abschnitt Netzwerkzuordnung die richtige VPC und mindesten s zwei öffentliche Subnetze aus verschiedenen Availabil ity Zones aus. • Wählen Sie im Abschnitt Listener und Routing die Zielgruppe aus `PSFTWEB` und geben Sie das richtige Protokoll und die richtige Portnummer an.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Load Balancer für die Elasticsearch-Server.	Erstellen Sie einen Application Load Balancer mit dem Namen für `PSFTSCH` den Lastenausgleich des Datenverkehrs zu den Elasticsearch-Servern. • Geben Sie den Namen des Load Balancers an. • Wählen Sie für Schema die Option Intern aus. • Wählen Sie im Abschnitt Netzwerkzuordnung die richtige VPC und die richtigen privaten Subnetze aus. • Wählen Sie im Abschnitt Listener und Routing die Zielgruppe aus `PSFTSRCH` und geben Sie das richtige Protokoll und die richtige Portnummer an.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Route 53	Erstellen Sie auf der Amazon Route 53 53-Konsole einen Datensatz in der Hosting-Zone, der die PeopleSoft Anwendung bedienen wird. Anweisungen finden Sie in der Dokumentation zu Amazon Route 53 Dadurch wird sichergestellt, dass der gesamte Datenverkehr den Load PSFTLB Balancer durchläuft.	Cloud-Administrator

Zugehörige Ressourcen

- PeopleSoft Oracle-Webseite
- AWS-Dokumentation

Richten Sie die Notfallwiederherstellung für Oracle JD Edwards EnterpriseOne mit AWS Elastic Disaster Recovery ein

Erstellt von Thanigaivel Thirumalai (AWS)

Übersicht

Katastrophen, die durch Naturkatastrophen, Anwendungsausfälle oder Serviceunterbrechungen ausgelöst werden, beeinträchtigen den Umsatz und führen zu Ausfallzeiten von Unternehmensanwendungen. Um die Auswirkungen solcher Ereignisse zu verringern, ist die Planung der Notfallwiederherstellung (DR) für Unternehmen, die EnterpriseOne Enterprise Resource Planning (ERP) -Systeme von JD Edwards und andere betriebs- und geschäftskritische Software einsetzen, von entscheidender Bedeutung.

Dieses Muster erklärt, wie Unternehmen AWS Elastic Disaster Recovery als DR-Option für ihre JD EnterpriseOne Edwards-Anwendungen verwenden können. Außerdem werden die Schritte zur Verwendung von Elastic Disaster Recovery Failover und Failback beschrieben, um eine regionsübergreifende DR-Strategie für Datenbanken zu entwickeln, die auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance in der AWS-Cloud gehostet werden.

> **Note**
>
> Dieses Muster erfordert, dass die primären und sekundären Regionen für die regionsübergreifende DR-Implementierung auf AWS gehostet werden.

Oracle JD Edwards EnterpriseOne ist eine integrierte ERP-Softwarelösung für mittelständische bis große Unternehmen in einer Vielzahl von Branchen.

AWS Elastic Disaster Recovery minimiert Ausfallzeiten und Datenverluste durch eine schnelle, zuverlässige Wiederherstellung von lokalen und cloudbasierten Anwendungen mithilfe von erschwinglichem Speicher, minimalem Rechenaufwand und point-in-time minimaler Wiederherstellung.

AWS bietet vier zentrale DR-Architekturmuster. Dieses Dokument konzentriert sich auf die Einrichtung, Konfiguration und Optimierung mithilfe der Pilot-Light-Strategie. Diese Strategie hilft Ihnen dabei, eine kostengünstigere DR-Umgebung zu schaffen, in der Sie zunächst einen Replikationsserver für die Replikation von Daten aus der Quelldatenbank bereitstellen und den

eigentlichen Datenbankserver erst bereitstellen, wenn Sie eine DR-Installation und Wiederherstellung starten. Durch diese Strategie entfallen die Kosten für die Wartung eines Datenbankservers in der DR-Region. Stattdessen zahlen Sie für eine kleinere EC2 Instance, die als Replikationsserver dient.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine JD EnterpriseOne Edwards-Anwendung, die auf Oracle Database oder Microsoft SQL Server mit einer unterstützten Datenbank in einem laufenden Zustand auf einer verwalteten EC2 Instanz ausgeführt wird. Diese Anwendung sollte alle JD EnterpriseOne Edwards-Basiskomponenten (Enterprise Server, HTML Server und Database Server) enthalten, die in einer AWS-Region installiert sind.
- Eine AWS Identity and Access Management (IAM) -Rolle zur Einrichtung des Elastic Disaster Recovery-Service.
- Das Netzwerk für die Ausführung von Elastic Disaster Recovery wurde gemäß den erforderlichen Konnektivitätseinstellungen konfiguriert.

Einschränkungen

- Sie können dieses Muster verwenden, um alle Stufen zu replizieren, es sei denn, die Datenbank wird auf Amazon Relational Database Service (Amazon RDS) gehostet. In diesem Fall empfehlen wir, die regionsübergreifende Kopierfunktion von Amazon RDS zu verwenden.
- Elastic Disaster Recovery ist nicht mit CloudEndure Disaster Recovery kompatibel, aber Sie können ein Upgrade von CloudEndure Disaster Recovery durchführen. Weitere Informationen finden Sie in den häufig gestellten Fragen in der Elastic Disaster Recovery-Dokumentation.
- Amazon Elastic Block Store (Amazon EBS) begrenzt die Geschwindigkeit, mit der Sie Schnappschüsse erstellen können. Mit Elastic Disaster Recovery können Sie eine maximale Anzahl von 300 Servern in einem einzigen AWS-Konto replizieren. Um mehr Server zu replizieren, können Sie mehrere AWS-Konten oder mehrere AWS-Zielregionen verwenden. (Sie müssen Elastic Disaster Recovery für jedes Konto und jede Region separat einrichten.) Weitere Informationen finden Sie unter Best Practices in der Elastic Disaster Recovery-Dokumentation.
- Die Quell-Workloads (die JD EnterpriseOne Edwards-Anwendung und Datenbank) müssen auf EC2 Instances gehostet werden. Dieses Muster unterstützt keine Workloads, die sich vor Ort oder in anderen Cloud-Umgebungen befinden.

- Dieses Muster konzentriert sich auf die Komponenten von JD Edwards EnterpriseOne . Ein vollständiger DR- und Business Continuity-Plan (BCP) sollte weitere Kerndienste beinhalten, darunter:
  - Netzwerke (virtuelle private Cloud, Subnetze und Sicherheitsgruppen)
  - Active Directory
  - Amazon WorkSpaces
  - Elastic Load Balancing
  - Ein verwalteter Datenbankservice wie Amazon Relational Database Service (Amazon RDS)

Weitere Informationen zu Voraussetzungen, Konfigurationen und Einschränkungen finden Sie in der Elastic Disaster Recovery-Dokumentation.

Produktversionen

- Oracle JD Edwards EnterpriseOne (von Oracle und SQL Server unterstützte Versionen, die auf den technischen Mindestanforderungen von Oracle basieren)

Architektur

Zieltechnologie-Stack

- Eine einzige Region und eine einzige Virtual Private Cloud (VPC) für Produktion und Nichtproduktion sowie eine zweite Region für DR
- Single Availability Zones, um eine geringe Latenz zwischen Servern zu gewährleisten
- Ein Application Load Balancer, der den Netzwerkverkehr verteilt, um die Skalierbarkeit und Verfügbarkeit Ihrer Anwendungen auf mehrere Availability Zones zu verbessern
- Amazon Route 53 zur Bereitstellung der DNS-Konfiguration (Domain Name System)
- Amazon bietet WorkSpaces Benutzern ein Desktop-Erlebnis in der Cloud
- Amazon Simple Storage Service (Amazon S3) zum Speichern von Backups, Dateien und Objekten
- Amazon CloudWatch für Anwendungsprotokollierung, Überwachung und Alarme
- Amazon Elastic Disaster Recovery für die Notfallwiederherstellung

Zielarchitektur

Das folgende Diagramm zeigt die regionsübergreifende Disaster Recovery-Architektur für JD Edwards EnterpriseOne unter Verwendung von Elastic Disaster Recovery.

Verfahren

Hier finden Sie einen Überblick über den Prozess auf hoher Ebene. Einzelheiten finden Sie im Abschnitt Epics.

- Die Elastic Disaster Recovery-Replikation beginnt mit einer ersten Synchronisierung. Während der ersten Synchronisierung repliziert der AWS Replication Agent alle Daten von den Quellfestplatten auf die entsprechende Ressource im Staging-Bereich-Subnetz.
- Die kontinuierliche Replikation wird auf unbestimmte Zeit fortgesetzt, nachdem die erste Synchronisierung abgeschlossen ist.
- Sie überprüfen die Startparameter, zu denen servicespezifische Konfigurationen und eine EC2 Amazon-Startvorlage gehören, nachdem der Agent installiert und die Replikation gestartet wurde. Wenn angezeigt wird, dass der Quellserver für die Wiederherstellung bereit ist, können Sie Instances starten.
- Wenn Elastic Disaster Recovery eine Reihe von API-Aufrufen ausgibt, um den Startvorgang zu starten, wird die Wiederherstellungsinstanz gemäß Ihren Starteinstellungen sofort auf AWS gestartet. Der Service richtet beim Start automatisch einen Konvertierungsserver ein.
- Die neue Instance wird nach Abschluss der Konvertierung auf AWS hochgefahren und ist einsatzbereit. Der Status des Quellservers zum Zeitpunkt des Starts wird durch die Volumes dargestellt, die der gestarteten Instance zugeordnet sind. Der Konvertierungsprozess beinhaltet Änderungen an den Treibern, dem Netzwerk und der Betriebssystemlizenz, um sicherzustellen, dass die Instance nativ auf AWS gestartet wird.
- Nach dem Start werden die neu erstellten Volumes nicht mehr mit den Quellservern synchronisiert. Der AWS Replication Agent repliziert weiterhin routinemäßig Änderungen, die an Ihren Quellservern vorgenommen wurden, auf die Volumes im Staging-Bereich, aber die gestarteten Instances spiegeln diese Änderungen nicht wider.
- Wenn Sie eine neue Drill- oder Recovery-Instance starten, werden die Daten immer im neuesten Status wiedergegeben, der vom Quellserver in das Staging-Area-Subnetz repliziert wurde.
- Wenn der Quellserver als für die Wiederherstellung vorbereitet markiert ist, können Sie Instanzen starten.

> **Note**
>
> Der Prozess funktioniert in beide Richtungen: für ein Failover von einer primären AWS-Region zu einer DR-Region und für ein Failback zum primären Standort, wenn dieser wiederhergestellt wurde. Sie können sich auf ein Failback vorbereiten, indem Sie die Richtung der Datenreplikation vom Zielcomputer zurück zum Quellcomputer auf vollständig orchestrierte Weise umkehren.

Zu den Vorteilen dieses in diesem Muster beschriebenen Prozesses gehören:

- Flexibilität: Replikationsserver werden je nach Datensatz und Replikationszeit nach oben und unten skaliert, sodass Sie DR-Tests durchführen können, ohne die Quell-Workloads oder die Replikation zu unterbrechen.
- Zuverlässigkeit: Die Replikation ist robust, unterbrechungsfrei und kontinuierlich.
- Automatisierung: Diese Lösung bietet einen einheitlichen, automatisierten Prozess für Test, Wiederherstellung und Failback.
- Kostenoptimierung: Sie können nur die benötigten Volumes replizieren und dafür bezahlen und für Rechenressourcen am DR-Standort nur bezahlen, wenn diese Ressourcen aktiviert sind. Sie können eine kostenoptimierte Replikationsinstanz (wir empfehlen, einen rechenoptimierten Instance-Typ zu verwenden) für mehrere Quellen oder eine einzelne Quelle mit einem großen EBS-Volume verwenden.

Automatisierung und Skalierung

Wenn Sie eine Notfallwiederherstellung in großem Umfang durchführen, sind die JD EnterpriseOne Edwards-Server von anderen Servern in der Umgebung abhängig. Zum Beispiel:

- JD EnterpriseOne Edwards-Anwendungsserver, die beim Booten eine Verbindung zu einer von JD Edwards EnterpriseOne unterstützten Datenbank herstellen, sind von dieser Datenbank abhängig.
- JD EnterpriseOne Edwards-Server, die eine Authentifizierung erfordern und beim Booten eine Verbindung zu einem Domänencontroller herstellen müssen, um Dienste zu starten, sind vom Domänencontroller abhängig.

Aus diesem Grund empfehlen wir, Failover-Aufgaben zu automatisieren. Sie können beispielsweise AWS Lambda oder AWS Step Functions verwenden, um die JD EnterpriseOne Edwards-Startskripts

und Load Balancer-Änderungen zu automatisieren, um den end-to-end Failover-Prozess zu automatisieren. Weitere Informationen finden Sie im Blogbeitrag Erstellen eines skalierbaren Notfallwiederherstellungsplans mit AWS Elastic Disaster Recovery.

Tools

AWS-Services

- Amazon Elastic Block Store (Amazon EBS) bietet Speichervolumes auf Blockebene zur Verwendung mit Instances. EC2
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- AWS Elastic Disaster Recovery minimiert Ausfallzeiten und Datenverluste durch schnelle, zuverlässige Wiederherstellung von lokalen und cloudbasierten Anwendungen mit erschwinglichem Speicher, minimalem Rechenaufwand und point-in-time minimaler Wiederherstellung.
- Amazon Virtual Private Cloud (Amazon VPC) gibt Ihnen die volle Kontrolle über Ihre virtuelle Netzwerkumgebung, einschließlich Ressourcenplatzierung, Konnektivität und Sicherheit.

Bewährte Methoden

Allgemeine bewährte Methoden

- Halten Sie einen schriftlichen Plan bereit, was im Falle eines echten Wiederherstellungsereignisses zu tun ist.
- Nachdem Sie Elastic Disaster Recovery korrekt eingerichtet haben, erstellen Sie eine CloudFormation AWS-Vorlage, mit der die Konfiguration bei Bedarf bei Bedarf erstellt werden kann. Legen Sie die Reihenfolge fest, in der Server und Anwendungen gestartet werden sollen, und notieren Sie dies im Wiederherstellungsplan.
- Führen Sie eine regelmäßige Übung durch (es gelten die EC2 Standardtarife von Amazon).
- Überwachen Sie den Zustand der laufenden Replikation mithilfe der Elastic Disaster Recovery-Konsole oder programmgesteuert.
- Schützen Sie die point-in-time Snapshots und bestätigen Sie dies, bevor Sie die Instances beenden.
- Erstellen Sie eine IAM-Rolle für die Installation von AWS Replication Agent.

- Aktivieren Sie den Kündigungsschutz für Wiederherstellungsinstanzen in einem echten DR-Szenario.
- Verwenden Sie die Aktion Verbindung zu AWS trennen in der Elastic Disaster Recovery-Konsole nicht für Server, für die Sie Wiederherstellungsinstanzen gestartet haben, auch nicht bei einem echten Wiederherstellungsereignis. Wenn Sie die Verbindung trennen, werden alle Replikationsressourcen im Zusammenhang mit diesen Quellservern beendet, einschließlich Ihrer point-in-time (PIT-) Wiederherstellungspunkte.
- Ändern Sie die PIT-Richtlinie, um die Anzahl der Tage für die Aufbewahrung von Snapshots zu ändern.
- Bearbeiten Sie die Startvorlage in den Starteinstellungen von Elastic Disaster Recovery, um das richtige Subnetz, die richtige Sicherheitsgruppe und den richtigen Instance-Typ für Ihren Zielserver festzulegen.
- Automatisieren Sie den end-to-end Failover-Prozess, indem Sie Lambda oder Step Functions verwenden, um die EnterpriseOne Startskripte von JD Edwards und Änderungen am Load Balancer zu automatisieren.

Optimierung und Überlegungen zu JD Edwards EnterpriseOne

- Wechseln Sie PrintQueuein die Datenbank.
- Gehen Sie MediaObjectsin die Datenbank.
- Schließt die Protokolle und den temporären Ordner von den Batch- und Logikservern aus.
- Schließen Sie den temporären Ordner aus Oracle aus. WebLogic
- Erstellen Sie Skripts für den Start nach dem Failover.
- Schließen Sie die tempdb für SQL Server aus.
- Schließen Sie die temporäre Datei für Oracle aus.

Epen

Führen Sie die ersten Aufgaben und die Konfiguration durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie das Replikati onsnetzwerk ein.	Implementieren Sie Ihr JD EnterpriseOne Edwards-S	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ystem in der primären AWS-Region und identifizieren Sie die AWS-Region für DR. Folgen Sie den Schritten im Abschnitt Anforderungen an das Replikationsnetzwerk in der Elastic Disaster Recovery-Dokumentation, um Ihr Replikations- und DR-Netzwerk zu planen und einzurichten.	
Ermitteln Sie RPO und RTO.	Identifizieren Sie das Recovery Time Objective (RTO) und das Recovery Point Objective (RPO) für Ihre Anwendungsserver und Datenbank.	Cloud-Architekt, DR-Architekt
Aktivieren Sie die Replikation für Amazon EFS.	Aktivieren Sie gegebenen falls die Replikation von der AWS-Primärregion zur DR-Region für gemeinsam genutzte Dateisysteme wie Amazon Elastic File System (Amazon EFS) mithilfe von AWS DataSync, rsync oder einem anderen geeigneten Tool.	Cloud-Administrator
DNS verwalten im Fall von DR	Identifizieren Sie den Prozess zur Aktualisierung des Domain Name Systems (DNS) während der DR-Übung oder bei der eigentlichen DR	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle für die Einrichtung.	Folgen Sie den Anweisungen im Abschnitt Initialisierung und Berechtigungen von Elastic Disaster Recovery der Elastic Disaster Recovery-Dokumentation, um eine IAM-Rolle zur Initialisierung und Verwaltung des AWS-Service zu erstellen.	Cloud-Administrator
Richten Sie VPC-Peering ein.	Stellen Sie sicher, dass Quelle und Ziel per VPCs Peering miteinander verbunden sind und aufeinander zugreifen können. Anweisungen zur Konfiguration finden Sie in der Amazon VPC-Dokumentation.	AWS-Administrator

Konfigurieren Sie die Elastic Disaster Recovery-Replikationseinstellungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initialisieren Sie Elastic Disaster Recovery.	Öffnen Sie die Elastic Disaster Recovery-Konsole, wählen Sie die AWS-Zielregion aus (in der Sie Daten replizieren und Wiederherstellungsinstanzen starten werden) und wählen Sie dann Standard-Replikationseinstellungen festlegen aus.	AWS-Administrator
Richten Sie Replikationsserver ein.	1. Geben Sie im Bereich Replikationsserver einrichten den Staging-Bereich, das Subnetz und den Instanzty	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	p des Replikationsservers ein. Standardmäßig ist der Instance-Typ `t3.small` ausgewählt. Konfiguri eren Sie diese Einstellu ng entsprechend Ihren Anforderungen und denken Sie daran, die Instance-Preise zu berücksichtigen. Weitere Informationen finden Sie unter EC2 Amazon-Preise. 2. Wählen Sie im Abschnitt Servicezugriff die Option Details anzeigen aus, um die mit dem Service verknüpfte Rolle und zusätzliche Richtlinien zu überprüfen, die während der Serviceinitialisierung erstellt wurden. 3. Wählen Sie Weiter aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Volumes und Sicherheitsgruppen.	1. Wählen Sie im Bereich Volumes und Sicherheitsgruppen den EBS-Volume-Typ für den Replikationsserver aus und setzen Sie die Amazon EBS-Verschlüsselung auf Standard. 2. Wählen Sie Immer die Sicherheitsgruppe AWS Elastic Disaster Recovery verwenden aus, damit Elastic Disaster Recovery die Standardsicherheitsgruppe automatisch anhängt und überwacht. 3. Wählen Sie Weiter aus.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie zusätzliche Einstellungen.	1. Konfigurieren Sie im Bereich Zusätzliche Einstellungen das Routing und die Drosselung von Daten, die PIT-Richtlinie und Tags. • Datenrouting und Drosselung steuern, wie Daten vom externen Server zu den Replikationsservern fließen. Wählen Sie Private IP für die Datenreplikation verwenden. Andernfalls wird den Replikationsservern automatisch eine öffentliche IP zugewiesen, und die Daten werden über das öffentliche Internet übertragen. • Konfigurieren Sie im Abschnitt Point-in-Time-Richtlinie (PIT) eine Aufbewahrungsrichtlinie, die festlegt, nach welcher Dauer keine Snapshots mehr benötigt werden. Der Standardaufbewahrungszeitraum beträgt sieben Tage. • Fügen Sie im Abschnitt Tags benutzerdefinierte Tags zu Ressourcen	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	hinzu, die von Elastic Disaster Recovery in Ihrem AWS-Konto erstellt wurden. 2. Wählen Sie Weiter, überprüfen Sie die Einstellungen im nächsten Bereich und wählen Sie dann Create default, um die Standardvorlage zu erstellen.	

Installieren Sie den AWS Replication Agent

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle.	Erstellen Sie eine IAM-Rolle, die die `AWSElasticDisasterRecoveryAgentInstallationPolicy` Richtlinie enthält. Aktivieren Sie im Abschnitt AWS-Zugriffstyp auswählen den programmatischen Zugriff. Notieren Sie sich die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel. Sie benötigen diese Informationen während der Installation des AWS Replication Agent.	AWS-Administrator
Überprüfen Sie die Anforderungen.	Überprüfen und erfüllen Sie die Voraussetzungen in der Elastic Disaster Recovery-	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dokumentation für die Installation des AWS Replication Agent.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den AWS Replication Agent.	Folgen Sie den Installationsanweisungen für Ihr Betriebssystem und installieren Sie den AWS Replication Agent. • Für Microsoft Windows: Laden Sie die Setup-Dateien herunter und führen Sie die EXE-Datei als Administrator aus. Beantworten Sie die Anweisungen, um die Installation abzuschließen. • Für Linux: Kopieren Sie die folgenden Befehle (in der angegebenen Reihenfolge) und fügen Sie sie in Ihre Secure Shell (SSH) -Sitzung ein. Mit dem ersten Befehl wird das Installationsprogramm heruntergeladen und mit dem zweiten Befehl wird es ausgeführt. `wget -O ./aws-replication-installer-init.py https://aws-elastic-disaster-recovery-us-west-2.s3.amazonaws.com/latest/linux/aws-replication-installer-init.py`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`sudo python3 aws-replication-installer-init.py` Beantworten Sie die Anweisungen, um die Installation abzuschließen. **Note** Ändern Sie die URL so, dass sie Ihrer Region entspricht. Wiederholen Sie diese Schritte für den verbleibenden Server.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überwachen Sie die Replikation.	Kehren Sie zum Bereich Elastic Disaster Recovery Source Servers zurück, um den Replikationsstatus zu überwachen. Die erste Synchronisierung wird je nach Größe der Datenübertragung einige Zeit in Anspruch nehmen. Wenn der Quellserver vollständig synchronisiert ist, wird der Serverstatus auf Bereit aktualisiert. Das bedeutet, dass im Staging-Bereich ein Replikationsserver erstellt wurde und die EBS-Volumes vom Quellserver in den Staging-Bereich repliziert wurden.	AWS-Administrator

Starteinstellungen konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bearbeiten Sie die Starteinstellungen.	Um die Starteinstellungen für die Drill- und Recovery-Instances zu aktualisieren, wählen Sie in der Elastic Disaster Recovery-Konsole den Quellserver aus und klicken Sie dann auf Aktionen, Starteinstellungen bearbeiten. Oder Sie können Ihre replizier	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	enden Quellcomputer auf der Seite Quellserver auswählen und dann den Tab Starteins tellungen wählen. Diese Registerkarte besteht aus zwei Abschnitten: Allgemein e Starteinstellungen und EC2 Startvorlage.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die allgemeinen Starteinstellungen.	Überarbeiten Sie die allgemeinen Starteinstellungen entsprechend Ihren Anforderungen. • Richtige Dimensionierung des Instance-Typs: Wenn Sie Basic wählen, umgeht Elastic Disaster Recovery den Instance-Typ, den Sie in der EC2 Amazon-Startvorlage ausgewählt haben, und wählt den Instance-Typ automatisch basierend auf dem Betriebssystem, der CPU und dem RAM des Quellservers aus. • Private IP kopieren: Wählen Sie aus, ob Elastic Disaster Recovery sicherstellen soll, dass die von der Drill- oder Recovery-Instance verwendete private IP mit der vom Quellserver verwendeten privaten IP übereinstimmt. Wenn Sie Ja wählen, stellen Sie sicher, dass der IP-Bereich des Subnetzes, das Sie in der EC2 Amazon-Startvorlage festgelegt haben, die private IP-Adresse enthält.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter Allgemeine Starteinstellungen in der Elastic Disaster Recovery-Dokumentation.	
Konfigurieren Sie die EC2 Amazon-Startvorlage.	Elastic Disaster Recovery verwendet EC2 Amazon-Startvorlagen, um Drill- und Recovery-Instances für jeden Quellserver zu starten. Die Startvorlage wird automatisch für jeden Quellserver erstellt, den Sie nach der Installation des AWS Replication Agent zu Elastic Disaster Recovery hinzufügen. Sie müssen die EC2 Amazon-Startvorlage als Standard-Startvorlage festlegen, wenn Sie sie mit Elastic Disaster Recovery verwenden möchten. Weitere Informationen finden Sie unter EC2 Launch Template in der Elastic Disaster Recovery-Dokumentation.	AWS-Administrator

DR-Drill und Failover einleiten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Drill einleiten	1. Öffnen Sie auf der Elastic Disaster Recovery-Konsole die Seite Quellserver und überprüfen Sie, ob der Status des Quellservers Bereit ist. 2. Wählen Sie alle Quellserver aus, für die Sie den DR-Drill durchführen möchten. 3. Wählen Sie im Menü Wiederherstellungsauftrag initiieren die Option Drill initiieren und wählen Sie den entsprechenden point-in-time Snapshot aus. Dadurch wird ein Wiederherstellungsauftrag für die ausgewählten Quellserver gestartet. Sie können den Status des Jobs auf der Registerkarte Verlauf der Wiederherstellungsaufträge überwachen. Die gestartete Drill-Instance wird auch auf der Seite Wiederherstellungsinstanzen angezeigt. **Note** Weitere Änderungen am Quellserver	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	werden mit dem Replikationsserver synchronisiert, nicht mit der Drill-Ins tance. 4. Testen und verifizieren Sie die DR-Drill-Instance. 5. Wählen Sie auf der Seite Wiederherstellungs instanzen die Drill-Instance aus und klicken Sie dann auf Aktionen, Verbindung zu AWS trennen. Dadurch wird der AWS Replication Agent aus der Wiederher stellungsinstanz und alle mit der Wiederher stellungsinstanz verknüpft en Ressourcen aus Elastic Disaster Recovery gelöscht. 6. Wählen Sie Wiederher stellungsinstanzen löschen aus. Dadurch wird die Darstellung der Instanz aus der Elastic Disaster Recovery-Konsole gelöscht und die Instance vollständ ig vom Elastic Disaster Recovery-Dienst getrennt. Die zugrunde liegende EC2 Instance wird dadurch nicht gelöscht.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Beenden Sie die DR-Drill-Instance von der EC2 Amazon-Konsole aus. Weitere Informationen finden Sie unter Preparing for Failover in der Elastic Disaster Recovery-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie die Übung.	Im vorherigen Schritt haben Sie neue Ziel-Instances in der DR-Region gestartet. Die Ziel-Instances sind Replikate der Quellserver, die auf dem Snapshot basieren, der bei der Initiierung des Starts erstellt wurde. In diesem Verfahren stellen Sie eine Verbindung zu Ihren EC2 Amazon-Zielcomputern her, um zu überprüfen, ob sie wie erwartet laufen. 1. Öffnen Sie die EC2 Amazon-Konsole. 2. Wählen Sie Instances (running). 3. Wählen Sie die Zielinstanz aus und notieren Sie sich ihre private IPv4 Adresse. 4. Stellen Sie sicher, dass Sie eine Verbindung zur EC2 Instanz herstellen können und dass JD Edwards EnterpriseOne und die zugehörigen Komponenten erwartungsgemäß repliziert werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initiieren Sie einen Failover.	Ein Failover ist die Umleitung des Datenverkehrs von einem Primärsystem zu einem Sekundärsystem. Elastic Disaster Recovery unterstützt Sie bei der Durchführung eines Failovers, indem es Wiederherstellungsinstanzen auf AWS startet. Wenn die Wiederherstellungsinstanzen gestartet wurden, leiten Sie den Datenverkehr von Ihren Primärsystemen zu diesen Instances um. 1. Öffnen Sie in der Elastic Disaster Recovery-Konsole die Seite Quellserver und vergewissern Sie sich, dass in der Spalte Bereit zur Wiederherstellung für den Quellserver Ready und in der Spalte Data Replication-Status Healthy angezeigt wird. 2. Wählen Sie den Quellserver aus. Wählen Sie im Menü Wiederherstellungsauftrag initiieren die Option Wiederherstellung initiieren aus. 3. Wählen Sie den point-in-time Snapshot aus, von dem aus die Wiederher	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	stellungsinstanz gestartet werden soll, und wählen Sie dann Wiederherstellung initiieren aus. Dadurch wird ein Wiederherstellungsjob gestartet. Sie können den Status des Jobs auf der Seite Wiederherstellungsinstanzen überwachen. 4. Testen und verifizieren Sie die Wiederherstellungsinstanz. Passen Sie bei Bedarf die DNS-Konfiguration an und verbinden Sie Ihre JD EnterpriseOne Edwards-Anwendung mit der Datenbank. 5. Sie können jetzt die Verbindung zum JD EnterpriseOne Edwards-Quellserver trennen und ihn außer Betrieb nehmen, da alle Änderungen in die neue Wiederherstellungsinstanz geschrieben wurden. 6. Registrieren Sie die Wiederherstellungsinstanz als Quellserver in der DR-Region, indem Sie den im Abschnitt Install the AWS Replication Agent beschriebenen Prozess befolgen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter Durchführen eines Failovers in der Elastic Disaster Recovery-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initiieren Sie ein Failback.	Das Verfahren zum Initiiere n eines Failbacks ähnelt dem Verfahren zum Initiieren eines Failovers. 1. Öffnen Sie die Elastic Disaster Recovery-Konsole in der primären Region. Navigieren Sie zur Seite Wiederherstellungs instanzen, wählen Sie die Drill-Instance aus und wählen Sie dann Actions, Disconnect from AWS, Delete Recovery Instances aus. 2. Öffnen Sie die Elastic Disaster Recovery-Konsole in der DR-Region. Registrie ren Sie Ihren neuen JD EnterpriseOne Edwards-Server als Quellserver in der DR-Region, indem Sie den AWS Replicati on Agent installieren. Die Daten werden mit einem neuen Replikationsserver synchronisiert, der im neuen Staging-Subnetz bereitgestellt wird. **Note** Wenn der neue JD EnterpriseOne	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Edwards-Server als Quellserver registrie rt ist, sehen Sie in der Elastic Disaster Recovery-Konsole möglicherweise zwei Quellserver: einen Server, der aus der primären EC2 Instance erstellt wurde, und den neuen Server, der aus der Wiederher stellungsinstanz erstellt wurde. Wir empfehlen, die Server korrekt zu taggen, um Verwirrung zu vermeiden, und den neuen Server vorzugsweise zur Startvorlage hinzuzufügen. 3. Um die DR-Replikation von der primären Region aus neu zu starten, trennen Sie die gestartete Wiederher stellungsinstanz von der Elastic Disaster Recovery-Konsole in der DR-Region und registrieren Sie den	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Host als Quellserver in der primären Region. Weitere Informationen finden Sie unter Durchführen eines Failbacks in der Elastic Disaster Recovery-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Enterpris eOne Komponenten von JD Edwards.	1. Starten Sie die JD EnterpriseOne Edwards-D atenbank, indem Sie sich beim Datenbankserver anmelden. 2. Wenn die Datenbank läuft, starten Sie die JD Enterpris eOne Edwards-Logik- und Batchserver. 3. Starten Sie WebLogic auf den Webservern und starten Sie eine JAS-Insta nz auf den JAS-Servern. 4. Starten Sie WebLogic auf dem Provisionsserver und auf dem Server für die SM-Konsole. 5. Starten Sie SM Agent auf den Servern. 6. Vergewissern Sie sich, dass die Anmeldung bei JD Edwards korrekt Enterpris eOne funktioniert. Sie müssen die Änderungen in Route 53 und Application Load Balancer integrieren, damit der JD EnterpriseOne Edwards-L ink funktioniert. Sie können diese Schritte mithilfe von Lambda, Step Functions und Systems	J.D. Edwards CNC Enterpris eOne

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Manager (Run Command) automatisieren. **Note** Elastic Disaster Recovery führt die Replikation der EBS-Volumes der EC2 Quellinstanz auf Blockebene durch, die das Betriebssystem und die Dateisysteme hosten. Gemeinsam genutzte Dateisyst eme, die mithilfe von Amazon EFS erstellt wurden, sind nicht Teil dieser Replikation. Sie können gemeinsam genutzte Dateisyst eme mithilfe von AWS in die DR-Region replizieren DataSync, wie im ersten Epos erwähnt, und diese replizierten Dateisyst eme dann im DR-System mounten.	

Fehlerbehebung

Problem	Lösung
Der Status der Datenreplikation auf dem Quellserver ist Blockiert und die Replikation verzögert sich. Wenn Sie die Details überprüfen, wird im Datenreplikationsstatus „Agent nicht gesehen“ angezeigt.	Vergewissern Sie sich, dass der gestoppte Quellserver läuft. **Note** Wenn der Quellserver ausfällt, wird der Replikationsserver automatisch beendet. Weitere Informationen zu Verzögerungsproblemen finden Sie unter Probleme mit der Replikationsverzögerung in der Elastic Disaster Recovery-Dokumentation.
Die Installation des AWS Replication Agent in der EC2 Quellinstanz schlägt in RHEL 8.2 nach dem Scannen der Festplatten fehl. `aws_replication_agent_installer.log` zeigt, dass Kernel-Header fehlen.	Bevor Sie den AWS Replication Agent auf RHEL 8, CentOS 8 oder Oracle Linux 8 installieren, führen Sie Folgendes aus: `sudo yum install elfutils-libelf-devel` Weitere Informationen finden Sie in den Linux-Installationsanforderungen in der Elastic Disaster Recovery-Dokumentation.
Auf der Elastic Disaster Recovery-Konsole wird der Quellserver als Bereit mit einer Verzögerung und der Datenreplikationsstatus als Blockiert angezeigt. Je nachdem, wie lange der AWS Replication Agent nicht verfügbar war, kann der Status auf	Verwenden Sie einen Betriebssystembefehl, um zu bestätigen, dass der AWS Replication Agent in der EC2 Quell-Instance ausgeführt wird, oder um zu bestätigen, dass die Instance läuft. Nachdem Sie alle Probleme behoben haben, startet Elastic Disaster Recovery den

Problem	Lösung
eine hohe Verzögerung hinweisen, aber das Problem bleibt dasselbe.	Scanvorgang erneut. Warten Sie, bis alle Daten synchronisiert wurden und der Replikationsstatus Fehlerfrei ist, bevor Sie eine DR-Übung starten.
Erste Replikation mit hoher Verzögerung. Auf der Elastic Disaster Recovery-Konsole können Sie sehen, dass der anfängliche Synchronisierungsstatus für einen Quellserver extrem langsam ist.	Suchen Sie nach den Problemen mit der Replikationsverzögerung, die im Abschnitt Probleme mit der Replikationsverzögerung in der Elastic Disaster Recovery-Dokumentation dokumentiert sind. Der Replikationsserver kann die Last aufgrund systemeigener Rechenoperationen möglicherweise nicht bewältigen. Versuchen Sie in diesem Fall, den Instance-Typ nach Rücksprache mit dem technischen Support-Team von AWS zu aktualisieren.

Zugehörige Ressourcen

- AWS Elastic Disaster Recovery-Benutzerhandbuch
- Erstellung eines skalierbaren Notfallwiederherstellungsplans mit AWS Elastic Disaster Recovery (AWS-Blogbeitrag)
- AWS Elastic Disaster Recovery — Eine technische Einführung (AWS Skill Builder-Kurs; Anmeldung erforderlich)
- Kurzanleitung für AWS Elastic Disaster Recovery

Richten Sie die AWS CloudFormation Drifterkennung in einer Organisation mit mehreren Regionen und mehreren Konten ein

Erstellt von Ram Kandaswamy (AWS)

Übersicht

Benutzer von Amazon Web Services (AWS) suchen häufig nach einer effizienten Methode, um Diskrepanzen in der Ressourcenkonfiguration, einschließlich Abweichungen in AWS CloudFormation Stacks, zu erkennen und diese so schnell wie möglich zu beheben. Dies ist insbesondere der Fall, wenn es verwendet AWS Control Tower wird.

Dieses Muster bietet eine präskriptive Lösung, mit der das Problem effizient gelöst werden kann, indem konsolidierte Änderungen an der Ressourcenkonfiguration verwendet und auf diese Änderungen reagiert werden, um Ergebnisse zu erzielen. Die Lösung ist für Szenarien konzipiert, in denen mehrere AWS CloudFormation Stapel in mehr als einem Konto oder in mehr als einem AWS-Region Konto oder einer Kombination aus beidem erstellt werden. Die Lösung hat folgende Ziele:

- Vereinfachen Sie den Prozess zur Drifterkennung
- Richten Sie Benachrichtigungen und Warnmeldungen ein
- Richten Sie eine konsolidierte Berichterstattung ein

Voraussetzungen und Einschränkungen

Voraussetzungen

- AWS Config ist in allen Regionen und Konten aktiviert, die überwacht werden müssen

Einschränkungen

- Der generierte Bericht unterstützt nur die Ausgabeformate Kommagetrennte Werte (CSV) und JSON.

Architektur

Das folgende Diagramm zeigt die AWS Organizations Einrichtung mit mehreren Konten. AWS Config Regeln kommunizieren zwischen den Konten.

Der Workflow umfasst die folgenden Schritte:

1. Die AWS Config Regel erkennt Abweichungen.
2. Ergebnisse der Drift-Erkennung, die in anderen Konten gefunden wurden, werden an das Verwaltungskonto gesendet.
3. Die CloudWatch Amazon-Regel ruft eine AWS Lambda Funktion auf.
4. Die Lambda-Funktion fragt die AWS Config Regel nach aggregierten Ergebnissen ab.
5. Die Lambda-Funktion benachrichtigt Amazon Simple Notification Service (Amazon SNS), der eine E-Mail-Benachrichtigung über die Abweichung sendet.

Automatisierung und Skalierung

Die hier vorgestellte Lösung kann sowohl für zusätzliche Regionen als auch für Konten skaliert werden.

Tools

AWS-Services

- AWS Configbietet einen detaillierten Überblick über die Konfiguration der AWS Ressourcen in Ihrem AWS-Konto. Dazu gehört auch, wie die Ressourcen jeweils zueinander in Beziehung stehen und wie sie in der Vergangenheit konfiguriert wurden, damit Sie sehen können, wie sich die Konfigurationen und Beziehungen im Laufe der Zeit verändern.
- Amazon CloudWatch hilft Ihnen dabei, die Kennzahlen Ihrer AWS Ressourcen und der Anwendungen, auf denen Sie laufen, AWS in Echtzeit zu überwachen.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.

Epen

Automatisieren Sie die Drifterkennung für AWS CloudFormation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Aggregator.	1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole unter https://console.aws.amazon.com/config. 2. Erstellen Sie einen Aggregator im Verwaltungskonto. 3. Stellen Sie sicher, dass die Datenreplikation aktiviert ist, damit Daten von den Quellkonten abgerufen werden AWS Config können. 4. Wählen Sie alle zutreffenden den Regionen und Konten aus. Sie können Konten basierend auf auswählen AWS Organizations. Wir empfehlen diesen Ansatz, da neue Konten in der Organisation automatisch Teil des Aggregators sind.	Cloud-Architekt
Erstellen Sie eine AWS verwaltete Regel.	Fügen Sie die `cloudformation-stack-drift-detection-check` AWS verwaltete Regel hinzu. Die Regel benötigt einen	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Parameterwert:`cloudformationArn` . Geben Sie die IAM-Rolle Amazon Resource Name (ARN) ein, die berechtigt ist, Stack-Drift zu erkennen. Die Rolle muss über eine Vertrauensrichtlinie verfügen, die es ermöglicht, die Rolle AWS Config zu übernehmen.	
Erstellen Sie den Abschnitt für erweiterte Abfragen des Aggregators.	Um driftete Stapel aus mehreren Quellen abzurufen , erstellen Sie die folgende Abfrage: `SELECT resourceId, configuration.driftInformation.stackDriftStatus WHERE resourceType = 'AWS::CloudFormation::Stack' AND configuration.driftInformation.stackDriftStatus IN ('DRIFTED')`	Cloud-Architekt, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Automatisieren Sie die Ausführung der Abfrage und veröffentlichen Sie sie.	1. Erstellen Sie eine Lambda-Funktion mithilfe des angehängten Codes. Lambda veröffentlicht die Ergebnisse in einem SNS-Thema, das als Umgebungsvariable in der Lambda-Funktion bereitgestellt wird. 2. Um Benachrichtigungen zu erhalten, erstellen Sie ein E-Mail-Abonnement für das SNS-Thema.	Cloud-Architekt, Entwickler
Erstellen Sie eine CloudWatch Regel.	Erstellen Sie eine zeitplanbasierte CloudWatch Regel, um die Lambda-Funktion aufzurufen, die für die Alarmierung zuständig ist.	Cloud-Architekt

Zugehörige Ressourcen

Ressourcen

- Was ist AWS Config?
- Datenaggregation für mehrere Konten und mehrere Regionen
- Erkennung nicht verwalteter Konfigurationsänderungen an Stacks und Ressourcen
- IAM: Übergeben Sie eine IAM-Rolle an einen bestimmten AWS-Service
- Was ist Amazon SNS?

Zusätzliche Informationen

Überlegungen

Wir empfehlen, die in diesem Muster vorgestellte Lösung zu verwenden, anstatt benutzerdefinierte Lösungen zu verwenden, die API-Aufrufe in bestimmten Intervallen beinhalten, um die Drifterkennung für jeden CloudFormation Stack oder Stack-Set zu initiieren. Benutzerdefinierte Lösungen, die API-Aufrufe in bestimmten Intervallen verwenden, können zu einer großen Anzahl von API-Aufrufen führen und die Leistung beeinträchtigen. Aufgrund der Anzahl der API-Aufrufe kann es zu einer Drosselung kommen. Ein weiteres potenzielles Problem ist eine Verzögerung bei der Erkennung, wenn Ressourcenänderungen nur anhand eines Zeitplans erkannt werden.

Da Stack-Sets aus Stapeln bestehen, können Sie diese Lösung verwenden. Details zur Stack-Instanz sind auch als Teil der Lösung verfügbar.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Erfolgreicher Import eines S3-Buckets als CloudFormation AWS-Stack

Erstellt von Ram Kandaswamy (AWS)

Übersicht

Wenn Sie Amazon Web Services (AWS) -Ressourcen wie Amazon Simple Storage Service (Amazon S3) -Buckets verwenden und einen Infrastructure-as-Code-Ansatz (IaC) verwenden möchten, können Sie Ihre Ressourcen in AWS importieren CloudFormation und als Stack verwalten.

Dieses Muster enthält Schritte für den erfolgreichen Import eines S3-Buckets als CloudFormation AWS-Stack. Durch die Verwendung des Ansatzes dieses Musters können Sie mögliche Fehler vermeiden, die auftreten können, wenn Sie Ihren S3-Bucket in einer einzigen Aktion importieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine bestehende S3-Bucket- und S3-Bucket-Richtlinie. Weitere Informationen dazu finden Sie im AWS Knowledge Center unter Welche S3-Bucket-Richtlinie sollte ich verwenden, um die AWS Config-Regel s3- bucket-ssl-requests-only einzuhalten.
- Ein vorhandener AWS Key Management Service (AWS KMS) -Schlüssel und sein Alias. Weitere Informationen dazu finden Sie unter Working with Aliases in der AWS KMS KMS-Dokumentation.
- Die `CloudFormation-template-S3-bucket` CloudFormation AWS-Beispielvorlage (im Anhang), heruntergeladen auf Ihren lokalen Computer.

Architektur

Das Diagramm zeigt den folgenden Workflow:

1. Der Benutzer erstellt eine AWS-Vorlage im JSON- oder YAML-Format. CloudFormation
2. Die Vorlage erstellt einen CloudFormation AWS-Stack zum Importieren des S3-Buckets.
3. Der CloudFormation AWS-Stack verwaltet den S3-Bucket, den Sie in der Vorlage angegeben haben.

Technologie-Stack

- AWS CloudFormation
- AWS Identity and Access Management (IAM)
- AWS KMS
- Amazon S3

Tools

- AWS CloudFormation — AWS CloudFormation hilft Ihnen dabei, AWS-Infrastrukturbereitstellungen vorhersehbar und wiederholt zu erstellen und bereitzustellen.
- AWS Identity and Access Management (IAM) — IAM ist ein Webservice zur sicheren Steuerung des Zugriffs auf AWS-Services.
- AWS KMS — AWS Key Management Service (AWS KMS) ist ein für die Cloud skalierter Verschlüsselungs- und Schlüsselverwaltungsservice.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist Speicher für das Internet.

Epen

Importieren Sie einen S3-Bucket mit AWS KMS key basierter Verschlüsselung als CloudFormation AWS-Stack

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine Vorlage, um den S3-Bucket und den KMS-Schlüssel zu importieren.	Erstellen Sie auf Ihrem lokalen Computer mithilfe der folgenden Beispielvorlage eine Vorlage zum Importieren Ihres S3-Buckets und KMS-Schlüssels:
	`AWSTemplateFormatVersion: 2010-09-09`
	
	`Parameters:`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> bucketName:
	
	    Type: String
	
	Resources:
	
	  S3Bucket:
	
	    Type: 'AWS::S3:
	:Bucket'
	
	    DeletionPolicy:
	 Retain
	
	    Properties:
	
	      BucketName: !Ref
	 bucketName
	
	      BucketEncryption:
	
	        ServerSid
	eEncryptionConfigu
	ration:
	
	          - ServerSid
	eEncryptionByDefault:
	
	              SSEAlgori
	thm: 'aws:kms'
	
	              KMSMaster
	KeyID: !GetAtt
	
	                -
	 KMSS3Encryption
	
	                - Arn
	
	  KMSS3Encryption:</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> Type: 'AWS::KMS
	::Key'
	
	    DeletionPolicy:
	 Retain
	
	    Properties:
	
	      Enabled: true
	
	      KeyPolicy: !Sub
	 |-
	
	        {
	
	            "Id": "key-
	consolepolicy-3",
	
	            "Version":
	 "2012-10-17",
	
	            "Statemen
	t": [
	
	                {
	
	 "Sid": "Enable IAM User
	 Permissions",
	
	 "Effect": "Allow",
	
	 "Principal": {
	
	 "AWS": ["arn:aws:iam::
	${AWS::AccountId}:roo
	t"]
	
	                    },</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Action": "kms:*",
	
	"Resource": "*"
	}
	}
	]
	}
	
	EnableKey Rotation: true</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Stack.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die CloudFormation AWS-Konsole, wählen Sie Stack anzeigen, dann Stack erstellen und dann Mit vorhandenen Ressourcen (Ressourcen importieren). 2. Wählen Sie Vorlagendatei hochladen und laden Sie dann die Vorlagendatei hoch, die Sie zuvor erstellt haben. 3. Geben Sie einen Namen für Ihren Stack ein und konfigurieren Sie die verbleibenden Optionen gemäß Ihren Anforderungen. 4. Wählen Sie Stack erstellen und warten Sie, bis sich der Status des Stacks zu ändert`IMPORT_COMPLETE` .	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den KMS-Schlüsselalias.	1. Wählen Sie in der CloudFormation AWS-Konsole Stacks, wählen Sie den Namen des Stacks, den Sie zuvor erstellt haben, wählen Sie den Bereich Vorlage und dann In Designer anzeigen aus.
	2. Fügen Sie dem `Resource` Abschnitt Ihrer Vorlage das folgende Snippet hinzu, wählen Sie dann Create Stack und schließen Sie den Assistenten ab:
	
	`KMSS3EncryptionAlias:`
	
	`Type: 'AWS::KMS ::Alias'`
	
	`DeletionPolicy: Retain`
	
	`Properties:`
	
	`AliasName: alias/ S3BucketKey`
	
	`TargetKeyId: !Ref KMSS3Encryption`
	
	Weitere Informationen dazu finden Sie unter CloudFormation AWS-Stack-Updates in
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der CloudFormation AWS-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisieren Sie den Stack so, dass er die S3-Bucket-Richtlinie enthält.	1. Wählen Sie in der CloudFormation AWS-Konsole Stacks, wählen Sie den Namen des Stacks, den Sie zuvor erstellt haben, wählen Sie den Bereich Vorlage und dann In Designer anzeigen aus.
	2. Fügen Sie dem `Resource` Abschnitt der Vorlage den folgenden Ausschnitt hinzu, wählen Sie dann Stack erstellen und schließen Sie den Assistenten ab:
	
	`S3BucketPolicy:`
	
	`  Type: 'AWS::S3::BucketPolicy'`
	
	`  Properties:`
	
	`    Bucket: !Ref S3Bucket`
	
	`    PolicyDocument: !Sub |-`
	
	`      {`
	
	`  "Version": "2008-10-17",`
	
	`                  "Id": "restricthttp",`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	"Statement": [
	{
	"Sid": "denyhttp",
	"Effect": "Deny",
	"Principal": {
	"AWS": "*"
	},
	"Action": "s3:*",
	"Resource": ["arn:aws:s3:::${S3Bucket}","arn:aws:s3:::${S3Bucket}/*"],
	"Condition": {
	"Bool": {
	"aws:SecureTransport": "false"
	}	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>}
	}
	]
	}</pre>
	Note
	Diese S3-Bucket-Richtlinie enthält eine Deny-Anweisung, die API-Aufrufe einschränkt, die nicht sicher sind.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die wichtigsten Richtlinien.	1. Wählen Sie in der CloudFormation AWS-Konsole Stacks, wählen Sie den Namen des Stacks, den Sie zuvor erstellt haben, wählen Sie den Bereich Vorlage und dann In Designer anzeigen aus. 2. Ändern Sie die KMS-Ressource der Vorlage so, dass sie die Schlüsselrichtlinie enthält, die es Administratoren ermöglicht, den KMS-Schlüssel zu verwalten. 3. Wählen Sie Stack erstellen und dann Weiter aus, und führen Sie den Assistenten dann entsprechend Ihren Anforderungen aus. Weitere Informationen finden Sie AWS KMS in der AWS KMS KMS-Dokumentation unter Wichtige Richtlinien.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie Tags auf Ressourcenebene hinzu.	1. Wählen Sie in der CloudFormation AWS-Konsole Stacks, wählen Sie den Namen des Stacks, den Sie zuvor erstellt haben, wählen Sie den Bereich Vorlage und dann In Designer anzeigen aus.
	2. Fügen Sie das folgende Snippet zum Amazon S3 `Properties` S3-Ressourcenbereich der Vorlage hinzu, wählen Sie dann Stack erstellen und schließen Sie den Assistenten ab:
	`Tags:`
	`  - Key: createdBy`
	`  Value: Cloudformation`
		AWS DevOps

Zugehörige Ressourcen

- Einbindung vorhandener Ressourcen in das CloudFormation AWS-Management
- AWS re:Invent 2017: Tiefer Einblick in AWS CloudFormation (Video)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Synchronisieren Sie Daten zwischen Amazon EFS-Dateisystemen in verschiedenen AWS-Regionen mithilfe von AWS DataSync

Erstellt von Sarat Chandra Pothula (AWS) und Aditya Ambati (AWS)

Übersicht

Diese Lösung bietet ein robustes Framework für eine effiziente und sichere Datensynchronisierung zwischen Amazon Elastic File System (Amazon EFS) -Instances in verschiedenen AWS-Regionen. Dieser Ansatz ist skalierbar und ermöglicht eine kontrollierte, regionsübergreifende Datenreplikation. Diese Lösung kann Ihre Strategien zur Notfallwiederherstellung und Datenredundanz verbessern.

Durch die Verwendung des AWS Cloud Development Kit (AWS CDK) verwendet dieses Muster einen Infrastructure-as-Code-Ansatz (IaC) zur Bereitstellung der Lösungsressourcen. Die AWS CDK-Anwendung stellt die wesentlichen Ressourcen von AWS DataSync, Amazon EFS, Amazon Virtual Private Cloud (Amazon VPC) und Amazon Elastic Compute Cloud (Amazon EC2) bereit. Dieses IaC bietet einen wiederholbaren und versionskontrollierten Bereitstellungsprozess, der vollständig auf die bewährten AWS-Methoden abgestimmt ist.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 2.9.11 oder höher, installiert und konfiguriert
- AWS CDK Version 2.114.1 oder höher, installiert und gebootet
- NodeJS Version 20.8.0 oder höher, installiert

Einschränkungen

- Die Lösung erbt Einschränkungen von DataSync Amazon EFS, wie z. B. Datenübertragungsraten, Größenbeschränkungen und regionale Verfügbarkeit. Weitere Informationen finden Sie unter DataSync AWS-Kontingente und Amazon EFS-Kontingente.
- Diese Lösung unterstützt nur Amazon EFS. DataSync unterstützt andere AWS-Services wie Amazon Simple Storage Service (Amazon S3) und Amazon FSx for Lustre. Diese Lösung erfordert jedoch Änderungen, um Daten mit diesen anderen Diensten zu synchronisieren.

Architektur

Diese Lösung stellt die folgenden AWS-CDK-Stacks bereit:

- Amazon VPC-Stack — Dieser Stack richtet Virtual Private Cloud (VPC) -Ressourcen ein, darunter Subnetze, ein Internet-Gateway und ein NAT-Gateway sowohl in der primären als auch in der sekundären AWS-Region.
- Amazon EFS-Stack — Dieser Stack stellt Amazon EFS-Dateisysteme in den primären und sekundären Regionen bereit und verbindet sie mit ihren jeweiligen VPCs Regionen.
- EC2 Amazon-Stack — Dieser Stack startet EC2 Instances in der primären und sekundären Region. Diese Instances sind so konfiguriert, dass sie das Amazon EFS-Dateisystem mounten, wodurch sie auf den gemeinsam genutzten Speicher zugreifen können.
- DataSync Standort-Stack — Dieser Stack verwendet ein benutzerdefiniertes Konstrukt, das aufgerufen wird`DataSyncLocationConstruct`, um DataSync Standortressourcen in den primären und sekundären Regionen zu erstellen. Diese Ressourcen definieren Endpunkte für die Datensynchronisierung.
- DataSync Aufgabenstapel — Dieser Stapel verwendet ein benutzerdefiniertes Konstrukt`DataSyncTaskConstruct`, das aufgerufen wird, um eine DataSync Aufgabe in der primären Region zu erstellen. Diese Aufgabe ist so konfiguriert, dass Daten zwischen der primären und der sekundären Region mithilfe der DataSync Quell- und Zielorte synchronisiert werden.

Tools

AWS-Services

- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS DataSync ist ein Online-Datenübertragungs- und Erkennungsservice, mit dem Sie Dateien oder Objektdaten zu, von und zwischen AWS-Speicherservices verschieben können.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Elastic File System (Amazon EFS) unterstützt Sie bei der Erstellung und Konfiguration gemeinsam genutzter Dateisysteme in der AWS-Cloud.

- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.

Code-Repository

Der Code für dieses Muster ist im GitHub Amazon EFS Cross-Region DataSync Project Repository verfügbar.

Bewährte Methoden

Folgen Sie den unter Bewährte Methoden für die Verwendung des AWS-CDK bei der Erstellung von TypeScript IaC-Projekten beschriebenen bewährten Methoden.

Epen

Stellen Sie die AWS CDK-App bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Projekt-Repository.	Geben Sie den folgenden Befehl ein, um das Amazon EFS Cross-Region DataSync Project-Repository zu klonen. `git clone https://github.com/aws-samples/aws-efs-crossregion-datasync.git`	AWS DevOps
Installieren Sie die NPM-Abhängigkeiten.	Geben Sie den folgenden Befehl ein. `npm ci`	AWS DevOps
Wählen Sie die primäre und die sekundäre Region aus.	Navigieren Sie im geklonten Repository zum `src/infa`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Verzeichnis. Aktualisieren Sie in der `Launcher.ts` Datei die `SECONDARY_AWS_REGION` Werte `PRIMARY_AWS_REGION` und. Verwenden Sie die entsprechenden Regionalcodes. `const primaryRegion = { account: account, region: '<PRIMARY_AWS_REGION>' }; const secondaryRegion = { account: account, region: '<SECONDARY_AWS_REGION>' };`	
Bootstrapping für die Umgebung.	Geben Sie den folgenden Befehl ein, um das AWS-Konto und die AWS-Region, die Sie verwenden möchten, zu booten. `cdk bootstrap <aws_account>/<aws_region>` Weitere Informationen finden Sie unter Bootstrapping in der AWS CDK-Dokumentation.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Listet die AWS CDK-Stacks auf.	Geben Sie den folgenden Befehl ein, um eine Liste der AWS CDK-Stacks in der App anzuzeigen. `cdk ls`	AWS DevOps
Synthetisieren Sie die AWS-CDK-Stacks.	Geben Sie den folgenden Befehl ein, um eine CloudFormation AWS-Vorlage für jeden in der AWS CDK-App definierten Stack zu erstellen. `cdk synth`	AWS DevOps
Stellen Sie die AWS CDK-App bereit.	Geben Sie den folgenden Befehl ein, um alle Stacks auf Ihrem AWS-Konto bereitzustellen, ohne dass eine manuelle Genehmigung für Änderungen erforderlich ist. `cdk deploy --all --require-approval never`	AWS DevOps

Validieren Sie die Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie sich bei der EC2 Instanz in der primären Region an.	1. Melden Sie sich mit Session Manager, einer Funktion von AWS Systems Manager, bei der EC2	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Instance in der primären Region an. Anweisungen finden Sie unter Stellen Sie mit AWS Systems Manager Session Manager eine Verbindung zu Ihrer Linux-Instance her. 2. Ändern Sie die Verzeichnisse in den Amazon EFS-Mountpfad. `cd /mnt/efs`	

Erstellen Sie eine temporäre Datei.	Geben Sie den folgenden Befehl ein, um eine temporäre Datei im Amazon EFS-Mountpfad zu erstellen.
	`sudo dd if=/dev/zero \`
	`of=tmptst.dat \`
	`bs=1G \`
	`seek=5 \`
	`count=0`
	
	`ls -lrt tmptst.dat`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Starten Sie die DataSync Aufgabe.	Geben Sie den folgenden Befehl ein, um die temporäre Datei von der primären Region in die sekundäre Region zu replizieren. Dabei `<ARN-task>` handelt es sich um den Amazon-Ressourcennamen (ARN) Ihrer DataSync Aufgabe.
	`aws datasync start-task-execution \ --task-arn <ARN-task>`
	Der Befehl gibt den ARN der Aufgabenausführung im folgenden Format zurück.
	`arn:aws:datasync:<region>:<account-ID>:task/task-execution/<exec-ID>`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Status der Datenübertragung.	Geben Sie den folgenden Befehl ein, um die DataSync Ausführungsaufgabe zu beschreiben. Dabei `<ARN-task-execution>` handelt es sich um den ARN der Aufgabenausführung. `aws datasync describe-task-execution \ --task-execution-arn <ARN-task-execution>` Die DataSync Aufgabe ist abgeschlossen`PrepareStatus` , wenn`TransferStatus` , und `VerifyStatus` alle den Wert haben`SUCCESS`.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie sich bei der EC2 Instance in der sekundären Region an.	1. Melden Sie sich mit Session Manager, einer Funktion von AWS Systems Manager, bei der EC2 Instance in der sekundäre n Region an. Anweisungen finden Sie unter Stellen Sie mit AWS Systems Manager Session Manager eine Verbindung zu Ihrer Linux-Instance her. 2. Ändern Sie die Verzeichn isse in den Amazon EFS-Mountpfad. `cd /mnt/efs`	AWS DevOps
Validieren Sie die Replikation.	Geben Sie den folgenden Befehl ein, um zu überprüfe n, ob die temporäre Datei im Amazon EFS-Dateisystem vorhanden ist. `ls -lrt tmptst.dat`	AWS DevOps

Zugehörige Ressourcen

AWS-Dokumentation

- AWS-CDK-API-Referenz
- Konfiguration von DataSync AWS-Übertragungen mit Amazon EFS
- Behebung von Problemen mit DataSync AWS-Übertragungen

Andere AWS-Ressourcen

- AWS DataSync FAQs

Testen Sie die AWS Infrastruktur mithilfe LocalStack von Terraform-Tests

Erstellt von Ivan Girardi (AWS) und Ioannis Kalyvas (AWS)

Übersicht

Dieses Muster hilft Ihnen, Infrastruktur als Code (IaC) für AWS in Terraform lokal zu testen, ohne die Infrastruktur in Ihrer Umgebung bereitstellen zu müssen. AWS Es integriert das Terraform Tests-Framework mit. LocalStack Der LocalStack Docker-Container bietet eine lokale Entwicklungsumgebung, die verschiedene emuliert. AWS-Services Auf diese Weise können Sie Infrastrukturbereitstellungen testen und iterieren, ohne dass Kosten für die. AWS Cloud

Diese Lösung bietet die folgenden Vorteile:

- Kostenoptimierung — Durch die Durchführung von Tests gegen LocalStack entfällt die Notwendigkeit der Nutzung AWS-Services. Dies verhindert, dass Ihnen Kosten entstehen, die mit der Erstellung, dem Betrieb und der Änderung dieser AWS Ressourcen verbunden sind.
- Geschwindigkeit und Effizienz — Lokales Testen ist in der Regel auch schneller als das Bereitstellen der AWS Ressourcen. Diese schnelle Feedback-Schleife beschleunigt Entwicklung und Debugging. Da sie lokal LocalStack ausgeführt wird, können Sie Ihre Terraform-Konfigurationsdateien ohne Internetverbindung entwickeln und testen. Sie können Terraform-Konfigurationsdateien lokal debuggen und sofort Feedback erhalten, was den Entwicklungsprozess rationalisiert.
- Konsistenz und Reproduzierbarkeit — LocalStack bietet eine konsistente Testumgebung. Diese Konsistenz trägt dazu bei, dass Tests unabhängig von externen AWS Änderungen oder Netzwerkproblemen dieselben Ergebnisse liefern.
- Isolierung — Das Testen mit LocalStack verhindert, dass Sie versehentlich AWS Live-Ressourcen oder Produktionsumgebungen beeinträchtigen. Diese Isolierung macht es sicher, verschiedene Konfigurationen zu experimentieren und zu testen.
- Automatisierung — Durch die Integration mit einer CI/CD-Pipeline (Continuous Integration and Continuous Delivery) können Sie Terraform-Konfigurationsdateien automatisch testen. Die Pipeline testet den IaC vor der Bereitstellung gründlich.
- Flexibilität — Sie können verschiedene AWS-Regionen, und Servicekonfigurationen simulieren AWS-Konten, um sie besser an Ihre Produktionsumgebungen anzupassen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Installieren von Docker
- Aktivieren Sie den Zugriff auf den Standard-Docker-Socket (`/var/run/docker.sock`). Weitere Informationen finden Sie in der LocalStack -Dokumentation.
- Installieren Sie Docker Compose
- Installieren Sie Terraform Version 1.6.0 oder höher
- Installieren Sie Terraform CLI
- Konfigurieren Sie den Terraform-Anbieter AWS
- (Optional) Installieren und konfigurieren Sie das AWS Command Line Interface ()AWS CLI. Ein Beispiel für die Verwendung von with finden Sie in den AWS CLI GitHub Repositorien Test AWS infrastructure using LocalStack und Terraform Tests. LocalStack

Einschränkungen

- Dieses Muster enthält explizite Beispiele für das Testen von Amazon Simple Storage Service (Amazon S3), AWS Lambda AWS Step Functions, und Amazon DynamoDB DynamoDB-Ressourcen. Sie können diese Lösung jedoch um zusätzliche AWS Ressourcen erweitern.
- Dieses Muster enthält Anweisungen zum lokalen Ausführen von Terraform-Tests. Sie können Tests jedoch in jede CI/CD-Pipeline integrieren.
- Dieses Muster enthält Anweisungen zur Verwendung des Community-Images. LocalStack Wenn Sie das LocalStack Pro-Image verwenden, lesen Sie in der LocalStack Pro-Dokumentation nach.
- LocalStack bietet Emulationsdienste für verschiedene AWS APIs. Eine vollständige Liste finden Sie unter Umfang der AWS Servicefunktionen. Für einige erweiterte Funktionen ist möglicherweise ein Abonnement für LocalStack Pro erforderlich.

Architektur

Das folgende Diagramm zeigt die Architektur für diese Lösung. Die Hauptkomponenten sind ein Quellcode-Repository, eine CI/CD-Pipeline und ein LocalStack Docker-Container. Der LocalStack Docker-Container hostet lokal Folgendes: AWS-Services

- Ein Amazon S3 S3-Bucket zum Speichern von Dateien

- Amazon CloudWatch für die Überwachung und Protokollierung
- Eine AWS Lambda Funktion zum Ausführen von serverlosem Code
- Eine AWS Step Functions Zustandsmaschine zur Orchestrierung mehrstufiger Workflows
- Eine Amazon DynamoDB-Tabelle zum Speichern von NoSQL-Daten

Das Diagramm zeigt den folgenden Workflow:

1. Sie fügen eine Terraform-Konfigurationsdatei hinzu und übertragen sie in das Quellcode-Repository.
2. Die CI/CD-Pipeline erkennt die Änderungen und leitet einen Build-Prozess für die statische Terraform-Codeanalyse ein. Die Pipeline erstellt und führt den Docker-Container aus. LocalStack Dann startet die Pipeline den Testprozess.
3. Die Pipeline lädt ein Objekt in einen Amazon S3 S3-Bucket hoch, der im LocalStack Docker-Container gehostet wird.
4. Durch das Hochladen des Objekts wird eine Funktion aufgerufen. AWS Lambda
5. Die Lambda-Funktion speichert die Amazon S3 S3-Ereignisbenachrichtigung in einem CloudWatch Protokoll.
6. Die Lambda-Funktion startet eine AWS Step Functions Zustandsmaschine.
7. Die Zustandsmaschine schreibt den Namen des Amazon S3 S3-Objekts in eine DynamoDB-Tabelle.
8. Der Testprozess in der CI/CD-Pipeline überprüft, ob der Name des hochgeladenen Objekts mit dem Eintrag in der DynamoDB-Tabelle übereinstimmt. Außerdem wird überprüft, ob der S3-Bucket mit dem angegebenen Namen bereitgestellt wurde und ob die Funktion erfolgreich bereitgestellt wurde. AWS Lambda

Tools

AWS-Services

- Amazon CloudWatch hilft Ihnen dabei, die Kennzahlen Ihrer AWS Ressourcen und der Anwendungen, auf denen Sie laufen, AWS in Echtzeit zu überwachen.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.

- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Step Functionsist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Funktionen und andere Funktionen kombinieren können, um geschäftskritische AWS-Services Anwendungen zu erstellen.

Andere Tools

- Docker ist eine Reihe von Platform-as-a-Service (PaaS) -Produkten, die Virtualisierung auf Betriebssystemebene nutzen, um Software in Containern bereitzustellen.
- Docker Compose ist ein Tool zum Definieren und Ausführen von Multi-Container-Anwendungen.
- LocalStackist ein Cloud-Service-Emulator, der in einem einzigen Container läuft. Mithilfe LocalStack von können Sie Workloads auf Ihrem lokalen Computer ausführen, die verwenden AWS-Services, ohne eine Verbindung zu dem herzustellen. AWS Cloud
- Terraform ist ein IaC-Tool von HashiCorp , mit dem Sie Cloud- und lokale Ressourcen erstellen und verwalten können.
- Terraform Tests hilft Ihnen dabei, Aktualisierungen der Terraform-Modulkonfiguration durch Tests zu validieren, die Integrations- oder Komponententests ähneln.

Code-Repository

Der Code für dieses Muster ist in den Repositorien GitHub Test AWS Infrastructure using LocalStack und Terraform Tests verfügbar.

Bewährte Methoden

- Diese Lösung testet die AWS Infrastruktur, die in den Terraform-Konfigurationsdateien angegeben ist, und stellt diese Ressourcen nicht in der bereit. AWS Cloud Wenn Sie die Ressourcen bereitstellen möchten, folgen Sie dem Prinzip der geringsten Rechte (IAM-Dokumentation) und konfigurieren Sie das Terraform-Backend ordnungsgemäß (Terraform-Dokumentation).
- Bei der Integration LocalStack in eine CI/CD-Pipeline empfehlen wir, den Docker-Container nicht im Rechtemodus auszuführen. LocalStack Weitere Informationen finden Sie unter Runtime-

Rechte und Linux-Funktionen (Docker-Dokumentation) und Sicherheit für selbstverwaltete Runner (Dokumentation). GitLab

Epen

Stellen Sie die Lösung bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Geben Sie in einer Bash-Shell den folgenden Befehl ein. Dadurch wird die AWS Testinfrastruktur mithilfe eines Terraform LocalStack Tests-Repositorys geklont von: GitHub `git clone https://github.com/aws-samples/localstack-terraform-test.git`	DevOps Ingenieur

Lass den LocalStack Container laufen.	1. Geben Sie den folgenden Befehl ein, um zum geklonten Repository zu navigieren:
	`cd localstack-terraform-test`
	2. Geben Sie den folgenden Befehl ein, um den LocalStack Docker-Container im getrennten Modus zu starten:
	`docker-compose up -d`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Warten Sie, bis der LocalStack Docker-Container betriebsbereit ist.	
Initialisieren Sie Terraform.	Geben Sie den folgenden Befehl ein, um Terraform zu initialisieren: `terraform init`	DevOps Ingenieur

Führen Sie Terraform-Tests durch.	1. Geben Sie den folgenden Befehl ein, um Terraform-Tests auszuführen:
	`terraform test`
	2. Stellen Sie sicher, dass alle Tests erfolgreich abgeschlossen wurden. Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:
	`Success! 3 passed, 0 failed.`
		DevOps Ingenieur

Bereinigen von Ressourcen.	Geben Sie den folgenden Befehl ein, um den LocalStack Container zu zerstören: `docker-compose down`	DevOps Ingenieur

Fehlerbehebung

Problem	Lösung

`Error: reading DynamoDB Table Item (Files|README.md): empty` Ergebnis bei der Ausführung des `terraform test` Befehls.	1. Geben Sie den `terraform test` Befehl erneut ein.
	2. Wenn der Fehler dadurch nicht behoben wird, bearbeiten Sie die Datei main.tf, um das Schlaf-Timeout auf einen Wert von mehr als 15 Sekunden zu erhöhen:
	`resource "time_sleep" "wait" {`
	`  create_duration = "15s"`
	`  triggers = {`
	`  s3_object = local.key_json`
	`  }`
	`}`

Zugehörige Ressourcen

- Erste Schritte mit Terraform: Anleitungen für AWS CDK Experten (Prescriptive Guidance) AWS CloudFormation AWS
- Bewährte Methoden für die Verwendung des AWS Terraform Providers (Prescriptive Guidance)AWS
- Terraform CI/CD und weitere Tests AWS mit dem neuen Terraform Test Framework (Blogbeitrag)AWS
- Beschleunigung der Softwarebereitstellung mit LocalStack Cloud Emulator von (Blogbeitrag) AWS MarketplaceAWS

Zusätzliche Informationen

Integration mit Aktionen GitHub

Mithilfe von Aktionen können Sie Tests in eine CI/CD-Pipeline integrieren LocalStack und Terraform-Tests in eine CI/CD-Pipeline einbauen. GitHub Weitere Informationen finden Sie in der

Dokumentation zu Aktionen. GitHub Im Folgenden finden Sie ein Beispiel für eine GitHub Actions-Konfigurationsdatei:

```
name: LocalStack Terraform Test

on:
  push:
    branches:
      - '**'

  workflow_dispatch: {}

jobs:
  localstack-terraform-test:
    runs-on: ubuntu-latest

    steps:
    - uses: actions/checkout@v4

    - name: Build and Start LocalStack Container
      run: |
        docker compose up -d

    - name: Setup Terraform
      uses: hashicorp/setup-terraform@v3
      with:
        terraform_version: latest

    - name: Run Terraform Init and Validation
      run: |
        terraform init
        terraform validate
        terraform fmt --recursive --check
        terraform plan
        terraform show

    - name: Run Terraform Test
      run: |
        terraform test

    - name: Stop and Delete LocalStack Container
      if: always()
      run: docker compose down
```

Aktualisieren Sie SAP Pacemaker-Cluster von ENSA1 auf ENSA2

Erstellt von Gergely Cerdi (AWS) und Balazs Sandor Skublics (AWS)

Übersicht

In diesem Muster werden die Schritte und Überlegungen für das Upgrade eines SAP Pacemaker-Clusters, das auf dem Standalone Enqueue Server () basiert, auf erklärt. ENSA1 ENSA2 Die Informationen in diesem Muster gelten sowohl für die Betriebssysteme SUSE Linux Enterprise Server (SLES) als auch für Red Hat Enterprise Linux (RHEL).

Pacemaker-Cluster auf SAP NetWeaver 7.52 oder S/4HANA 1709 und früheren Versionen laufen auf einer Architektur und sind speziell für sie konfiguriert. ENSA1 ENSA1 Wenn Sie Ihre SAP-Workloads auf Amazon Web Services (AWS) ausführen und daran interessiert sind ENSA2, zu wechseln, stellen Sie möglicherweise fest, dass die SAP-, SUSE- und RHEL-Dokumentation keine umfassenden Informationen enthält. Dieses Muster beschreibt die technischen Schritte, die zur Neukonfiguration von SAP-Parametern und Pacemaker-Clustern für das Upgrade von zu erforderlich sind. ENSA1 ENSA2 Es enthält Beispiele für SUSE-Systeme, aber das Konzept ist dasselbe für RHEL-Cluster.

> Hinweise: ENSA1 Da es sich um Konzepte ENSA2 handelt, die sich nur auf SAP-Anwendungen beziehen, gelten die Informationen in diesem Muster nicht für SAP HANA oder andere Clusterty pen.
>
> Technisch gesehen ENSA2 kann es mit oder ohne Enqueue Replicator 2 verwendet werden. Für Hochverfügbarkeit (HA) und Failover-Automatisierung (durch eine Cluster-Lösung) ist jedoch Enqueue Replicator 2 erforderlich. In diesem Muster wird der Begriff ENSA2 Cluster für Cluster mit Standalone Enqueue Server 2 und Enqueue Replicator 2 verwendet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein funktionierender ENSA1 Cluster, der Pacemaker und Corosync auf SLES oder RHEL verwendet.
- Mindestens zwei Amazon Elastic Compute Cloud (Amazon EC2) -Instances, auf denen die (ABAP) SAP Central Services (ASCS/SCS) und Enqueue Replication Server (ERS) -Instances ausgeführt werden.

- Kenntnisse in der Verwaltung von SAP-Anwendungen und -Clustern.
- Zugriff auf die Linux-Umgebung als Root-Benutzer.

Einschränkungen

- ENSA1basierte Cluster unterstützen nur eine Architektur mit zwei Knoten.
- ENSA2basierte Cluster können nicht für NetWeaver SAP-Versionen vor 7.52 bereitgestellt werden.
- EC2 Instanzen in Clustern sollten sich in verschiedenen AWS-Verfügbarkeitszonen befinden.

Produktversionen

- NetWeaver SAP-Version 7.52 oder höher
- Ab S/4HANA 2020 werden nur Cluster unterstützt ENSA2
- Kernel 7.53 oder höher, der Enqueue Replicator 2 unterstützt ENSA2
- SLES für SAP-Anwendungen Version 12 oder höher
- RHEL für SAP mit High Availability (HA) Version 7.9 oder höher

Architektur

Quelltechnologie-Stack

- SAP NetWeaver 7.52 mit SAP Kernel 7.53 oder höher
- SLES- oder RHEL-Betriebssystem

Zieltechnologie-Stack

- SAP NetWeaver 7.52 mit SAP Kernel 7.53 oder höher, einschließlich S/4HANA 2020 mit ABAP-Plattform
- SLES- oder RHEL-Betriebssystem

Zielarchitektur

Das folgende Diagramm zeigt eine HA-Konfiguration von ASCS/SCS- und ERS-Instanzen auf der Grundlage eines Clusters. ENSA2

Vergleich von und Clustern ENSA1 ENSA2

SAP wurde ENSA2 als Nachfolger von eingeführt ENSA1. Ein Cluster ENSA1 auf Basis von zwei Knoten unterstützt eine Architektur mit zwei Knoten, bei der die ASCS/SCS instance fails over to ERS when an error occurs. This limitation stems from how the ASCS/SCS instance regains the lock table information from the shared memory of the ERS node after failover. ENSA2-based clusters with Enqueue Replicator 2 eliminate this limitation, because the ASCS/SCS instance can collect the lock information from the ERS instance over the network. ENSA2-based clusters can have more than two nodes, because the ASCS/SCS instance is no longer required to fail over to the ERS node. (However, in a two-node ENSA2 cluster environment, the ASCS/SCS Instanz trotzdem einen Failover zum ERS-Knoten durchführt, da es im Cluster keine anderen Knoten gibt, auf die ein Failover durchgeführt werden kann.) ENSA2 wird ab SAP Kernel 7.50 mit einigen Einschränkungen unterstützt. Für ein HA-Setup, das Enqueue Replicator 2 unterstützt, ist die Mindestanforderung NetWeaver 7.52 (siehe SAP OSS Hinweis 2630416). S/4HANA 1809 wird standardmäßig mit einer empfohlenen ENSA2 Architektur geliefert, wohingegen S/4HANA erst ab Version 2020 unterstützt. ENSA2

Automatisierung und Skalierung

Der HA-Cluster in der Zielarchitektur sorgt dafür, dass ASCS automatisch auf andere Knoten umschaltet.

Szenarien für die Umstellung auf ENSA2 basierte Cluster

Es gibt zwei Hauptszenarien für das Upgrade auf ENSA2 basierte Cluster:

- Szenario 1: Sie entscheiden sich für ein Upgrade ENSA2 ohne begleitendes SAP-Upgrade oder S/4HANA-Konvertierung, vorausgesetzt, dass Ihr SAP-Release und Ihre Kernel-Version dies unterstützen. ENSA2
- Szenario 2: Sie wechseln im ENSA2 Rahmen eines Upgrades oder einer Konvertierung (z. B. zu S/4HANA 1809 oder höher), indem Sie SUM verwenden.

Der Abschnitt Epics behandelt die Schritte für diese beiden Szenarien. Im ersten Szenario müssen Sie SAP-bezogene Parameter manuell einrichten, bevor Sie die Clusterkonfiguration für ändern. ENSA2 Im zweiten Szenario werden die Binärdateien und SAP-bezogenen Parameter von SUM bereitgestellt, und Ihre einzige verbleibende Aufgabe besteht darin, die Clusterkonfiguration für HA

zu aktualisieren. Wir empfehlen weiterhin, die SAP-Parameter zu überprüfen, nachdem Sie SUM verwendet haben. In den meisten Fällen ist die S/4HANA-Konvertierung der Hauptgrund für ein Cluster-Upgrade.

Tools

- Für Betriebssystem-Paketmanager empfehlen wir die Tools Zypper (für SLES) oder YUM (für RHEL).
- Für die Clusterverwaltung empfehlen wir crm-Shells (für SLES) oder pcs-Shells (für RHEL).
- Tools zur SAP-Instanzverwaltung wie. SAPControl
- (Optional) SUM-Tool für das Upgrade der S/4HANA-Konvertierung.

Bewährte Methoden

- Bewährte Methoden für die Verwendung von SAP-Workloads auf AWS finden Sie im SAP Lens for the AWS Well-Architected Framework.
- Berücksichtigen Sie die Anzahl der Clusterknoten (ungerade oder gerade) in Ihrer ENSA2 Architektur mit mehreren Knoten.
- Richten Sie den ENSA2 Cluster für SLES 15 gemäß dem SAP S/4-HA-CLU 1.0-Zertifizierungsstandard ein.
- Speichern oder sichern Sie immer Ihren vorhandenen Cluster- und Anwendungsstatus, bevor Sie ein Upgrade auf durchführen. ENSA2

Epen

Konfigurieren Sie SAP-Parameter manuell für ENSA2 (nur Szenario 1)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Parameter im Standardprofil.	Wenn Sie auf dieselbe SAP-Version aktualisieren möchten ENSA2 oder wenn Ihre Zielversion standardmäßig auf die Standardversion eingestel lt ist ENSA1, setzen Sie die Parameter im Standardprofil	SAP

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	(Datei DEFAULT.PFL) auf die folgenden Werte.
	
	`enq/enable=TRUE`
	`enq/serverhost=sapascsvirt`
	`enq/serverinst=10`
	`(instance number of ASCS/SCS instance)`
	`enque/process_location=REMOTESA`
	`enq/replicatorhost=sapersvirt`
	`enq/replicatorinst=11`
	`(instance number of ERS instance)`
	
	wo `sapascsvirt` ist der virtuelle Hostname für die ASCS-Instanzen und `sapersvirt` der virtuelle Hostname für die ERS-Instanzen. Sie können diese an Ihre Zielumgebung anpassen.
	
	Note
	Um diese Upgrade-Option verwenden zu können, müssen Ihr SAP-Release und Ihre Kernel-Version Enqueue Replicator 2 unterstützen ENSA2 .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie das ASCS/SCS-Instanzprofil.	Wenn Sie auf dieselbe SAP-Version aktualisieren möchten ENSA2 oder wenn Ihre Zielversion standardmäßig auf die gleiche SAP-Version eingestellt ist ENSA1, legen Sie die folgenden Parameter im ASCS/SCS-Instanzprofil fest. Der Abschnitt des Profils, in dem definiert ENSA1 ist, sieht ungefähr wie folgt aus. `#------------------ ------------------ ------------------ --------- Start SAP enqueue server #------------------- ------------------ ------------------ ------- _EN = en.sap$(S APSYSTEMNAME)$(INS TANCE_NAME) Execute_04 = local rm - f $(_EN) Execute_05 = local ln - s -f $(DIR_EXECUTABLE)/ enserver$(FT_EXE) $(_EN) Start_Program_01 = local $(_EN) pf=$(_PF)` Um diesen Abschnitt neu zu konfigurieren für ENSA2:	SAP

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	1. Ändern Sie das `_EN` Programmpräfix auf `_ENQ` basierend auf den neuesten Informationen von SAP (OSS-Hinweis 2501860; erfordert ein SAP ONE Support Launchpad-Benutzerkonto).
	2. Ändern Sie die Binärdatei für den Enqueue-Server von auf. `enserver` `enq_server`
	3. Setzen Sie den neuen Parameter `enq/server/replication/enable` auf`TRUE`.
	4. Stellen Sie sicher, dass`Autostart = 0`.
	
	Dieser Profilbereich würde nach Ihren Änderungen etwa wie folgt aussehen.
	
	`#----------`
	`----------`
	`----------`
	`---------`
	`Start SAP enqueue server`
	`#----------`
	`----------`
	`----------`
	`-------`
	`_ENQ = enq.sap$(`
	`SAPSYSTEMNAME)$(IN`
	`STANCE_NAME)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`Execute_04 = local rm -f $(_ENQ)`
	`Execute_05 = local ln -s -f $(DIR_EXECUTABLE)/enq_server$(FT_EXE) $(_ENQ)`
	`Start_Program_01 = local $(_ENQ) pf=$(_PF)`
	`...`
	`enq/server/replication/enable = TRUE`
	`Autostart = 0`
	
	Important
	_ENQDie Neustartoption darf nicht aktiviert sein. Wenn auf eingestellt `RestartProgram_01` ist_ENQ, ändern Sie es in`StartProgram_01` . Dadurch wird verhindert, dass SAP den Dienst neu startet oder die clusterverwalteten Ressourcen beeinträchtigt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie das ERS-Profil.	Wenn Sie auf dieselbe SAP-Version aktualisieren möchten ENSA2 oder wenn Ihre Zielversion standardmäßig auf die Standardversion eingestellt ist ENSA1, legen Sie die folgenden Parameter im ERS-Instanzprofil fest. Suchen Sie den Abschnitt, in dem der Enqueue-Replikator definiert ist. Er wird dem Folgenden ähnlich sein. `#------------------ ------------------ ------------------ Start enqueue replicati on server #------------------ ------------------ ------------------ _ER = er.sap$(S APSYSTEMNAME)$(INS TANCE_NAME) Execute_03 = local rm - f $(_ER) Execute_04 = local ln - s -f $(DIR_EXECUTABLE)/ enrepserver$(FT_EXE) $(_ER) Start_Program_00 = local $(_ER) pf=$(_PF) NR=$(SCSID)`	SAP

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Um diesen Abschnitt für Enqueue Replicator 2 neu zu konfigurieren:
	1. Ändern Sie das `_ER` Programmpräfix auf `_ENQR` basierend auf den neuesten Hinweisen von SAP (OSS-Hinweis 2501860; erfordert ein SAP ONE Support Launchpad-Benutzerkonto).
	2. Ändern Sie die Binärdatei für den Enqueue-Replikator auf statt auf. `enq_replicator enrepserver`
	3. Stellen Sie sicher, dass. `Autostart = 0`
	
	Dieser Profilbereich sollte nach Ihren Änderungen in etwa wie folgt aussehen.
	`#----------`
	`----------`
	`----------`
	`Start enqueue replicati`
	`on server`
	`#----------`
	`----------`
	`----------`
	`_ENQR = enqr.sap$`
	`(SAPSYSTEMNAME)$(I`
	`NSTANCE_NAME)`
	`Execute_01 = local rm -`
	`f $(_ENQR)`
	`Execute_02 = local ln -`
	`s -f $(DIR_EXECUTABLE)/`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`enq_replicator$(FT _EXE) $(_ENQR)`
	`Start_Program_00 =  local $(_ENQR) pf= $(_PF) NR=$(SCSID)`
	`…`
	`Autostart = 0`
	
	Important
	_ENQRDie Neustartoption darf nicht aktiviert sein. Wenn auf eingestellt `RestartProgram_01` ist_ENQR, ändern Sie es in`StartProgram_01` . Dadurch wird verhindert, dass SAP den Dienst neu startet oder die clusterverwalteten Dienste beeinträchtigt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Starten Sie SAP Start Services neu.	Nachdem Sie die zuvor in diesem Epic beschriebenen Profile geändert haben, starten Sie die SAP Start Services sowohl für ASCS/SCS als auch für ERS neu.
	`sapcontrol -nr 10 -function RestartService SCT`
	`sapcontrol -nr 11 -function RestartService SCT`
	wobei `SCT` auf die SAP-System-ID Bezug genommen wird und davon ausgegangen wird, dass 10 und 11 die Instanznummern für ASCS/SCS- bzw. ERS-Instanzen sind.
		SAP

Konfigurieren Sie den Cluster für neu ENSA2 (für beide Szenarien erforderlich)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Versionsnummern in den SAP-Ressourcenagenten.	Wenn Sie SUM verwenden, um SAP auf S/4HANA 1809 oder höher zu aktualisieren, verarbeitet SUM die Parameteränderungen in den SAP-Profilen. Nur der Cluster muss manuell angepasst werden. Wir empfehlen jedoch, die Parametereinstellu	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ngen zu überprüfen, bevor Sie Änderungen am Cluster vornehmen. **Note** Bei den Beispielen in diesem Epos wird davon ausgegang en, dass Sie das SUSE-Betriebssyste m verwenden. Wenn Sie RHEL verwenden , müssen Sie Tools wie YUM und die PCS-Shell anstelle von Zypper und crm verwenden. Überprüfen Sie beide Knoten in der Architektur, um sicherzustellen, dass das `resource-agents` Paket der von SAP empfohlenen Mindestversion entsprich t. Informationen zu SLES finden Sie in der SAP-OSS-A nmerkung 2641019. Informati onen zu RHEL finden Sie im SAP OSS-Hinweis 2641322. (Für SAP-Hinweise ist ein SAP ONE Support Launchpad-Benutzerkonto erforderlich.)	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`sapers:sctadm 23> zypper search -s -i resource-agents Loading repository data... Reading installed packages... S | Name | Type | Version | Arch | Repository --+------------ ----+---------+--- ------------------ ---------------+-- ------+----------- ------------------ i | resource-agents | package | 4.8.0+git 30.d0077df0-150300 .8.28.1 | x86_64 | SLE-Product-HA15-SP3- Updates`  Aktualisieren Sie die `resource-agents` Version, falls erforderlich.	
Sichern Sie die Cluster-K onfiguration.	Sichern Sie die CRM-Clust erkonfiguration wie folgt. `crm configure show > /tmp/cluster_confi g_backup.txt`	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Wartungsmodus ein.	Stellen Sie den Cluster in den Wartungsmodus. `crm configure property maintenance-mode="true"`	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Cluster-K onfiguration.	Überprüfen Sie die aktuelle Clusterkonfiguration.
	`crm configure show`
	Hier ist ein Auszug aus der vollständigen Ausgabe:
	`node 1: sapascs`
	`node 2: sapers`
	`...`
	`primitive rsc_sap_S`
	`CT_ASCS10 SAPInstance`
	`\`
	`operations $id=rsc_s`
	`ap_SCT_ASCS10-oper`
	`ations \`
	`op monitor interval=120`
	`timeout=60 on-fail=r`
	`estart \`
	`params InstanceN`
	`ame=SCT_ASCS10_sap`
	`ascsvirt START_PRO`
	`FILE="/sapmnt/SCT/`
	`profile/SCT_ASCS10`
	`_sapascsvirt" \`
	`AUTOMATIC_RECOVER=`
	`false \`
	`meta resource-stickines`
	`s=5000 failure-t`
	`imeout=60 migration-`
	`threshold=1 priority=`
	`10`
	`primitive rsc_sap_S`
	`CT_ERS11 SAPInstance \`
	`operations $id=rsc_s`
	`ap_SCT_ERS11-opera`
	`tions \`
	`op monitor interval=120`
	`timeout=60 on-fail=r`
	`estart \`
		AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>params InstanceN
	ame=SCT_ERS11_sape
	rsvirt START_PRO
	FILE="/sapmnt/SCT/
	profile/SCT_ERS11_
	sapersvirt" \
	   AUTOMATIC_RECOVER=
	false IS_ERS=true \
	meta priority=1000
	...
	colocation col_sap_S
	CT_no_both -5000:
	 grp_SCT_ERS11
	 grp_SCT_ASCS10
	location loc_sap_S
	CT_failover_to_ers
	 rsc_sap_SCT_ASCS10 \
	rule 2000: runs_ers_SCT
	 eq 1
	order ord_sap_S
	CT_first_start_asc
	s Optional: rsc_sap_S
	CT_ASCS10:start
	 rsc_sap_SCT_ERS11:
	stop symmetrical=false
	...</pre> wo `sapascsvirt` sich auf den virtuellen Hostnamen für die ASCS-Instanzen `sapersvirt` bezieht, sich auf den virtuellen Hostnamen für die ERS-Instanzen bezieht und SCT sich auf die SAP-System-ID bezieht.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die Failover-Colocation-Einschränkung.	Im vorherigen Beispiel `loc_sap_SCT_failover_to_ers` gibt die Standortbeschränkung an, dass die ENSA1 ASCS-Funktion beim Failover immer der ERS-Instanz folgen soll. Mit sollte ASCS in der Lage sein ENSA2, ungehindert ein Failover zu allen beteiligten Knoten durchzuführen, sodass Sie diese Einschränkung aufheben können. `crm configure delete loc_sap_SCT_failover_to_ers`	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie die Primitive an.	Sie müssen auch geringfüg ige Änderungen an den ASCS SAPInstance - und ERS-Primi tiven vornehmen. Hier ist ein Beispiel für ein SAPInstance ASCS-Primitiv, für das konfiguriert ist. ENSA1 `primitive rsc_sap_S CT_ASCS10 SAPInstance \ operations $id=rsc_s ap_SCT_ASCS10-oper ations \ op monitor interval=120 timeout=60 on-fail=r estart \ params InstanceN ame=SCT_ASCS10_sap ascsvirt START_PRO FILE="/sapmnt/SCT/ profile/SCT_ASCS10 _sapascsvirt" \ AUTOMATIC_RECOVER= false \ meta resource-stickines s=5000 failure-t imeout=60 migration- threshold=1 priority= 10`  Um ein Upgrade auf durchzufü hren ENSA2, ändern Sie diese Konfiguration wie folgt.  `primitive rsc_sap_S CT_ASCS10 SAPInstance \`	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	operations $id=rsc_s ap_SCT_ASCS10-oper ations \ op monitor interval=120 timeout=60 on-fail=r estart \ params InstanceN ame=SCT_ASCS10_sap ascsvirt START_PRO FILE="/sapmnt/SCT/ profile/SCT_ASCS10 _sapascsvirt" \ AUTOMATIC_RECOVER= false \ meta resource-stickines s=3000 Dies ist ein Beispiel für ein SAPInstance ERS-Primitiv, für das konfiguriert ist ENSA1. primitive rsc_sap_S CT_ERS11 SAPInstance \ operations $id=rsc_s ap_SCT_ERS11-opera tions \ op monitor interval=120 timeout=60 on-fail=r estart \ params InstanceN ame=SCT_ERS11_sape rsvirt START_PRO FILE="/sapmnt/SCT/ profile/SCT_ERS11_ sapersvirt" \ AUTOMATIC_RECOVER= false IS_ERS=true \ meta priority=1000	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Um ein Upgrade durchzufü hren ENSA2, ändern Sie diese Konfiguration wie folgt.
	
	`primitive rsc_sap_S CT_ERS11 SAPInstance \ operations $id=rsc_s ap_SCT_ERS11-opera tions \ op monitor interval=120 timeout=60 on-fail=r estart \ params InstanceN ame=SCT_ERS11_sape rsvirt START_PRO FILE="/sapmnt/SCT/ profile/SCT_ERS11_ sapersvirt" \ AUTOMATIC_RECOVER= false IS_ERS=true`
	
	Sie können Primitive auf verschiedene Arten ändern. Sie können sie beispiels weise in einem Editor wie vi überarbeiten, wie im folgenden Beispiel.
	
	`crm configure edit rsc_sap_SCT_ERS11`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Deaktivieren Sie den Wartungsmodus.	Deaktivieren Sie den Wartungsmodus auf dem Cluster. `crm configure property maintenance-mode="false"` Wenn sich der Cluster außerhalb des Wartungsmodus befindet, versucht er, die ASCS- und ERS-Instances mit den neuen ENSA2 Einstellungen online zu schalten.	AWS-Systemadministrator

(Optional) Fügen Sie Clusterknoten hinzu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Informieren Sie sich über bewährte Verfahren.	Bevor Sie weitere Knoten hinzufügen, sollten Sie sich mit den bewährten Methoden vertraut machen, z. B. ob Sie eine ungerade oder eine gerade Anzahl von Knoten verwenden sollten.	AWS-Systemadministrator
Fügen Sie Knoten hinzu.	Das Hinzufügen weiterer Knoten umfasst eine Reihe von Aufgaben, wie z. B. die Aktualisierung des Betriebssystems, die Installation von Softwarepaketen, die den vorhandenen Knoten entsprechen, und die Bereitste	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	llung von Halterungen. Sie können die Option „Zusätzlic hen Host vorbereiten“ im SAP Software Provisioning Manager (SWPM) verwenden , um eine SAP-spezifische Baseline des Hosts zu erstellen. Weitere Informati onen finden Sie in den SAP-Leitfäden, die im nächsten Abschnitt aufgeführt sind.	

Zugehörige Ressourcen

SAP- und SUSE-Referenzen

Um auf SAP Notes zugreifen zu können, benötigen Sie ein SAP ONE Support Launchpad-Benutzerkonto. Weitere Informationen finden Sie auf der SAP-Supportwebsite.

- SAP-Hinweis 2501860 – Dokumentation für den NetWeaver SAP-Anwendungsserver für ABAP 7.52
- SAP-Hinweis 2641019 – Installation von ENSA2 und Update von bis ENSA1 in der SUSE HA-Umgebung ENSA2
- SAP-Hinweis 2641322 – Installation von ENSA2 und Update von ENSA1 bis ENSA2 bei Verwendung der Red Hat HA-Lösungen für SAP
- SAP-Hinweis 2711036 – Verwendung des Standalone Enqueue Servers 2 in einer HA-Umgebung
- Eigenständiger Enqueue-Server 2 (SAP-Dokumentation)
- SAP S/4 HANA – Hochverfügbarkeitscluster von Enqueue Replication 2 — Einrichtungshandbuch (SUSE-Dokumentation)

AWS-Referenzen

- SAP HANA on AWS: Leitfaden zur Hochverfügbarkeitskonfiguration für SLES und RHEL
- SAP Lens — AWS Well-Architected Framework

Verwenden Sie konsistente Availability Zones VPCs für verschiedene AWS-Konten

Erstellt von Adam Spicer (AWS)

Übersicht

In der Amazon Web Services (AWS) -Cloud hat eine Availability Zone einen Namen, der je nach Ihren AWS-Konten variieren kann, und eine Availability Zone ID (AZ ID), die ihren Standort identifiziert. Wenn Sie AWS verwenden CloudFormation , um virtuelle private Clouds (VPCs) zu erstellen, müssen Sie beim Erstellen der Subnetze den Namen oder die ID der Availability Zone angeben. Wenn Sie mehrere Konten erstellen VPCs , wird der Name der Availability Zone nach dem Zufallsprinzip ausgewählt, was bedeutet, dass Subnetze in jedem Konto unterschiedliche Availability Zones verwenden.

Um dieselbe Availability Zone für Ihre Konten zu verwenden, müssen Sie den Availability Zone-Namen in jedem Konto derselben AZ-ID zuordnen. Das folgende Diagramm zeigt beispielsweise, dass die `use1-az6` AZ-ID `us-east-1a` in AWS-Konto A und `us-east-1c` AWS-Konto Z benannt ist.

Dieses Muster trägt dazu bei, die zonale Konsistenz sicherzustellen, indem es eine kontoübergreifende, skalierbare Lösung für die Verwendung derselben Availability Zones in Ihren Subnetzen bietet. Durch die zonale Konsistenz wird sichergestellt, dass Ihr kontenübergreifender Netzwerkverkehr Netzwerkpfade zwischen Availability Zones vermeidet, wodurch die Datenübertragungskosten gesenkt und die Netzwerklatenz zwischen Ihren Workloads verringert wird.

Dieses Muster ist ein alternativer Ansatz zur CloudFormation AvailabilityZoneId AWS-Eigenschaft.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Mindestens zwei aktive AWS-Konten in derselben AWS-Region.
- Prüfen Sie, wie viele Availability Zones zur Unterstützung Ihrer VPC-Anforderungen in der Region erforderlich sind.
- Identifizieren und notieren Sie die AZ-ID für jede Availability Zone, die Sie unterstützen müssen. Weitere Informationen dazu finden Sie unter Availability Zone IDs für Ihre AWS-Ressourcen in der AWS Resource Access Manager-Dokumentation.

- Eine geordnete, durch Kommas getrennte Liste Ihrer AZ. IDs Beispielsweise wird die erste Availability Zone auf Ihrer Liste als zugeordnet`az1`, die zweite Availability Zone als, und diese Zuordnungsstruktur wird fortgesetzt`az2`, bis Ihre kommagetrennte Liste vollständig zugeordnet ist. Es gibt keine maximale Anzahl von AZ, die zugeordnet werden können. IDs
- Die `az-mapping.yaml` Datei aus dem Mapping-Repository für die Availability Zone mit GitHub mehreren Konten, die auf Ihren lokalen Computer kopiert wurde

Architektur

Das folgende Diagramm zeigt die Architektur, die in einem Konto bereitgestellt wird und die Werte für den AWS Systems Manager Parameter Store erstellt. Diese Parameter Store-Werte werden verwendet, wenn Sie eine VPC im Konto erstellen.

Das Diagramm zeigt den folgenden Workflow:

1. Die Lösung dieses Musters wird für alle Konten bereitgestellt, die zonale Konsistenz für eine VPC erfordern.
2. Die Lösung erstellt Parameter Store-Werte für jede AZ-ID und speichert den neuen Availability Zone-Namen.
3. Die CloudFormation AWS-Vorlage verwendet den Availability Zone-Namen, der in jedem Parameter Store-Wert gespeichert ist, und dies gewährleistet die zonale Konsistenz.

Das folgende Diagramm zeigt den Arbeitsablauf für die Erstellung einer VPC mit der Lösung dieses Musters.

Das Diagramm zeigt den folgenden Workflow:

1. Reichen Sie eine Vorlage für die Erstellung einer VPC an AWS CloudFormation ein.
2. AWS CloudFormation löst die Parameter Store-Werte für jede Availability Zone auf und gibt den Availability Zone-Namen für jede AZ-ID zurück.
3. Eine VPC wird mit der richtigen AZ erstellt, die für die zonale Konsistenz IDs erforderlich ist.

Nachdem Sie die Lösung für dieses Muster bereitgestellt haben, können Sie Subnetze erstellen, die auf die Parameter Store-Werte verweisen. Wenn Sie AWS verwenden CloudFormation, können Sie auf die Werte der Availability Zone-Zuordnungsparameter aus dem folgenden YAML-formatierten Beispielcode verweisen:

```
Resources:
    PrivateSubnet1AZ1:
        Type: AWS::EC2::Subnet
        Properties:
            VpcId: !Ref VPC
            CidrBlock: !Ref PrivateSubnetAZ1CIDR
            AvailabilityZone:
                !Join
                    - ''
                    - - '{{resolve:ssm:/az-mapping/az1:1}}'
```

Dieser Beispielcode ist in der `vpc-example.yaml` Datei aus dem Mapping-Repository für GitHub mehrere Accounts Availability Zone enthalten. Es zeigt Ihnen, wie Sie eine VPC und Subnetze erstellen, die sich aus Gründen der zonalen Konsistenz an den Werten des Parameterspeichers orientieren.

Technologie-Stack

- AWS CloudFormation
- AWS Lambda
- AWS Systems Manager Parameter Store

Automatisierung und Skalierung

Sie können dieses Muster mithilfe von AWS CloudFormation StackSets oder der Lösung Customizations for AWS Control Tower für all Ihre AWS-Konten bereitstellen. Weitere Informationen finden Sie unter Working with AWS CloudFormation StackSets in der AWS Cloudformation-Dokumentation und unter Anpassungen für AWS Control Tower in der AWS-Lösungsbibliothek.

Nachdem Sie die CloudFormation AWS-Vorlage bereitgestellt haben, können Sie sie so aktualisieren, dass sie die Parameter Store-Werte verwendet und Ihre VPCs In-Pipelines oder gemäß Ihren Anforderungen bereitstellen.

Tools

AWS-Services

- AWS CloudFormation hilft Ihnen dabei, Ihre AWS-Ressourcen zu modellieren und einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus zu verwalten. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben und sie zusammen als Stapel zu starten und zu konfigurieren, anstatt Ressourcen einzeln zu verwalten. Sie können Stacks für mehrere AWS-Konten und AWS-Regionen verwalten und bereitstellen.
- AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.
- AWS Systems Manager Parameter Store ist eine Funktion von AWS Systems Manager. Es bietet sicheren, hierarchischen Speicher für die Verwaltung von Konfigurationsdaten und Geheimnissen.

Code

Der Code für dieses Muster befindet sich im Mapping-Repository für die Availability Zone mit GitHub mehreren Konten.

Epen

Stellen Sie die Datei az-mapping.yaml bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie die erforderl ichen Availability Zones für die Region.	1. Ermitteln Sie die AZ IDs , die in Ihrer Region konsistent verwendet werden muss. 2. Notieren Sie diese AZ IDs in einer durch Kommas getrennten Liste und in der Reihenfolge, in der	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	sie angewendet werden sollen. Beispielsweise wird die erste Availability Zone auf Ihrer Liste als `az1` und die zweite als zugeordnet. `az2` Es gibt keine maximale Anzahl von AZ IDs , die zugeordnet werden können.	
Stellen Sie die Datei az-mapping.yaml bereit.	Verwenden Sie die `az-mapping.yaml` Datei, um einen CloudFormation AWS-Stack in allen erforderlichen AWS-Konten zu erstellen. Verwenden Sie im `AZIds` Parameter die kommagetr ennte Liste, die Sie zuvor erstellt haben. Wir empfehlen Ihnen, AWS CloudFormation StackSets oder die Customizations for AWS Control Tower Solution zu verwenden.	Cloud-Architekt

Stellen Sie das VPCs in Ihren Konten bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie die CloudForm ation AWS-Vorlagen an.	Wenn Sie die Subnetze mit AWS erstellen CloudForm ation, passen Sie die Vorlagen so an, dass sie die Parameter Store-Werte verwenden, die Sie zuvor erstellt haben.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Eine Beispielvorlage finden Sie in der `vpc-example.yaml` Datei im Mapping-Repository für die Availability Zone mit GitHub mehreren Konten.	
Stellen Sie das bereit VPCs.	Stellen Sie die benutzerdefinierten CloudFormation AWS-Vorlagen in Ihren Konten bereit. Jede VPC in der Region hat dann zonale Konsistenz in den Availability Zones, die für die Subnetze verwendet werden.	Cloud-Architekt

Zugehörige Ressourcen

- Availability Zone IDs für Ihre AWS-Ressourcen (AWS Resource Access Manager-Dokumentation)
- AWS::EC2::Subnet(CloudFormation AWS-Dokumentation)

Verwenden Sie Benutzer IDs in IAM-Richtlinien für Zugriffskontrolle und Automatisierung

Erstellt von Srinivas Ananda Babu (AWS) und Ram Kandaswamy (AWS)

Übersicht

Dieses Muster erklärt die potenziellen Fallstricke bei der Verwendung von benutzernamenbasierten Richtlinien in AWS Identity and Access Management (IAM), die Vorteile der Verwendung von Benutzern und die Integration dieses Ansatzes in die Automatisierung. IDs AWS CloudFormation

In der hilft Ihnen der IAM-Dienst dabei AWS Cloud, Benutzeridentitäten und Zugriffskontrolle präzise zu verwalten. Wenn Sie sich bei der Erstellung von IAM-Richtlinien auf Benutzernamen verlassen, kann dies jedoch zu unvorhergesehenen Sicherheitsrisiken und Problemen mit der Zugriffskontrolle führen. Stellen Sie sich zum Beispiel dieses Szenario vor: Ein neuer Mitarbeiter, John Doe, tritt Ihrem Team bei, und Sie erstellen ein IAM-Benutzerkonto mit dem Benutzernamen, der ihm über IAM-Richtlinien`j.doe`, die auf Benutzernamen verweisen, Berechtigungen gewährt. Wenn John das Unternehmen verlässt, wird das Konto gelöscht. Das Problem beginnt, wenn eine neue Mitarbeiterin, Jane Doe, Ihrem Team beitritt und der `j.doe` Benutzername neu erstellt wird. Die bestehenden Richtlinien gewähren Jane Doe jetzt dieselben Berechtigungen wie John Doe. Dies führt zu einem potenziellen Albtraum in Bezug auf Sicherheit und Compliance.

Die manuelle Aktualisierung jeder Richtlinie, um neue Benutzerdaten zu berücksichtigen, ist ein zeitaufwändiger und fehleranfälliger Prozess, insbesondere wenn Ihr Unternehmen wächst. Die Lösung besteht darin, eine eindeutige und unveränderliche Benutzer-ID zu verwenden. Wenn Sie ein IAM-Benutzerkonto erstellen, AWS weist Sie dem IAM-Benutzer eine eindeutige Benutzer-ID (oder Prinzipal-ID) zu. Sie können diese Benutzer IDs in Ihren IAM-Richtlinien verwenden, um eine konsistente und zuverlässige Zugriffskontrolle zu gewährleisten, die nicht durch Änderungen oder Wiederverwendung von Benutzernamen beeinträchtigt wird.

Eine IAM-Richtlinie, die eine Benutzer-ID verwendet, könnte beispielsweise so aussehen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::example-bucket",
            "Principal": { "AWS": "arn:aws:iam::123456789012:user/abcdef01234567890" }
```

```
        }
      ]
}
```

Die Verwendung von Usern IDs in IAM-Richtlinien bietet unter anderem folgende Vorteile:

- Einzigartigkeit. Benutzer IDs sind in allen AWS-Konten Bereichen einzigartig und bieten daher eine korrekte und konsistente Berechtigungsanwendung.
- Unveränderlichkeit. Der Benutzer IDs kann nicht geändert werden, daher bieten sie eine stabile Kennung für die Referenzierung von Benutzern in Richtlinien.
- Prüfung und Einhaltung der Vorschriften. AWS-Services nehmen häufig Benutzer IDs in Logs und Audit-Trails auf, sodass Aktionen leicht auf bestimmte Benutzer zurückgeführt werden können.
- Automatisierung und Integration. Durch die Verwendung von IDs AWS APIs SDKs Benutzerprogrammierungsskripten oder Automatisierungsskripten wird sichergestellt, dass Prozesse von Benutzernamenänderungen nicht beeinträchtigt werden.
- Zukunftssicherheit. Durch die Verwendung von IDs Benutzerrichtlinien von Anfang an können potenzielle Probleme mit der Zugriffskontrolle oder umfangreiche Richtlinienaktualisierungen vermieden werden.

Automation

Wenn Sie IaC-Tools (Infrastructure as Code) verwenden AWS CloudFormation, können die Fallstricke benutzernamenbasierter IAM-Richtlinien immer noch zu Problemen führen. Die IAM-Benutzerressource gibt den Benutzernamen zurück, wenn Sie die systeminterne Funktion aufrufen. `Ref` Im Zuge der Weiterentwicklung der Infrastruktur Ihres Unternehmens kann der Zyklus des Erstellens und Löschens von Ressourcen, einschließlich IAM-Benutzerkonten, zu unbeabsichtigten Problemen bei der Zugriffskontrolle führen, wenn Sie Benutzernamen wiederverwenden.

Um dieses Problem zu beheben, empfehlen wir Ihnen, Benutzer IDs in Ihre Vorlagen zu integrieren. CloudFormation Es kann jedoch schwierig sein, Benutzer IDs für diesen Zweck zu finden. Hier können benutzerdefinierte Ressourcen hilfreich sein. Sie können CloudFormation benutzerdefinierte Ressourcen verwenden, um die Funktionalität des Dienstes zu erweitern, indem Sie ihn mit AWS APIs oder mit externen Diensten integrieren. Indem Sie eine benutzerdefinierte Ressource erstellen, die die Benutzer-ID für einen bestimmten IAM-Benutzer abruft, können Sie die Benutzer-ID in Ihren CloudFormation Vorlagen verfügbar machen. Dieser Ansatz rationalisiert den Prozess der Benutzerreferenzierung IDs und stellt sicher, dass Ihre Automatisierungsworkflows robust und zukunftssicher bleiben.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Eine IAM-Rolle für einen Cloud-Administrator zum Ausführen der Vorlage AWS CloudFormation

Einschränkungen

- Einige AWS-Services sind nicht in allen AWS-Regionen verfügbar. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie auf der Seite Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Architektur

Zielarchitektur

Das folgende Diagramm zeigt, wie eine benutzerdefinierte Ressource, unterstützt von, AWS CloudFormation verwendet wird AWS Lambda , um die IAM-Benutzer-ID abzurufen.

Automatisierung und Skalierung

Sie können die CloudFormation Vorlage mehrfach für verschiedene AWS-Regionen Konten verwenden. Sie müssen sie in jeder Region oder jedem Konto nur einmal ausführen.

Tools

AWS-Services

- IAM — AWS Identity and Access Management (IAM) ist ein Webservice, mit dem Sie den Zugriff AWS auf Ressourcen sicher kontrollieren können. Sie verwenden IAM, um zu steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzt) ist, Ressourcen zu nutzen.
- AWS CloudFormation— AWS CloudFormation unterstützt Sie bei der Modellierung und Einrichtung Ihrer AWS Ressourcen, sodass Sie weniger Zeit mit der Verwaltung dieser Ressourcen verbringen und sich mehr auf Ihre Anwendungen konzentrieren können, auf denen sie ausgeführt werden. AWS Sie erstellen eine Vorlage, die die AWS Ressourcen beschreibt, die Sie benötigen, und CloudFormation kümmert sich um die Bereitstellung und Konfiguration dieser Ressourcen für Sie.

- AWS Lambda— AWS Lambda ist ein Rechendienst, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.

Bewährte Methoden

Wenn Sie bei Null anfangen oder eine Implementierung auf der grünen Wiese planen, empfehlen wir Ihnen dringend, eine zentralisierte AWS IAM Identity CenterBenutzerverwaltung zu verwenden. IAM Identity Center lässt sich in Ihre vorhandenen Identitätsanbieter (wie Active Directory oder Okta) integrieren, um Benutzeridentitäten zu bündeln AWS, sodass Sie IAM-Benutzer nicht mehr direkt erstellen und verwalten müssen. Dieser Ansatz gewährleistet nicht nur eine konsistente Zugriffskontrolle, sondern vereinfacht auch die Verwaltung des Benutzerlebenszyklus und trägt zur Verbesserung von Sicherheit und Compliance in Ihrer gesamten Umgebung bei. AWS

Epen

Bestätigen Sie die Berechtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie Ihre AWS-Konto und Ihre IAM-Rolle.	Vergewissern Sie sich, dass Sie über eine IAM-Rolle mit Berechtigungen zum Bereitstellen von CloudFormation Vorlagen in Ihrem verfügen. AWS-Konto Wenn Sie planen, die Vorlage im letzten Schritt dieses Verfahrens AWS CLI anstelle der CloudFormation Konsole bereitzustellen, sollten Sie auch temporäre Anmeldeinformationen für die Ausführung von AWS CLI Befehlen einrichten. Anweisungen	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	finden Sie in der IAM-Dokumentation.	

Erstellen Sie eine CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CloudFormation Vorlage.	1. Erstellen Sie eine CloudFormation Vorlage, indem Sie den Anweisungen in der CloudFormation Dokumentation folgen. Sie können entweder das JSON- oder das YAML-Format verwenden. Bei diesem Muster wird davon ausgegangen, dass Sie das YAML-Format verwenden. 2. Speichern Sie die Vorlage mit dem Namen `get_unique_user_id.yaml` .	AWS DevOps, Cloud-Architekt

Fügen Sie einen Eingabeparameter für den Benutzernamen hinzu.	Fügen Sie dem `Parameters` Abschnitt der CloudFormation Vorlage den folgenden Code hinzu:
	`Parameters:`
	`  NewIamUserName:`
	`  Type: String`
	`  Description: Unique username for the new IAM user`
		AWS DevOps, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dieser Parameter fordert den Benutzer zur Eingabe des Benutzernamens auf.	

Fügen Sie eine benutzerdefinierte Ressource hinzu, um einen IAM-Benutzer zu erstellen.	Fügen Sie dem `Resources` Abschnitt der CloudFormation Vorlage den folgenden Code hinzu:
	`Resources:`
	`  rNewIamUser:`
	`  Type: 'AWS::IAM ::User'`
	`  Properties:`
	`  UserName: !Ref NewIamUserName`
	Dieser Code fügt eine CloudFormation Ressource hinzu, die einen IAM-Benutzer mit dem durch den `NewIamUserName` Parameter angegebenen Namen erstellt.
		AWS DevOps, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie eine Ausführungsrolle für die Lambda-Funktion hinzu.	In diesem Schritt erstellen Sie eine IAM-Rolle, die einer AWS Lambda Funktion die Berechtigung zum Abrufen des IAM erteilt. `UserId` Geben Sie die folgenden Mindestberechtigungen an, die für die Ausführung von Lambda erforderlich sind: • `logs:CreateLogStream` • `logs:PutLogEvents` • `CreateLogGroup` • `iam:GetUser` • `AssumeRole` für `lambda.amazonaws.com` Anweisungen zum Erstellen einer Ausführungsrolle finden Sie in der Lambda-Dokumentation. Sie werden im nächsten Schritt, wenn Sie die Lambda-Funktion erstellen, auf diese Rolle verweisen.	AWS-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie eine Lambda-Funktion hinzu, um das eindeutige `UserId` IAM zu erhalten.	In diesem Schritt definieren Sie eine Lambda-Funktion mit einer Python-Laufzeit, um das eindeutige `UserId` IAM zu erhalten. Fügen Sie dazu dem `Resources` Abschnitt der Vorlage den folgenden Code hinzu. CloudFormation `<<ROLENAME>>` Ersetzen Sie ihn durch den Namen der Ausführungsrolle, die Sie im letzten Schritt erstellt haben. `GetUserLambdaFunction: Type: 'AWS::Lambda::Function' Properties: Handler: index.handler Role: <<ROLENAME>> Timeout: 30 Runtime: python3.11 Code: ZipFile: | import cfnresponse, boto3 def handler(event, context): try: print(event) user = boto3.client('iam').get_user(UserName=event['ResourceP`	AWS DevOps, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	roperties'][‘NewIa mUserName'])['User'] cfnrespon se.send(event, context, cfnrespon se.SUCCESS, {'NewIamU serId': user['Use rId'], 'NewIamUs erPath': user['Pat h'], 'NewIamUserArn': user['Arn']}) except Exception as e: cfnrespon se.send(event, context, cfnrespon se.FAILED, {'NewIamU ser': str(e)})	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie eine benutzerd efinierte Ressource hinzu.	Fügen Sie dem `Resources` Abschnitt der CloudFormation Vorlage den folgenden Code hinzu: `rCustomGetUniqueUserId: Type: 'Custom::rCustomGetUniqueUserIdWithLambda' Properties: ServiceToken: !GetAtt GetUserLambdaFunction.Arn NewIamUserName: !Ref NewIamUserName` Diese benutzerdefinierte Ressource ruft die Lambda-Funktion auf, um das `UserID` IAM abzurufen.	AWS DevOps, Cloud-Architekt
Definieren Sie CloudFormation Ausgaben.	Fügen Sie dem `Outputs` Abschnitt der CloudFormation Vorlage den folgenden Code hinzu: `Outputs: NewIamUserId: Value: !GetAtt rCustomGetUniqueUserId.NewIamUserId` Dadurch wird das IAM `UserID` für den neuen IAM-Benutzer angezeigt.	AWS DevOps, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Speichern Sie die Vorlage.	Speichern Sie Ihre Änderungen an der CloudFormation Vorlage.	AWS DevOps, Cloud-Architekt

Stellen Sie die CloudFormation Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation Vorlage bereit.	Folgen Sie den Anweisungen in der CloudFormation Dokumentation, um die `get_unique_user_id.yaml` Vorlage mithilfe der CloudFormation Konsole bereitzustellen. Alternativ können Sie den folgenden AWS CLI Befehl ausführen, um die Vorlage bereitzustellen: `aws cloudformation create-stack \ --stack-name DemoNewUser \ --template-body file://get_unique_user_id.yaml \ --parameters Parameter Key=NewIamUserName,ParameterValue=demouser \ --capabilities CAPABILITY_NAMED_IAM`	AWS DevOps, Cloud-Architekt

Zugehörige Ressourcen

- Erstellen Sie einen Stack von der CloudFormation Konsole aus (CloudFormation Dokumentation)
- Lambda-gestützte benutzerdefinierte Ressourcen (Dokumentation) CloudFormation
- Eindeutige Identifikatoren (IAM-Dokumentation)
- Verwenden Sie temporäre Anmeldeinformationen mit AWS Ressourcen (IAM-Dokumentation)

Validieren Sie den Account Factory for Terraform (AFT) -Code lokal

Erstellt von Alexandru Pop (AWS) und Michal Gorniak (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Dieses Muster zeigt, wie HashiCorp Terraform-Code, der von AWS Control Tower Account Factory for Terraform (AFT) verwaltet wird, lokal getestet wird. Terraform ist ein IaC-Tool (Infrastructure as Code), mit dem Sie mithilfe von Code Cloud-Infrastruktur und -Ressourcen bereitstellen und verwalten können. AFT richtet eine Terraform-Pipeline ein, mit der Sie mehrere Eingänge bereitstellen und anpassen können. AWS-Konten AWS Control Tower

Während der Codeentwicklung kann es hilfreich sein, Ihre Terraform-Infrastruktur als Code (IaC) lokal außerhalb der AFT-Pipeline zu testen. Dieses Muster zeigt, wie Sie Folgendes tun können:

- Rufen Sie eine lokale Kopie des Terraform-Codes ab, der in den AWS CodeCommit Repositorys Ihres AFT-Verwaltungskontos gespeichert ist.
- Simulieren Sie die AFT-Pipeline lokal mithilfe des abgerufenen Codes.

Dieses Verfahren kann auch verwendet werden, um Terraform-Befehle auszuführen, die nicht Teil der normalen AFT-Pipeline sind. Sie können diese Methode beispielsweise verwenden, um Befehle wie`terraform validate`, `terraform plan`terraform destroy, und auszuführen. `terraform import`

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine aktive Umgebung AWS mit mehreren Konten, die Folgendes verwendet AWS Control Tower
- Eine vollständig bereitgestellte AFT-Umgebung
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert
- AWS CLI Credential Helper für AWS CodeCommit, installiert und konfiguriert
- Python 3.x
- Git, auf Ihrem lokalen Computer installiert und konfiguriert
- `git-remote-commit`Hilfsprogramm, installiert und konfiguriert

- Terraform, installiert und konfiguriert (die lokale Terraform-Paketversion muss mit der Version übereinstimmen, die in der AFT-Bereitstellung verwendet wird)

Einschränkungen

- Dieses Muster deckt nicht die Bereitstellungsschritte ab AWS Control Tower, die für AFT oder bestimmte Terraform-Module erforderlich sind.
- Die Ausgabe, die während dieses Verfahrens lokal generiert wird, wird nicht in den Laufzeitprotokollen der AFT-Pipeline gespeichert.

Architektur

Zieltechnologie-Stack

- AFT-Infrastruktur, die innerhalb einer AWS Control Tower Bereitstellung bereitgestellt wird
- Terraform
- Git
- AWS CLI Version 2

Automatisierung und Skalierung

Dieses Muster zeigt, wie Terraform-Code für globale AFT-Kontoanpassungen in einem einzigen von AFT verwalteten System lokal aufgerufen wird. AWS-Konto Nachdem Ihr Terraform-Code validiert wurde, können Sie ihn auf die verbleibenden Konten in Ihrer Umgebung mit mehreren Konten anwenden. Weitere Informationen finden Sie in der Dokumentation unter Anpassungen erneut aufrufen. AWS Control Tower

Sie können auch einen ähnlichen Prozess verwenden, um AFT-Kontoanpassungen in einem lokalen Terminal auszuführen. Um Terraform-Code lokal aus AFT-Kontoanpassungen aufzurufen, klonen Sie das aft-account-customizationsRepository anstelle des Repositorys CodeCommit in Ihrem aft-global-account-customizationsAFT-Verwaltungskonto.

Tools

AWS-Services

- AWS Control Towerhilft Ihnen bei der Einrichtung und Verwaltung einer Umgebung mit AWS mehreren Konten und folgt dabei den vorgeschriebenen Best Practices.

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie AWS-Services über Befehle in Ihrer Befehlszeilen-Shell interagieren können.

Andere Dienste

- HashiCorp Terraform ist ein Infrastructure-as-Code-Tool (IaC), mit dem Sie mithilfe von Code Cloud-Infrastruktur und -Ressourcen bereitstellen und verwalten können.
- Git ist ein verteiltes Open-Source-Versionskontrollsystem.

Code

Im Folgenden finden Sie ein Beispiel für ein Bash-Skript, mit dem Terraform-Code, der von AFT verwaltet wird, lokal ausgeführt werden kann. Folgen Sie den Anweisungen im Abschnitt Epics dieses Musters, um das Skript zu verwenden.

```
#! /bin/bash
# Version: 1.1 2022-06-24 Unsetting AWS_PROFILE since, when set, it interferes with
 script operation
#          1.0 2022-02-02 Initial Version
#
# Purpose: For use with AFT: This script runs the local copy of TF code as if it were
 running within AFT pipeline.
#        * Facilitates testing of what the AFT pipline will do
#           * Provides the ability to run terraform with custom arguments (like 'plan'
 or 'move') which are currently not supported within the pipeline.
#
# © 2021 Amazon Web Services, Inc. or its affiliates. All Rights Reserved.
# This AWS Content is provided subject to the terms of the AWS Customer Agreement
# available at http://aws.amazon.com/agreement or other written agreement between
# Customer and either Amazon Web Services, Inc. or Amazon Web Services EMEA SARL or
 both.
#
# Note: Arguments to this script are passed directly to 'terraform' without parsing nor
 validation by this script.
#
# Prerequisites:
#    1. local copy of ct GIT repositories
#    2. local backend.tf and aft-providers.tf filled with data for the target account
 on which terraform is to be run
#       Hint: The contents of above files can be obtain from the logs of a previous
 execution of the AFT pipeline for the target account.
```

```
#    3. 'terraform' binary is available in local PATH
#    4. Recommended: .gitignore file containing 'backend.tf', 'aft_providers.tf' so the
 local copy of these files are not pushed back to git

readonly credentials=$(aws sts assume-role \
    --role-arn arn:aws:iam::$(aws sts get-caller-identity --query "Account" --output
 text ):role/AWSAFTAdmin \
    --role-session-name AWSAFT-Session \
    --query Credentials )

unset AWS_PROFILE
export AWS_ACCESS_KEY_ID=$(echo $credentials | jq -r '.AccessKeyId')
export AWS_SECRET_ACCESS_KEY=$(echo $credentials | jq -r '.SecretAccessKey')
export AWS_SESSION_TOKEN=$(echo $credentials | jq -r '.SessionToken')
terraform "$@"
```

Epen

Speichern Sie den Beispielcode als lokale Datei

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Speichern Sie den Beispielcode als lokale Datei.	1. Kopieren Sie das Bash-Beispielskript, das sich im Codeabschnitt dieses Musters befindet, und fügen Sie es in einen Code-Editor ein. 2. Benennen Sie die Datei `ct_terraform.sh` und speichern Sie die Datei dann lokal in einem dafür vorgesehenen Ordner, z. B. `~/scripts` oder`~/bin`.	AWS-Administrator
Machen Sie den Beispielcode lauffähig.	Öffnen Sie ein Terminalfenster und authentifizieren Sie sich AWS bei Ihrem AFT-Verwaltungskonto, indem Sie	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	einen der folgenden Schritte ausführen: • Verwenden Sie ein vorhandenes AWS CLI Profil, das mit den für den Zugriff auf das AFT-Verwaltungskonto erforderlichen Berechtigungen konfiguriert ist. Um das Profil zu verwenden, können Sie den folgenden Befehl ausführen: `export AWS_PROFILE=<aft account profile name>` • Wenn Ihre Organisation SSO für den Zugriff verwendet AWS, geben Sie die Anmeldeinformationen für Ihr AFT-Verwaltungskonto auf der SSO-Seite Ihrer Organisation ein. **Note** Ihre Organisation verfügt möglicherweise auch über ein benutzerdefiniertes Tool, mit dem Sie Anmeldeinformationen für Ihre AWS	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Umgebung bereitste llen können.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie den korrekten Zugriff auf das AFT-Verwaltungskonto AWS-Region.	**⚠ Important**
	Stellen Sie sicher, dass Sie dieselbe Terminalsitzung verwenden, mit der Sie sich bei Ihrem AFT-Verwaltungskonto authentifiziert haben.
	
	1. Navigieren Sie zu Ihren AFT-Bereitstellungen, AWS-Region indem Sie den folgenden Befehl ausführen:
	`export AWS_REGION=<aft_region>`
	2. Vergewissern Sie sich, dass Sie das richtige Konto haben.
	a. Führen Sie den folgenden Befehl aus:
	`aws code-commit list-repositories`
	b. Stellen Sie sicher, dass die in der Ausgabe aufgeführten Repositorys mit den Namen der Repositorys in Ihrem AFT-Verwaltungskonto übereinstimmen.
		AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie ein neues, lokales Verzeichnis zum Speichern des AFT-Repository-Codes.	Führen Sie in derselben Terminalsitzung die folgenden Befehle aus:
	`mkdir my_aft`
	`cd my_aft`
		AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie den Remote-AFT-Repository-Code.	1. Führen Sie in Ihrem lokalen Terminal den folgenden Befehl aus: `git clone codecommit::$AWS_REGION://aft-global-customizations` **Note** Der Einfachheit halber verwenden dieses Verfahren und AFT nur einen Hauptcodezweig. Um die Codeverzweigung zu verwenden, können Sie hier auch Befehle zur Codeverzweigung eingeben. Alle vorgenommenen Änderungen aus dem Nicht-Hauptzweig werden jedoch rückgängig gemacht, wenn die AFT-Automatisierung Code aus dem Hauptzweig anwendet.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Navigieren Sie in das geklonte Verzeichnis: `cd aft-global-customizations/terraform`	

Erstellen Sie die Terraform-Konfigurationsdateien, die für die lokale Ausführung der AFT-Pipeline erforderlich sind

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Öffnen Sie eine zuvor ausgeführte AFT-Pipeline und kopieren Sie die Terraform-Konfigurationsdateien in einen lokalen Ordner.	**Note** Die `backend.tf` in diesem Epos erstellten `aft-providers.tf` Konfigurationsdateien werden benötigt, damit die AFT-Pipeline lokal ausgeführt werden kann. Diese Dateien werden automatisch innerhalb der cloudbasierten AFT-Pipeline erstellt, müssen aber manuell erstellt werden, damit die Pipeline lokal ausgeführt werden kann. Für die lokale Ausführung der AFT-Pipeline ist ein Satz von Dateien erforderlich, die den Betrieb	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Pipeline innerhalb einer einzigen Datei repräsentieren AWS-Konto. 1. Melden Sie sich mit den Anmeldeinformationen Ihres AWS Control Tower Verwaltungskontos bei der AWS Management Console an und öffnen Sie die AWS CodePipeline Konsole. Stellen Sie sicher, dass Sie sich an derselben AWS-Region Stelle befinden, an der Sie AFT bereitgestellt haben. 2. Wählen Sie im linken Navigationsbereich die Option Pipelines aus. 3. Wählen Sie ##########-customizations-pipeline. (Die ############ ist die ID, die Sie verwenden , um Terraform-Code lokal auszuführen.) AWS-Konto 4. Vergewissern Sie sich, dass für „Letzte Ausführung markiert“ der Wert Erfolgrei ch angezeigt wird. Wenn der Wert anders ist, müssen Sie Ihre Anpassungen in der AFT-Pipeline erneut	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	aufrufen. Weitere Informationen finden Sie in der Dokumentation unter Anpassungen erneut aufrufen. AWS Control Tower 5. Wählen Sie die neueste Laufzeit aus, um deren Details aufzurufen. 6. Suchen Sie im Abschnitt Apply-AFT-Global-Customizations nach der Apply-Terraform-Stufe. 7. Wählen Sie den Abschnitt Details der Apply-Terraform-Phase aus. 8. Suchen Sie das Laufzeitprotokoll für die Apply-Terraform-Stufe. 9. Suchen Sie im Laufzeitprotokoll nach dem Abschnitt, der mit den folgenden Zeilen beginnt und endet: `"\n\n aft-providers.tf ... "\n \n backend.tf"` 10. Kopieren Sie die Ausgabe zwischen diesen beiden Labels und speichern Sie sie als lokale Datei mit dem Namen `aft-providers.tf` im lokalen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Terraform-Ordner (dem aktuellen Arbeitsverzeichnis Ihrer Terminalsitzung).
	
	Beispiel für eine auto generierte providers.tf-Anweisung
	
	`## Autogenerated providers.tf ## ## Updated on: 2022-05-31 16:27:45 ## provider "aws" { region = "us-east-2" assume_role { role_arn = "arn:aws:iam::######## :role/AWSAFTExecution" } default_tags { tags = { managed_by = "AFT" } } }`
	
	11. Suchen Sie im Laufzeitprotokoll nach dem Abschnitt, der mit den folgenden Zeilen beginnt und endet:
	
	`"\n\n tf ... "\n \n backend.tf"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	12. Kopieren Sie die Ausgabe zwischen diesen beiden Labels und speichern Sie sie als lokale Datei mit dem Namen `tf` im lokalen Terraform-Ordner (dem aktuellen Arbeitsverzeichnis Ihrer Terminalsitzung). Beispiel für eine automatisch generierte backend.tf-Anweisung `## Autogenerated backend.tf ## ## Updated on: 2022-05-31 16:27:45 ## terraform { required_version = ">= 0.15.0" backend "s3" { region = "us-east-2" bucket = "aft-backend-###########-primary-region" key = "############-aft-global-customizations/terraform.tfstate" dynamodb_table = "aft-backend-#######" encrypt = "true"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
    kms_key_id     =
 "########-####-####-
####-############"
    role_arn       =
 "arn:aws:iam::####
#########:role/AWS
AFTExecution"
  }
}
```

> **Note**
>
> Die `aft-providers.tf` Dateien `backend.tf` und sind an eine bestimmte AFT-Bereitstellung und einen bestimmten AWS-Konto Ordner gebunden. Diese Dateien unterscheiden sich auch, je nachdem, ob sie sich im aft-global-customizationsaft-account-customizationsand-Repository innerhalb derselben AFT-Bereitstellung befinden. Stellen Sie sicher, dass Sie beide Dateien aus derselben Runtime-Liste generieren.

Führen Sie die AFT-Pipeline lokal aus, indem Sie das Bash-Beispielskript verwenden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Implementieren Sie die Terraform-Konfigurationsänderungen, die Sie validieren möchten.	1. Navigieren Sie zum geklonten aft-global-customizationsRepository, indem Sie den folgenden Befehl ausführen: `cd aft-global-customizations/terraform` **Note** Die Dateien `backend.tf` und `aft-providers.tf` befinden sich in diesem Verzeichnis. Das Verzeichnis enthält auch Terraform-Dateien aus dem aft-global-customizations Repository. 2. Integrieren Sie die Terraform-Codeänderungen, die Sie lokal testen möchten, in die Konfigurationsdateien.	AWS-Administrator
Führen Sie das `ct_terraform.sh` Skript aus und überprüfen Sie die Ausgabe.	1. Navigieren Sie zu dem lokalen Ordner, der das Sh-Skript enthält.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	2. Um Ihren geänderten n Terraform-Code zu validieren, führen Sie das `ct_terraform.sh` Skript aus, indem Sie den folgenden Befehl ausführen:
	`~/scripts/ct_terraform.sh apply`
	`terraform --help`
	Note
	In diesem Schritt können Sie jeden Terraform-Befehl ausführen. Führen Sie den folgenden Befehl aus, um eine vollständige Liste der Terraform -Befehle anzuzeige n:
	3. Überprüfen Sie die Befehlsausgabe und debuggen Sie dann die Codeänderungen lokal, bevor Sie die Änderungen festschreiben und an das AFT-Repository zurücksen den.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Important • Alle lokal vorgenommenen und nicht an das Remote-Repository zurückgeschickten Änderungen sind temporär und können jederzeit durch eine laufende AFT-Pipeline-Automatisierung rückgängig gemacht werden. • Die AFT-Automatisierung kann jederzeit ausgeführt werden, da sie von anderen Benutzern und AFT-Automatisierungsauslösern aufgerufen werden kann. • AFT wendet immer Code aus dem Hauptzweig des Repositorys an und macht alle noch nicht festgeschriebenen Änderungen rückgängig.	

Übertragen Sie Ihre lokalen Codeänderungen zurück in das AFT-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Verweise auf die `aft-providers.tf` Dateien `backend.tf` und	Fügen Sie die `aft-providers.tf` Dateien `backend.tf` und, die	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

zu einer `.gitignore` Datei hinzu.	Sie erstellt haben, zu einer `.gitignore` Datei hinzu, indem Sie die folgenden Befehle ausführen:
	`echo backend.tf >> .gitignore`
	`echo aft-providers.tf >>.gitignore`
	Note
	Durch das Verschieben der Dateien in die `.gitignore` Datei wird sichergestellt, dass sie nicht festgeschrieben und in das Remote-AFT-Repository zurückgeschickt werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Übergeben Sie Ihre Codeänderungen und übertragen Sie sie an das Remote-AFT-Repository.	1. Führen Sie den folgenden Befehl aus, um dem Repository neue Terraform -Konfigurationsdateien hinzuzufügen:
	`git add <filename>`
	2. Führen Sie die folgenden Befehle aus, um Ihre Änderungen zu übernehme n und sie in CodeCommitt das Remote-AFT-Reposit ory zu übertragen:
	`git commit -a`
	`git push`
	Important
	Die Codeänderungen, die Sie vornehmen , wenn Sie dieses Verfahren bis zu diesem Zeitpunkt befolgen, gelten AWS-Konto nur für eine.
		AWS-Administrator

Führen Sie die Änderungen auf mehrere Konten aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Nehmen Sie die Änderungen auf all Ihre Konten vor, die von AFT verwaltet werden.	Folgen Sie den Anweisungen in der Dokumentation unter Anpassungen erneut aufrufen AWS-Konten, um die Änderungen auf mehrere, die von AFT verwaltet werden, anzuwenden. AWS Control Tower	AWS-Administrator

Mehr Muster

- Fügen Sie HA mithilfe einer Read Replica zu Oracle PeopleSoft auf Amazon RDS Custom hinzu
- Automatische Prüfung von AWS Sicherheitsgruppen, die den Zugriff von öffentlichen IP-Adressen aus ermöglichen
- Automatisieren Sie die Kontoerstellung mit dem Landing Zone Accelerator auf AWS
- Automatisieren Sie das Hinzufügen oder Aktualisieren von Windows-Registrierungseinträgen mit AWS Systems Manager
- Automatisieren Sie die AWS-Ressourcenbewertung
- Automatisieren Sie das AWS Service Catalog-Portfolio und die Produktbereitstellung mithilfe von AWS CDK
- Automatisieren Sie regionsübergreifendes Failover und Failback mithilfe des DR Orchestrator Framework
- Automatisieren Sie das Löschen von AWS CloudFormation Stacks und zugehörigen Ressourcen
- Automatisieren Sie die Erfassung und Visualisierung von benutzerdefinierten Amazon MWAA-Metriken auf Amazon Managed Grafana mithilfe von Terraform
- Automatisieren Sie die RabbitMQ-Konfiguration in Amazon MQ
- Automatisieren Sie die Replikation von Amazon RDS-Instances auf AWS-Konten
- Automatisches Hinzufügen einer von AWS verwalteten Richtlinie für Systems Manager zu EC2 Instanzprofilen mithilfe von Cloud Custodian und AWS CDK
- Automatisches Erstellen von CI/CD-Pipelines und Amazon ECS-Clustern für Microservices mithilfe von AWS CDK
- Automatische Erkennung von Änderungen und Initiierung verschiedener CodePipeline Pipelines für ein Monorepo in CodeCommit
- Automatisches Reaktivieren CloudTrail von AWS mithilfe einer benutzerdefinierten Behebungsregel in AWS Config
- Erstellen Sie mit dem AWS DataOps Development Kit eine Datenpipeline, um Google Analytics-Daten aufzunehmen, zu transformieren und zu analysieren
- Erstellen Sie ein Micro Focus Enterprise Server PAC mit Amazon EC2 Auto Scaling und Systems Manager
- Erstellen und übertragen Sie Docker-Images mithilfe von GitHub Actions und Terraform auf Amazon ECR

- Zentralisieren Sie die Verwaltung von IAM-Zugriffsschlüsseln in AWS Organizations mithilfe von Terraform
- Zentralisieren Sie die Verteilung von Softwarepaketen in AWS Organizations mithilfe von Terraform
- Verketten Sie AWS-Services mithilfe eines serverlosen Ansatzes
- Konfiguration einer Rechenzentrumserweiterung für VMware Cloud on AWS mithilfe des Hybrid Linked Mode
- Konfigurieren Sie die Protokollierung von Modellaufrufen in Amazon Bedrock mithilfe von AWS CloudFormation
- Konfigurieren Sie das schreibgeschützte Routing in einer Always-On-Verfügbarkeitsgruppe in SQL Server auf AWS
- Konfigurieren Sie VMware vRealize Automation für die Bereitstellung VMs in der VMware Cloud auf AWS
- Erstellen Sie ein Portal für Mikro-Frontends mithilfe AWS Amplify von Angular und Module Federation
- Erstellen Sie eine kontoübergreifende EventBridge Amazon-Verbindung in einer Organisation
- Automatisches Erstellen dynamischer CI-Pipelines für Java- und Python-Projekte
- Stellen Sie eine Amazon API Gateway Gateway-API auf einer internen Website mithilfe von privaten Endpunkten und einem Application Load Balancer bereit
- Bereitstellen und Debuggen von Amazon EKS-Clustern
- Implementieren und verwalten Sie AWS Control Tower Kontrollen mithilfe von AWS CDK und CloudFormation
- Stellen Sie AWS Control Tower Kontrollen mithilfe von Terraform bereit und verwalten Sie sie
- Stellen Sie CloudWatch Synthetics Canaries mithilfe von Terraform bereit
- Stellen Sie mithilfe von Terraform und DRA ein Lustre-Dateisystem für die Hochleistungsdatenverarbeitung bereit
- Stellen Sie mithilfe AWS von Terraform und Amazon Bedrock einen RAG-Anwendungsfall bereit
- Bereitstellen von Ressourcen in einer AWS Wavelength Zone mithilfe von Terraform
- Stellen Sie mithilfe von Terraform SQL Server-Failover-Cluster-Instances auf Amazon EC2 und Amazon FSx bereit
- Stellen Sie die Security Automations for AWS WAF Solution mithilfe von Terraform bereit
- Erkennen Sie Amazon RDS- und Aurora-Datenbank-Instances mit ablaufenden CA-Zertifikaten
- Dokumentieren Sie Ihr AWS-Landingzone-Design

- Stellen Sie sicher, dass ein IAM-Profil mit einer EC2 Instance verknüpft ist
- Exportieren Sie AWS Backup Backup-Berichte aus einer gesamten Organisation in AWS Organizations als CSV-Datei
- Generieren Sie mit Amazon Personalize personalisierte und neu eingestufte Empfehlungen
- Identifizieren und benachrichtigen Sie, wenn Amazon Data Firehose-Ressourcen nicht mit einem AWS KMS Schlüssel verschlüsselt sind
- Implementieren Sie Account Factory for Terraform (AFT) mithilfe einer Bootstrap-Pipeline
- Implementieren Sie eine pfadbasierte API-Versionierung mithilfe benutzerdefinierter Domains in Amazon API Gateway
- Installieren Sie SSM Agent mithilfe von Kubernetes auf Amazon EKS-Worker-Knoten DaemonSet
- Installieren Sie den SSM-Agent und den CloudWatch Agenten auf Amazon EKS-Worker-Knoten mit preBootstrapCommands
- Integrieren Sie VMware vRealize Network Insight mit VMware Cloud on AWS
- Verwalten Sie AWS IAM Identity Center Berechtigungssätze als Code, indem Sie AWS CodePipeline
- AWS Service Catalog-Produkte in mehreren AWS-Konten und AWS-Regionen verwalten
- Verwalten Sie lokale Containeranwendungen, indem Sie Amazon ECS Anywhere mit dem AWS CDK einrichten
- AWS Organizations Richtlinien mithilfe AWS CodePipeline von Amazon Bedrock als Code verwalten
- Massenmigrieren von DNS-Einträgen in eine private gehostete Zone von Amazon Route 53
- Migrieren Sie die Oracle E-Business Suite zu Amazon RDS Custom
- Migrieren Sie Oracle PeopleSoft zu Amazon RDS Custom
- Migrieren Sie RHEL-BYOL-Systeme mithilfe von AWS MGN zu Instances mit AWS-Lizenz
- Migrieren Sie VMware SDDC mithilfe von VMware HCX zur Cloud auf AWS VMware
- Richten Sie einen nutzbaren Mindestdatenraum für die gemeinsame Nutzung von Daten zwischen Organisationen ein
- ElastiCache Amazon-Cluster auf Verschlüsselung im Ruhezustand überwachen
- Überwachen Sie die Anwendungsaktivität mithilfe von CloudWatch Logs Insights
- ElastiCache Cluster für Sicherheitsgruppen überwachen
- Überwachen Sie SAP RHEL Pacemaker-Cluster mithilfe von AWS-Services

- Optimieren Sie serverlose Bereitstellungen mit mehreren Konten mithilfe der AWS CDK Workflows und Aktionen GitHub
- Greifen Sie privat von mehreren aus auf einen zentralen AWS-Serviceendpunkt zu VPCs
- Bereitstellen von AWS Service Catalog Produkten auf der Grundlage von AWS CloudFormation Vorlagen mithilfe von GitHub Aktionen
- Stellen Sie IAM-Rollen mit den geringsten Rechten bereit, indem Sie eine Rollenautomatenlösung bereitstellen
- Entfernen Sie EC2 Amazon-Einträge AWS Managed Microsoft AD mithilfe AWS-Konten von AWS Lambda Automatisierung
- Entfernen Sie EC2 Amazon-Einträge in derselben AWS-Konto Form AWS Managed Microsoft AD mithilfe von AWS Lambda Automatisierung
- Datenbankanmeldedaten rotieren, ohne Container neu zu starten
- Eine Benachrichtigung senden, wenn ein IAM-Benutzer erstellt wird
- Senden Sie mithilfe von VMware Aria Operations AWS for Logs Logs von VMware Cloud on an Splunk
- Richten Sie einen serverlosen Mobilfunkrouter für eine zellenbasierte Architektur ein
- Richten Sie mithilfe von AWS CDK eine CI/CD-Pipeline für Hybrid-Workloads auf Amazon ECS Anywhere ein und GitLab
- Richten Sie mithilfe von NICE EnginFrame und NICE DCV Session Manager eine auto skalierende virtuelle Desktop-Infrastruktur ein
- Richten Sie eine HA/DR-Architektur für Oracle E-Business Suite auf Amazon RDS Custom mit einer aktiven Standby-Datenbank ein
- Richten Sie die DNS-Auflösung für Hybridnetzwerke in einer Umgebung mit mehreren Konten AWS ein
- Richten Sie mithilfe von Amazon eine Multi-AZ-Infrastruktur für einen SQL Server Always On FCI ein FSx
- Richten Sie die Oracle UTL_FILE-Funktionalität auf Aurora PostgreSQL-Compatible ein
- Vereinfachen Sie die Anwendungsauthentifizierung mit gegenseitigem TLS in Amazon ECS mithilfe von Application Load Balancer
- Vereinfachen Sie die Verwaltung privater Zertifikate mithilfe von AWS Private CA und AWS RAM
- Optimieren Sie mithilfe von SageMaker KI und Hydra Workflows für maschinelles Lernen — von der lokalen Entwicklung bis hin zu skalierbaren Experimenten
- Automatisches Taggen Transit Gateway Gateway-Anhängen mithilfe von AWS Organizations

- Rollen für eine PeopleSoft Oracle-Anwendung auf Amazon RDS Custom for Oracle wechseln
- Verwenden Sie Amazon Q Developer als Programmierassistenten, um Ihre Produktivität zu steigern

Web- und mobile Apps

Themen

- Authentifizieren Sie bestehende Benutzer von React-Anwendungen mithilfe von Amazon Cognito und AWS Amplify UI
- Kontinuierliche Bereitstellung einer modernen AWS Amplify Amplify-Webanwendung aus einem AWS-Repository CodeCommit
- Erstellen Sie eine React-App mithilfe von AWS Amplify und fügen Sie die Authentifizierung mit Amazon Cognito hinzu
- Erstellen Sie ein Portal für Mikro-Frontends mithilfe AWS Amplify von Angular und Module Federation
- Stellen Sie eine React-basierte Einzelseitenanwendung auf Amazon S3 bereit und CloudFront
- Stellen Sie eine Amazon API Gateway Gateway-API auf einer internen Website mithilfe von privaten Endpunkten und einem Application Load Balancer bereit
- Betten Sie ein QuickSight Amazon-Dashboard in eine lokale Angular-Anwendung ein
- Entdecken Sie die Full-Stack-Entwicklung von cloudnativen Webanwendungen mit Green Boost
- Führen Sie Komponententests für eine Node.js -Anwendung mithilfe GitHub von AWS aus CodeBuild
- Strukturieren Sie ein Python-Projekt in hexagonaler Architektur mit AWS Lambda
- Mehr Muster

Authentifizieren Sie bestehende Benutzer von React-Anwendungen mithilfe von Amazon Cognito und AWS Amplify UI

Erstellt von Daniel Kozhemyako (AWS)

Übersicht

Dieses Muster zeigt, wie einer vorhandenen Frontend-React-Anwendung mithilfe einer AWS Amplify UI-Bibliothek und eines Amazon Cognito Cognito-Benutzerpools Authentifizierungsfunktionen hinzugefügt werden.

Das Muster verwendet Amazon Cognito, um Authentifizierung, Autorisierung und Benutzerverwaltung für die Anwendung bereitzustellen. Es verwendet auch eine Komponente aus Amplify UI, einer Open-Source-Bibliothek, die die Funktionen der AWS Amplify Benutzeroberflächenentwicklung (UI) erweitert. Die Authenticator-UI-Komponente verwaltet Anmeldesitzungen und führt den mit der Cloud verbundenen Workflow aus, der Benutzer über Amazon Cognito authentifiziert.

Nachdem Sie dieses Muster implementiert haben, können sich Benutzer mit beliebigen der folgenden Anmeldeinformationen anmelden:

- Benutzername und Passwort
- Anbieter sozialer Identitäten wie Apple, Facebook, Google und Amazon
- Identitätsanbieter für Unternehmen, die entweder SAML 2.0-kompatibel oder OpenID Connect (OIDC) kompatibel sind

> **Note**
>
> Um eine benutzerdefinierte Authentifizierungs-UI-Komponente zu erstellen, können Sie die Authenticator-Benutzeroberflächenkomponente im Headless-Modus ausführen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine aktive AWS-Konto
- Eine Webanwendung mit React 18.2.0 oder höher

- Node.js und npm 6.14.4 oder höher, installiert

Einschränkungen

- Dieses Muster gilt nur für React-Webanwendungen.
- Dieses Muster verwendet eine vorgefertigte Amplify-UI-Komponente. Die Lösung deckt nicht die Schritte ab, die zur Implementierung einer benutzerdefinierten UI-Komponente erforderlich sind.

Produktversionen

- Amplify UI 6.1.3 oder höher (Gen 1)
- Amplify 6.0.16 oder höher (Gen 1)

Architektur

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur, die Amazon Cognito verwendet, um Benutzer für eine React-Webanwendung zu authentifizieren.

Tools

AWS-Services

- Amazon Cognito bietet Authentifizierung, Autorisierung und Benutzerverwaltung für Web- und mobile Apps.

Andere Tools

- Amplify UI ist eine Open-Source-UI-Bibliothek, die anpassbare Komponenten bereitstellt, die Sie mit der Cloud verbinden können.
- Node.js ist eine ereignisgesteuerte JavaScript Laufzeitumgebung, die für die Erstellung skalierbarer Netzwerkanwendungen entwickelt wurde.
- npm ist eine Softwareregistrierung, die in einer Node.js -Umgebung ausgeführt wird und verwendet wird, um Pakete gemeinsam zu nutzen oder auszuleihen und die Bereitstellung von privaten Paketen zu verwalten.

Bewährte Methoden

Wenn Sie eine neue Anwendung erstellen, empfehlen wir Ihnen, Amplify Gen 2 zu verwenden.

Epen

Erstellen Sie einen Amazon Cognito Cognito-Benutzerpool

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Benutzerpool.	Erstellen Sie einen Amazon Cognito Cognito-Benutzerpool. Konfigurieren Sie die Anmeldeoptionen und Sicherheitsanforderungen des Benutzerpools entsprechend Ihrem Anwendungsfall.	App-Developer
Fügen Sie einen App-Client hinzu.	Konfigurieren Sie einen Benutzerpool-App-Client. Dieser Client ist erforderlich, damit Ihre Anwendung mit dem Amazon Cognito Cognito-Benutzerpool interagieren kann.	App-Developer

Integrieren Sie Ihren Amazon Cognito Cognito-Benutzerpool in die Authenticator-UI-Komponente

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die Abhängigkeiten.	Um die `@aws-amplify/ui-react` Pakete `aws-amplify` und zu installieren, führen Sie den folgenden Befehl im Stammverzeichnis Ihrer Anwendung aus:	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`npm i @aws-amplify/ui-react aws-amplify`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie den Benutzerpool.	Erstellen Sie anhand des folgenden Beispiels eine `aws-exports.js` Datei und speichern Sie sie im `src` Ordner. Die Datei sollte die folgenden Informationen enthalten:
	• AWS-Region in dem sich Ihr Amazon Cognito Cognito-Benutzerpool befindet
	• Amazon Cognito Cognito-Benutzerpool-ID
	• App-Client-ID
	
	`// replace the user pool region, id, and app client id details`
	`const awsmobile = {`
	`"aws_project_region": "put_your_region_here",`
	`"aws_cognito_region": "put_your_region_here",`
	`"aws_user_pools_id": "put_your_user_pool_id_here",`
	`"aws_user_pools_web_client_id": "put_your_user_pool_app_id_here"`
	`}`
	
	`export default awsmobile;`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Importieren und konfigurieren Sie den Amplify-Dienst.	1. Importieren und laden Sie die Datei in der Einstiegspunktdatei der `aws-exports.js` Anwendung (z. B.`App.js`), indem Sie die folgenden Codezeilen eingeben:
	`import { Amplify } from 'aws-amplify'; import awsExports from './aws-exports';`
	2. Konfigurieren Sie den Amplify-Client anhand des folgenden Beispiels mithilfe der `aws-exports.js` Datei:
	`// Configure Amplify in index file or root file Amplify.configure({ ...awsExports });`
	Weitere Informationen finden Sie unter Amplify-Kategorien konfigurieren in der Amplify-Dokumentation.
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie die Authenticator-UI-Komponente hinzu.	Um die `Authenticator` UI-Komponente anzuzeigen, fügen Sie der Einstiegspunktdatei (`App.js`) der Anwendung die folgenden Codezeilen hinzu:
	`import { Authenticator } from '@aws-amplify/ui-react';`
	`import '@aws-amplify/ui-react/styles.css';`
	Note
	Das Beispielcode-Snippet importiert die `Authenticator` UI-Komponente und die Amplify UI-Datei styles.css, die erforderlich ist, wenn die vorgefertigten Designs der Komponente verwendet werden.
	Die `Authenticator` UI-Komponente bietet zwei Rückgabewerte:
	• Angaben zum Benutzer
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Eine Funktion, die aufgerufen werden kann, um den Benutzer abzumelden Sehen Sie sich die folgende Beispielkomponente an: `function App() { return ( <Authenticator> {({ signOut, user }) => ( <div> <p>Welcome {user.username}</p> <button onClick={signOut}>Sign out</button> </div> )} </Authenticator> ); }` **Note** Eine `App.js` Beispieldatei finden Sie im Abschnitt Zusätzliche Informationen dieses Musters.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

(Optional) Rufen Sie Sitzungsinformationen ab.	Nachdem ein Benutzer authentifiziert wurde, können Sie vom Amplify-Client Daten über seine Sitzung abrufen. Sie können beispielsweise das JSON-Webtoken (JWT) aus der Sitzung eines Benutzers abrufen, sodass Sie die Anfragen aus seiner Sitzung an eine Backend-API authentifizieren können.
	
	Sehen Sie sich das folgende Beispiel für einen Anforderungsheader an, der ein JWT enthält:
	
	`import { fetchAuthSession } from 'aws-amplify/auth';`
	`(await fetchAuthSession()).tokens?.idToken?.toString();`
		App-Developer

Fehlerbehebung

Problem	Lösung
Neue Benutzer können sich nicht für die Anwendung registrieren.	Stellen Sie wie folgt sicher, dass Ihr Amazon Cognito Cognito-Benutzerpool so konfiguriert ist, dass Benutzer sich selbst für den Benutzerpool anmelden können:

Problem	Lösung
	• Melden Sie sich bei der AWS Management Console an und öffnen Sie dann die Amazon Cognito Cognito-Konsole. • Wählen Sie im linken Navigationsbereich Benutzerpools aus. • Wählen Sie Ihren Benutzerpool aus der Liste aus. • Wählen Sie unter Allgemeine Einstellungen die Option Richtlinien aus. • Wählen Sie Benutzern erlauben, sich selbst zu registrieren.
Die Auth-Komponente funktioniert nach dem Upgrade von Version 5 auf Version 6 nicht mehr.	Die `Auth` Kategorie wurde in Amplify v6 auf einen funktionalen Ansatz umgestellt und Parameter benannt. Sie müssen die Funktion jetzt APIs direkt aus dem `aws-amplify/auth` Pfad importieren. Weitere Informationen finden Sie unter Migration von v5 zu v6 in der Amplify-Dokumentation.

Zugehörige Ressourcen

- Erste Schritte mit Amazon Cognito (AWS Website)
- Erstellen Sie eine neue React-App (React-Dokumentation)
- Was ist Amazon Cognito? (Amazon Cognito Cognito-Dokumentation)
- Amplify-UI-Bibliothek (Amplify-Dokumentation)

Zusätzliche Informationen

Die `App.js` Datei sollte den folgenden Code enthalten:

```
import './App.css';
import { Amplify } from 'aws-amplify';
import awsExports from './aws-exports';
```

```
import { fetchAuthSession } from 'aws-amplify/auth';
import { Authenticator } from '@aws-amplify/ui-react';
import '@aws-amplify/ui-react/styles.css';
Amplify.configure({ ...awsExports });
let token = (await fetchAuthSession()).tokens?.idToken?.toString();
function App() {
  return (
      <Authenticator>
        {({ signOut, user }) => (
            <div>
              <p>Welcome {user.username}</p>
                <p>Your token is: {token}</p>
              <button onClick={signOut}>Sign out</button>
            </div>
        )}
      </Authenticator>
  );
}

export default App;
```

Kontinuierliche Bereitstellung einer modernen AWS Amplify Amplify-Webanwendung aus einem AWS-Repository CodeCommit

Erstellt von Deekshitulu Pentakota (AWS) und Sai Katakam (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen.

Moderne Webanwendungen sind als einseitige Anwendungen (SPAs) aufgebaut, die alle Anwendungskomponenten in statische Dateien packen. Mithilfe von AWS Amplify Hosting können Sie eine CI/CD-Pipeline (Continuous Integration and Continuous Deployment) aufbauen, die eine moderne Webanwendung erstellt, bereitstellt und hostet, die in einem Git-basierten Repository verwaltet wird. Wenn Sie Amplify Hosting mit dem Code-Repository verbinden, initiiert jeder Commit einen einzigen Workflow zur Bereitstellung des Frontends und Backends der Anwendung. Der Vorteil dieses Ansatzes besteht darin, dass die Webanwendung erst aktualisiert wird, nachdem die Bereitstellung erfolgreich abgeschlossen wurde, wodurch Inkonsistenzen zwischen Frontend und Backend vermieden werden.

In diesem Muster verwenden Sie ein CodeCommit AWS-Repository, um Ihre moderne Webanwendung zu verwalten. Die Beispiel-Webanwendung in dieser Anleitung verwendet das React SPA-Framework. Amplify Hosting unterstützt jedoch viele andere SPA-Frameworks wie Angular, Vue, Next.js und unterstützt auch Single-Site-Generatoren wie Gatsby, Hugo und Jekyll.

Dieses Muster richtet sich an AWS-Entwickler, die Erfahrung mit den folgenden Services und Konzepten haben:

- AWS CodeCommit
- AWS Amplify Hosting
- React
- JavaScript
- Node.js
- npm
- Git

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Berechtigungen zum Erstellen von Ressourcen in Amplify und CodeCommit. Weitere Informationen finden Sie unter Identity and Access Management für Amplify und Identity and Access Management für AWS CodeCommit.
- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert.
- Ein Texteditor oder Code-Editor.
- CodeCommit, eingerichtet für HTTPS-Benutzer mit Git-Anmeldeinformationen.
- Eine IAM-Servicerolle für Amplify.
- npm und Node.js, installiert (npm-Dokumentation).

Einschränkungen

- Dieses Muster behandelt nicht die Entwicklung und Integration eines Backends für die Amplify-Anwendung, wie z. B. eine API, Authentifizierung oder Datenbank. Weitere Informationen zu Backends finden Sie unter Erstellen eines Backends in der Amplify-Dokumentation.

Produktversionen

- AWS-CLI Version 2.0
- Node.js Version 16.x oder höher

Architektur

Zieltechnologie-Stack

- CodeCommitAWS-Repository mit einem React-SPA
- AWS Amplify Hosting-Arbeitsablauf

Zielarchitektur

Tools

AWS-Services

- AWS Amplify Hosting bietet einen Git-basierten Workflow für das Hosten serverloser Full-Stack-Webanwendungen mit kontinuierlicher Bereitstellung.
- AWS CodeCommit ist ein Versionskontrollservice, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.

Andere Tools

- Node.js ist eine ereignisgesteuerte JavaScript Laufzeitumgebung, die für die Erstellung skalierbarer Netzwerkanwendungen entwickelt wurde.
- npm ist eine Softwareregistrierung, die in einer Node.js -Umgebung ausgeführt wird und verwendet wird, um Pakete gemeinsam zu nutzen oder auszuleihen und die Bereitstellung von privaten Paketen zu verwalten.

Epen

Erstellen Sie ein Repository CodeCommit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein -Repository.	Anweisungen finden Sie in der CodeCommit Dokumentation unter Erstellen eines CodeCommit AWS-Repositorys.	AWS DevOps
Klonen Sie das Repository	Anweisungen finden Sie in der CodeCommit Dokumentation unter Connect zum CodeCommit Repository durch Klonen des Repositor	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ys. Wenn Sie dazu aufgefordert werden, geben Sie die Git-Anmeldeinformationen ein.	

Erstellen Sie eine React-Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine neue React-Anwendung.	1. Geben Sie den folgenden Befehl ein, um zum geklonten Repo zu navigieren. Ersetzen Sie es `<repo name>` durch den Namen Ihres CodeCommit Repos.
	`$ cd <repo name>`
	2. Geben Sie den folgenden Befehl ein, um eine neue React-Anwendung im geklonten Repository zu erstellen.
	`$ npx create-react-app .`
	3. Codieren Sie die Anwendung und geben Sie dann den folgenden Befehl ein, um sie zu starten.
	`$ npm start`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen zum Erstellen einer benutzerd efinierten React-Anwendung finden Sie in der Anleitung Create React App in der Dokumentation Create React App. Sie können auch eine React-Beispielanwendung für Ihr Amplify-Konto bereitste llen, indem Sie den Anweisung en unter Bereitstellen eines Frontends in der Amplify-D okumentation folgen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie einen Branch und übertragen Sie den Code.	1. Geben Sie den folgenden Befehl ein, um lokal einen neuen Zweig zu erstellen. Dabei <branch> handelt es sich um den Namen, den Sie dem neuen Zweig zuweisen möchten.
	`$ git checkout -b <branch>`
	2. Geben Sie den folgenden Befehl ein, um den Branch in das CodeCommit Repository zu übertragen. Dort <branch> befindet sich der Name, den Sie im vorherigen Schritt zugewiesen haben. Weitere Informationen finden Sie unter Mit Commits arbeiten.
	`$ git push --set-upstream origin <branch>`
		App-Developer

Stellen Sie die Anwendung in AWS Amplify Hosting bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Connect Amplify mit dem Repository.	Anweisungen finden Sie unter Ein Repository Connect in der Amplify Hosting-Dokumentation. Wählen Sie AWS CodeCommit und das	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Repository und den Branch aus, die Sie zuvor erstellt haben.	

Definieren Sie die Frontend-Build-Einstellungen.	Anweisungen finden Sie unter Bestätigen der Build-Einstellungen für das Frontend in der Amplify Hosting-Dokumentation. Akzeptieren Sie die Standardeinstellungen oder geben Sie Folgendes ein.
	`Build settings:`
	`version: 0.1`
	`frontend:`
	`  phases:`
	`  preBuild:`
	`  commands:`
	`  - npm ci`
	`  build:`
	`  commands:`
	`  - npm run build`
	`  artifacts:`
	`  baseDirectory:`
	`build`
	`  files:`
	`  - '**/*'`
	`  cache:`
	`  paths:`
	`  - node_modules/`
	`**/*`
		App-Developer

Überprüfen und bereitstellen.	Anweisungen finden Sie unter Speichern und Bereitstellen in der Amplify Hosting-Dokumentation. Warten Sie, bis der Bereitstellungsvorgang abgeschlossen ist.	App-Developer

Bestätigen Sie die kontinuierliche Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die erste Bereitstellung.	Wenn der Bereitstellungsvorgang abgeschlossen ist, wählen Sie unter Domain den Link aus. Stellen Sie sicher, dass die Anwendung wie erwartet funktioniert.	App-Developer
Senden Sie eine Änderung in das Code-Repository.	Bearbeiten Sie den Code auf Ihrer lokalen Workstation und übertragen Sie die Änderungen in das CodeCommit Repository. Amplify Hosting erkennt die Änderung im Repository und startet automatisch den Build- und Bereitstellungsprozess. Vergewissern Sie sich, dass die Anwendungsupdates auf der Domain sichtbar sind.	App-Developer

Zugehörige Ressourcen

CodeCommit AWS-Dokumentation

- Einrichtung für AWS CodeCommit
  - Einrichtung für HTTPS-Benutzer mit Git-Anmeldeinformationen
  - Einrichtungsschritte für HTTPS-Verbindungen zu CodeCommit AWS-Repositorys unter Linux, macOS oder Unix mit dem AWS CLI Credential Helper
- Erste Schritte mit AWS CodeCommit

Dokumentation zum AWS Amplify Hosting

- Erste Schritte mit vorhandenem Code
- Benutzerdefinierte Domains einrichten

React-Ressourcen

- Erstellen Sie eine React App-Website
- Erstellen Sie die React-App-Dokumentation
- Erstellen Sie ein React-App-Repository (GitHub)

Erstellen Sie eine React-App mithilfe von AWS Amplify und fügen Sie die Authentifizierung mit Amazon Cognito hinzu

Erstellt von Rishi Singla (AWS)

Übersicht

Dieses Muster zeigt, wie Sie mit AWS Amplify eine React-basierte App erstellen und wie Sie mithilfe von Amazon Cognito Authentifizierung zum Frontend hinzufügen. AWS Amplify besteht aus einer Reihe von Tools (Open-Source-Framework, visuelle Entwicklungsumgebung, Konsole) und Services (Web-App und statisches Website-Hosting), um die Entwicklung von Mobil- und Web-Apps auf AWS zu beschleunigen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Node.js und npm sind auf Ihrem Computer installiert

Produktversionen

- Node.js Version 10.x oder höher (um Ihre Version zu überprüfen, führen Sie es `node -v` in einem Terminalfenster aus)
- npm Version 6.x oder höher (um Ihre Version zu überprüfen, führen Sie es `npm -v` in einem Terminalfenster aus)

Architektur

Zieltechnologie-Stack

- AWS Amplify
- Amazon Cognito

Tools

- Befehlszeilenschnittstelle (CLI) Amplify

- Amplify Libraries (Open-Source-Clientbibliotheken)
- Amplify Studio (visuelle Oberfläche)

Epen

Installieren Sie AWS Amplify CLI

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie die Amplify CLI.	Die Amplify CLI ist eine einheitliche Toolchain zur Erstellung von AWS-Cloud-Services für Ihre React-App. Führen Sie Folgendes aus, um die Amplify-CLI zu installieren:
	`npm install -g @aws-amplify/cli`
	npm benachrichtigt Sie, wenn eine neue Hauptversion verfügbar ist. Wenn ja, verwenden Sie den folgenden Befehl, um Ihre Version von npm zu aktualisieren:
	`npm install -g npm@9.8.0`
	wobei sich 9.8.0 auf die Version bezieht, die Sie installieren möchten.
		App-Developer

Erstelle eine React-App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine React-App.	Verwenden Sie den folgenden Befehl, um eine neue React-App zu erstellen:
	`npx create-react-app amplify-react-application`
	wo `ampify-react-application` ist der Name der App.
	Wenn die App erfolgreich erstellt wurde, wird die Meldung angezeigt:
	`Success! Created amplify-react-application`
	Für die React-App wird ein Verzeichnis mit verschiedenen Unterordnern erstellt.
		App-Developer

Starten Sie die App auf Ihrem lokalen Computer.	Gehen Sie zu dem Verzeichnis `amplify-react-application`, das im vorherigen Schritt erstellt wurde, und führen Sie den folgenden Befehl aus: `amplify-react-application% npm start`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dadurch wird die React-App auf Ihrem lokalen Computer gestartet.	

Konfigurieren Sie die Amplify CLI

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Amplify für die Verbindung mit Ihrem AWS-Konto.	Konfigurieren Sie Amplify, indem Sie den folgenden Befehl ausführen: `amplify-react-application % amplify configure` Die Amplify CLI fordert Sie auf, die folgenden Schritte auszuführen, um den Zugriff auf Ihr AWS-Konto einzurichten: 1. Melden Sie sich mit Ihrem AWS-Administratorkonto an. 2. Geben Sie die AWS-Region an, die Sie verwenden möchten. 3. Erstellen Sie einen AWS Identity and Access Management (IAM) - Benutzer mit programmatischem Zugriff und hängen Sie die `AdministratorAccess-Amplify`	Allgemein AWS, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Berechtigungsrichtlinie an den Benutzer an. 4. Erstellen Sie die Zugriffss chlüssel-ID und den geheimen Zugriffsschlüssel und kopieren Sie sie anschließend. 5. Geben Sie diese Daten in das Terminal ein. 6. Erstellen Sie einen Profilnamen oder verwenden Sie das Standardprofil. ⚠ Warning Für dieses Szenario sind IAM-Benut zer mit programma tischem Zugriff und langfristigen Anmeldeinformation en erforderlich, was ein Sicherheitsrisiko darstellt. Um dieses Risiko zu minimieren, empfehlen wir, diesen Benutzern nur die Berechtigungen zu gewähren, die sie für die Ausführung der Aufgabe benötigen, und diese Benutzer zu entfernen, wenn sie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	nicht mehr benötigt werden. Die Zugriffss chlüssel können bei Bedarf aktualisiert werden. Weitere Informationen finden Sie unter Aktualisieren von Zugriffsschlüsseln im IAM-Benutzerhandbuch.
	
	Diese Schritte werden im Terminal wie folgt angezeigt.
	
	`Follow these steps to set up access to your AWS account:`
	`Sign in to your AWS administrator account: https://console.aws.amazon.com/`
	`Press Enter to continue`
	`Specify the AWS Region`
	`? region: us-east-1`
	`Follow the instructions at https://docs.amplify.aws/cli/start/install/#configure-the-amplify-cli`
	`to complete the user creation in the AWS console`
	`https://console.aws.amazon.com/iamv2/home#/users/create`
	`Press Enter to continue`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	``` Enter the access key of the newly created user: ? accessKeyId: ******************** ? secretAccessKey: ****************** ****************** **** This would update/cr eate the AWS Profile in your local machine ? Profile Name: new Successfully set up the new user. ``` Weitere Informationen zu diesen Schritten finden Sie in der Dokumentation im Amplify Dev Center.	

Amplify initialisieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initialisieren Sie Amplify.	1. Um Amplify im neuen Verzeichnis zu initialisieren, führen Sie Folgendes aus: ``` amplify init ``` Amplify fordert Sie zur Eingabe des Projektnamens und der Konfigurationspara meter auf	App-Entwickler, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	2. Geben Sie alle Parameter an und drücken Sie dann Y, um das Projekt mit der angegebenen Konfiguration zu initialisieren.
	
	`Project information`
	`| Name: amplifyreactproject`
	
	`| Environment: dev`
	
	`| Default editor: Visual Studio Code`
	
	`| App type: javascript`
	
	`| Javascript framework: react`
	
	`| Source Directory Path: src`
	
	`| Distribution Directory Path: build`
	
	`| Build Command: npm run-script build`
	
	`| Start Command: npm run-script start`
	
	3. Wählen Sie das Profil aus, das Sie im vorherigen Schritt erstellt haben. Die Ressourcen werden in der `dev` Umgebung des von	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Ihnen erstellten Amplify-P rojekts bereitgestellt.
	4. Um zu bestätigen, dass die Ressourcen erstellt wurden, können Sie die AWS Amplify Amplify-Konsole öffnen und die CloudFormation AWS-Vorla ge, die zur Erstellung der Ressourcen verwendet wurde, sowie die Details anzeigen.
	`Deploying root stack amplifyreactproject [ ========== ---------- ---- ] 2/4 amplify-amplif yreactproject-d… AWS::CloudFormatio n::Stack CREATE_IN_PROGRESS`
	`UnauthRole AWS::IAM: :Role CREATE_COMPLETE`
	`DeploymentBucket AWS::S3:: Bucket CREATE_IN_PROGRESS`
	`AuthRole AWS::IAM:`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`:Role CREATE_COMPLETE`	

Fügen Sie dem Frontend eine Authentifizierung hinzu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Authentifizierung hinzufügen.	Sie können den `amplify add <category>` Befehl verwenden, um Funktionen wie eine Benutzeranmeldung oder eine Backend-API hinzuzufügen. In diesem Schritt verwenden Sie den Befehl, um die Authentif izierung hinzuzufügen. Amplify bietet einen Backend-Authentifizierungsservice mit Amazon Cognito, Frontend-Bibliotheken und einer Drop-In-Authenticator-UI-Ko mponente. Zu den Funktionen gehören Benutzeranmeldung, Benutzeranmeldung, Multi-Faktor-Authentifizierung, Benutzerabmeldung und passwortlose Anmeldung. Sie können Benutzer auch authentifizieren, indem Sie föderierte Identitätsanbieter wie Amazon, Google und Facebook integrieren. Die Amplify-Authentifizierungsk	App-Entwickler, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	ategorie lässt sich nahtlos in andere Amplify-Kategorien wie API, Analytik und Speicher integrieren, sodass Sie Autorisierungsregeln für authentifizierte und nicht authentifizierte Benutzer definieren können.
	
	1. Führen Sie den folgenden Befehl aus, um die Authentif izierung für Ihre React-App zu konfigurieren:
	
	`amplify-react-appl ication1 % amplify add auth`
	
	Dadurch werden die folgenden Informationen und Eingabeaufforderungen angezeigt. Sie können je nach Ihren Geschäfts- und Sicherheitsanforderungen die passende Konfiguration auswählen.
	
	`Using service: Cognito, provided by: awscloudformation The current configure d provider is Amazon Cognito. Do you want to use the default authentic ation and security`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	configuration? (Use arrow keys) # Default configuration Default configuration with Social Provider (Federation) Manual configuration I want to learn more.	
	2. Wählen Sie für ein einfaches Beispiel die Standardkonfiguration und dann den Anmeldemechanismus für Benutzer (in diesem Fall E-Mail): How do you want users to be able to sign in? Username # Email Phone Number Email or Phone Number I want to learn more.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	3. Umgehen Sie die erweiterten Einstellungen, um das Hinzufügen von Authentifizierungsressourcen abzuschließen:
	`Do you want to configure advanced settings? (Use arrow keys)`
	`# No, I am done.`
	`Yes, I want to make some additional changes.`
	4. Erstellen Sie Ihre lokalen Backend-Ressourcen und stellen Sie sie in der Cloud bereit:
	`amplify-react-application1 % amplify push`
	Mit diesem Befehl werden die entsprechenden Änderungen an den Congito-Benutzerpools in Ihrem Konto vorgenommen.
	5. Drücken Sie Y, um die `auth` Ressource mithilfe von zu konfigurieren. CloudFormation	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Dadurch werden die folgenden Ressourcen konfiguriert:
	
	`UserPool AWS::Cognito::UserPool CREATE_COMPLETE`
	`UserPoolClientWeb AWS::Cognito::UserPoolClient CREATE_COMPLETE`
	
	`UserPoolClientWeb AWS::Cognito::UserPoolClient CREATE_COMPLETE`
	
	`UserPoolClientRole AWS::IAM::Role CREATE_COMPLETE`
	
	`UserPoolClientLambda AWS::Lambda::Function CREATE_COMPLETE`
	`UserPoolClientLambdaPolicy AWS::IAM::Policy CREATE_COMPLETE`
	
	`UserPoolClientLogPolicy AWS::IAM::Policy CREATE_IN_PROGRESS`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie können diese Ressourcen auch mit der AWS Cognito-Konsole anzeigen (suchen Sie nach Cognito-Benutzerpools und Identitätspools). In diesem Schritt wird die `aws-exports.js` Datei im `src` Ordner für Ihre React-App mit den Cognito-Benutzerpool- und Identität spool-Konfigurationen aktualisiert.	

Ändern Sie die Datei App.js

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Datei App.js.	Öffnen und überarbeiten Sie die `App.js` Datei in dem `src` Ordner. Die geänderte Datei sollte wie folgt aussehen: `{  App.Js File after modifications: import React from 'react'; import logo from './logo.svg'; import './App.css'; import { Amplify } from 'aws-amplify'; import { withAuthenticator, Button,`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`Heading } from '@aws-amplify/ui-react'; import awsconfig from './aws-exports'; Amplify.configure(awsconfig); function App({ signOut }) { return (    Thankyou for doing verification   My Content  <button onClick={signOut}>Sign out</button>   ); } export default withAuthenticator(App);`	
Importiere React-Pakete.	Die `App.js` Datei importiert zwei React-Pakete. Installieren Sie diese Pakete mit dem folgenden Befehl: `amplify-react-application1 % npm install --save aws-amplify @aws-amplify/ui-react`	App-Developer

Starten Sie die React-App und überprüfen Sie die Authentifizierung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starte die App.	Starten Sie die React-App auf Ihrem lokalen Computer: `amplify-react-application1 % npm start`	App-Entwickler, General AWS
Überprüfen Sie die Authentifizierung.	Prüfen Sie, ob die App zur Eingabe von Authentifizierungsparametern auffordert. (In unserem Beispiel haben wir E-Mail als Anmeldemethode konfiguriert.) Die Frontend-Benutzeroberfläche sollte Sie zur Eingabe der Anmeldeinformationen auffordern und eine Option zum Erstellen eines Kontos bieten. Sie können den Amplify-Build-Prozess auch so konfigurieren, dass das Backend als Teil eines kontinuierlichen Bereitstellungsworkflows hinzugefügt wird. Dieses Muster deckt diese Option jedoch nicht ab.	App-Entwickler, General AWS

Zugehörige Ressourcen

- Erste Schritte (npm-Dokumentation)
- Ein eigenständiges AWS-Konto erstellen (Dokumentation zur AWS-Kontoverwaltung)

- Dokumentation zu AWS Amplify
- Amazon Cognito Cognito-Dokumentation

Erstellen Sie ein Portal für Mikro-Frontends mithilfe AWS Amplify von Angular und Module Federation

Erstellt von Milena Godau (AWS) und Pedro Garcia (AWS)

Übersicht

Eine Micro-Frontend-Architektur ermöglicht es mehreren Teams, unabhängig voneinander an verschiedenen Teilen einer Frontend-Anwendung zu arbeiten. Jedes Team kann ein Fragment des Frontends entwickeln, erstellen und bereitstellen, ohne andere Teile der Anwendung zu beeinträchtigen. Aus Sicht des Endbenutzers scheint es sich um eine einzige, zusammenhängende Anwendung zu handeln. Sie interagieren jedoch mit mehreren unabhängigen Anwendungen, die von verschiedenen Teams veröffentlicht werden.

In diesem Dokument wird beschrieben, wie Sie mithilfe des Angular-Frontend-Frameworks und der AWS AmplifyModule Federation eine Mikro-Frontend-Architektur erstellen. In diesem Muster werden die Mikrofrontends auf der Clientseite durch eine Shell-Anwendung (oder übergeordnete Anwendung) kombiniert. Die Shell-Anwendung fungiert als Container, der die Mikrofrontends abruft, anzeigt und integriert. Die Shell-Anwendung übernimmt das globale Routing, das verschiedene Mikrofrontends lädt. Das @angular -architects/module-federation Plugin integriert Module Federation mit Angular. Sie stellen die Shell-Anwendung und die Mikro-Frontends bereit, indem Sie. AWS Amplify Endbenutzer greifen über ein webbasiertes Portal auf die Anwendung zu.

Das Portal ist vertikal aufgeteilt. Das bedeutet, dass es sich bei den Mikrofrontends um ganze Ansichten oder Gruppen von Ansichten handelt, anstatt um Teile derselben Ansicht. Daher lädt die Shell-Anwendung jeweils nur ein Mikro-Frontend.

Die Mikrofrontends sind als Remote-Module implementiert. Die Shell-Anwendung lädt diese Remote-Module langsam, wodurch die Mikro-Frontend-Initialisierung verzögert wird, bis sie benötigt wird. Dieser Ansatz optimiert die Anwendungsleistung, indem nur die benötigten Module geladen werden. Dies reduziert die anfängliche Ladezeit und verbessert die allgemeine Benutzererfahrung. Darüber hinaus teilen Sie über die Webpack-Konfigurationsdatei (webpack.config.js) gemeinsame Abhängigkeiten zwischen den Modulen. Diese Vorgehensweise fördert die Wiederverwendung von Code, reduziert Doppelarbeit und optimiert den Bündelungsprozess.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto

- Node.js und npm, installiert
- Amplify CLI, installiert
- Angular CLI, installiert
- Zu verwendende Berechtigungen AWS Amplify
- Vertrautheit mit Angular

Produktversionen

- Angular CLI Version 13.1.2 oder höher
- @angular -architects/module-federation Version 14.0.1 oder höher
- Webpack-Version 5.4.0 oder höher
- AWS Amplify Generation 1

Einschränkungen

Eine Micro-Frontend-Architektur ist ein leistungsstarker Ansatz für die Erstellung skalierbarer und robuster Webanwendungen. Es ist jedoch wichtig, die folgenden potenziellen Herausforderungen zu verstehen, bevor Sie diesen Ansatz anwenden:

- Integration — Eine der größten Herausforderungen ist die potenzielle Zunahme der Komplexität im Vergleich zu monolithischen Frontends. Die Orchestrierung mehrerer Mikro-Frontends, die Verwaltung der Kommunikation zwischen ihnen und die Verwaltung gemeinsamer Abhängigkeiten können komplizierter sein. Darüber hinaus kann mit der Kommunikation zwischen den Mikrofrontends ein Leistungsaufwand verbunden sein. Diese Kommunikation kann die Latenz erhöhen und die Leistung verringern. Diesem Problem muss durch effiziente Nachrichtenmechanismen und Strategien für den Datenaustausch begegnet werden.
- Codeduplizierung — Da jedes Mikro-Frontend unabhängig entwickelt wird, besteht die Gefahr, dass Code für gemeinsame Funktionen oder gemeinsam genutzte Bibliotheken dupliziert wird. Dies kann die Gesamtgröße der Anwendung erhöhen und zu Problemen bei der Wartung führen.
- Koordination und Verwaltung — Die Koordination der Entwicklungs- und Bereitstellungsprozesse über mehrere Mikrofrontends hinweg kann eine Herausforderung sein. Die Sicherstellung einer konsistenten Versionierung, die Verwaltung von Abhängigkeiten und die Aufrechterhaltung der Kompatibilität zwischen den Komponenten werden in einer verteilten Architektur immer wichtiger. Die Einrichtung klarer Governance, Richtlinien und automatisierter Test- und Bereitstellungspipelines ist für eine reibungslose Zusammenarbeit und Bereitstellung unerlässlich.

- Testen — Das Testen von Mikro-Frontend-Architekturen kann komplexer sein als das Testen monolithischer Frontends. Es erfordert zusätzlichen Aufwand und spezielle Teststrategien, um komponentenübergreifende Integrationstests und end-to-end Tests durchzuführen und konsistente Benutzererlebnisse über mehrere Mikrofrontends hinweg zu validieren.

Bevor Sie sich für den Micro-Frontend-Ansatz entscheiden, empfehlen wir Ihnen, den Artikel Micro-Frontends verstehen und implementieren auf zu lesen. AWS

Architektur

In einer Micro-Frontend-Architektur entwickelt und implementiert jedes Team Funktionen unabhängig. Das folgende Bild zeigt, wie mehrere DevOps Teams zusammenarbeiten. Das Portalteam entwickelt die Shell-Anwendung. Die Shell-Anwendung fungiert als Container. Sie ruft die Micro-Frontend-Anwendungen ab, zeigt sie an und integriert sie, die von anderen Teams veröffentlicht wurden. DevOps Sie verwenden, AWS Amplify um die Shell-Anwendung und die Micro-Frontend-Anwendungen zu veröffentlichen.

Das Architekturdiagramm zeigt den folgenden Arbeitsablauf:

1. Das Portalteam entwickelt und verwaltet die Shell-Anwendung. Die Shell-Anwendung orchestriert die Integration und das Rendern der Mikrofrontends, um das gesamte Portal zusammenzustellen.
2. Die Teams A und B entwickeln und warten ein oder mehrere Mikrofrontends oder Funktionen, die in das Portal integriert sind. Jedes Team kann unabhängig an seinen jeweiligen Mikrofrontends arbeiten.
3. Der Endbenutzer authentifiziert sich mithilfe von Amazon Cognito.
4. Der Endbenutzer greift auf das Portal zu und die Shell-Anwendung wird geladen. Während der Benutzer navigiert, kümmert sich die Shell-Anwendung um das Routing und ruft das angeforderte Mikro-Frontend ab, wobei das Paket geladen wird.

Tools

AWS-Services

- AWS Amplifyist eine Reihe von speziell entwickelten Tools und Funktionen, mit denen Frontend-Web- und Mobilentwickler schnell Full-Stack-Anwendungen erstellen können. AWS In

diesem Muster verwenden Sie die Amplify-CLI, um die Amplify-Micro-Frontend-Anwendungen bereitzustellen.

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie AWS-Services über Befehle in Ihrer Befehlszeilen-Shell interagieren können.

Andere Tools

- @angular -architects/module-federation ist ein Plugin, das Angular in Module Federation integriert.
- Angular ist ein Open-Source-Framework für Webanwendungen zum Erstellen moderner, skalierbarer und testbarer einseitiger Anwendungen. Es folgt einer modularen und komponentenbasierten Architektur, die die Wiederverwendung und Wartung von Code fördert.
- Node.js ist eine ereignisgesteuerte JavaScript Laufzeitumgebung, die für die Erstellung skalierbarer Netzwerkanwendungen konzipiert wurde.
- npm ist eine Softwareregistrierung, die in einer Node.js -Umgebung ausgeführt wird und verwendet wird, um Pakete gemeinsam zu nutzen oder auszuleihen und die Bereitstellung von privaten Paketen zu verwalten.
- Webpack Module Federation hilft Ihnen dabei, Code, der unabhängig kompiliert und bereitgestellt wird, wie Mikro-Frontends oder Plugins, in eine Anwendung zu laden.

Code-Repository

Der Code für dieses Muster ist im Micro-Frontend-Portal unter Verwendung des Angular- und Module GitHub Federation-Repositorys verfügbar. Dieses Repository enthält die folgenden zwei Ordner:

- `shell-app`enthält den Code für die Shell-Anwendung.
- `feature1-app`enthält ein Beispiel-Mikrofrontend. Die Shell-Anwendung ruft dieses Mikro-Frontend ab und zeigt es als Seite innerhalb der Portalanwendung an.

Bewährte Methoden

Mikro-Frontend-Architekturen bieten zahlreiche Vorteile, bringen aber auch Komplexität mit sich. Im Folgenden finden Sie einige bewährte Methoden für eine reibungslose Entwicklung, hochwertigen Code und eine hervorragende Benutzererfahrung:

- Planung und Kommunikation — Um die Zusammenarbeit zu optimieren, sollten Sie im Vorfeld in Planung, Design und klare Kommunikationskanäle investieren.

- Einheitliches Design — Sorgen Sie mithilfe von Designsystemen, Styleguides und Komponentenbibliotheken für einen einheitlichen visuellen Stil auf allen Mikro-Frontends. Dies sorgt für ein einheitliches Benutzererlebnis und beschleunigt die Entwicklung.
- Abhängigkeitsmanagement — Da sich Mikro-Frontends unabhängig weiterentwickeln, sollten Sie standardisierte Verträge und Versionsstrategien anwenden, um Abhängigkeiten effektiv zu verwalten und Kompatibilitätsprobleme zu vermeiden.
- Mikro-Frontend-Architektur — Um eine unabhängige Entwicklung und Bereitstellung zu ermöglichen, sollte jedes Mikro-Frontend eine klare und klar definierte Verantwortung für eine gekapselte Funktionalität haben.
- Integration und Kommunikation — Um eine reibungslose Integration zu ermöglichen und Konflikte zu minimieren, sollten Sie klare Verträge und Kommunikationsprotokolle zwischen Mikrofrontends definieren, einschließlich Ereignisse und gemeinsam genutzter Datenmodelle. APIs
- Testen und Qualitätssicherung — Implementieren Sie Testautomatisierung und kontinuierliche Integrationspipelines für Mikro-Frontends. Dies verbessert die Gesamtqualität, reduziert den manuellen Testaufwand und validiert die Funktionalität zwischen den Mikro-Frontend-Interaktionen.
- Leistungsoptimierung — Überwachen Sie kontinuierlich die Leistungskennzahlen und verfolgen Sie die Abhängigkeiten zwischen den Mikrofrontends. Auf diese Weise können Sie Engpässe erkennen und eine optimale Anwendungsleistung aufrechterhalten. Verwenden Sie zu diesem Zweck Tools zur Leistungsüberwachung und Abhängigkeitsanalyse.
- Entwicklererfahrung — Konzentrieren Sie sich auf die Erfahrung der Entwickler, indem Sie klare Dokumentationen, Tools und Beispiele bereitstellen. Auf diese Weise können Sie die Entwicklung optimieren und neue Teammitglieder einarbeiten.

Epen

Erstellen Sie die Shell-Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Shell-Anwendung.	1. Geben Sie in der Angular-CLI den folgenden Befehl ein: `ng new shell --routing`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Geben Sie den folgenden Befehl ein, um zum Projektordner zu navigieren: `cd shell` **Note** Die Ordner- und Projektstruktur für die Shell- und Micro-Frontend-Anwendungen kann völlig unabhängig sein. Sie können als unabhängige Angular-Anwendungen behandelt werden.	
Installieren Sie das -Plug-in.	Geben Sie in der Angular-CLI den folgenden Befehl ein, um das @angular -architects/module-federation Plugin zu installieren: `ng add @angular-architects/module-federation --project shell --port 4200`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die Micro-Frontend-URL als Umgebungsvariable hinzu.	1. Öffnen Sie die Datei environment.ts. 2. Zum `mfe1URL: 'http://localhost:5000'` Objekt hinzufügen: `environment` `export const environment = { production: false, mfe1URL: 'http://localhost:5000', };` 3. Speichern und schließen Sie die Datei environment.ts.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Definieren Sie das Routing.	1. Öffnen Sie die Datei app-routing.module.ts.
	2. Geben Sie in der Angular-CLI den folgenden Befehl ein, um das `loadRemoteModule` Modul aus dem @angular -architects/module-federation Plugin zu importieren:
	`import { loadRemoteModule } from '@angular-architects/module-federation';`
	3. Stellen Sie die Standardroute wie folgt ein:
	`{ path: '', pathMatch: 'full', redirectTo: 'mfe1' },`
	4. Stellen Sie die Route für das Micro-Frontend ein:
	`{ path: 'mfe1', loadChildren: () => loadRemoteModule({ type: 'module',`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>remoteEntry: `${environment.mfe1URL}/remoteEntry.js`, exposedModule: './Module' }) .then(m => m.Mfe1Module) },</pre> 5. Speichern und schließen Sie die Datei app-routing.module.ts.	
`mfe1`Deklarieren Sie das Modul.	1. Erstellen Sie in dem `src` Ordner eine neue Datei mit dem Namen decl.d.ts. 2. Öffnen Sie die Datei decl.d.ts. 3. Fügen Sie der Datei Folgendes hinzu: <pre>declare module 'mfe1/Module';</pre> 4. Speichern und schließen Sie die Datei decl.d.ts.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bereiten Sie das Preloading für das Micro-Frontend vor.	Das Vorladen des Mikro-Frontends hilft dem Webpack, die gemeinsam genutzten Bibliotheken und Pakete richtig auszuhandeln.
	1. Öffnen Sie die Datei main.ts.
	2. Ersetzen Sie den Inhalt durch Folgendes:
	`import { loadRemoteEntry } from '@angular-architects/module-federation';`
	`Promise.all([ loadRemoteEntry(`${environment.mfe1URL}/remoteEntry.js`, 'mfe1'), ]) .catch(err => console.error('Error loading remote entries', err)) .then(() => import('./bootstrap')) .catch(err => console.error(err) );`
	3. Speichern und schließen Sie die Datei main.ts.
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie den HTML-Inhalt an.	1. Öffnen Sie die Datei app.component.html. 2. Ersetzen Sie den Inhalt durch Folgendes: `<h1>Shell application is running!</h1> <router-outlet></router-outlet>` 3. Speichern und schließen Sie die Datei app.component.html.	App-Developer

Erstellen Sie die Micro-Frontend-Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie das Mikro-Frontend.	1. Geben Sie in der Angular-CLI den folgenden Befehl ein:
	`ng new mfe1 --routing`
	2. Geben Sie den folgenden Befehl ein, um zum Projektordner zu navigieren:
	`cd mfe1`
		App-Developer

Installieren Sie das -Plug-in.	Geben Sie den folgenden Befehl ein, um das @angular-architects/module-federation Plugin zu installieren: `ng add @angular-architects/module-`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`federation --project mfe1 --port 5000`	

Erstellen Sie ein Modul und eine Komponente.	Geben Sie die folgenden Befehle ein, um ein Modul und eine Komponente zu erstellen und sie als Fernzugriffsmodul zu exportieren:
	`ng g module mfe1 --routing`
	`ng g c mfe1`
		App-Developer

Legen Sie den Standard-Routingpfad fest.	1. Öffnen Sie die Datei mfe-routing.module.ts. 2. Stellen Sie die Standardr oute wie folgt ein: `{ path: '', component: Mfe1Component },` 3. Speichern und schließen Sie die Datei mfe-routi ng.module.ts.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen `mfe1` Sie die Route hinzu.	1. Öffnen Sie die Datei app-routing.module.ts.
	2. Stellen Sie die Standardroute wie folgt ein:
	`{ path: '', pathMatch: 'full', redirectTo: 'mfe1' },`
	3. Fügen Sie die folgende `mfe1` Route hinzu:
	`{ path: 'mfe1', loadChildren: () => import('./mfe1/mfe1.module').then((m) => m.Mfe1Module), },`
	4. Speichern und schließen Sie die Datei app-routing.module.ts.
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bearbeiten Sie die Datei webpack.config.js.	1. Öffnen Sie die Datei webpack.config.js.
	2. Bearbeiten Sie den `For remotes` Abschnitt so, dass er dem Folgenden entspricht:
	`// For remotes (please adjust)`
	`name: "mfe1",`
	`filename: "remoteEntry.js",`
	`exposes: {`
	`'./Module': './src/app/mfe1/mfe1.module.ts',`
	`},`
	3. Fügen Sie im `shared` Abschnitt alle Abhängigkeiten hinzu, die die `mfe1` Anwendung mit der Shell-Anwendung gemeinsam hat:
	`shared: share({`
	`"@angular/core": { singleton: true, strictVersion: true, requiredVersion: 'auto' },`
	`"@angular/common": { singleton: true, strictVersion: true, requiredVersion: 'auto' },`
	`"@angular/common/http": { singleton: true,`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>strictVersion: true,
	requiredVersion:
	'auto' },
	"@angular/
	router": { singleton
	: true, strictVer
	sion: true, requiredV
	ersion: 'auto' },
	
	...shared
	Mappings.getDescri
	ptors()
	})</pre> 4. Speichern und schließen Sie die Datei webpack.c onfig.js.	

Passen Sie den HTML-Inhalt an.	1. Öffnen Sie die Datei app.component.html.
	2. Ersetzen Sie den Inhalt durch Folgendes:
	<pre><router-outlet></r
	outer-outlet></pre> 3. Speichern und schließen Sie die Datei app.compo nent.html.
		App-Developer

Führen Sie die Anwendungen lokal aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die `mfe1` Anwendung aus.	1. Geben Sie den folgenden Befehl ein, um die `mfe1` Anwendung zu starten:	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`npm start` 2. Greifen Sie in einem Webbrowser zu `http://localhost:5000` . 3. Stellen Sie sicher, dass das Micro-Frontend eigenständig ausgeführt werden kann. Die `mfe1` Anwendung sollte ordnungsgemäß und ohne Fehler gerendert werden.	
Führen Sie die Shell-Anwendung aus.	1. Geben Sie den folgenden Befehl ein, um die Shell-Anwendung zu starten: `npm start` 2. Greifen Sie in einem Webbrowser zu `http://localhost:4200/mfe1` . 3. Stellen Sie sicher, dass das `mfe1` Micro-Frontend in die Shell-Anwendung eingebettet ist. Die Portalanwendung sollte ordnungsgemäß und ohne Fehler gerendert werden, und die `mfe1` Anwendung sollte in sie eingebettet sein.	App-Developer

Refaktorieren Sie die Shell-Anwendung, um einen Fehler beim Laden des Mikro-Frontends zu beheben

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie ein Modul und eine Komponente.	Geben Sie im Stammordner der Shell-Anwendung die folgenden Befehle ein, um ein Modul und eine Komponente für eine Fehlerseite zu erstellen:
	`ng g module error-page --routing`
	`ng g c error-page`
		App-Developer

Passen Sie den HTML-Inhalt an.	1. Öffnen Sie die Datei error-page.component.html. 2. Ersetzen Sie den Inhalt durch Folgendes: `<p>Sorry, this page is not available.</p>` 3. Speichern und schließen Sie die Datei error-page.component.html.	App-Developer
Legen Sie den Standard-Routing-Pfad fest.	1. Öffnen Sie die Datei error-page-routing.module.ts. 2. Stellen Sie die Standardroute wie folgt ein: `{ path: '', component: ErrorPageComponent },`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Speichern und schließen Sie die Datei error-page-routing.module.ts.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine Funktion zum Laden von Mikro-Frontends.	1. Öffnen Sie die Datei app-routing.module.ts.
	2. Erstellen Sie die folgende Funktion:
	`function loadMFE(url: string) { return loadRemoteModule({ type: 'module', remoteEntry: `${url}/remoteEntry.js`, exposedModule: './Module' }) .then(m => m.Mfe1Module) .catch( () => import('./error-page/error-page.module').then(m => m.ErrorPageModule) ); }`
	3. Ändern Sie die `mfe1` Route so, dass sie wie folgt aussieht:
	`{ path: 'mfe1', loadChildren: () => loadMFE(environment.mfe1URL) },`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Speichern und schließen Sie die Datei app-routing.module.ts.	

Testen Sie die Fehlerbehandlung.	1. Falls es noch nicht läuft, geben Sie den folgenden Befehl ein, um die Shell-Anwendung zu starten:
	`npm start`
	2. Greifen Sie in einem Webbrowser zu `http://localhost:4200/mfe1` .
	3. Stellen Sie sicher, dass die Fehlerseite gerendert wurde. Sie sollten den folgenden Text sehen:
	`Sorry, this page is not available.`
		App-Developer

Stellen Sie die Anwendungen bereit, indem Sie AWS Amplify

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie das Mikro-Frontend bereit.	1. Navigieren Sie in der Amplify-CLI zum Stammordner der Micro-Frontend-Anwendung. 2. Geben Sie den folgenden Befehl ein, um Amplify zu initialisieren:	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`amplify init` 3. Wenn Sie aufgefordert werden, einen Namen für Ihr Amplify-Projekt einzugeben, drücken Sie die Eingabetaste. Dadurch wird der Name aus der Datei package.json wiederverwendet. 4. Wenn Sie aufgefordert werden, das Projekt mit der obigen Konfiguration zu initialisieren, geben Sie ein. `Yes` 5. Wenn Sie aufgefordert werden, eine Authentif izierungsmethode auszuwählen, wählen Sie`AWS Profile`. 6. Wählen Sie das Profil aus, das Sie verwenden möchten. 7. Warten Sie, bis Amplify das Projekt initialisiert hat. Wenn dieser Vorgang abgeschlossen ist, erhalten Sie eine Bestätigungsnachri cht im Terminal. 8. Geben Sie den folgenden Befehl ein, um dem Micro-Frontend eine Amplify-H	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	osting-Kategorie hinzuzufügen:
	`amplify add hosting`
	9. Wenn Sie aufgefordert werden, das Plugin-Modul auszuwählen, wählen Sie. `Hosting with Amplify Console`
	10. Wenn Sie aufgefordert werden, einen Typ auszuwählen, wählen Sie `Manual deployment` .
	11. Installieren Sie die NPM-Abhängigkeiten des Projekts, indem Sie den folgenden Befehl eingeben:
	`npm install`
	12. Veröffentlichen Sie die Anwendung auf der Amplify-Konsole, indem Sie den folgenden Befehl eingeben:
	`amplify publish -y`
	Wenn die Veröffentlichung abgeschlossen ist, gibt Amplify die URL des Mikrofrontends zurück.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	13. Kopieren Sie die URL. Sie benötigen diesen Wert, um die Shell-Anwendung zu aktualisieren.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die Shell-Anwendung bereit.	1. Öffnen Sie in dem src/app/environmentsOrdner die Datei environments.prod.ts.
	2. Ersetzen Sie den `mfe1URL` Wert durch die URL des bereitgestellten Mikro-Frontends:
	`export const environment = { production: true, mfe1URL: 'https://<env>.<Amplify-app-ID>.amplifyapp.com' };`
	3. Speichern und schließen Sie die Datei environments.prod.ts.
	4. Navigieren Sie in der Amplify CLI zum Stammordner der Shell-Anwendung.
	5. Geben Sie den folgenden Befehl ein, um Amplify zu initialisieren:
	`amplify init`
	6. Wenn Sie aufgefordert werden, einen Namen für Ihr Amplify-Projekt einzugeben, drücken Sie die Eingabetaste. Dadurch wird der Name
		App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	aus der Datei package.json wiederverwendet. 7. Wenn Sie aufgefordert werden, das Projekt mit der obigen Konfiguration zu initialisieren, geben Sie ein. `Yes` 8. Wenn Sie aufgefordert werden, eine Authentif izierungsmethode auszuwählen, wählen Sie `AWS Profile`. 9. Wählen Sie das Profil aus, das Sie verwenden möchten. 10. Warten Sie, bis Amplify das Projekt initialisiert hat. Wenn dieser Vorgang abgeschlossen ist, erhalten Sie eine Bestätigungsnachri cht im Terminal. 11. Fügen Sie der Shell-Anw endung eine Amplify-H osting-Kategorie hinzu: `amplify add hosting` 12. Wenn Sie aufgefordert werden, das Plugin-Mo dul auszuwählen, wählen Sie `Hosting with Amplify Console`. 13. Wenn Sie aufgeford ert werden, einen Typ	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	auszuwählen, wählen Sie `Manual deployment`.
	14. Installieren Sie die NPM-Abhängigkeiten des Projekts, indem Sie den folgenden Befehl eingeben:
	`npm install`
	15. Veröffentlichen Sie die Shell-Anwendung auf der Amplify-Konsole, indem Sie den folgenden Befehl eingeben:
	`amplify publish -y`
	Wenn die Veröffentlichung abgeschlossen ist, gibt Amplify die URL der bereitgestellten Shell-Anwendung zurück.
	16. Notieren Sie sich die URL für die Shell-Anwendung.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie CORS.	Da die Shell- und Micro-Frontend-Anwendungen unabhängig voneinander auf verschiedenen Domänen gehostet werden, müssen Sie Cross-Origin Resource Sharing (CORS) auf dem Mikrofrontend aktivieren. Dadurch kann die Shell-Anwendung den Inhalt von einem anderen Ursprung laden. Um CORS zu aktivieren, fügen Sie benutzerdefinierte Header hinzu. 1. Navigieren Sie in der Amplify-CLI zum Stammordner des Micro-Frontends. 2. Geben Sie den folgenden Befehl ein: `amplify configure hosting` 3. Wenn Sie aufgefordert werden, benutzerdefinierte Einstellungen zu konfigurieren, geben Sie ein. Y 4. Melden Sie sich bei der AWS Management Console an und öffnen Sie dann die Amplify-Konsole. 5. Wählen Sie das Micro-Frontend.	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	6. Wählen Sie im Navigationsbereich Hosting und dann Benutzerdefinierte Kopfzeilen aus.
	7. Wählen Sie Bearbeiten aus.
	8. Geben Sie im Fenster Benutzerdefinierte Header bearbeiten Folgendes ein:
	`customHeaders:`
	`  - pattern: '*.js'`
	`    headers:`
	`      - key: Access-Control-Allow-Origin`
	`        value: '*'`
	`      - key: Access-Control-Allow-Methods`
	`        value: 'GET, OPTIONS'`
	`      - key: Access-Control-Allow-Headers`
	`        value: '*'`
	9. Wählen Sie Speichern.
	10. Stellen Sie das Mikro-Frontend erneut bereit, um die neuen benutzerdefinierten Header anzuwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Rewrite-Regel für die Shell-Anwendung.	Die Angular-Shell-Anwendung ist für die Verwendung von HTML5 Routing konfiguriert. Wenn der Benutzer eine Hard-Refresh durchführt, versucht Amplify, eine Seite von der aktuellen URL zu laden. Dies generiert einen 403-Fehler. Um dies zu vermeiden, fügen Sie in der Amplify-Konsole eine Rewrite-Regel hinzu. Gehen Sie folgendermaßen vor, um die Rewrite-Regel zu erstellen: 1. Navigieren Sie in der Amplify CLI zum Stammordner der Shell-Anwendung. 2. Geben Sie den folgenden Befehl ein: `amplify configure hosting` 3. Wenn Sie aufgefordert werden, benutzerdefinierte Einstellungen zu konfiguri eren, geben Sie einY. 4. Öffnen Sie die Amplify-K onsole. 5. Wählen Sie die Shell-Anw endung.	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Wählen Sie im Navigationsbereich Hosting und dann Rewrites and redirects aus. 7. Wählen Sie auf der Seite Umschreibungen und Weiterleitungen die Option Weiterleitungen verwalten aus. 8. Wählen Sie Texteditor öffnen. 9. Geben Sie im JSON-Editor die folgende Weiterleitung ein: `[ { "source": "/<*>", "target": "/index.html", "status": "404-200", "condition": null } ]` 10. Wählen Sie Speichern.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie das Webportal.	1. Geben Sie in einem Webbrowser die URL der bereitgestellten Shell-Anwendung ein. 2. Stellen Sie sicher, dass die Shell-Anwendung und das Micro-Frontend ordnungsgemäß geladen werden.	App-Developer

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die Anwendungen.	Wenn Sie die Shell- und Micro-Frontend-Anwendungen nicht mehr benötigen, löschen Sie sie. Auf diese Weise können Sie vermeiden, dass Gebühren für Ressourcen anfallen, die Sie nicht nutzen. 1. Melden Sie sich bei der AWS Management Console an und öffnen Sie dann die Amplify-Konsole. 2. Wählen Sie das Micro-Frontend. 3. Wählen Sie im Navigationsbereich App-Einstellungen und dann Allgemeine Einstellungen aus. 4. Wählen Sie App löschen.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Geben Sie im Bestätigungsfenster die Eingabe ein `delete` und wählen Sie dann App löschen. 6. Wiederholen Sie diese Schritte, um die Shell-Anwendung zu löschen.	

Fehlerbehebung

Problem	Lösung
Bei der Ausführung des `amplify init` Befehls ist kein AWS Profil verfügbar	Wenn Sie kein AWS Profil konfiguriert haben, können Sie trotzdem mit dem `amplify init` Befehl fortfahren. Sie müssen die `AWS access keys` Option jedoch auswählen, wenn Sie zur Eingabe der Authentifizierungsmethode aufgefordert werden. Halten Sie Ihren AWS Zugriffsschlüssel und Ihren geheimen Schlüssel bereit. Alternativ können Sie ein benanntes Profil für die konfigurieren AWS CLI. Anweisungen finden Sie in der AWS CLI Dokumentation unter Einstellungen für die Konfiguration und die Anmeldeinformationsdatei.
Fehler beim Laden von Remote-Einträgen	Wenn beim Laden der Remote-Einträge in der Datei main.ts der Shell-Anwendung ein Fehler auftritt, stellen Sie sicher, dass die `environment.mfe1URL` Variable richtig gesetzt ist. Der Wert dieser Variablen sollte die URL des Mikrofrontends sein.

Problem	Lösung
404-Fehler beim Zugriff auf das Micro-Frontend	Wenn Sie beim Versuch, auf das lokale Micro-Frontend zuzugreifen, einen 404-Fehler erhalten, z. B. unter`http://localhost:4200/mfe1` , überprüfen Sie Folgendes: • Stellen Sie für die Shell-Anwendung sicher, dass die Routing-Konfiguration in der Datei app-routing.module.ts korrekt eingerichtet ist, und stellen Sie sicher, dass die Funktion das Micro-Frontend ordnungsgemäß aufruft. `loadRemoteModule` • Stellen Sie für das Micro-Frontend sicher, dass die Datei webpack.config.js die richtige Konfiguration hat, und stellen Sie sicher, dass die Datei remoteEntry.js korrekt generiert wird. **`exposes`**

Zusätzliche Informationen

AWS Dokumentation

- Mikrofrontends verstehen und implementieren auf AWS (AWS Prescriptive Guidance)
- Amplify CLI (Amplify-Dokumentation)
- Amplify Hosting (Amplify-Dokumentation)

Andere Referenzen

- Modul Federation
- Node.js
- Eckig
- @angular -architects/module-federation

Stellen Sie eine React-basierte Einzelseitenanwendung auf Amazon S3 bereit und CloudFront

Erstellt von Jean-Baptiste Guillois (AWS)

Übersicht

Eine einseitige Anwendung (SPA) ist eine Website oder Webanwendung, die den Inhalt einer angezeigten Webseite dynamisch aktualisiert, indem sie JavaScript APIs Dieser Ansatz verbessert die Benutzererfahrung und Leistung einer Website, da nur neue Daten aktualisiert werden, anstatt die gesamte Webseite vom Server neu zu laden.

Dieses Muster bietet einen step-by-step Ansatz zum Codieren und Hosten eines SPA, das in React auf Amazon Simple Storage Service (Amazon S3) und Amazon geschrieben ist CloudFront. Das SPA in diesem Muster verwendet eine REST-API, die in Amazon API Gateway konfiguriert und über eine CloudFront Amazon-Distribution verfügbar gemacht wird, um das Cross-Origin Resource Sharing (CORS) -Management zu vereinfachen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver. AWS-Konto
- Node.js und`npm`, installiert und konfiguriert. Weitere Informationen finden Sie im Abschnitt Downloads der Dokumentation zu Node.js.
- Yarn, installiert und konfiguriert. Weitere Informationen finden Sie in der Yarn-Dokumentation.
- Git, installiert und konfiguriert. Weitere Informationen finden Sie in der Git-Dokumentation.

Architektur

Diese Architektur wird automatisch mithilfe von AWS CloudFormation (Infrastruktur als Code) bereitgestellt. Es verwendet regionale Dienste wie Amazon S3 zum Speichern der statischen Ressourcen und Amazon CloudFront mit Amazon API Gateway, um regionale API-Endpunkte (REST) verfügbar zu machen. Die Anwendungsprotokolle werden mithilfe von Amazon gesammelt CloudWatch. Alle AWS API-Aufrufe werden geprüft. AWS CloudTrail Die gesamte Sicherheitskonfiguration (z. B. Identitäten und Berechtigungen) wird in AWS Identity and Access

Management (IAM) verwaltet. Statische Inhalte werden über das Amazon CloudFront Content Delivery Network (CDN) bereitgestellt, und DNS-Abfragen werden von Amazon Route 53 bearbeitet.

Tools

AWS-Services

- Amazon API Gateway unterstützt Sie bei der Erstellung, Veröffentlichung, Wartung, Überwachung und Sicherung von REST, HTTP und WebSocket APIs in jeder Größenordnung.
- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend AWS-Konten zu verwalten.
- Amazon CloudFront beschleunigt die Verteilung Ihrer Webinhalte, indem es sie über ein weltweites Netzwerk von Rechenzentren bereitstellt, was die Latenz senkt und die Leistung verbessert.
- AWS CloudTrailhilft Ihnen bei der Prüfung der Unternehmensführung, der Einhaltung von Vorschriften und des betrieblichen Risikos Ihrer AWS-Konto.
- Amazon CloudWatch hilft Ihnen dabei, die Kennzahlen Ihrer AWS Ressourcen und der Anwendungen, auf denen Sie laufen, AWS in Echtzeit zu überwachen.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code

Der Beispielanwendungscode dieses Musters ist im GitHub React-basierten einseitigen CORS-Anwendungs-Repository verfügbar.

Bewährte Methoden

Mithilfe des Amazon S3 S3-Objektspeichers können Sie die statischen Ressourcen Ihrer Anwendung auf sichere, hochbelastbare, leistungsstarke und kostengünstige Weise speichern. Für diese Aufgabe ist es nicht erforderlich, einen dedizierten Container oder eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance zu verwenden.

Durch die Nutzung des Amazon CloudFront Content Delivery Network können Sie die Latenz reduzieren, die Ihren Benutzern beim Zugriff auf Ihre Anwendung entstehen kann. Sie können auch eine Firewall für Webanwendungen (AWS WAF) anbringen, um Ihre Ressourcen vor böswilligen Angriffen zu schützen.

Epen

Erstellen und implementieren Sie Ihre Anwendung lokal

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Führen Sie den folgenden Befehl aus, um das Repository der Beispielanwendung zu klonen: `git clone https://github.com/aws-samples/react-cors-spa react-cors-spa && cd react-cors-spa`	App-Entwickler, AWS DevOps
Stellen Sie die Anwendung lokal bereit.	1. Führen Sie im Projektverzeichnis den `npm install` Befehl aus, um die Anwendungsabhängigkeiten zu initiieren. 2. Führen Sie den `yarn dev` Befehl aus, um die Anwendung lokal zu starten.	App-Entwickler, AWS DevOps
Lokaler Zugriff auf die Anwendung.	Öffnen Sie ein Browserfenster und geben Sie die `http://localhost:3000` URL für den Zugriff auf die Anwendung ein.	App-Entwickler, AWS DevOps

Bereitstellen der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die AWS CloudFormation Vorlage bereit.	1. Melden Sie sich bei der an AWS Management Console, und öffnen Sie dann die AWS CloudFormation Konsole. 2. Wählen Sie „Stack erstellen“ und anschließend „Mit neuen Ressourcen (Standard)“. 3. Wählen Sie Upload a template file (Vorlagendatei hochladen). 4. Wählen Sie „Datei auswählen“, wählen Sie die `react-cors-spa-stack.yaml` Datei aus dem geklonten Repository aus und klicken Sie dann auf „Weiter“. 5. Geben Sie einen Namen für Ihren Stack ein und wählen Sie dann Weiter. 6. Behalten Sie alle Standardoptionen bei und wählen Sie dann Weiter. 7. Überprüfen Sie die endgültigen Einstellungen für Ihren Stapel und wählen Sie dann Stapel erstellen aus.	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie Ihre Anwendung squelldateien an.	1. Öffnen Sie nach der Bereitstellung Ihres Stacks die Registerkarte Ausgabe und identifizieren Sie den `Bucket` Namen und den `APIDomain` Wert. 2. Kopieren Sie die CloudFron t Distributionsdomäne für die REST-API. 3. Navigieren Sie zu `<project_root>/src /pages/index.tsx` und fügen Sie diese Domain dann in den `APIEndPoint` Variablen wert in Zeile 13 der `index.tsx` Datei ein oder fügen Sie sie ein.	App-Developer
Erstellen Sie das Anwendung spaket.	Führen Sie in Ihrem Projektverzeichnis den `yarn build` Befehl aus, um das Anwendungspaket zu erstellen .	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie das Anwendung spaket bereit.	1. Öffnen Sie die Amazon S3-Konsole. 2. Identifizieren und wählen Sie den S3-Bucket aus, der zuvor vom CloudFormation Stack erstellt wurde. 3. Wählen Sie Upload und anschließend Dateien hinzufügen aus. 4. Wählen Sie den Inhalt Ihres `out` Ordners aus. 5. Wählen Sie Ordner hinzufügen und wählen Sie dann das `_next` Verzeichn is aus. **Important** Wählen Sie das `_next` Verzeichnis, nicht den Inhalt. 6. Wählen Sie Upload, um die Dateien und das Verzeichn is in Ihren S3-Bucket hochzuladen.	App-Entwickler, AWS DevOps

Testen der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Greifen Sie auf die Anwendung zu und testen Sie sie.	Öffnen Sie ein Browserfe nster und fügen Sie dann die CloudFront Verteilun	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	gsdomäne (die `SPADomain` Ausgabe des CloudFormation Stacks, den Sie zuvor bereitgestellt haben) ein, um auf die Anwendung zuzugreifen.	

Säubere die Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie den Inhalt des S3-Buckets.	1. Öffnen Sie die Amazon S3 S3-Konsole und wählen Sie den Bucket aus, der zuvor vom Stack erstellt wurde (der erste Bucket, dessen Name mit beginnt `react-cors-spa-`). 2. Wählen Sie Leer, um den Inhalt des Buckets zu löschen. 3. Wählen Sie den zweiten Bucket aus, der zuvor vom Stack erstellt wurde (den zweiten Bucket, dessen Name mit beginnt `react-cors-spa-` und endet mit `-logs`). 4. Wählen Sie Leer, um den Inhalt des Buckets zu löschen.	AWS DevOps, App-Entwickler
Löschen Sie den AWS CloudFormation Stack.	1. Öffnen Sie die AWS CloudFormation Konsole	AWS DevOps, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und wählen Sie den Stack aus, den Sie zuvor erstellt haben. 2. Wählen Sie Löschen, um den Stack und alle zugehörigen Ressourcen zu löschen.	

Zugehörige Ressourcen

Um Ihre Webanwendung bereitzustellen und zu hosten, können Sie auch AWS Amplify Hosting verwenden, das einen Git-basierten Workflow für das Hosten serverloser Full-Stack-Web-Apps mit kontinuierlicher Bereitstellung bietet. Amplify Hosting ist Teil von AWS Amplify, das eine Reihe von speziell entwickelten Tools und Funktionen bietet, mit denen Frontend-Web- und Mobilentwickler schnell und einfach Full-Stack-Anwendungen erstellen können. AWS

Zusätzliche Informationen

Um ungültige Anfragen URLs des Benutzers zu behandeln, die zu 403-Fehlern führen könnten, fängt eine benutzerdefinierte Fehlerseite, die in der CloudFront Distribution konfiguriert ist, 403-Fehler ab und leitet sie an den Einstiegspunkt der Anwendung weiter (). `index.html`

Um die Verwaltung von CORS zu vereinfachen, wird die REST-API über eine CloudFront Distribution verfügbar gemacht.

Stellen Sie eine Amazon API Gateway Gateway-API auf einer internen Website mithilfe von privaten Endpunkten und einem Application Load Balancer bereit

Erstellt von Saurabh Kothari (AWS)

Übersicht

Dieses Muster zeigt Ihnen, wie Sie eine Amazon API Gateway Gateway-API auf einer internen Website bereitstellen, auf die von einem lokalen Netzwerk aus zugegriffen werden kann. Sie lernen, einen benutzerdefinierten Domainnamen für eine private API zu erstellen, indem Sie eine Architektur verwenden, die mit privaten Endpunkten, einem Application Load Balancer PrivateLink, AWS und Amazon Route 53 konzipiert ist. Diese Architektur verhindert die unbeabsichtigten Folgen der Verwendung eines benutzerdefinierten Domainnamens und eines Proxyservers zur Unterstützung des domänenbasierten Routing auf einer API. Wenn Sie beispielsweise einen VPC-Endpunkt (Virtual Private Cloud) in einem nicht routbaren Subnetz bereitstellen, kann Ihr Netzwerk das API Gateway nicht erreichen. Eine gängige Lösung besteht darin, einen benutzerdefinierten Domainnamen zu verwenden und dann die API in einem routingfähigen Subnetz bereitzustellen. Dies kann jedoch andere interne Websites beschädigen, wenn die Proxykonfiguration Traffic (`execute-api.{region}.vpce.amazonaws.com`) an AWS Direct Connect weiterleitet. Schließlich kann Ihnen dieses Muster dabei helfen, die organisatorischen Anforderungen für die Verwendung einer privaten API, die vom Internet aus nicht erreichbar ist, und eines benutzerdefinierten Domainnamens zu erfüllen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Server Name Indication (SNI) -Zertifikat für Ihre Website und API
- Eine Verbindung von einer lokalen Umgebung zu einem AWS-Konto, das mithilfe von AWS Direct Connect oder AWS Site-to-Site VPN eingerichtet wurde
- Eine private gehostete Zone mit einer entsprechenden Domain (z. B. domain.com), die von einem lokalen Netzwerk aus aufgelöst wird und DNS-Abfragen an Route 53 weiterleitet
- Ein routbares privates Subnetz, das von einem lokalen Netzwerk aus erreichbar ist

Einschränkungen

Weitere Informationen zu Kontingenten (früher als Limits bezeichnet) für Load Balancer, Regeln und andere Ressourcen finden Sie unter Kontingente für Ihre Application Load Balancers in der Elastic Load Balancing Balancing-Dokumentation.

Architektur

Technologie-Stack

- Amazon API Gateway
- Amazon Route 53
- Application Load Balancer
- AWS Certificate Manager
- AWS PrivateLink

Zielarchitektur

Das folgende Diagramm zeigt, wie ein Application Load Balancer in einer VPC bereitgestellt wird, der Web-Traffic auf der Grundlage von Application Load Balancer Balancer-Listener-Regeln an eine Website-Zielgruppe oder API-Gateway-Zielgruppe weiterleitet. Die API Gateway-Zielgruppe ist eine Liste von IP-Adressen für den VPC-Endpunkt in API Gateway. API Gateway ist so konfiguriert, dass die API mit ihrer Ressourcenrichtlinie privat ist. Die Richtlinie lehnt alle Anrufe ab, die nicht von einem bestimmten VPC-Endpunkt stammen. Benutzerdefinierte Domainnamen im API-Gateway werden aktualisiert und verwenden nun api.domain.com für die API und ihre Phase. Application Load Balancer Balancer-Regeln werden hinzugefügt, um den Datenverkehr auf der Grundlage des Hostnamens weiterzuleiten.

Das Diagramm zeigt den folgenden Workflow:

1. Ein Benutzer aus einem lokalen Netzwerk versucht, auf eine interne Website zuzugreifen. Die Anfrage wird an ui.domain.com und api.domain.com gesendet. Anschließend wird die Anfrage an den internen Application Load Balancer des routbaren privaten Subnetzes weitergeleitet. Das SSL wird am Application Load Balancer für ui.domain.com und api.domain.com beendet.
2. Listener-Regeln, die auf dem Application Load Balancer konfiguriert sind, suchen nach dem Host-Header.

a. Wenn der Host-Header api.domain.com lautet, wird die Anfrage an die API Gateway Gateway-Zielgruppe weitergeleitet. Der Application Load Balancer initiiert eine neue Verbindung zum API Gateway über Port 443.

b. Wenn der Host-Header ui.domain.com lautet, wird die Anfrage an die Zielgruppe der Website weitergeleitet.

3. Wenn die Anfrage API Gateway erreicht, bestimmt die in API Gateway konfigurierte benutzerdefinierte Domänenzuordnung den Hostnamen und die auszuführende API.

Automatisierung und Skalierung

Die Schritte in diesem Muster können mithilfe von AWS CloudFormation oder dem AWS Cloud Development Kit (AWS CDK) automatisiert werden. Um die Zielgruppe der API-Gateway-Aufrufe zu konfigurieren, müssen Sie eine benutzerdefinierte Ressource verwenden, um die IP-Adresse des VPC-Endpunkts abzurufen. API-Aufrufe an die IP-Adressen describe-vpc-endpointsund die Sicherheitsgruppe und geben diese describe-network-interfaceszurück. Diese können verwendet werden, um die API-Zielgruppe von IP-Adressen zu erstellen.

Tools

- Amazon API Gateway unterstützt Sie bei der Erstellung, Veröffentlichung, Wartung, Überwachung und Sicherung von REST, HTTP und WebSocket APIs in jeder Größenordnung.
- Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Web-Service.
- AWS Certificate Manager (ACM) unterstützt Sie bei der Erstellung, Speicherung und Erneuerung von öffentlichen und privaten SSL/TLS X.509-Zertifikaten und Schlüsseln, die Ihre AWS-Websites und -Anwendungen schützen.
- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS PrivateLink hilft Ihnen dabei, unidirektionale, private Verbindungen von Ihren VPCs zu Services außerhalb der VPC herzustellen.

Epen

Erstellen Sie ein SNI-Zertifikat

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein SNI-Zertifikat und importieren Sie das Zertifikat in ACM.	1. Erstellen Sie ein SNI-Zertifikat für ui.domain.com und api.domain.com. Weitere Informationen finden Sie in der CloudFront Amazon-Dokumentation unter Auswählen, wie CloudFront HTTPS-Anfragen bearbeitet werden. 2. Importieren Sie die SNI-Zertifikate in AWS Certificate Manager (ACM). Weitere Informationen finden Sie in der ACM-Dokumentation unter Zertifikate in AWS Certificate Manager importieren.	Netzwerkadministrator

Stellen Sie einen VPC-Endpunkt in einem nicht routbaren privaten Subnetz bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen VPC-Schnittstellen-Endpunkt in API Gateway.	Um einen VPC-Schnittstellen-Endpunkt zu erstellen, folgen Sie den Anweisungen unter Zugreifen auf einen AWS-Service mithilfe eines Schnittstellen-VPC-Endpunkts in der Dokumentation zu Amazon	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Virtual Private Cloud (Amazon VPC).	

Den Application Load Balancer konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Zielgruppe für Ihre Bewerbung.	Erstellen Sie eine Zielgruppe für die UI-Ressourcen Ihrer Anwendung.	Cloud-Administrator
Erstellen Sie eine Zielgruppe für den API-Gateway-Endpunkt.	1. Erstellen Sie eine Zielgruppe mit einem IP-Adresstyp und fügen Sie dann die IP-Adresse des VPC-Endpunkts für den API-Gateway-Endpunkt zur Zielgruppe hinzu. 2. Konfigurieren Sie Integritätsprüfungen für Ihre Zielgruppen mit dem Erfolgscode 403. 403 ist erforderlich, da der VPC-Endpunkt für das API Gateway einen 403-Code zurückgibt, wenn er vom Zielgruppen-Gesundheitscheck ohne Header aufgerufen wird.	Cloud-Administrator
Erstellen Sie einen Application Load Balancer.	1. Erstellen Sie einen Application Load Balancer (intern) in einem routbaren privaten Subnetz.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Fügen Sie den 443-Listener zum Application Load Balancer hinzu und wählen Sie dann das Zertifikat von ACM aus.	
Erstellen Sie Regeln für Zuhörer.	Erstellen Sie Listener-Regeln, um Folgendes zu tun: 1. Leiten Sie den Host api.domain.com an die API Gateway Gateway-Zielgruppe weiter 2. Leiten Sie den Host ui.domain.com an die Zielgruppe für die UI-Ressourcen weiter	Cloud-Administrator

Route 53 konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine private gehostete Zone.	Erstellen Sie eine private gehostete Zone für domain.com.	Cloud-Administrator
Domaindatensätze erstellen.	Erstellen Sie CNAME-Einträge für Folgendes: • Eine API, deren Wert auf den DNS-Namen des Application Load Balancer gesetzt ist • Eine Benutzeroberfläche, deren Wert auf den DNS-	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Namen des Application Load Balancer gesetzt ist	

Erstellen Sie einen privaten API-Endpunkt in API Gateway

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und konfigurieren Sie einen privaten API-Endpunkt.	1. Um einen privaten API-Endpunkt zu erstellen, folgen Sie den Anweisungen unter Erstellen einer privaten API in Amazon API Gateway in der API Gateway-Dokumentation. 2. Konfigurieren Sie die Ressourcenrichtlinie so, dass nur API-Aufrufe vom VPC-Endpunkt aus zulässig sind. Weitere Informationen finden Sie unter Steuern des Zugriffs auf eine API mit API-Gateway-Ressourcenrichtlinien in der API Gateway Gateway-Dokumentation.	App-Entwickler, Cloud-Administrator
Erstellen Sie einen benutzerdefinierten Domainnamen.	1. Erstellen Sie einen benutzerdefinierten Domainnamen für api.domain.com. Weitere Informationen finden Sie unter Einrichten benutzerdefinierter Domainnamen für REST APIs in der	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	API Gateway Gateway-Dokumentation. 2. Wählen Sie die erstellte API und die Phase aus. Weitere Informationen finden Sie unter Arbeiten mit API-Zuordnungen für REST APIs in der API Gateway Gateway-Dokumentation.	

Zugehörige Ressourcen

- Amazon API Gateway
- Amazon Route 53
- Application Load Balancer
- AWS PrivateLink
- AWS Certificate Manager

Betten Sie ein QuickSight Amazon-Dashboard in eine lokale Angular-Anwendung ein

Erstellt von Sean Griffin (AWS) und Milena Godau (AWS)

Übersicht

Dieses Muster bietet Anleitungen für die Einbettung eines QuickSight Amazon-Dashboards in eine lokal gehostete Angular-Anwendung zur Entwicklung oder zum Testen. Die eingebettete Analysefunktion in unterstützt diese Funktionalität QuickSight nicht nativ. Es erfordert ein QuickSight Konto mit einem vorhandenen Dashboard und Kenntnisse von Angular.

Wenn Sie mit eingebetteten QuickSight Dashboards arbeiten, müssten Sie Ihre Anwendung normalerweise auf einem Webserver hosten, um das Dashboard anzeigen zu können. Dies erschwert die Entwicklung, da Sie Ihre Änderungen kontinuierlich auf den Webserver übertragen müssen, um sicherzustellen, dass sich alles korrekt verhält. Dieses Muster zeigt, wie Sie einen lokal gehosteten Server ausführen und QuickSight eingebettete Analysen verwenden, um den Entwicklungsprozess einfacher und effizienter zu gestalten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS) -Konto
- Ein aktives QuickSight Konto mit Preisgestaltung für Sitzungskapazität
- QuickSight Das Embedding SDK ist installiert
- Angular CLI installiert
- Vertrautheit mit Angular
- mkcert ist installiert

Einschränkungen

- Dieses Muster bietet Anleitungen zum Einbetten eines QuickSight Dashboards mithilfe des Authentifizierungstyps `ANONYMOUS` (öffentlich zugänglich). Wenn Sie AWS Identity and Access Management (IAM) oder die QuickSight Authentifizierung mit Ihren eingebetteten Dashboards verwenden, gilt der angegebene Code nicht. Die Schritte zum Hosten der Angular-Anwendung im Abschnitt Epics sind jedoch weiterhin gültig.

- Für die Verwendung der GetDashboardEmbedUrlAPI mit dem `ANONYMOUS` Identitätstyp ist ein QuickSight Kapazitätspreisplan erforderlich.

Versionen

- Angular CLI versie 13.3.4
- QuickSight Einbetten der SDK-Version 2.3.1

Architektur

Technologie-Stack

- Eckiges Frontend
- Backend für AWS Lambda und Amazon API Gateway

Architektur

In dieser Architektur ermöglicht das HTTP APIs im API Gateway der lokalen Angular-Anwendung, die Lambda-Funktion aufzurufen. Die Lambda-Funktion gibt die URL zum Einbetten des QuickSight Dashboards zurück.

Automatisierung und Skalierung

Sie können die Backend-Bereitstellung mithilfe von AWS CloudFormation oder AWS Serverless Application Model (AWS SAM) automatisieren.

Tools

Tools

- Angular CLI ist ein Befehlszeilenschnittstellentool, mit dem Sie Angular-Anwendungen direkt von einer Befehlsshell aus initialisieren, entwickeln, einrichten und verwalten können.
- QuickSight Das Embedding SDK wird verwendet, um Dashboards in Ihren HTML-Code einzubetten. QuickSight
- mkcert ist ein einfaches Tool zum Erstellen lokal vertrauenswürdiger Entwicklungszertifikate. Es erfordert keine Konfiguration. mkcert ist erforderlich, da nur HTTPS-Anfragen zum Einbetten von Dashboards QuickSight zulässig sind.

AWS-Services

- Amazon API Gateway ist ein AWS-Service für die Erstellung, Veröffentlichung, Wartung, Überwachung und Sicherung von REST, HTTP und WebSocket APIs in jeder Größenordnung.
- AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.
- Amazon QuickSight ist ein Geschäftsanalysedienst, mit dem Sie Visualisierungen erstellen, Ad-hoc-Analysen durchführen und Geschäftserkenntnisse aus Ihren Daten gewinnen können.

Epen

Generieren Sie eine EmbedUrl

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine EmbedUrl Richtlinie.	Erstellen Sie eine IAM-Richtlinie mit QuicksightGetDashboardEmbedUrldem Namen und den folgenden Eigenschaften. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "quicksight:GetDashboardEmbedUrl", "quickSight:GetAnonymousUserEmbedUrl"`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>],
	
	"Resource": "*"
	}
	]
	}</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

So erstellen Sie die Lambda-Funktion:	1. Öffnen Sie in der Lambda-Konsole die Seite Funktionen.
	
	2. Wählen Sie Create Function.
	
	3. Wählen Sie Von Grund auf neu schreiben aus.
	
	4. Geben Sie für Function name (Funktionsname) `get-qs-embed-url` ein.
	
	5. Wählen Sie für Runtime (Laufzeit) die Option Python 3.9 aus.
	
	6. Wählen Sie Create Function.
	
	7. Kopieren Sie auf der Registerkarte Code den folgenden Code in die Lambda-Funktion.
	
	`import json`
	`import boto3`
	`from botocore.`
	`exceptions import`
	` ClientError`
	`import time`
	`from os import environ`
	
	`qs = boto3.client('quic`
	`ksight',region_nam`
	`e='us-east-1')`
	`sts = boto3.cli`
	`ent('sts')`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	ACCOUNT_ID = boto3.client('sts').get_caller_identity().get('Account')
	DASHBOARD_ID = environ['DASHBOARD_ID']
	
	def getDashboardURL(accountId, dashboardId, quicksightNamespace, resetDisabled, undoRedoDisabled):
	  try:
	  response = qs.get_dashboard_embed_url(
	  AwsAccountId = accountId,
	  DashboardId = dashboardId,
	  Namespace = quicksightNamespace,
	  IdentityType = 'ANONYMOUS',
	  SessionLifetimeInMinutes = 600,
	  UndoRedoDisabled = undoRedoDisabled,
	  ResetDisabled = resetDisabled
	  )
	  return response
	
	  except ClientError as e:
	  print(e)
	  return "Error generating embeddedURL: " + str(e)	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`def lambda_handler(eve nt, context):`
	`  url = getDashbo ardURL(ACCOUNT_ID,`
	` DASHBOARD_ID,`
	` "default", True, True) ['EmbedUrl']`
	`  return {`
	`  'statusCode':`
	` 200,`
	`  'url': url`
	`  }`
	
	8. Wählen Sie Bereitstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die Dashboard-ID als Umgebungsvariable hinzu.	Fügen Sie Ihrer Lambda-Funktion `DASHBOARD_ID` als Umgebungsvariable hinzu: 1. Wählen Sie auf der Registerkarte Konfiguration die Optionen Umgebungsvariablen, Bearbeiten, Umgebungsvariable hinzufügen aus. 2. Fügen Sie mit dem Schlüssel eine Umgebungsvariable hinzu`DASHBOARD_ID` . 3. Um den Wert von zu `DASHBOARD_ID` ermitteln, navigieren Sie zu Ihrem Dashboard QuickSight und kopieren Sie die UUID am Ende der URL in Ihren Browser. Wenn die URL beispielsweise lautet`https://us-east-1.quicksight.aws.amazon.com/sn/dashboards/<dashboard-id>` , geben Sie den `<dashboard-id>` Teil der URL als Schlüsselwert an. 4. Wählen Sie Speichern.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Berechtigungen für die Lambda-Funktion hinzu.	Ändern Sie die Ausführungsrolle der Lambda-Funktion und fügen Sie ihr die QuicksightGetDashboardEmbedUrlRichtlinie hinzu. 1. Wählen Sie auf der Registerkarte Konfiguration die Option Berechtigungen und dann den Rollennamen aus. 2. Wählen Sie Richtlinien anhängen, suchen Sie nach `QuicksightGetDashboardEmbedUrl`, aktivieren Sie das entsprechende Kontrollkästchen und wählen Sie dann Richtlinie anhängen aus.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Lambda-Funktion.	Erstellen Sie ein Testereignis und führen Sie es aus. Sie können die Vorlage „Hello World“ verwenden, da die Funktion keine der Daten des Testereignisses verwendet. 1. Wählen Sie die Registerkarte Test. 2. Geben Sie Ihrem Testereignis einen Namen und wählen Sie dann Speichern. 3. Um Ihre Lambda-Funktion zu testen, wählen Sie Test. Die Antwort sollte in etwa so aussehen wie die folgende. `{ "statusCode": 200, "url": "\"https://us-east-1.quicksight.aws.amazon.com/embed/f1acc0786687783b9a4543a05ba929b3a/dashboards/..." }` **Note** Wie im Abschnitt Voraussetzungen und Einschränkungen erwähnt, muss für Ihr QuickSight Konto	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ein Preisplan für Sitzungskapazität gelten. Andernfalls wird bei diesem Schritt eine Fehlermeldung angezeigt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine API in API Gateway.	1. Wählen Sie in der API Gateway Gateway-Konsole Create API und dann REST API, Build aus. • Geben Sie als API-Name ein `qs-embed-api` . • Wählen Sie Create API (API erstellen) aus. 2. Wählen Sie unter Aktionen die Option Methode erstellen aus. • Wählen Sie GET und bestätigen Sie mit dem Häkchen. • Wählen Sie Lambda-Funktion als Integrationstyp. • Geben `get-qs-embed-url` Sie für Lambda-Funktion den Wert ein. • Wählen Sie Speichern. • Wählen Sie im Feld Add Permission to Lambda Function die Option OK aus. 3. Aktivieren Sie CORS. • Wählen Sie unter Aktionen die Option CORS aktivieren aus. • Geben Sie für Access-Control-Allow-Origin ein.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`'https://my-qs-app.net:4200'` • Wählen Sie „CORS aktivieren“ und ersetzen Sie die vorhandenen CORS-Header, und bestätigen Sie. 4. Stellen Sie die API bereit. • Wählen Sie für Aktionen die Option Deploy API aus. • Wählen Sie für Deployment stage (Bereitstellungsstufe) [New Stage] ([Neue Stufe]) aus. • Geben Sie für Stage name (Stufenname) `dev` ein. • Wählen Sie Deploy (Bereitstellen) aus. • Kopieren Sie die Aufruf-URL. **Note** `my-qs-app.net` kann eine beliebige Domain sein. Wenn Sie einen anderen Domainnamen verwenden möchten, stellen Sie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	sicher, dass Sie die Access-Control-Allow-Origin-Informationen in Schritt 3 aktualisieren und in den nachfolge nden Schritten ändern. `my-qs-app.net`	

Erstellen Sie die Angular-Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Anwendung mit der Angular CLI.	1. Erstellen Sie die Anwendung.
	`ng new quicksight-app --defaults`
	`cd quicksight-app/src/app`
	2. Erstellen Sie die Dashboard-Komponente.
	`ng g c dashboard`
	3. Navigieren Sie zu Ihrer `src/environments/environment.ts` Datei und fügen Sie `apiUrl: '<Invoke URL from previous steps>'` sie dem Umgebungsobjekt hinzu.
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`export const environment = { production: false, apiUrl: '<Invoke URL from previous steps>', };`	

Fügen Sie das QuickSight Embedding SDK hinzu.	1. Installieren Sie das QuickSight Embedding SDK, indem Sie den folgenden Befehl im Stammordner Ihres Projekts ausführen.
	`npm i amazon-quicksight-embedding-sdk`
	2. Erstellen Sie eine neue `decl.d.ts` Datei in dem `src` Ordner mit dem folgenden Inhalt.
	`declare module 'amazon-quicksight-embedding-sdk';`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie Ihrer Datei dashboard.component.ts Code hinzu.	`import { Component, OnInit } from '@angular/core';`
	`import { HttpClient } from '@angular/common/http';`
	`import * as QuicksightEmbedding from 'amazon-quicksight-embedding-sdk';`
	`import { environment } from "../../environments/environment";`
	`import { take } from 'rxjs';`
	`import { EmbeddingContext } from 'amazon-quicksight-embedding-sdk/dist/types';`
	`import { createEmbeddingContext } from 'amazon-quicksight-embedding-sdk';`
	
	`@Component({`
	`  selector: 'app-dashboard',`
	`  templateUrl: './dashboard.component.html',`
	`  styleUrls: ['./dashboard.component.scss']`
	`})`
	`export class DashboardComponent implements OnInit {`
	
	`  constructor(private http: HttpClient) { }`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`  loadingError = false;`
	`  dashboard: any;`
	
	`  ngOnInit() {`
	`  this.GetDashboardU`
	`RL();`
	`  }`
	
	`  public GetDashbo`
	`ardURL() {`
	`  this.http.get(envi`
	`ronment.apiUrl)`
	`  .pipe(`
	`  take(1),`
	`  )`
	`  .subscribe((data:`
	` any) => this.Dash`
	`board(data.url));`
	`  }`
	
	`  public async Dashboard`
	`(embeddedURL: any) {`
	`  var containerDiv`
	` = document.getElemen`
	`tById("dashboardCo`
	`ntainer") || '';`
	`  const frameOptions`
	` = {`
	`  url: embeddedURL,`
	`  container:`
	` containerDiv,`
	`  height: "850px",`
	`  width: "100%",`
	`  resizeHei`
	`ghtOnSizeChangedEv`
	`ent: true,`
	`  }`
	`  const embedding`
	`Context: Embedding`
	`Context = await`
	` createEmbeddingCon`
	`text();`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`this.dashboard = embeddingContext.embedDashboard(frameOptions); } }`	
Fügen Sie Code zu Ihrer Datei dashboard.component.html hinzu.	Fügen Sie nun folgenden Code in die Datei `src/app/dashboard/dashboard.component.html` ein: `<div id="dashboardContainer"></div>`	App-Developer
Ändern Sie Ihre app.component.html-Datei, um Ihre Dashboard-Komponente zu laden.	1. Löschen Sie den Inhalt der Datei. `src/app/app.component.html` 2. Fügen Sie Folgendes hinzu. `<app-dashboard></app-dashboard>`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Importieren Sie HttpClientModule in Ihre app.module.ts-Datei.	1. Fügen Sie am Anfang der `src/app/app.module.ts` Datei Folgendes hinzu. `import { HttpClientModule } from '@angular/common/http';` 2. Fügen Sie `HttpClientModule` das **`imports`**Array für Ihr hinzu`AppModule` .	App-Developer

Hosten Sie die Angular-Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie mkcert.	**Note** Die folgenden Befehle gelten für Unix- oder MacOS-Computer. Wenn Sie Windows verwenden, finden Sie im Abschnitt Zusätzliche Informationen den entsprechenden Befehl echo. 1. Erstellen Sie eine lokale Zertifizierungsstelle (CA) auf Ihrem Computer.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`mkcert -install`
	2. Konfigurieren `my-qs-app.net` Sie so, dass immer auf Ihren lokalen PC umgeleitet wird.
	`echo "127.0.0.1 my-qs-app.net" | sudo tee -a /private/etc/hosts`
	3. Stellen Sie sicher, dass Sie sich im `src` Verzeichnis des Angular-Projekts befinden.
	`mkcert my-qs-app.net 127.0.0.1`	

Konfigurieren Sie QuickSight es so, dass Ihre Domain zugelassen wird.	1. Wählen Sie in QuickSight der oberen rechten Ecke Ihren Namen aus und wählen Sie dann Manage Quicksight aus. 2. Navigieren Sie zu Domains und Einbettung. 3. `https://my-qs-app.net:4200` Als zulässige Domain hinzufügen.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Lösung.	Starten Sie einen lokalen Angular-Entwicklungsserver, indem Sie den folgenden Befehl ausführen. `ng serve --host my-qs-app.net --port 4200 --ssl --ssl-key "./src/my-qs-app.net-key.pem" --ssl-cert "./src/my-qs-app.net.pem" -o` Dadurch wird Secure Sockets Layer (SSL) mit dem benutzerdefinierten Zertifikat aktiviert, das Sie zuvor erstellt haben. Wenn der Build abgeschlossen ist, wird ein Browserfenster geöffnet und Sie können Ihr eingebettetes QuickSight Dashboard anzeigen, das lokal in Angular gehostet wird.	App-Developer

Zugehörige Ressourcen

- Angular-Webseite
- Einbetten von QuickSight Daten-Dashboards für anonyme (nicht registrierte) Benutzer (Dokumentation) QuickSight
- QuickSight SDK einbetten
- Tool mkcert

Zusätzliche Informationen

Wenn Sie Windows verwenden, führen Sie das Befehlszeilenfenster als Administrator aus und konfigurieren Sie mit dem folgenden Befehl, dass immer `my-qs-app.net` zu Ihrem lokalen PC umgeleitet wird.

```
echo 127.0.0.1 my-qs-app.net >> %WINDIR%\System32\Drivers\Etc\Hosts
```

Entdecken Sie die Full-Stack-Entwicklung von cloudnativen Webanwendungen mit Green Boost

Erstellt von Ben Stickley (AWS) und Amiin Samatar (AWS)

Übersicht

Als Reaktion auf die sich wandelnden Bedürfnisse von Entwicklern ist sich Amazon Web Services (AWS) der dringenden Nachfrage nach einem effizienten Ansatz für die Entwicklung cloudnativer Webanwendungen bewusst. Der Schwerpunkt von AWS liegt darauf, Sie bei der Überwindung häufiger Hindernisse im Zusammenhang mit der Bereitstellung von Web-Apps in der AWS-Cloud zu unterstützen. Durch die Nutzung der Funktionen moderner Technologien wie AWS Cloud Development Kit (AWS CDK) TypeScript, React und Node.js zielt dieses Muster darauf ab, den Entwicklungsprozess zu rationalisieren und zu beschleunigen.

Das Muster basiert auf dem Green Boost (GB) -Toolkit und bietet einen praktischen Leitfaden für die Erstellung von Webanwendungen, die die umfangreichen Funktionen von AWS in vollem Umfang nutzen. Es dient als umfassende Roadmap, die Sie durch den Prozess der Bereitstellung einer grundlegenden CRUD-Webanwendung (Create, Read, Update, Delete) führt, die in die Amazon Aurora PostgreSQL-Compatible Edition integriert ist. Dies wird durch die Verwendung der Green Boost-Befehlszeilenschnittstelle (Green Boost CLI) und die Einrichtung einer lokalen Entwicklungsumgebung erreicht.

Nach der erfolgreichen Bereitstellung der Anwendung befasst sich das Pattern mit den wichtigsten Komponenten der Web-App, einschließlich Infrastrukturdesign, Backend- und Frontend-Entwicklung sowie mit wichtigen Tools wie cdk-dia für die Visualisierung, die ein effizientes Projektmanagement ermöglichen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Git installiert
- Visual Studio Code (VS Code) ist installiert
- AWS-Befehlszeilenschnittstelle (AWS CLI) installiert
- AWS CDK Toolkit installiert
- Node.js 18 installiert oder Node.js 18 mit aktiviertem pnpm

- pnpm ist installiert, falls es nicht Teil Ihrer Node.js Installation ist
- Grundkenntnisse in AWS CDK TypeScript, Node.js und React
- Ein aktives AWS-Konto
- Ein AWS-Konto, das mithilfe von AWS CDK in gestartet wurde. `us-east-1` Die `us-east-1` AWS-Region ist für die Unterstützung der Amazon CloudFront Lambda @Edge -Funktionen erforderlich.
- AWS-SicherheitsanmeldedatenAWS_ACCESS_KEY_ID, einschließlich korrekt konfigurierter Anmeldeinformationen in Ihrer Terminalumgebung
- Für Windows-Benutzer ein Terminal im Administratormodus (um der Art und Weise Rechnung zu tragen, wie pnpm mit Knotenmodulen umgeht)

Produktversionen

- AWS-SDK für JavaScript Version 3
- AWS CDK Version 2
- AWS-CLI Version 2.2
- Node.js, Version 18
- React-Version 18

Architektur

Zieltechnologie-Stack

- Amazon Aurora PostgreSQL-Compatible Edition
- Amazon CloudFront
- Amazon CloudWatch
- Amazon Elastic Compute Cloud (Amazon EC2)
- AWS Lambda
- AWS Secrets Manager
- Amazon-Simple-Notification-Service (Amazon-SNS)
- Amazon Simple Storage Service (Amazon-S3)
- AWS WAF

Zielarchitektur

Das folgende Diagramm zeigt, dass Benutzeranfragen Amazon CloudFront, AWS WAF und AWS Lambda durchlaufen, bevor sie mit einem S3-Bucket, einer Aurora-Datenbank, einer EC2 Instance interagieren und letztendlich Entwickler erreichen. Administratoren hingegen verwenden Amazon SNS und Amazon CloudWatch für Benachrichtigungen und Überwachungszwecke.

Um nach der Bereitstellung einen tieferen Einblick in die Anwendung zu erhalten, können Sie ein Diagramm mithilfe von cdk-dia erstellen, wie im folgenden Beispiel gezeigt.

Diese Diagramme zeigen die Architektur der Webanwendung aus zwei unterschiedlichen Blickwinkeln. Das cdk-dia-Diagramm bietet einen detaillierten technischen Überblick über die AWS-CDK-Infrastruktur und hebt bestimmte AWS-Services wie Amazon Aurora PostgreSQL-Compatible und AWS Lambda hervor. Im Gegensatz dazu nimmt das andere Diagramm eine breitere Perspektive ein und betont den logischen Datenfluss und die Benutzerinteraktionen. Der Hauptunterschied liegt im Detaillierungsgrad: Das cdk-dia befasst sich mit technischen Feinheiten, während das erste Diagramm eine eher benutzerorientierte Ansicht bietet.

Die Erstellung des cdk-dia-Diagramms wird im Epos Verstehen der App-Infrastruktur mithilfe von AWS CDK behandelt.

Tools

AWS-Services

- Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt.
- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Amazon CloudFront beschleunigt die Verteilung Ihrer Webinhalte, indem es sie über ein weltweites Netzwerk von Rechenzentren bereitstellt, was die Latenz senkt und die Leistung verbessert.
- Amazon CloudWatch hilft Ihnen dabei, die Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie auf AWS ausführen, in Echtzeit zu überwachen.

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Secrets Manager hilft Ihnen dabei, hartcodierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Geheimnis programmgesteuert abzurufen.
- AWS Systems Manager unterstützt Sie bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der AWS-Cloud ausgeführt werden. Es vereinfacht das Anwendungs- und Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme und hilft Ihnen, Ihre AWS-Ressourcen sicher und skalierbar zu verwalten. Dieses Muster verwendet AWS Systems Manager Session Manager.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, mit dem Sie beliebige Datenmengen speichern, schützen und abrufen können. Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.
- AWS WAF ist eine Firewall für Webanwendungen, mit der Sie HTTP- und HTTPS-Anfragen überwachen können, die an Ihre geschützten Webanwendungsressourcen weitergeleitet werden.

Andere Tools

- Git ist ein verteiltes Open-Source-Versionskontrollsystem.
- Green Boost ist ein Toolkit für die Erstellung von Web-Apps auf AWS.
- Next.js ist ein React-Framework zum Hinzufügen von Funktionen und Optimierungen.
- Node.js ist eine ereignisgesteuerte JavaScript Laufzeitumgebung, die für die Erstellung skalierbarer Netzwerkanwendungen entwickelt wurde.
- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL. Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, verwalten und verwenden können.
- pnpm ist ein Paketmanager für Node.js Projektabhängigkeiten.

Bewährte Methoden

Weitere Informationen zu den folgenden Empfehlungen finden Sie im Abschnitt Epics:

- Überwachen Sie die Infrastruktur mithilfe von Amazon CloudWatch Dashboards und Alarmen.
- Setzen Sie bewährte AWS-Verfahren durch, indem Sie cdk-nag verwenden, um statische Infrastructure-as-Code-Analysen (IaC) durchzuführen.
- Richten Sie die DB-Portweiterleitung über SSH-Tunneling (Secure Shell) mit Systems Manager Session Manager ein. Dies ist sicherer als eine öffentlich zugängliche IP-Adresse.
- Verwalten Sie Sicherheitslücken, indem Sie Folgendes ausführen: `pnpm audit`
- Setzen Sie bewährte Verfahren durch ESLint, indem Sie statische TypeScript Codeanalysen durchführen, und Prettier zur Standardisierung der Codeformatierung verwenden.

Epen

Stellen Sie eine CRUD-Web-App mit Aurora PostgreSQL-kompatibel bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die Green Boost CLI.	Führen Sie den folgenden Befehl aus, um Green Boost CLI zu installieren. `pnpm add -g gboost`	App-Developer
Erstellen Sie eine GB-App.	1. Führen Sie den Befehl aus, um eine App mit Green Boost zu erstellen`boost create`. 2. Wählen Sie als Vorlage `CRUD App with Aurora PostgreSQL` aus.	App-Developer
Installieren Sie Abhängigkeiten und stellen Sie die App bereit.	1. Navigieren Sie zum Projektverzeichnis:`cd <your directory> .`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Führen Sie den Befehl aus, um Abhängigkeiten zu installieren`pnpm i`. 3. Navigieren Sie zum Infra-Verzeichnis:`cd infra`. 4. Führen Sie den Befehl `pnpm deploy:local` aus, um die App lokal bereitzustellen. Dies ist ein Alias für einen `cdk deploy ...` Befehl, der in definiert ist`infra/package.json` . Warten Sie, bis die Bereitstellung abgeschlossen ist (ca. 20 Minuten). Überwachen Sie die CloudFormation AWS-Stacks in der CloudFormation Konsole, während Sie warten. Beachten Sie, wie die im Code definierten Konstrukte der bereitgestellten Ressource zugeordnet sind. Sehen Sie sich die CDK Construct-Strukturansicht in der CloudFormation Konsole an.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Greifen Sie auf die App zu.	Nachdem Sie Ihre GB-App lokal bereitgestellt haben, können Sie über die CloudFront URL darauf zugreifen. Die URL wird in der Terminalausgabe gedruckt, aber es kann etwas überwältigend sein, sie zu finden. Gehen Sie wie folgt vor, um sie schneller zu finden: 1. Öffnen Sie das Terminal, in dem Sie den `pnpm deploy:local` Befehl ausgeführt haben. 2. Suchen Sie in der Terminalausgabe nach einem Abschnitt, der dem folgenden Text ähnelt. `myapp5stickbui9C39A55A.CloudFrontDomainName = d1q16n5pof924c.cloudfront.net` Die URL wird für Ihre Bereitstellung eindeutig sein. Alternativ können Sie die CloudFront URL finden, indem Sie auf die CloudFront Amazon-Konsole zugreifen:	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Melden Sie sich bei der AWS-Managementkonsole an und navigieren Sie zum CloudFront Service. 2. Suchen Sie in der Liste nach der zuletzt bereitgestellten Distribution. Kopieren Sie den Domainnamen, der der Distribution zugeordnet ist. Es wird ähnlich aussehen wie `your-unique-id.cloudfront.net` .	

Überwachen Sie mithilfe von Amazon CloudWatch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich das CloudWatch Dashboard an.	1. Öffnen Sie die CloudWatch Konsole und wählen Sie Dashboards. 2. Wählen Sie das Dashboard mit dem Namen - - Dashboard <appId><stageName>aus. 3. Überprüfen Sie das Dashboard. Welche Ressourcen werden überwacht? Welche Kennzahlen werden aufgezeichnet? Dieses Dashboard wird durch	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	das Open-Source-Konstr ukt cdk-monitoring-con structsermöglicht.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Alarme aktivieren.	Ein CloudWatch Dashboard hilft Ihnen dabei, Ihre Web-App aktiv zu überwachen. Um Ihre Web-App passiv zu überwachen, können Sie Warnmeldungen aktivieren.
	1. Navigieren Sie zu `/infra/src/app/stateless/monitor-stack.ts` , was den Monitor-Stack definiert.
	2. Kommentieren Sie die folgende Zeile aus und `admin@example.com` ersetzen Sie sie durch Ihre E-Mail-Adresse.
	`onAlarmTopic.addSubscription(new EmailSubscription("admin@example.com"));`
	3. Fügen Sie die folgenden Importinformationen am Anfang der Datei hinzu.
	`import { EmailSubscription } from "aws-cdk-lib/aws-sns-subscriptions";`
	4. Führen Sie darin den folgenden Befehl aus. `infra/`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cdk deploy "*/monitor" --exclusively.` 5. Um Ihr Abonnement für das SNS-Thema zu bestätigen, das ausgelöst wird, wenn ein Überwachungsalarm ausgelöst wird, klicken Sie auf den Link in der E-Mail-Nachricht.	

Verstehen Sie die App-Infrastruktur mithilfe von AWS CDK

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Architekturdiagramm.	Generieren Sie mithilfe von cdk-dia ein Architekturdiagramm Ihrer Web-App. Die Visualisierung der Architektur trägt dazu bei, das Verständnis und die Kommunikation zwischen den Teammitgliedern zu verbessern. Es bietet einen klaren Überblick über die Komponenten des Systems und ihre Beziehungen. 1. Installieren Sie Graphviz. 2. Führen Sie `infra/` darin den Befehl aus. `pnpm cdk-dia` 3. Sehen Sie sich Ihre `aninfra/diagram.png` .	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie cdk-nag, um bewährte Verfahren durchzuse tzen.	Verwenden Sie cdk-nag, um eine sichere und regelkonf orme Infrastruktur aufrechtz uerhalten, indem Sie bewährte Verfahren durchsetzen und so das Risiko von Sicherhei tslücken und Fehlkonfi gurationen verringern. 1. Erfahren Sie im Abschnitt Regeln, wie cdk-nag bewährte Verfahren durchsetzt, einschließlich der Prüfungen aus dem Regelpaket der AWS Solutions Library. 2. Um zu sehen, wie cdk-nag Regeln durchsetzt, nehmen Sie eine Änderung im Code vor. Ändern Sie beispielsweise in `infra/src/app/stateful/data-stacks.ts` zu. `storageEncrypted: true` `storageEncrypted: false` 3. Führen Sie darin den Befehl aus `cdk synth "*/data"`. `infra/` Während der Synthese wird ein Build-Fehler auftreten, der auf einen Regelverstoß hinweist.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`AwsSolutions-RDS2: The RDS instance or Aurora DB cluster does not have storage encryption enabled.`
	
	Dieser Fehler zeigt, dass cdk-nag ein Sicherheitsmechanismus ist, der bewährte Methoden für die Infrastruktur durchsetzt und Sicherheitsfehlkonfigurationen verhindert.
	4. Bei Bedarf können Sie auch Regeln in unterschiedlichen Bereichen unterdrücken. Um beispielsweise AwsSolutions - zu unterdrückenRDS2, fügen Sie den folgenden Code unter der Instanziierung von hinzu. `DbIamCluster`
	
	`NagSuppressions.addResourceSuppressions( cluster.node.findChild("Resource"), [ { id: "AwsSolutions-RDS2", reason: "Customer requirement necessitates`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>having unencrypted
	DB storage",
	},
	],
	);</pre>
	5. Führen Sie den Vorgang nach der Unterdrückung erneut aus`cdk synth "*/data"`. Ihre AWS CDK-App sollte jetzt erfolgreich synthetisiert werden. Sie finden alle unterdrückten Regeln unter. `infra/cdk.out/assembly-<appId>-<stageName>/AwsSolutions-<appId>-<stageName>-${stackId}-NagReport.csv`	

Evaluieren Sie die Datenbankkonfiguration und das Schema

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erwerben Sie Umgebungsvariablen.	Gehen Sie wie folgt vor, um die erforderlichen Umgebungsvariablen abzurufen: 1. Um die zu finden`DB_BASTION_ID` , melden Sie sich bei der Konsole an und navigieren Sie zur EC2 Konsole. Wählen Sie Instances (running) aus und suchen	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie die Zeile, die - ssm-db-bastion Name <stageName>enthält. Die Instanz-ID beginnt mit i-. 2. Um das zu findenDB_ENDPOINT , wählen Sie in der Amazon Relational Database Service (Amazon RDS) -Konsole DB Instances und dann den regionalen Cluster aus, dessen DB-ID mit - -data <appId><stageName>- beginnt. Suchen Sie den Writer-Instance-Endpunkt, der auf rds.amazonaws.com endet.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Portweiterleitung ein.	Gehen Sie wie folgt vor, um die Portweiterleitung einzurichten: 1. Installieren Sie das AWS Systems Manager Session Manager-Plug-In. 2. Starten Sie die Portweiterleitung, indem `core/` Sie `pnpm db:connect` within ausführen, um eine sichere Verbindung über den Bastion-Host herzustellen. 3. Nachdem Sie den Text `Waiting for connections...,` in Ihrem Terminal sehen, wurde erfolgreich ein SSH-Tunnel zwischen Ihrem lokalen Computer und dem Aurora-Server über den EC2 Bastion-Host eingerichtet.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie das Timeout für den Systems Manager Session Manager an.	(Optional) Wenn das standardmäßige Sitzungstimeout von 20 Minuten zu kurz ist, können Sie es in der Systems Manager Manager-Konsole auf bis zu 60 Minuten erhöhen, indem Sie Sitzungsmanager, Einstellungen, Bearbeiten, Timeout für Leerlaufsitzungen wählen.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Visualisieren Sie die Datenbank.	pgAdmin ist ein benutzerf reundliches Open-Source-Tool zur Verwaltung von PostgreSQL-Datenbanken. Es vereinfacht Datenbank aufgaben und ermöglicht es Ihnen, Datenbanken effizient zu erstellen, zu verwalten und zu optimieren. Dieser Abschnitt führt Sie durch die Installation von pgAdmin und die Verwendung seiner Funktionen für die PostgreSQ L-Datenbankverwaltung. 1. Öffnen Sie im Objekt-Ex plorer das Kontextmenü (Rechtsklick) für Server und wählen Sie dann Register, Server. 2. Geben Sie auf der Registerkarte Allgemein - <appId><stageName>für das Feld Name ein. 3. Um das DB-Passwort abzurufen, öffnen Sie die AWS Secrets Manager Manager-Konsole, wählen Sie das Geheimnis mit der vom CDK generiert en Beschreibung für den Stack: - -data <appId><s tageName>aus und wählen Sie die Secret Value-Karte	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	aus. Wählen Sie Retrieve Secret Value und kopieren Sie den Secret-Wert mit einem Passwortschlüssel. 4. Geben Sie auf der Registerkarte Verbindung 0.0.0.0 für das Feld Hostname/Adresse und _admin für das Feld Benutzername ein. <appId> Verwenden Sie für das Feld Passwort den geheimen Schlüssel, den Sie zuvor abgerufen haben. Wählen Sie Ja für das Feld Passwort speichern? Feld. 5. Wählen Sie Speichern. 6. Um die Tabellen anzuzeigen, navigieren Sie zu -, Datenbanken, _db, Schemas,, Tabellen. <appId><stageName> <appId><appId> 7. Öffnen Sie das Kontextmenü (Rechtsklick) für die Elementtabelle und wählen Sie dann Daten anzeigen/bearbeiten, Alle Zeilen aus. 8. Erkunden Sie die Tabelle.	

Debuggen Sie mit Node.js

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Debuggen Sie den Anwendungsfall „Objekt erstellen“.	Gehen Sie wie folgt vor, um den Anwendungsfall „Element erstellen“ zu debuggen: 1. Öffnen Sie die `core/src/modules/item/create-item.use-case.ts` Datei und fügen Sie den folgenden Code ein. 2. Der im vorherigen Schritt hinzugefügte Code stellt sicher, dass die `createItemUseCase` Funktion aufgerufen wird, wenn dieses Modul direkt	App-Developer

```
import { fileURLTo
Path } from "node:url
";

// existing create-it
em.use-case.ts code
 here

if (process.argv[1]
 === fileURLTo
Path(import.meta.u
rl)) {
  createItemUseCase(
{
    description:
 "Item 1's Descripti
on",
    name: "Item 1",
  });
}
```

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ausgeführt wird. Setzen Sie Haltepunkte in den Zeilen innerhalb dieses Codeblocks, in denen Sie das line-by-line Debugging einleiten möchten. 1. Öffnen Sie das VS Code JavaScript Debug Terminal und führen Sie es dann aus, `pnpm tsx core/src/modules/item/create-item.use-case.ts` um den Code mit Debugging auszuführen. line-by-line Sie können auch `console.log` Anweisungen verwenden, aber Print-Anweisungen können unzureichend sein, wenn Sie mit komplexer Geschäftslogik arbeiten. Line-by-lineDurch das Debuggen erhalten Sie mehr Kontext.	

Entwickeln Sie das Frontend

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie den Entwicklungsserver ein.	1. Navigieren Sie zum `ui/` Entwicklungsserver Next.js und führen Sie ihn aus,	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`pnpm dev` um ihn zu starten. 2. Greifen Sie lokal auf Ihre Web-App zu unter `http://localhost:3000` . Der Entwicklungsserver Next.js ist mit sofortigem Fast Refresh-Feedback zu Änderungen an Ihren React-Komponenten eingerichtet. 3. Experimentieren Sie mit der Anpassung der Farbe der App-Leiste. Öffnen Sie die `ui/src/components/theme/theme.tsx` Datei und suchen Sie den Abschnitt, der das Thema für die App-Leiste definiert. Aktualisieren Sie in dem `colorSchemes.light.palette.primary` Abschnitt den Hauptwert von `colors.lagoon` `biscolors.carrot` . Nachdem Sie diese Änderung vorgenommen haben, speichern Sie die Datei und beobachten Sie das Update in Ihrem Browser. 4. Experimentieren Sie, indem Sie Text und Komponent	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en ändern und neue Seiten hinzufügen.	

Tooling mit Green Boost

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Monorepo und den pnpm-Paketmanager ein.	1. Sehen Sie `pnpm-workspace.yaml` im Stammverzeichnis Ihres GB-Repositorys nach und achten Sie darauf, wie Workspaces definiert sind. Weitere Informationen zu Workspaces finden Sie in der pnpm-Dokumentation. 2. Lesen Sie `ui/package.json` sich durch und achten Sie darauf, wie es `core/` mit dem Paketnamen auf den Workspace verweist. `"<appId>/core": "workspace:^",` 3. Beachten Sie, wie TypeScript die ESLint Konfiguration in den darin definierten Utility-Paketen zentralisiert ist`packages/` . Diese Konfiguration wird dann von Anwendungspaketen wie `core/infra/`, und verwendet`ui/`. Dies ist	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	hilfreich, wenn Ihre App skaliert und Sie mehr Anwendungspakete definieren, die auf die Dienstprogrammpakete verweisen können, ohne den Konfigurationscode zu duplizieren.	
Führen Sie pnpm-Skripte aus.	Führen Sie die folgenden Befehle im Stammverzeichnis Ihres Repositorys aus: 1. Führen Sie `pnpm lint`. Dieser Befehl führt eine statische Codeanalyse mit aus ESLint. 2. Führen Sie `pnpm typecheck .` Dieser Befehl führt den TypeScript Compiler aus, um die Typen Ihres Codes zu überprüfen. 3. Führen Sie `pnpm test`. Dieser Befehl führt Vitest aus, um Komponententests auszuführen. Beachten Sie, wie diese Befehle in allen Arbeitsbereichen ausgeführt werden. Die Befehle sind in den Feldern der einzelnen Workspaces definiert. `package.json#scripts`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wird ESLint für die statische Codeanalyse verwendet.	Gehen Sie wie folgt vor ESLint, um die Fähigkeit zur statischen Codeanalyse von zu testen: 1. Stellen Sie zunächst sicher, dass die VS ESLint Code-Erweiterung (ID:`dbaeumer.vscode-eslint`) installiert ist. Wir empfehlen, auch VS Code Error Lens (ID:`usernamehw.errorlens`) zu installieren, um Fehler direkt anzuzeigen. 2. Fügen Sie Ihrem Code bewusst eine Codezeile hinzu, die die `eval()` Funktion verwendet, wie im folgenden Beispiel gezeigt. `const userInput = "import("fs").then((fs) => console.log(fs.readFileSync("/etc/passwd", { encoding: "utf8" })))"; eval(userInput);` **Important** Dies dient nur zu Testzwecken. `eval()`Die Verwendung	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wird als potenziell gefährlich angesehen und sollte aufgrund von Sicherheitsrisiken vermieden werden. 3. Nachdem Sie die `eval()` Zeile eingefügt haben, öffnen Sie Ihren Code-Editor, um anhand roter Schnörkel zu überprüfen, ob der Codegeruch ESLint angezeigt wurde. 4. Weitere Informationen zu den ESLint Plugins und der Konfiguration finden Sie unter. `packages/eslint-config-{node,next}/.eslintrc.cjs`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwalte Abhängigkeiten und Sicherheitslücken.	1. Führen Sie das Programm `pnpm audit` im Stammverzeichnis Ihres Repositorys aus, um allgemeine Sicherhei tslücken und Risiken (CVEs) zu identifizieren. Dort sollte die Meldung Keine bekannten Sicherhei tslücken gefunden angezeigt werden. 2. Installieren Sie ein absichtlich anfälliges Paket darin`pnpm add minimist@0.2.3 core/` , indem Sie es ausführen und dann ausführen`pnpm audit`. Beachten Sie die gemeldete Sicherheitslücke. 3. Deinstallieren Sie das darin enthaltene anfällige Paket, `core/` indem Sie Folgendes ausführen`pnpm remove minimist`.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Hooks mit Husky vor dem Commit.	1. Nehmen Sie ein paar kleine Änderungen an den TypeScript Dateien im gesamten Repository vor. Die Änderungen können so einfach sein wie das Hinzufügen von Kommentaren. 2. Stellen Sie diese Änderungen bereit und übernehmen Sie sie, indem Sie `git add -A` und then verwenden`git commit -m "test husky"`. Der Husky-Pre-Commit-Hook-Trigger, der in definiert ist`.husky/pre-commit` , führt den Befehl aus. `pnpm lint-staged` 3. Beobachten Sie, wie lint-staged Befehle, die in `*/.lintstagedrc.js` Dateien angegeben sind, im gesamten Repository auf Dateien ausführt, die von Git bereitgestellt wurden. Diese Tools sind Mechanismen, die verhindern sollen, dass böser Code in Ihre Anwendung gelangt.	App-Developer

Reißen Sie die Infrastruktur nieder

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die Bereitstellung aus Ihrem Konto.	1. Um die Infrastruktur, die Sie im ersten Epic bereitgestellt haben, durch Run `pnpm destroy:local` In `infra/` abzubauen. 2. Warten Sie 15 Minuten, bis der `pnpm destroy:local` Vorgang abgeschlossen ist, und löschen Sie dann die beibehaltene Lambda @Edge -Funktion , indem Sie in der Lambda-Konsole nach Ihrer App-ID suchen. Lambda @Edge -Funktionen werden repliziert, was es schwierig macht, sie zu löschen. Weitere Informationen zum Löschen von Lambda @Edge -Funktionen finden Sie in der CloudFront Dokumentation.	App-Developer

Fehlerbehebung

Problem	Lösung
Die Portweiterleitung konnte nicht eingerichtet werden	Stellen Sie sicher, dass Ihre AWS-Anmeldeinformationen ordnungsgemäß konfiguriert sind und über die erforderlichen Berechtigungen verfügen.

Problem	Lösung
	Vergewissern Sie sich, dass die Umgebungsvariablen Bastion-Host-ID (`DB_BASTION_ID`) und Datenbank-Endpunkt (`DB_ENDPOINT`) korrekt gesetzt sind. Falls weiterhin Probleme auftreten, finden Sie in der AWS-Dokumentation Informationen zur Fehlerbehebung bei SSH-Verbindungen und im Session Manager.
Die Website wird nicht geladen `localhost:3000`	Vergewissern Sie sich, dass die Terminalausgabe eine erfolgreiche Portweiterleitung anzeigt, einschließlich der Weiterleitungsadresse. Stellen Sie sicher, dass es keine widersprüchlichen Prozesse gibt, die Port 3000 auf Ihrem lokalen Computer verwenden. Stellen Sie sicher, dass die Green Boost-Anwendung ordnungsgemäß konfiguriert ist und auf dem erwarteten Port (3000) ausgeführt wird. Überprüfen Sie Ihren Webbrowser auf Sicherheitserweiterungen oder Einstellungen, die lokale Verbindungen blockieren könnten.
Fehlermeldungen bei der lokalen Bereitstellung (`pnpm deploy:local`)	Überprüfen Sie die Fehlermeldungen sorgfältig, um die Ursache des Problems zu ermitteln. Stellen Sie sicher, dass die erforderlichen Umgebungsvariablen und Konfigurationsdateien korrekt eingestellt sind.

Zugehörige Ressourcen

- AWS-CDK-Dokumentation

- Green Boost-Dokumentation
- Dokumentation zu Next.js
- Dokumentation zu Node.js
- React-Dokumentation
- TypeScript Dokumentation

Führen Sie Komponententests für eine Node.js -Anwendung mithilfe GitHub von AWS aus CodeBuild

Erstellt von Thomas Scott (AWS) und Jean-Baptiste Guillois (AWS)

Übersicht

Dieses Muster enthält Beispielquellcode und wichtige Komponententestkomponenten für eine Spiele-API von Node.js. Es enthält auch Anweisungen zum Ausführen dieser Komponententests von einem GitHub Repository aus mithilfe von AWS CodeBuild als Teil Ihres CI/CD-Workflows (Continuous Integration and Continuous Delivery).

Unit-Tests sind ein Softwareentwicklungsprozess, bei dem verschiedene Teile einer Anwendung, sogenannte Units, einzeln und unabhängig voneinander auf ihren korrekten Betrieb getestet werden. Tests validieren die Qualität des Codes und bestätigen, dass er erwartungsgemäß funktioniert. Andere Entwickler können sich auch leicht mit Ihrer Codebasis vertraut machen, indem sie die Tests konsultieren. Unit-Tests reduzieren die future Refactoring-Zeit, helfen Ingenieuren dabei, sich schneller mit Ihrer Codebasis vertraut zu machen, und schaffen Vertrauen in das erwartete Verhalten.

Unit-Tests beinhalten das Testen einzelner Funktionen, einschließlich AWS Lambda Lambda-Funktionen. Um Unit-Tests zu erstellen, benötigen Sie ein Test-Framework und eine Methode zur Validierung von Tests (Assertions). Die Codebeispiele in diesem Muster verwenden das Mocha-Testframework und die Chai-Assertionsbibliothek.

Weitere Informationen zu Komponententests und Beispiele für Testkomponenten finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

- Ein aktives AWS-Konto mit den richtigen CodeBuild Berechtigungen
- Ein GitHub Konto (siehe Anweisungen zur Registrierung)
- Git (siehe Installationsanleitung)
- Ein Code-Editor, in den Sie Änderungen vornehmen und Ihren Code hochladen können GitHub

Architektur

Dieses Muster implementiert die Architektur, die im folgenden Diagramm dargestellt ist.

Tools

Tools

- Git ist ein Versionskontrollsystem, das Sie für die Codeentwicklung verwenden können.
- AWS CodeBuild ist ein vollständig verwalteter Continuous Integration Service, der Quellcode kompiliert, Tests durchführt und Softwarepakete produziert, die sofort einsatzbereit sind. Mit CodeBuild müssen Sie Ihre eigenen Build-Server nicht bereitstellen, verwalten und skalieren. CodeBuild skaliert kontinuierlich und verarbeitet mehrere Builds gleichzeitig, sodass Ihre Builds nicht in einer Warteschlange warten müssen. Mit den vorkonfigurierten Build-Umgebungen gelingt der Einstieg leicht. Jedoch können Sie auch benutzerdefinierte Build-Umgebungen mit Ihren eigenen Entwicklungstools erstellen. Mit CodeBuild werden Ihnen die von Ihnen genutzten Rechenressourcen minutengenau berechnet.

Code

Der Quellcode für dieses Muster ist im Repository der Beispielanwendung Game Unit Test verfügbar. GitHub Sie können aus diesem Beispiel Ihr eigenes GitHub Repository erstellen (Option 1) oder das Beispiel-Repository direkt (Option 2) für dieses Muster verwenden. Folgen Sie den Anweisungen für jede Option im nächsten Abschnitt. Welche Option Sie wählen, hängt von Ihrem Anwendungsfall ab.

Epen

Option 1 — Führen Sie Komponententests in Ihrem persönlichen GitHub Repository durch mit CodeBuild

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Ihr eigenes GitHub Repository auf der Grundlage des Beispielp rojekts.	1. Loggen Sie sich ein bei GitHub. 2. Erstellen Sie ein neues Repository. Anweisungen finden Sie in der GitHub Dokumentation. 3. Klonen Sie das Beispiel-Repository und übertrage	App-Entwickler, AWS-Admin istrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	n Sie es in das neue Repository in Ihrem Konto.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein neues CodeBuild Projekt.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CodeBuild Konsole unter https://console.aws.amazon.com/codesuite/codebuild/home. 2. Wählen Sie Create build project (Build-Projekt erstellen) aus. 3. Geben Sie im Abschnitt Projektkonfiguration als Projektname -js ein. aws-tests-sample-node 4. Wählen Sie im Abschnitt Quelle für Quellanbieter die Option GitHub. 5. Wählen Sie für Repository die Option Repository in my GitHub account aus und fügen Sie dann die URL in Ihr neu erstelltes GitHub Repository ein. 6. Wählen Sie im Abschnitt Primäre Webhook-Ereignisse die Option Jedes Mal neu erstellen, wenn eine Codeänderung in dieses Repository übertragen wird. 7. Wählen Sie als Ereignistyp PUSH.	App-Entwickler, AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Wählen Sie im Bereich Umgebung die Optionen Verwaltetes Image, Amazon Linux und das neueste Image aus. 9. Behalten Sie die Standarde instellungen für alle anderen Optionen bei und wählen Sie dann Build-Pro jekt erstellen.	
Starten Sie den Build.	Klicken Sie auf der Seite Review (Überprüfen) auf Start build (Build starten), um den Build auszuführen.	App-Entwickler, AWS-Admin istrator, AWS DevOps

Option 2 — Führen Sie Komponententests in einem öffentlichen Repository durch mit CodeBuild

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein neues CodeBuild Build-Projekt.	1. Melden Sie sich bei der AWS-Managementkons ole an und öffnen Sie die CodeBuild Konsole unter https://console.aws.amazon.com/codesuite/codebuild/home. 2. Wählen Sie Create build project (Build-Projekt erstellen) aus. 3. Geben Sie im Abschnitt Projektkonfiguration als Projektname -js ein. aws-tests-sample-node	App-Entwickler, AWS-Admin istrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie im Abschnitt Quelle für Quellanbieter die Option GitHub. 5. Wählen Sie für Repository die Option Öffentliches Repository aus und fügen Sie dann die URL ein: https://github.com/aws-samples/node-js-tests-sample. 6. Wählen Sie im Bereich Umgebung die Optionen Verwaltetes Image, Amazon Linux und das neueste Image aus. 7. Behalten Sie die Standardeinstellungen für alle anderen Optionen bei und wählen Sie dann Build-Projekt erstellen.	
Starten Sie den Build.	Klicken Sie auf der Seite Review (Überprüfen) auf Start build (Build starten), um den Build auszuführen.	App-Entwickler, AWS-Administrator, AWS DevOps

Analysieren Sie die Komponententests

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testergebnisse anzeigen.	Überprüfen Sie in der CodeBuild Konsole die Unit-Testergebnisse des CodeBuild Jobs. Sie sollten den Ergebnissen entsprech	App-Entwickler, AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en, die im Abschnitt Zusätzliche Informationen angezeigt werden. Diese Ergebnisse validieren die GitHub Repository-Integration mit CodeBuild.	
Wenden Sie einen Webhook an.	Sie können jetzt einen Webhook anwenden, sodass Sie automatisch einen Build starten können, wenn Sie Codeänderungen in den Hauptzweig Ihres Repositorys übertragen. Anweisungen finden Sie in der CodeBuild Dokumentation.	App-Entwickler, AWS-Administrator, AWS DevOps

Zugehörige Ressourcen

- Beispiel für eine Game-Unit-Testanwendung (GitHub Repository mit Beispielcode)
- CodeBuild AWS-Dokumentation
- GitHub Webhook-Ereignisse (CodeBuild Dokumentation)
- Ein neues Repository erstellen (GitHub Dokumentation)

Zusätzliche Informationen

Ergebnisse des Komponententests

In der CodeBuild Konsole sollten Sie die folgenden Testergebnisse sehen, nachdem das Projekt erfolgreich erstellt wurde.

Beispiele für Komponententests

In diesem Abschnitt werden die vier Arten von Testkomponenten beschrieben, die bei Unit-Tests verwendet werden: Assertions, Spies, Stubs und Mocks. Er enthält eine kurze Erklärung und ein Codebeispiel für jede Komponente.

Behauptungen

Eine Behauptung wird verwendet, um ein erwartetes Ergebnis zu verifizieren. Dies ist eine wichtige Testkomponente, da sie die erwartete Antwort einer bestimmten Funktion validiert. Die folgende Beispiel-Assertion bestätigt, dass die zurückgegebene ID bei der Initialisierung eines neuen Spiels zwischen 0 und 1000 liegt.

```
const { expect }  = require('chai');
const { Game } = require('../src/index');

describe('Game Function Group', () => {
 it('Check that the Game ID is between 0 and 1000', function() {
      const game = new Game();
      expect(game.id).is.above(0).but.below(1000)
 });
});
```

Spione

Ein Spion wird verwendet, um zu beobachten, was passiert, wenn eine Funktion ausgeführt wird. Beispielsweise möchten Sie möglicherweise überprüfen, ob die Funktion korrekt aufgerufen wurde. Das folgende Beispiel zeigt, dass Start- und Stop-Methoden für ein Game-Klassenobjekt aufgerufen werden.

```
const { expect }  = require('chai');
const { spy } = require('sinon');

const { Game } = require('../src/index');

describe('Game Function Group', () => {
   it('should verify that the correct function is called', () => {
      const spyStart = spy(Game.prototype, "start");
      const spyStop = spy(Game.prototype, "stop");

      const game = new Game();
      game.start();
      game.stop();
```

```
      expect(spyStart.called).to.be.true
      expect(spyStop.called).to.be.true
    });
});
```

Stubs

Ein Stub wird verwendet, um die Standardantwort einer Funktion zu überschreiben. Dies ist besonders nützlich, wenn die Funktion eine externe Anfrage stellt, da Sie vermeiden möchten, externe Anfragen aus Komponententests zu stellen. (Externe Anfragen eignen sich besser für Integrationstests, mit denen Anfragen zwischen verschiedenen Komponenten physisch getestet werden können.) Im folgenden Beispiel erzwingt ein Stub eine Rückgabe-ID von der GetID-Funktion.

```
const { expect }  = require('chai');
const {.stub } = require('sinon');

const { Game } = require('../src/index');

describe('Game Function Group', () =>  {
   it('Check that the Game ID is between 0 and 1000', function() {
      let generateIdStub = stub(Game.prototype, 'getId').returns(999999);

      const game = new Game();

      expect(game.getId).is.equal(999999);

      generateIdStub.restore();
    });
});
```

Verspottet

Ein Mock ist eine gefälschte Methode mit einem vorprogrammierten Verhalten zum Testen verschiedener Szenarien. Ein Mock kann als erweiterte Form eines Stubs betrachtet werden und kann mehrere Aufgaben gleichzeitig ausführen. Im folgenden Beispiel wird ein Mock verwendet, um drei Szenarien zu validieren:

- Die Funktion wird aufgerufen
- Die Funktion wird mit Argumenten aufgerufen
- Die Funktion gibt die Ganzzahl 9 zurück

```
const { expect }  = require('chai');
const {.mock } = require('sinon');

const { Game } = require('../src/index');

describe('Game Function Group', () =>  {
   it('Check that the Game ID is between 0 and 1000', function() {
      let mock = mock(Game.prototype).expects('getId').withArgs().returns(9);

      const game = new Game();
      const id = get.getId();

      mock.verify();
      expect(id).is.equal(9);
    });
});
```

Strukturieren Sie ein Python-Projekt in hexagonaler Architektur mit AWS Lambda

Erstellt von Furkan Oruc (AWS), Dominik Goby (AWS), Darius Kunce (AWS) und Michal Ploski (AWS)

Übersicht

Dieses Muster zeigt, wie ein Python-Projekt in hexagonaler Architektur mithilfe von AWS Lambda strukturiert wird. Das Muster verwendet das AWS Cloud Development Kit (AWS CDK) als Infrastructure-as-Code-Tool (IaC), Amazon API Gateway als REST-API und Amazon DynamoDB als Persistenzschicht. Die hexagonale Architektur folgt domänengesteuerten Designprinzipien. In der hexagonalen Architektur besteht Software aus drei Komponenten: Domäne, Ports und Adaptern. Ausführliche Informationen zu hexagonalen Architekturen und ihren Vorteilen finden Sie im Leitfaden Aufbau sechseckiger Architekturen auf AWS.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Erfahrung in Python
- Vertrautheit mit AWS Lambda, AWS CDK, Amazon API Gateway und DynamoDB
- Ein GitHub Konto (siehe Anweisungen zur Registrierung)
- Git (siehe Installationsanleitung)
- Ein Code-Editor, mit dem Sie Änderungen vornehmen und Ihren Code übertragen können GitHub (z. B. Visual Studio Code oder JetBrains PyCharm)
- Docker ist installiert und der Docker-Daemon ist betriebsbereit

Produktversionen

- Git Version 2.24.3 oder höher
- Python-Version 3.7 oder höher
- AWS CDK v2
- Poetry Version 1.1.13 oder höher

- AWS Lambda Powertools für Python Version 1.25.6 oder höher
- pytest Version 7.1.1 oder höher
- Moto-Version 3.1.9 oder höher
- pydantic Version 1.9.0 oder höher
- Boto3 Version 1.22.4 oder höher
- mypy-boto3-dynamodb Version 1.24.0 oder höher

Architektur

Zieltechnologie-Stack

Der Zieltechnologie-Stack besteht aus einem Python-Dienst, der API Gateway, Lambda und DynamoDB verwendet. Der Dienst verwendet einen DynamoDB-Adapter, um Daten zu speichern. Es bietet eine Funktion, die Lambda als Einstiegspunkt verwendet. Der Service verwendet Amazon API Gateway, um eine REST-API verfügbar zu machen. Die API verwendet AWS Identity and Access Management (IAM) für die Authentifizierung von Clients.

Zielarchitektur

Zur Veranschaulichung der Implementierung wird in diesem Muster eine serverlose Zielarchitektur bereitgestellt. Clients können Anfragen an einen API-Gateway-Endpunkt senden. API Gateway leitet die Anfrage an die Lambda-Zielfunktion weiter, die das hexagonale Architekturmuster implementiert. Die Lambda-Funktion führt Erstellungs-, Lese-, Aktualisierungs- und Löschvorgänge (CRUD) in einer DynamoDB-Tabelle durch.

> **Important**
>
> Dieses Muster wurde in einer PoC-Umgebung getestet. Bevor Sie eine Architektur in einer Produktionsumgebung einsetzen, müssen Sie eine Sicherheitsüberprüfung durchführen, um das Bedrohungsmodell zu identifizieren und eine sichere Codebasis zu erstellen.

Die API unterstützt fünf Operationen an einer Produktentität:

- `GET /products`gibt alle Produkte zurück.

- `POST /products`erstellt ein neues Produkt.
- `GET /products/{id}`gibt ein bestimmtes Produkt zurück.
- `PUT /products/{id}`aktualisiert ein bestimmtes Produkt.
- `DELETE /products/{id}`löscht ein bestimmtes Produkt.

Sie können die folgende Ordnerstruktur verwenden, um Ihr Projekt so zu organisieren, dass es dem hexagonalen Architekturmuster folgt:

```
app/  # application code
|--- adapters/  # implementation of the ports defined in the domain
     |--- tests/  # adapter unit tests
|--- entrypoints/  # primary adapters, entry points
     |--- api/  # api entry point
          |--- model/  # api model
          |--- tests/  # end to end api tests
|--- domain/  # domain to implement business logic using hexagonal architecture
     |--- command_handlers/  # handlers used to execute commands on the domain
     |--- commands/  # commands on the domain
     |--- events/  # events triggered via the domain
     |--- exceptions/  # exceptions defined on the domain
     |--- model/  # domain model
     |--- ports/  # abstractions used for external communication
     |--- tests/  # domain tests
|--- libraries/  # List of 3rd party libraries used by the Lambda function
infra/  # infrastructure code
simple-crud-app.py  # AWS CDK v2 app
```

Tools

AWS-Services

- Amazon API Gateway ist ein vollständig verwalteter Service, der Entwicklern die Erstellung, Veröffentlichung, Wartung, Überwachung und Sicherung APIs in jeder Größenordnung erleichtert.
- Amazon DynamoDB ist eine vollständig verwaltete, serverlose NoSQL-Datenbank mit Schlüsselwerten, die für die Ausführung von Hochleistungsanwendungen in jeder Größenordnung konzipiert ist.
- AWS Lambda ist ein serverloser, ereignisgesteuerter Rechenservice, mit dem Sie Code für praktisch jede Art von Anwendung oder Backend-Service ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Sie können Lambda-Funktionen von über 200 AWS-

Services und SaaS-Anwendungen (Software as a Service) aus starten und zahlen nur für das, was Sie tatsächlich nutzen.

Tools

- Git wird in diesem Muster als Versionskontrollsystem für die Codeentwicklung verwendet.
- Python wird als Programmiersprache für dieses Muster verwendet. Python bietet Datenstrukturen auf hoher Ebene und einen Ansatz für objektorientierte Programmierung. AWS Lambda bietet eine integrierte Python-Laufzeit, die den Betrieb von Python-Services vereinfacht.
- Visual Studio Code wird als IDE für die Entwicklung und das Testen dieses Musters verwendet. Sie können jede IDE verwenden, die die Python-Entwicklung unterstützt (z. B. PyCharm).
- Das AWS Cloud Development Kit (AWS CDK) ist ein Open-Source-Framework für die Softwareentwicklung, mit dem Sie Ihre Cloud-Anwendungsressourcen mithilfe vertrauter Programmiersprachen definieren können. Dieses Muster verwendet das CDK, um die Cloud-Infrastruktur als Code zu schreiben und bereitzustellen.
- Poesie wird verwendet, um Abhängigkeiten im Muster zu verwalten.
- Docker wird vom AWS CDK verwendet, um das Lambda-Paket und die Lambda-Layer zu erstellen.

Code

Der Code für dieses Muster ist im Beispiel-Repository für die hexagonale Architektur von GitHub Lambda verfügbar.

Bewährte Methoden

Um dieses Muster in einer Produktionsumgebung zu verwenden, folgen Sie diesen bewährten Methoden:

- Verwenden Sie vom Kunden verwaltete Schlüssel in AWS Key Management Service (AWS KMS), um CloudWatch Amazon-Protokollgruppen und Amazon DynamoDB-Tabellen zu verschlüsseln.
- Konfigurieren Sie AWS WAF für Amazon API Gateway so, dass der Zugriff nur über das Netzwerk Ihres Unternehmens möglich ist.
- Ziehen Sie andere Optionen für die API Gateway Gateway-Autorisierung in Betracht, wenn IAM Ihre Anforderungen nicht erfüllt. Sie können beispielsweise Amazon Cognito Cognito-Benutzerpools oder API Gateway Lambda-Autorisierer verwenden.
- Verwenden Sie DynamoDB-Backups.

- Konfigurieren Sie Lambda-Funktionen mit einer Virtual Private Cloud (VPC) -Bereitstellung, um den Netzwerkverkehr in der Cloud zu halten.
- Aktualisieren Sie die zulässige Ursprungskonfiguration für Cross-Origin Resource Sharing (CORS) -Preflight, um den Zugriff nur auf die anfragende Ursprungsdomäne zu beschränken.
- Verwenden Sie cdk-nag, um den AWS-CDK-Code auf bewährte Sicherheitsmethoden zu überprüfen.
- Erwägen Sie die Verwendung von Tools zum Scannen von Code, um häufig auftretende Sicherheitsprobleme im Code zu finden. Bandit ist beispielsweise ein Tool, das entwickelt wurde, um häufig auftretende Sicherheitsprobleme im Python-Code zu finden. PIP-Audit durchsucht Python-Umgebungen nach Paketen, die bekannte Sicherheitslücken aufweisen.

Dieses Muster verwendet AWS X-Ray, um Anfragen über den Einstiegspunkt, die Domäne und die Adapter der Anwendung zu verfolgen. AWS X-Ray hilft Entwicklern dabei, Engpässe zu identifizieren und hohe Latenzen zu ermitteln, um die Anwendungsleistung zu verbessern.

Epen

Initialisieren Sie das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Ihr eigenes Repository.	1. Loggen Sie sich ein bei GitHub. 2. Erstellen Sie ein neues Repository. Anweisungen finden Sie in der GitHub Dokumentation. 3. Klonen Sie das Beispiel-Repository für dieses Muster und übertragen Sie es in das neue Repository in Ihrem Konto.	App-Developer
Installieren Sie die Abhängigkeiten.	1. Installieren Sie Poetry. `pip install poetry`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	2. Installiere Pakete aus dem Stammverzeichnis. Der folgende Befehl installie rt die Anwendung und die AWS CDK-Paket e. Außerdem werden Entwicklungspakete installie rt, die für die Ausführun g von Komponententests erforderlich sind. Alle installierten Pakete werden in einer neuen virtuellen Umgebung platziert.
	`poetry install`
	3. Um eine grafische Darstellu ng der installierten Pakete zu sehen, führen Sie den folgenden Befehl aus.
	`poetry show --tree`
	4. Aktualisieren Sie alle Abhängigkeiten.
	`poetry update`
	5. Öffnen Sie eine neue Shell in der neu erstellten virtuelle n Umgebung. Sie enthält alle installierten Abhängigk eiten.
	`poetry shell`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Ihre IDE.	Wir empfehlen Visual Studio Code, aber Sie können jede IDE Ihrer Wahl verwenden , die Python unterstützt. Die folgenden Schritte gelten für Visual Studio Code. 1. Aktualisieren Sie die `.vscode/settings` Datei. `{ "python.testing.pytestArgs": [ "app/adapters/tests", "app/entrypoints/api/tests", "app/domain/tests" ], "python.testing.unittestEnabled": false, "python.testing.pytestEnabled": true, "python.envFile": "${workspaceFolder}/.env", }` 2. Erstellen Sie eine `.env` Datei im Stammverzeichnis des Projekts. Dadurch wird sichergestellt, dass das Stammverzeichnis des Projekts im Verzeichnis	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	enthalten ist, `PYTHONPATH` sodass Sie es `pytest` finden und alle Pakete richtig erkennen können. `PYTHONPATH=.`	
Führen Sie Komponententests aus, Option 1: Verwenden Sie Visual Studio Code.	1. Wählen Sie den Python-Interpreter der virtuellen Umgebung, die von Poetry verwaltet wird. 2. Führen Sie Tests im Test Explorer aus.	App-Developer

Unit-Tests ausführen, Option 2: Verwenden Sie Shell-Befehle.	1. Starten Sie eine neue Shell in der virtuellen Umgebung.
	`poetry shell`
	2. Führen Sie den `pytest` Befehl im Stammverzeichnis aus.
	`python -m pytest`
	Alternativ können Sie den Befehl direkt von Poetry aus ausführen.
	`poetry run python -m pytest`
		App-Developer

Stellen Sie die Anwendung bereit und testen Sie sie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fordern Sie temporäre Anmeldeinformationen an.	Um bei der Ausführung AWS-Anmeldeinformationen auf der Shell zu haben`cdk deploy`, erstellen Sie mithilfe von AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) temporäre Anmeldeinformationen. Anweisungen finden Sie im Blogbeitrag So rufen Sie kurzfristige Anmeldeinformationen für die CLI-Verwendung mit AWS IAM Identity Center ab.	App-Entwickler, AWS DevOps

Stellen Sie die Anwendung bereit.	1. Installieren Sie das AWS CDK v2.
	`npm install -g aws-cdk`
	Weitere Informationen finden Sie in der AWS-CDK-Dokumentation.
	2. Bootstrap Sie das AWS-CDK in Ihr Konto und Ihre Region.
	`cdk bootstrap aws://12345678900/us-east-1 --profile aws-profile-name`
	3. Stellen Sie die Anwendung mithilfe eines AWS-Profils
		App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	als CloudFormation AWS-Stack bereit. `cdk deploy --profile aws-profile-name`	
Testen Sie die API, Option 1: Verwenden Sie die Konsole.	Verwenden Sie die API Gateway Gateway-Konsole, um die API zu testen. Weitere Informationen zu API-Vorgängen und Anforderungs-/Antwortnachrichten finden Sie im Abschnitt API-Nutzung der Readme-Datei im Repository. GitHub	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die API, Option 2: Verwenden Sie Postman.	Wenn Sie ein Tool wie Postman verwenden möchten: 1. Installieren Sie Postman als eigenständige Anwendung oder Browsererweiterung. 2. Kopieren Sie die Endpunkt-URL für das API Gateway. Es wird das folgende Format haben. `https://{api-id}.execute-api.{region}.amazonaws.com/{stage}/{path}` 3. Konfigurieren Sie die AWS-Signatur auf der Registerkarte Autorisierung. Anweisungen finden Sie im AWS re:POST-Artikel zur Aktivierung der IAM-Authentifizierung für API Gateway REST. APIs 4. Verwenden Sie Postman, um Anfragen an Ihren API-Endpunkt zu senden.	App-Entwickler, AWS DevOps

Entwickeln Sie den Service

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schreiben Sie Komponententests für den Geschäftsbereich.	1. Erstellen Sie eine Python-Datei in dem `app/domain/tests` Ordner, indem	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie das `test_` Dateiname npräfix verwenden. 2. Erstellen Sie eine neue Testmethode, um die neue Geschäftslogik anhand des folgenden Beispiels zu testen. `def test_crea te_product_should_ store_in_repositor y(): # Arrange command = create_product_com mand.CreateProduct Command(name="Test Product", descripti on="Test Descripti on",) # Act create_pr oduct_command_hand ler.handle_create_ product_command(command=c ommand, unit_of_w ork=mock_unit_of_w ork) # Assert` 3. Erstellen Sie eine Befehlskl asse im `app/domain/ commands` Ordner.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wenn die Funktionalität neu ist, erstellen Sie im `app/domain/command_handlers` Ordner einen Stub für den Befehlshandler. 5. Führen Sie den Komponententest aus, um festzustellen, ob er fehlschlägt, da es immer noch keine Geschäftslogik gibt. `python -m pytest`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Implementieren Sie Befehle und Befehlshandler.	1. Implementieren Sie Geschäftslogik in der neu erstellten Befehlshandler-Datei.
	2. Deklarieren Sie für jede Abhängigkeit, die mit externen Systemen interagiert, eine abstrakte Klasse im `app/domain/ports` Ordner.
	
	`class ProductsRepository(ABC):`
	`  @abstractmethod`
	`  def add(self, product: product.Product) -> None:`
	`  ...`
	
	`class UnitOfWork(ABC):`
	`  products: ProductsRepository`
	
	`  @abstractmethod`
	`  def commit(self) -> None:`
	`  ...`
	
	`  @abstractmethod`
	`  def __enter__(self) -> typing.Any:`
	`  ...`
	
	`  @abstractmethod`
	`  def __exit__(self, *args) -> None:`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	...
	3. Aktualisieren Sie die Befehlshandler-Signatur, sodass sie die neu deklarierten Abhängigkeiten akzeptiert, indem Sie die abstrakte Port-Klasse als Typanmerkung verwenden.
	`def handle_create_product_command(`
	`command: create_product_command.CreateProductCommand,`
	`unit_of_work: unit_of_work.UnitOfWork,`
	`) -> str:`
	`...`
	4. Aktualisieren Sie den Komponententest, um das Verhalten aller deklarierten Abhängigkeiten für den Befehlshandler zu simulieren.
	`# Arrange`
	`mock_unit_of_work = unittest.mock.create_autospec(`
	`spec=unit_of_work.UnitOfWork, instance=True`
	`)`
	`mock_unit_of_work.products =`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>unittest.mock.create_autospec(
	spec=unit_of_work.ProductsRepository, instance=True
	)</pre>
	5. Aktualisieren Sie die Assertionslogik im Test, um nach den erwarteten Abhängigkeitsaufrufen zu suchen.
	<pre># Assert
	mock_unit_of_work.commit.assert_called_once()
	product = mock_unit_of_work.products.add.call_args.args[0]
	
	assertpy.assert_that(product.name).is_equal_to("Test Product")
	assertpy.assert_that(product.description).is_equal_to("Test Description")</pre>
	6. Führen Sie den Komponententest aus, um zu sehen, ob er erfolgreich ist.
	<pre>python -m pytest</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Schreiben Sie Integrationstests für sekundäre Adapter.	1. Erstellen Sie eine Testdatei in dem `app/adapters/tests` Ordner, indem Sie `test_` sie als Dateinamenpräfix verwenden.
	2. Verwenden Sie die Moto-Bibliothek, um AWS-Services nachzuahmen.
	`@pytest.fixture`
	`def mock_dynamodb():`
	`  with moto.mock_dynamodb():`
	`  yield boto3.resource("dynamodb", region_name="eu-central-1")`
	3. Erstellen Sie eine neue Testmethode für einen Integrationstest des Adapters.
	`def test_add_and_commit_should_store_product(mock_dynamodb):`
	`  # Arrange`
	`  unit_of_work = dynamodb_unit_of_work.DynamoDBUnitOfWork(`
	`  table_name=TEST_TABLE_NAME, dynamodb_client=mock_dynamodb.meta.client`
	`  )`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> current_time = datetime.datetime.now(datetime.timezone.utc).isoformat()
	
	    new_product_id = str(uuid.uuid4())
	    new_product = product.Product(
	        id=new_product_id,
	        name="test-name",
	        description="test-description",
	        createDate=current_time,
	        lastUpdateDate=current_time,
	    )
	
	    # Act
	    with unit_of_work:
	        unit_of_work.products.add(new_product)
	        unit_of_work.commit()
	
	    # Assert</pre> 4. Erstellen Sie eine Adapterklasse im `app/adapters` Ordner. Verwenden Sie die abstrakte Klasse aus dem Ports-Ordner als Basisklasse.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Führen Sie den Komponent entest aus, um festzuste llen, ob er fehlschlägt, da immer noch keine Logik vorhanden ist. `python -m pytest`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Implementieren Sie sekundäre Adapter.	1. Implementieren Sie Logik in der neu erstellten Adapterdatei.
	2. Aktualisieren Sie die Test-Assertionen.
	
	`# Assert`
	`    with unit_of_work_readonly:`
	`        product_from_db = unit_of_work_readonly.products.get(new_product_id)`
	
	`    assertpy.assert_that(product_from_db).is_not_none()`
	`    assertpy.assert_that(product_from_db.dict()).is_equal_to(`
	`        {`
	`            "id": new_product_id,`
	`            "name": "test-name",`
	`            "description": "test-description",`
	`            "createDate": current_time,`
	`            "lastUpdateDate": current_time,`
	`        }`
	`    )`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Führen Sie den Komponent entest aus, um zu sehen, ob er erfolgreich ist. `python -m pytest`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schreiben Sie end-to-end Tests.	1. Erstellen Sie eine Testdatei in dem `app/entry points/api/tests` Ordner, indem Sie `test_` sie als Dateinamenpräfix verwenden. 2. Erstellen Sie ein Lambda-Kontext-Fixture, das vom Test zum Aufrufen von Lambda verwendet wird. 3. Erstellen Sie eine Testmethode für den API-Aufruf.	App-Developer

```
@pytest.fixture
def lambda_co
ntext():
    @dataclass
    class LambdaCon
text:
        function_
name: str = "test"
        memory_li
mit_in_mb: int = 128
        invoked_f
unction_arn: str =
 "arn:aws:lambda:eu
-west-1:809313241:
function:test"
        aws_reque
st_id: str =
 "52fdfc07-2182-154
f-163f-5f0f9a621d7
2"

 return LambdaCon
text()
```

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`def test_crea te_product(lambda_ context):`
	`    # Arrange`
	`    name = "TestName"`
	`    description =  "Test description"`
	`    request =  api_model.CreatePr oductRequest(name= name, descripti on=description)`
	
	`    minimal_event =  api_gateway_proxy_ event.APIGatewayPr oxyEvent(`
	`        {`
	`            "path": "/ products",`
	`            "httpMeth od": "POST",`
	`            "requestC ontext": {  #  correlation ID`
	
	`  "requestId":  "c6af9ac6-7b61-11e 6-9a41-93e8deadbee f"`
	`            },`
	`            "body":  json.dumps(request .dict()),`
	`        }`
	`    )`
	
	`    create_pr oduct_func_mock =  unittest.mock.crea te_autospec(`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>spec=crea
	te_product_command
	_handler.handle_cr
	eate_product_comma
	nd
	)
	handler.c
	reate_product_comm
	and_handler.handle
	_create_product_co
	mmand = (
	create_pr
	oduct_func_mock
	)
	
	# Act
	handler.h
	andler(minimal_eve
	nt, lambda_context)</pre>	

	4. Führen Sie den Komponententest aus, um festzustellen, ob er fehlschlägt, da immer noch keine Logik vorhanden ist. <pre>python -m pytest</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Implementieren Sie Primäradapter.	1. Erstellen Sie eine Funktion für die API-Geschäftslogik und deklarieren Sie sie als API-Ressource.
	
	`@tracer.capture_method`
	`@app.post("/products")`
	`@utils.parse_event(model=api_model.CreateProductRequest, app_context=app)`
	`def create_product(`
	`request: api_model.CreateProductRequest,`
	`) -> api_model.CreateProductResponse:`
	`"""Creates a product."""`
	`...`
	
	Note
	Alle Decorators, die Sie sehen, sind Funktionen der AWS-Bibliothek Lambda Powertools for Python. Einzelheiten finden Sie auf der Website AWS Lambda Powertools for Python.
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	2. Implementieren Sie die API-Logik.
	
	`id=create_product_command_handler.handle_create_product_command(`
	`command=create_product_command.CreateProductCommand(`
	`name=request.name,`
	`description=request.description,`
	`),`
	`unit_of_work=unit_of_work,`
	`)`
	`response = api_model.CreateProductResponse(id=id)`
	`return response.dict()`
	
	3. Führen Sie den Komponententest aus, um zu sehen, ob er erfolgreich ist.
	
	`python -m pytest`	

Zugehörige Ressourcen

APG-Leitfaden

- Aufbau sechseckiger Architekturen auf AWS

AWS-Referenzen

- AWS Lambda Lambda-Dokumentation
- AWS-CDK-Dokumentation
  - Ihre erste AWS CDK-App
- API Gateway Gateway-Dokumentation
  - Steuern Sie den Zugriff auf eine API mit IAM-Berechtigungen
  - Verwenden Sie die API Gateway Gateway-Konsole, um eine REST-API-Methode zu testen
- Amazon DynamoDB DynamoDB-Dokumentation

Tools

- Webseite git-scm.com
- Git installieren
- Ein neues GitHub Repository erstellen
- Python-Webseite
- AWS Lambda Powertools für Python
- Postman-Webseite
- Python-Mock-Objektbibliothek
- Poesie-Website

IDEs

- Visual Studio Code-Webseite
- PyCharm website

Mehr Muster

- Zugriff über eine ASP.NET Core-App mithilfe AWS-Services von Amazon Cognito Cognito-Identitätspools
- Greifen Sie privat auf Container-Anwendungen auf Amazon ECS zu, indem Sie AWS Fargate PrivateLink, AWS und einen Network Load Balancer verwenden
- Greifen Sie mithilfe von AWS PrivateLink und einem Network Load Balancer privat auf Container-Anwendungen auf Amazon ECS zu
- Verknüpfen Sie ein AWS CodeCommit Repository in einem AWS-Konto mit Amazon SageMaker AI Studio Classic in einem anderen Konto
- Automatisieren Sie das Löschen von AWS CloudFormation Stacks und zugehörigen Ressourcen
- Beschränken Sie den Zugriff basierend auf IP-Adresse oder Geolokalisierung mithilfe von AWS WAF
- Erstellen Sie eine lose gekoppelte Architektur mit Microservices mithilfe von DevOps Praktiken und AWS Cloud9
- Erstellen Sie mithilfe von AWS Amplify eine serverlose mobile React Native-App
- Erstellen und testen Sie iOS-Apps mit AWS CodeCommit CodePipeline, AWS und AWS Device Farm
- Konfigurieren Sie die Protokollierung für .NET-Anwendungen in Amazon CloudWatch Logs mithilfe von NLog
- Erstellen Sie eine Pipeline und ein AMI mit CodePipeline und HashiCorp Packer
- Erstellen Sie eine Pipeline und stellen Sie Artefaktaktualisierungen für lokale Instanzen EC2 bereit mit CodePipeline
- Erstellen Sie eine Amazon ECS-Aufgabendefinition und mounten Sie mithilfe von Amazon EFS ein Dateisystem auf EC2 Instances
- Stellen Sie eine GRPC-basierte Anwendung auf einem Amazon EKS-Cluster bereit und greifen Sie mit einem Application Load Balancer darauf zu
- Stellen Sie eine ChatOps Lösung zur Verwaltung von SAST-Scanergebnissen bereit, indem Sie Amazon Q Developer in Chat-Anwendungen verwenden, benutzerdefinierte Aktionen und AWS CloudFormation
- Stellen Sie CloudWatch Synthetics Canaries mithilfe von Terraform bereit
- Bereitstellen von Java-Microservices auf Amazon ECS mithilfe von AWS Fargate
- Stellen Sie mithilfe AWS von Terraform und Amazon Bedrock einen RAG-Anwendungsfall bereit

- Bereitstellen von Ressourcen in einer AWS Wavelength Zone mithilfe von Terraform
- Implementieren Sie eine pfadbasierte API-Versionierung mithilfe benutzerdefinierter Domains in Amazon API Gateway
- Migrieren Sie eine Messaging-Warteschlange von Microsoft Azure Service Bus zu Amazon SQS
- Migrieren Sie eine.NET-Anwendung von Microsoft Azure App Service zu AWS Elastic Beanstalk
- Migrieren Sie eine lokale Go-Webanwendung mithilfe der binären Methode zu AWS Elastic Beanstalk
- Migrieren Sie einen lokalen SFTP-Server zur Verwendung von AWSAWS Transfer for SFTP
- Migrieren Sie von IBM WebSphere Application Server zu Apache Tomcat auf Amazon EC2
- Migrieren Sie EC2 mit Auto Scaling von IBM WebSphere Application Server zu Apache Tomcat auf Amazon
- Migrieren Sie von Oracle GlassFish zu AWS Elastic Beanstalk
- Migrieren Sie lokale Java-Anwendungen mit AWS App2Container zu AWS
- Migrieren Sie OpenText TeamSite Workloads in die AWS-Cloud
- Migrieren Sie Windows-SSL-Zertifikate mithilfe von ACM zu einem Application Load Balancer
- Modernisieren Sie ASP.NET Web Forms-Anwendungen auf AWS
- Überwachen Sie die Anwendungsaktivität mithilfe von CloudWatch Logs Insights
- Führen Sie einen ASP.NET Core-Web-API-Docker-Container auf einer Amazon EC2 Linux-Instance aus
- Statische Inhalte in einem Amazon S3 S3-Bucket über eine VPC mithilfe von Amazon bereitstellen CloudFront
- Richten Sie eine hochverfügbare PeopleSoft Architektur auf AWS ein
- Optimieren Sie die Entwicklung und Bereitstellung von Amazon Lex Lex-Bot mithilfe eines automatisierten Workflows
- Problembehebung bei Zuständen AWS Step Functions mithilfe von Amazon Bedrock
- Verwenden Sie die Network Firewall, um die DNS-Domänennamen aus der Servernamenanzeige für ausgehenden Datenverkehr zu erfassen
- Visualisieren Sie KI/ML-Modellergebnisse mit Flask und AWS Elastic Beanstalk

IoT

Themen

- Konfigurieren Sie die Protokollierung und Überwachung von Sicherheitsereignissen in Ihrer AWS IoT Umgebung
- Extrahieren und Abfragen von AWS IoT SiteWise Metadatenattributen in einem Data Lake
- Einrichtung und Fehlerbehebung von AWS IoT Greengrass mit Client-Geräten
- Mehr Muster

Konfigurieren Sie die Protokollierung und Überwachung von Sicherheitsereignissen in Ihrer AWS IoT Umgebung

Erstellt von Prateek Prakash (AWS)

Übersicht

Sicherzustellen, dass Ihre Internet of Things (IoT) -Umgebungen sicher sind, ist eine wichtige Priorität, vor allem, weil Unternehmen Milliarden von Geräten mit ihren IT-Umgebungen verbinden. Dieses Muster bietet eine Referenzarchitektur, mit der Sie die Protokollierung und Überwachung von Sicherheitsereignissen in Ihrer IoT-Umgebung auf dem implementieren können AWS Cloud. In der Regel besteht eine IoT-Umgebung auf der AWS Cloud aus den folgenden drei Ebenen:

- IoT-Geräte, die relevante Telemetriedaten generieren.
- AWS IoT Dienste (z. B., AWS IoT CoreAWS IoT Device Management, oder AWS IoT Device Defender), die Ihre IoT-Geräte mit anderen Geräten verbinden und AWS-Services.
- Backend AWS-Services , das bei der Verarbeitung von Telemetriedaten hilft und nützliche Einblicke für Ihre verschiedenen geschäftlichen Anwendungsfälle bietet.

Die im Whitepaper AWS IoT Lens — AWS Well-Architected Framework bereitgestellten bewährten Methoden können Ihnen helfen, Ihre Cloud-basierte Architektur zu überprüfen und zu verbessern und die geschäftlichen Auswirkungen Ihrer Designentscheidungen besser zu verstehen. Eine wichtige Empfehlung ist, dass Sie Anwendungsprotokolle und Metriken auf Ihren Geräten und in der analysieren. AWS Cloud Sie können dies erreichen, indem Sie verschiedene Ansätze und Techniken (z. B. Bedrohungsmodellierung) nutzen, um Metriken und Ereignisse zu identifizieren, die überwacht werden müssen, um potenzielle Sicherheitsprobleme zu erkennen.

Dieses Muster beschreibt, wie Sicherheitsdienste verwendet AWS IoT werden, um eine Referenzarchitektur für Sicherheitsprotokollierung und Überwachung für eine IoT-Umgebung auf dem zu entwerfen und zu implementieren AWS Cloud. Diese Architektur baut auf bestehenden bewährten AWS Sicherheitsmethoden auf und wendet sie auf Ihre IoT-Umgebung an.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine bestehende Landezonenumgebung. Weitere Informationen dazu finden Sie im Leitfaden Einrichtung einer sicheren und skalierbaren AWS Umgebung mit mehreren Konten auf der AWS Prescriptive Guidance-Website.
- Die folgenden Konten müssen in Ihrer landing zone verfügbar sein:
  - Log-Archive-Konto — Dieses Konto ist für Benutzer vorgesehen, die auf die Protokollinformationen für Konten in den Organisationseinheiten Ihrer Landing Zone zugreifen müssen (OUs). Weitere Informationen dazu finden Sie im Abschnitt Security OU — Log Archive account im Leitfaden AWS Security Reference Architecture auf der AWS Prescriptive Guidance-Website.
  - Sicherheitskonto — Ihre Sicherheits- und Compliance-Teams verwenden dieses Konto für Audits oder zur Durchführung von Sicherheitsmaßnahmen im Notfall. Dieses Konto wird auch als Administratorkonto für Amazon bezeichnet GuardDuty. Benutzer des Administratorkontos können neben der Anzeige und Verwaltung der GuardDuty Ergebnisse auch Einstellungen GuardDuty für ihr eigenes Konto und alle Mitgliedskonten vornehmen. Weitere Informationen dazu finden Sie GuardDutyin der GuardDuty Dokumentation unter Mehrere Konten verwalten.
  - IoT-Konto — Dieses Konto ist für Ihre IoT-Umgebung.

Architektur

Dieses Muster erweitert die Centralized Logging-Lösung aus der AWS Solutions Library um die Erfassung und Verarbeitung sicherheitsrelevanter IoT-Ereignisse. Die zentralisierte Protokollierungslösung wird im Sicherheitskonto bereitgestellt und hilft beim Sammeln, Analysieren und Anzeigen von CloudWatch Amazon-Protokollen in einem einzigen Dashboard. Diese Lösung konsolidiert, verwaltet und analysiert Protokolldateien aus mehreren Quellen. Schließlich verwendet die Centralized Logging-Lösung auch Amazon OpenSearch Service und OpenSearch Dashboards, um eine einheitliche Ansicht aller Protokollereignisse anzuzeigen.

Das folgende Architekturdiagramm zeigt die wichtigsten Komponenten einer IoT-Sicherheitsprotokollierung und Referenzarchitektur auf dem AWS Cloud.

Das Diagramm zeigt den folgenden Workflow:

1. IoT-Geräte sind Geräte, die auf ungewöhnliche Sicherheitsereignisse überwacht werden müssen. Auf diesen Geräten wird ein Agent ausgeführt, der Sicherheitsereignisse oder Metriken für AWS IoT Core und veröffentlicht. AWS IoT Device Defender

2. Wenn die AWS IoT Protokollierung aktiviert ist, werden Fortschrittsereignisse zu jeder Nachricht AWS IoT gesendet, während sie von Ihren Geräten über den Message Broker und die Regel-Engine an Amazon CloudWatch Logs weitergeleitet wird. Sie können CloudWatch Logs-Abonnements verwenden, um Ereignisse an eine zentralisierte Protokollierungslösung zu übertragen. Weitere Informationen dazu finden Sie in der AWS IoT Core Dokumentation unter AWS IoT Metriken und Dimensionen.
3. AWS IoT Device Defender hilft bei der Überwachung unsicherer Konfigurationen und Sicherheitsmetriken für Ihre IoT-Geräte. Wenn eine Anomalie erkannt wird, benachrichtigen Alarme den Amazon Simple Notification Service (Amazon SNS), der eine AWS Lambda Funktion als Abonnent hat. Die Lambda-Funktion sendet den Alarm als Nachricht an CloudWatch Logs. Sie können CloudWatch Logs-Abonnements verwenden, um Ereignisse an Ihre zentralisierte Logging-Lösung zu übertragen. Weitere Informationen dazu finden Sie in der Dokumentation unter Prüfprüfungen, Geräteseitige CloudWatch Protokolle hochladen und AWS IoT Protokollierung konfigurieren. AWS IoT Core
4. AWS CloudTrail protokolliert Aktionen auf der AWS IoT Core Kontrollebene, durch die Änderungen vorgenommen werden (z. B. das Erstellen, Aktualisieren oder Anhängen APIs). Wenn CloudTrail es als Teil einer landing zone Zone-Implementierung eingerichtet wird, sendet es Ereignisse an CloudWatch Logs. Sie können Abonnements verwenden, um Ereignisse an Ihre zentralisierte Logging-Lösung weiterzuleiten.
5. AWS Config verwaltete Regeln oder benutzerdefinierte Regeln bewerten Ressourcen, die Teil Ihrer IoT-Umgebung sind. Überwachen Sie Ihre Benachrichtigungen über Compliance-Änderungen, indem Sie CloudWatch Ereignisse mit CloudWatch Protokollen als Ziel verwenden. Nachdem Benachrichtigungen über Konformitätsänderungen an CloudWatch Logs gesendet wurden, können Sie mithilfe von Abonnements Ereignisse an Ihre zentralisierte Protokollierungslösung weiterleiten.
6. Amazon analysiert GuardDuty kontinuierlich CloudTrail Verwaltungsereignisse und hilft dabei, API-Aufrufe zu identifizieren, die von bekannten bösartigen IP-Adressen, ungewöhnlichen Geolokationen oder anonymisierenden Proxys an AWS IoT Core Endpunkte getätigt werden. Überwachen Sie GuardDuty Benachrichtigungen mithilfe von CloudWatch Ereignissen mit Protokollgruppen in Protokollen als Ziel. CloudWatch Wenn GuardDuty Benachrichtigungen an CloudWatch Logs gesendet werden, können Sie Abonnements verwenden, um Ereignisse an Ihre zentrale Überwachungslösung weiterzuleiten, oder die GuardDuty Konsole in Ihrem Sicherheitskonto verwenden, um die Benachrichtigungen anzuzeigen.
7. AWS Security Hub überwacht Ihr IoT-Konto mithilfe bewährter Sicherheitsmethoden. Überwachen Sie Security Hub Hub-Benachrichtigungen, indem Sie CloudWatch Ereignisse

mit Protokollgruppen in CloudWatch Logs als Ziel verwenden. Wenn Security Hub Hub-Benachrichtigungen an CloudWatch Logs gesendet werden, verwenden Sie Abonnements, um Ereignisse an Ihre Centralized Monitoring-Lösung zu übertragen, oder verwenden Sie die Security Hub Hub-Konsole in Ihrem Security-Konto, um sich die Benachrichtigungen anzusehen.

8. Amazon Detective bewertet und analysiert Informationen, um die Grundursache zu ermitteln und bei Sicherheitsergebnissen für ungewöhnliche Anrufe an AWS IoT Endpunkte oder andere Dienste in Ihrer IoT-Architektur Maßnahmen zu ergreifen.
9. Amazon Athena fragt die in Ihrem Log Archive-Konto gespeicherten Protokolle ab, um Ihr Verständnis von Sicherheitsergebnissen zu verbessern und Trends und böswillige Aktivitäten zu identifizieren.

Tools

- Amazon Athena ist ein interaktiver Abfrageservice, der es einfach macht, Daten direkt in Amazon Simple Storage Service (Amazon S3) mithilfe von Standard-SQL zu analysieren.
- AWS CloudTrailhilft Ihnen dabei, die Unternehmensführung, die Einhaltung der Vorschriften sowie die Betriebs- und Risikoprüfung Ihres AWS-Konto Unternehmens zu ermöglichen.
- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Sie können CloudWatch damit Metriken sammeln und verfolgen. Dabei handelt es sich um Variablen, die Sie für Ihre Ressourcen und Anwendungen messen können.
- Amazon CloudWatch Logs zentralisiert die Protokolle all Ihrer Systeme und Anwendungen, AWS-Services die Sie verwenden. Sie können die Protokolle anzeigen und überwachen, sie nach bestimmten Fehlercodes oder Mustern durchsuchen, sie nach bestimmten Feldern filtern oder sie für future Analysen sicher archivieren.
- AWS Configbietet einen detaillierten Überblick über die Konfiguration der AWS Ressourcen in Ihrem AWS-Konto.
- Amazon Detective macht es einfach, Sicherheitslücken oder verdächtige Aktivitäten zu analysieren, zu untersuchen und schnell die Ursache zu identifizieren.
- AWS Glueist ein vollständig verwalteter ETL-Service (Extrahieren, Transformieren und Laden), mit dem Sie Ihre Daten einfach und kostengünstig kategorisieren, bereinigen, anreichern und zuverlässig zwischen verschiedenen Datenspeichern und Datenströmen verschieben können.
- Amazon GuardDuty ist ein Dienst zur kontinuierlichen Sicherheitsüberwachung.

- AWS IoT Corebietet sichere, bidirektionale Kommunikation für mit dem Internet verbundene Geräte (wie Sensoren, Aktuatoren, eingebettete Geräte, drahtlose Geräte und intelligente Geräte), um sich AWS Cloud über MQTT, HTTPS und WAN mit dem Internet zu verbinden. LoRa
- AWS IoT Device Defender ist ein Sicherheitsservice, der es Ihnen ermöglicht, die Konfiguration Ihrer Geräte zu prüfen, verbundene Geräte zu überwachen, um anormales Verhalten zu erkennen, und Sicherheitsrisiken zu minimieren.
- Amazon OpenSearch Service ist ein verwalteter Service, der die Bereitstellung, den Betrieb und die Skalierung von OpenSearch Clustern in der erleichtert AWS Cloud.
- AWS Organizationsist ein Kontoverwaltungsservice, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie selbst erstellen und zentral verwalten.
- AWS Security Hubbietet einen umfassenden Überblick über Ihren Sicherheitsstatus AWS und hilft Ihnen dabei, Ihre Umgebung anhand von Industriestandards und Best Practices zu überprüfen.
- Amazon Virtual Private Cloud (Amazon VPC) bietet einen logisch isolierten Bereich, in AWS Cloud dem Sie AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können. Dieses virtuelle Netzwerk entspricht weitgehend einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben, kann jedoch die Vorzüge der skalierbaren Infrastruktur von AWS nutzen.

Epen

Richten Sie ein IoT-Konto in Ihrer landing zone Zone-Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Sicherhei tsleitplanken im IoT-Konto.	Stellen Sie sicher, dass die Guardrails für CloudTrail AWS Config, GuardDuty, und Security Hub in Ihrem IoT-Konto aktiviert sind.	AWS-Administrator
Stellen Sie sicher, dass Ihr IoT-Konto als Mitgliedskonto Ihres Sicherheitskontos konfiguriert ist.	Vergewissern Sie sich, dass Ihr IoT-Konto in Ihrem Security-Konto als Mitglieds konto für GuardDuty und Security Hub konfiguriert und verknüpft ist.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen dazu finden Sie AWS Organizations in der GuardDuty Dokumentation unter GuardDuty Konten verwalten mit und Administrator- und Mitgliedskonten verwalten in der Security Hub Hub-Dokumentation.	
Validieren Sie die Protokollarchivierung.	Stellen Sie sicher CloudTrail, dass AWS Config, und VPC Flow Logs im Log Archive-Konto gespeichert sind.	AWS-Administrator

Richten Sie die zentralisierte Protokollierungslösung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Lösung für die zentralisierte Protokollierung in Ihrem Sicherheitskonto ein.	Melden Sie sich mit dem AWS Management Console for your Security-Konto an und richten Sie die zentralisierte Protokollierungslösung aus der AWS Lösungsbibliothek ein, um CloudWatch Protokolle in Amazon OpenSearch Service und OpenSearch Dashboards zu sammeln, zu analysieren und anzuzeigen. Weitere Informationen dazu finden Sie unter Sammeln, Analysieren und Anzeigen von CloudWatch Amazon-Logs in einem einzigen Dashboard	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	mit der Centralized Logging-Lösung aus dem Implement ierungsleitfaden für Centraliz ed Logging in der AWS Lösungsbibliothek.	

AWS Ressourcen in Ihrem IoT-Konto einrichten und konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die AWS IoT Protokollierung ein.	Melden Sie sich AWS Management Console für Ihr IoT-Konto an. Richten Sie es ein und konfigurieren Sie AWS IoT Core es, um Protokolle an CloudWatch Logs zu senden. Weitere Informationen dazu finden Sie in der AWS IoT Core Dokumentation unter AWS IoT Protokollierung konfigurieren und AWS IoT mithilfe von CloudWatch Protokollen überwachen.	AWS-Administrator
Einrichten AWS IoT Device Defender.	Richten Sie ein AWS IoT Device Defender , um Ihre IoT-Ressourcen zu prüfen und Anomalien zu erkennen. Weitere Informationen dazu finden Sie AWS IoT Device Defender in der Dokumenta tion unter Erste Schritte mit. AWS IoT Core	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Einrichten CloudTrail.	CloudTrail So einrichten, dass Ereignisse an CloudWatch Logs gesendet werden. Weitere Informationen dazu finden Sie in der CloudTrail Dokumentation unter Ereignisse an CloudWatch Protokolle senden.	AWS-Administrator
Einrichtung AWS Config und AWS Config Regeln.	Einrichtung AWS Config und die erforderlichen AWS Config Regeln. Weitere Informationen dazu finden Sie in der AWS Config Dokumentation unter Einrichtung AWS Config mit der Konsole und Hinzufügen von AWS Config Regeln.	AWS-Administrator
Einrichten GuardDuty.	Richten Sie ein und konfigurieren Sie GuardDuty es, um Ergebnisse an Amazon CloudWatch Events mit Protokollgruppen in CloudWatch Logs als Ziel zu senden. Weitere Informationen dazu finden Sie in der GuardDuty Dokumentation unter Erstellen von benutzerdefinierten Antworten auf GuardDuty Ergebnisse mit Amazon CloudWatch Events.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Security Hub ein.	Richten Sie Security Hub ein und aktivieren Sie die Standards CIS AWS Foundations Benchmark und AWS Foundational Security Best Practices. Weitere Informationen dazu finden Sie unter Automatisierte Reaktion und Problembehebung in der Security Hub Hub-Dokumentation.	AWS-Administrator
Richten Sie Amazon Detective ein.	Richten Sie Detective ein, um die Analyse von Sicherheitsergebnissen zu erleichtern. Weitere Informationen dazu finden Sie unter Erste Schritte mit Amazon Detective in der Amazon Detective-Dokumentation.	AWS-Administrator
Richten Sie Amazon Athena ein und AWS Glue.	Richten Sie Athena ein und fragen AWS Glue Sie die AWS-Service Protokolle ab, die zur Untersuchung von Sicherheitsvorfällen dienen. Weitere Informationen dazu finden Sie unter Abfragen von AWS-Service Protokollen in der Amazon Athena Athena-Dokumentation.	AWS-Administrator

Zugehörige Ressourcen

- Was ist eine landing zone?

Extrahieren und Abfragen von AWS IoT SiteWise Metadatenattributen in einem Data Lake

Erstellt von Ambarish Dongaonkar (AWS)

Übersicht

AWS IoT SiteWise verwendet Anlagenmodelle und Hierarchien, um Ihre Industrieanlagen, Prozesse und Anlagen darzustellen. Jedes Modell oder Asset kann mehrere Attribute haben, die für Ihre Umgebung spezifisch sind. Zu den Metadatenattributen gehören beispielsweise der Standort oder der physische Standort der Anlage, Anlagendetails und Gerätekennungen. Diese Attributwerte ergänzen die Messdaten der Anlagen, um den Geschäftswert zu maximieren. Maschinelles Lernen (ML) kann zusätzliche Einblicke in diese Metadaten liefern und technische Aufgaben rationalisieren.

Metadatenattribute können jedoch nicht direkt vom Service abgefragt werden. AWS IoT SiteWise Um die Attribute abfragbar zu machen, müssen Sie sie extrahieren und in einen Data Lake aufnehmen. Dieses Muster verwendet ein Python-Skript, um die Attribute für alle AWS IoT SiteWise Assets zu extrahieren und sie in einen Data Lake in einem Amazon Simple Storage Service (Amazon S3) -Bucket aufzunehmen. Wenn Sie diesen Vorgang abgeschlossen haben, können Sie SQL-Abfragen in Amazon Athena verwenden, um auf die AWS IoT SiteWise Metadatenattribute und andere Datensätze, z. B. Messdatensätze, zuzugreifen. Die Informationen zu den Metadatenattributen sind auch nützlich, wenn Sie mit AWS IoT SiteWise Monitoren oder Dashboards arbeiten. Sie können auch ein QuickSight Amazon-Dashboard erstellen, indem Sie die extrahierten Attribute im Amazon S3-Bucket verwenden.

Das Muster hat einen Referenzcode, und Sie können den Code implementieren, indem Sie die für Ihren Anwendungsfall am besten geeigneten Rechendienste wie AWS Lambda oder verwenden AWS Glue.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto.
- Berechtigungen zum Einrichten von AWS Lambda Funktionen oder AWS Glue Jobs.
- Ein Amazon-S3-Bucket
- Die Asset-Modelle und Hierarchien sind in AWS IoT SiteWise eingerichtet. Weitere Informationen finden Sie in der AWS IoT SiteWise Dokumentation unter Asset-Modelle erstellen.

Architektur

Sie können eine Lambda-Funktion oder einen AWS Glue Job verwenden, um diesen Vorgang abzuschließen. Wir empfehlen die Verwendung von Lambda, wenn Sie weniger als 100 Modelle haben und jedes Modell durchschnittlich 15 oder weniger Attribute hat. Für alle anderen Anwendungsfälle empfehlen wir die Verwendung von AWS Glue.

Die Lösungsarchitektur und der Arbeitsablauf sind in der folgenden Abbildung dargestellt.

1. Der geplante AWS Glue Job oder die Lambda-Funktion wird ausgeführt. Es extrahiert die Asset-Metadatenattribute aus einem Amazon S3-Bucket AWS IoT SiteWise und nimmt sie in einen Amazon S3 S3-Bucket auf.
2. Ein AWS Glue Crawler crawlt die extrahierten Daten im Amazon S3 S3-Bucket und erstellt Tabellen in einem. AWS Glue Data Catalog
3. Mithilfe von Standard-SQL fragt Amazon Athena die Tabellen in der AWS Glue Data Catalog ab.

Automatisierung und Skalierung

Sie können die Lambda-Funktion oder den AWS Glue Lambda-Job so planen, dass sie täglich oder wöchentlich ausgeführt wird, je nach Aktualisierungshäufigkeit Ihrer AWS IoT SiteWise Asset-Konfigurationen.

Die Anzahl der AWS IoT SiteWise Assets, die der Beispielcode verarbeiten kann, ist unbegrenzt, aber eine große Anzahl von Assets kann den Zeitaufwand für den Abschluss des Prozesses erhöhen.

Tools

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon S3 analysieren können.
- AWS Glueist ein vollständig verwalteter ETL-Service (Extrahieren, Transformieren und Laden). Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.

- AWS IoT SiteWisehilft Ihnen dabei, Daten von Industrieanlagen in großem Maßstab zu sammeln, zu modellieren, zu analysieren und zu visualisieren.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS SDK für Python (Boto3)ist ein Softwareentwicklungskit, mit dem Sie Ihre Python-Anwendung, -Bibliothek oder Ihr Skript integrieren können AWS-Services.

Epen

Richten Sie den Job oder die Funktion ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Berechtigungen in IAM.	Erteilen Sie in der IAM-Konsole der IAM-Rolle, die von der Lambda-Funktion oder dem AWS Glue Lambda-Job angenommen wurde, die folgenden Berechtigungen: • Aus dem Service lesen AWS IoT SiteWise • Schreiben Sie in den Amazon S3 S3-Bucket Weitere Informationen finden Sie in der IAM-Dokumentation unter Eine AWS-Service Rolle für eine erstellen.	Allgemeines AWS
Erstellen Sie die Lambda-Funktion oder den AWS Glue Lambda-Job.	Wenn Sie Lambda verwenden, erstellen Sie eine neue Lambda-Funktion. Wählen Sie	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	für Runtime Python. Weitere Informationen finden Sie unter Erstellen von Lambda-Funktionen mit Python in der Lambda-Dokumentation. Wenn Sie verwenden AWS Glue, erstellen Sie einen neuen Python-Shell-Job in der AWS Glue Konsole. Weitere Informationen finden Sie in der AWS Glue Dokumentation unter Hinzufügen von Python-Shell-Jobs.	
Aktualisieren Sie die Lambda-Funktion oder den AWS Glue Lambda-Job.	Ändern Sie die neue Lambda-Funktion oder den neuen AWS Glue Lambda-Job und geben Sie das Codebeispiel in den Abschnitt Zusätzliche Informationen ein. Ändern Sie den Code nach Bedarf für Ihren Anwendungsfall. Weitere Informationen finden Sie in der Lambda-Dokumentation unter Code mit dem Konsolen-Editor bearbeiten und in der Dokumentation unter Arbeiten mit Skripts.AWS Glue	Allgemeines AWS

Führen Sie den Job oder die Funktion aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Lambda-Funktion oder den AWS Glue Lambda-Job aus.	Führen Sie die Lambda-Funktion oder den AWS Glue Lambda-Job aus. Weitere Informationen finden Sie in der Lambda-Dokumentation unter Aufrufen der Lambda-Funktion oder in der Dokumentation unter Jobs mithilfe von Triggern starten. AWS Glue Dadurch werden die Metadatenattribute für die Assets und Modelle in der AWS IoT SiteWise Hierarchie extrahiert und im angegebenen Amazon S3 S3-Bucket gespeichert.	Allgemeines AWS
Richten Sie einen AWS Glue Crawler ein.	Richten Sie einen AWS Glue Crawler mit dem erforderlichen Formatklassifizierer für eine CSV-formatierte Datei ein. Verwenden Sie den Amazon S3 S3-Bucket und die Präfixdetails, die in der Lambda-Funktion oder dem AWS Glue Lambda-Job verwendet werden. Weitere Informationen finden Sie in der Dokumentation unter Definieren von Crawlern. AWS Glue	Allgemeines AWS
Starte den AWS Glue Crawler.	Führen Sie den Crawler aus, um die von der Lambda-	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Funktion oder AWS Glue dem Lambda-Job erstellte Datendatei zu verarbeiten. Der Crawler erstellt eine Tabelle in der angegebenen Datei. AWS Glue Data Catalog Weitere Informationen finden Sie unter oder Crawler mithilfe von Triggern starten in der AWS Glue Dokumentation.	
Fragen Sie die Metadaten attribute ab.	Verwenden Sie Amazon Athena, um Standard-SQL abzufragen, AWS Glue Data Catalog wie es für Ihren Anwendungsfall erforderlich ist. Sie können die Metadaten -Attributtabelle mit anderen Datenbanken und Tabellen verknüpfen. Weitere Informationen finden Sie unter Erste Schritte in der Amazon Athena Athena-Dokumentation.	Allgemeines AWS

Zugehörige Ressourcen

- Amazon Athena Athena-Dokumentation
- AWS Glue Dokumentation
- AWS IoT SiteWise API-Referenz
- AWS IoT SiteWise benutzerhandbuch
  - Erste Schritte
  - Modellierung von Industrieanlagen
  - Definition von Beziehungen zwischen Anlagenmodellen (Hierarchien)

  - Vermögenswerte zuordnen und deren Zuordnung aufheben
  - Die Demo wird erstellt AWS IoT SiteWise
- IOTSiteWise (SDK für Python-Dokumentation)
- Lambda-Dokumentation

Zusätzliche Informationen

Code

Der bereitgestellte Beispielcode dient als Referenz, und Sie können diesen Code nach Bedarf für Ihren Anwendungsfall anpassen.

```
# Following code can be used in an AWS Lambda function or in an AWS Glue Python shell
 job.
# IAM roles used for this job need read access to the AWS IoT SiteWise service and
 write access to the S3 bucket.
sw_client = boto3.client('iotsitewise')
s3_client = boto3.client('s3')
output = io.StringIO()

attribute_list=[]
bucket = '{3_bucket name}'
prefix = '{s3_bucket prefix}'
output.write("model_id,model_name,asset_id,asset_name,attribuet_id,attribute_name,attribute_val
\n")

m_resp = sw_client.list_asset_models()
for m_rec in m_resp['assetModelSummaries']:
     model_id = m_rec['id']
     model_name = m_rec['name']

     attribute_list.clear()
     dam_response = sw_client.describe_asset_model(assetModelId=model_id)
     for rec in dam_response['assetModelProperties']:
         if 'attribute' in rec['type']:
            attribute_list.append(rec['name'])

     response = sw_client.list_assets(assetModelId=model_id, filter='ALL')
     for asset in response['assetSummaries']:
         asset_id = asset['id']
         asset_name = asset['name']
```

```
        resp = sw_client.describe_asset(assetId=asset_id)
        for rec in resp['assetProperties']:
           if rec['name'] in attribute_list:
               p_resp = sw_client.get_asset_property_value(assetId=asset_id,
 propertyId=rec['id'])
               if 'propertyValue' in p_resp:
                   if p_resp['propertyValue']['value']:
                       if 'stringValue' in p_resp['propertyValue']['value']:
                            output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['stringValue']) + "\n")

                       if 'doubleValue' in p_resp['propertyValue']['value']:
                            output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['doubleValue']) + "\n")
                       if 'integerValue' in p_resp['propertyValue']['value']:
                            output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['integerValue']) + "\n")
                        if 'booleanValue' in p_resp['propertyValue']['value']:
                            output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['booleanValue']) + "\n")

output.seek(0)
s3_client.put_object(Bucket=bucket, Key= prefix + '/data.csv', Body=output.getvalue())
output.close()
```

Einrichtung und Fehlerbehebung von AWS IoT Greengrass mit Client-Geräten

Erstellt von Marouane Sefiani und Akalanka De Silva (AWS)

Übersicht

AWS IoT Greengrass ist ein Open-Source-Edge-Laufzeit- und Cloud-Service für die Erstellung, Bereitstellung und Verwaltung von Internet of Things (IoT) -Software auf Edge-Geräten. Zu den Anwendungsfällen für AWS IoT Greengrass gehören:

- Intelligente Häuser, in denen ein AWS IoT Greengrass-Gateway als Hub für die Hausautomation verwendet wird
- Intelligente Fabriken, in denen AWS IoT Greengrass die Erfassung und lokale Verarbeitung von Daten aus der Fertigung erleichtern kann

AWS IoT Greengrass kann als sicherer, authentifizierter MQTT-Verbindungsendpunkt für andere Edge-Geräte (auch als Client-Geräte bezeichnet) fungieren, die andernfalls normalerweise eine direkte Verbindung zu AWS IoT Core herstellen würden. Diese Funktion ist nützlich, wenn Client-Geräte keinen direkten Netzwerkzugriff auf den AWS IoT Core Core-Endpunkt haben.

Sie können AWS IoT Greengrass für die Verwendung mit Client-Geräten für die folgenden Anwendungsfälle einrichten:

- Für Client-Geräte, um Daten an AWS IoT Greengrass zu senden
- Für AWS IoT Greengrass zur Weiterleitung von Daten an AWS IoT Core
- Um die Vorteile der erweiterten Funktionen der AWS IoT Core Rules Engine zu nutzen

Diese Funktionen erfordern die Installation und Konfiguration der folgenden Komponenten auf dem AWS IoT Greengrass-Gerät:

- MQTT-Broker
- MQTT-Brücke
- Authentifizierung von Client-Geräten
- IP-Detektor

Darüber hinaus müssen veröffentlichte Nachrichten von Client-Geräten im JSON-Format oder im Protocol Buffer-Format (Protobuf) vorliegen.

Dieses Muster beschreibt, wie diese erforderlichen Komponenten installiert und konfiguriert werden, und bietet Tipps und bewährte Methoden zur Fehlerbehebung.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 2
- Zwei Client-Geräte, auf denen Python 3.7 oder höher ausgeführt wird
- Ein Core-Gerät mit Java Runtime Environment (JRE) Version 8 oder höher und Amazon Corretto 11 oder OpenJDK 11

Einschränkungen

- Sie müssen eine AWS-Region wählen, in der AWS IoT Core verfügbar ist. Die aktuelle Liste der Regionen für AWS IoT Core finden Sie unter AWS-Services nach Regionen.
- Das Kerngerät muss über mindestens 172 MB RAM und 512 MB Festplattenspeicher verfügen.

Architektur

Das folgende Diagramm zeigt die Lösungsarchitektur für dieses Muster.

Die Architektur umfasst:

- Zwei Client-Geräte. Jedes Gerät enthält einen privaten Schlüssel, ein Gerätezertifikat und ein Zertifikat der Stammzertifizierungsstelle (CA). Das AWS IoT Device SDK, das einen MQTT-Client enthält, ist ebenfalls auf jedem Client-Gerät installiert.
- Ein Kerngerät, auf dem AWS IoT Greengrass mit den folgenden Komponenten bereitgestellt wird:
  - MQTT-Broker
  - MQTT-Brücke
  - Authentifizierung von Client-Geräten

- IP-Detektor

Diese Architektur unterstützt die folgenden Szenarien:

- Client-Geräte können ihren MQTT-Client verwenden, um über den MQTT-Broker des Kerngeräts miteinander zu kommunizieren.
- Client-Geräte können auch mit AWS IoT Core in der Cloud über den MQTT-Broker des Kerngeräts und die MQTT-Bridge kommunizieren.
- AWS IoT Core in der Cloud kann über den MQTT-Testclient und die MQTT-Bridge und den MQTT-Broker des Kerngeräts Nachrichten an Client-Geräte senden.

Weitere Informationen zur Kommunikation zwischen Client-Geräten und dem Core-Gerät finden Sie im Abschnitt Zusätzliche Informationen.

Tools

AWS-Services

- AWS IoT Greengrass ist ein Open-Source-Edge-Runtime- und Cloud-Service für das Internet der Dinge (IoT), mit dem Sie IoT-Anwendungen auf Ihren Geräten erstellen, bereitstellen und verwalten können.
- AWS IoT Core bietet sichere, bidirektionale Kommunikation für mit dem Internet verbundene Geräte, um eine Verbindung zur AWS-Cloud herzustellen.
- Das AWS IoT Device SDK ist ein Software-Entwicklungskit, das Open-Source-Bibliotheken, Entwicklerhandbücher mit Beispielen und Portierungsleitfäden enthält, sodass Sie innovative IoT-Produkte oder -Lösungen auf den Hardwareplattformen Ihrer Wahl entwickeln können.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.

Bewährte Methoden

- Die Nutzdaten der Nachrichten von Client-Geräten sollten entweder im JSON- oder Protobuf-Format vorliegen, um die erweiterten Funktionen der AWS IoT Core Rules Engine, wie Transformation und bedingte Aktionen, nutzen zu können.

- Konfigurieren Sie die MQTT-Bridge so, dass sie eine bidirektionale Kommunikation ermöglicht.
- Konfigurieren und implementieren Sie die IP-Detektorkomponente in AWS IoT Greengrass, um sicherzustellen, dass die IP-Adressen des Kerngeräts im Feld Subject Alternative Name (SAN) des MQTT-Brokerzertifikats enthalten sind.

Epen

Richten Sie das Kerngerät ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie AWS IoT Greengrass auf Ihrem Kerngerät ein.	Installieren Sie die AWS IoT Greengrass Core-Software, indem Sie den Anweisungen im Entwicklerhandbuch folgen.	AWS IoT Greengrass

Überprüfen Sie den Status Ihrer Installation.	Verwenden Sie den folgenden Befehl, um den Status des AWS IoT Greengrass-Service auf Ihrem Kerngerät zu überprüfen:
	`sudo systemctl status greengrass.service`
	Die erwartete Ausgabe des Befehls lautet:
	`Launched Nucleus successfully`
		Allgemeines AWS

Richten Sie eine IAM-Richtlinie ein und fügen Sie sie der Greengrass-Servicerolle hinzu.	1. Erstellen Sie eine IAM-Richtlinie, um die Kommunikation zur und von der MQTT-Bridge zu ermöglichen. Hier ist ein Beispiel für eine Richtlinie:	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>{
	    "Version":
	"2012-10-17",
	    "Statement": [
	
	        {
	            "Effect":
	"Allow",
	            "Action":
	[
	
	"iot:*"
	            ],
	            "Resource
	": "*"
	        },
	        {
	            "Sid":
	"GreengrassActions
	",
	            "Effect":
	"Allow",
	            "Action":
	[
	
	"greengrass:*"
	            ],
	            "Resource
	": "*"
	        }
	    ]
	}</pre> 2. Ordnen Sie die Richtlinie der Greengrass-Service rolle zu. Verwenden Sie den folgenden Befehl, um die Servicerolle abzurufen:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws greengrassv2 get-service-role-for-account --region <region>` wo `<region>` bezieht sich auf Ihre AWS-Region.	
Konfigurieren und implementieren Sie die erforderlichen Komponenten auf dem AWS IoT Greengrass-Kerngerät.	Konfigurieren und implementieren Sie die folgenden Komponenten: • `greengrass.clientdevices.mqtt.Moquette` (siehe Konfigurationsdetails) • `greengrass.clientdevices.mqtt.Bridge` (siehe Konfigurationsdetails und die nächste Aufgabe) • `greengrass.clientdevices.Auth` (siehe Konfigurationsdetails und die Aufgabe nach der nächsten) • `aws.greengrass.clientdevices.IPDetector` (siehe Konfigurationsdetails)	AWS IoT Greengrass

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vergewissern Sie sich, dass die MQTT-Bridge eine bidirektionale Kommunikation ermöglicht.	Um MQTT-Nachrichten zwischen Client-Geräten und AWS IoT Core weiterzuleiten, konfigurieren und implementieren Sie die MQTT-Bridge-Komponente und geben Sie die Themen an, die weitergeleitet werden sollen. Ein Beispiel: `{ "mqttTopicMapping": { "ClientDevicesToCloud": { "topic": "dt/#", "source": "LocalMqtt", "target": "IotCore" }, "CloudToClientDevices": { "topic": "cmd/#", "source": "IotCore", "target": "LocalMqtt" } } }`	AWS IoT Greengrass

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vergewissern Sie sich, dass die Authentifizierungskomponente es Client-Geräten ermöglicht, sich zu verbinden und Themen zu veröffentlichen oder zu abonnieren.	Die folgende `aws.greengrass.clientdevices.Auth` Konfiguration ermöglicht es allen Client-Geräten, eine Verbindung herzustellen, Nachrichten zu veröffentlichen und alle Themen zu abonnieren. `{ "deviceGroups": { "formatVersion": "2021-03-05", "definitions": { "MyPermissiveDeviceGroup": { "selectionRule": "thingName: *", "policyName": "MyPermissivePolicy" } }, "policies": { "MyPermissivePolicy": { "AllowAll": { "statementDescription": "Allow client devices to perform all actions.", "operations": ["*"], "resources": ["*"] }`	AWS IoT Greengrass

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>}
	}
	}
	}</pre>	

Richten Sie Client-Geräte ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie das AWS IoT Device SDK.	Installieren Sie das AWS IoT Device SDK auf Client-Geräten. Eine vollständige Liste der unterstützten Sprachen und der zugehörigen SDKs Sprachen finden Sie in der AWS IoT Core Core-Dokumentation. Das AWS IoT Device SDK für Python SDK befindet sich beispielsweise auf GitHub. Um dieses SDK zu installieren: 1. Vergewissern Sie sich, dass Python 3.7 oder höher installiert ist, wie auf der Seite Voraussetzungen des GitHub Repositorys beschrieben. 2. Verwenden Sie den Befehl pip, um das SDK zu installieren. Für macOS und Linux:	Allgemeines AWS IoT

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`python3 -m pip install awsiotsdk`
	
	Für Windows:
	
	`python -m pip install awsiotsdk`
	
	Alternativ können Sie das SDK aus dem Quell-Repository installieren:
	
	`# Create a workspace directory to hold all the SDK files`
	`mkdir sdk-workspace`
	`cd sdk-workspace`
	`# Clone the repository`
	`git clone https://github.com/aws/aws-iot-device-sdk-python-v2.git`
	`# Install using Pip (use 'python' instead of 'python3' on Windows)`
	`python3 -m pip install ./aws-iot-device-sdk-python-v2`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erschaffe etwas.	1. Wenn in der AWS IoT IoT-Konsole die Schaltfläche Erste Schritte angezeigt wird, wählen Sie sie aus. Andernfalls wählen Sie im Navigationsbereich Sicherheit, Richtlinien aus. 2. Wenn das Dialogfeld Sie haben noch keine Richtlinien angezeigt wird, wählen Sie Richtlinie erstellen aus. Wählen Sie andernfalls Erstellen. 3. Geben Sie einen Namen für die AWS-IoT-Richtlinie ein (z. B. `ClientDevicePolicy`). 4. Ersetzen Sie im Abschnitt Anweisungen hinzufügen die bestehende Richtlinie durch den folgenden JSON-Code. Ersetzen Sie `<region>` und `<account>` durch Ihre AWS-Region und AWS-Kontonummer. `{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": "iot:Connect",`	AWS IoT Core

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"Resource": "arn:aws:iot:region:account:client/*" }, { "Effect": "Allow", "Action": "iot:Publish", "Resource": "*" }, { "Effect": "Allow", "Action": "iot:Receive", "Resource": "*" }, { "Effect": "Allow", "Action": "iot:Subscribe", "Resource": "*" }, { "Effect": "Allow", "Action": ["iot:GetThingShadow", "iot:UpdateThingShadow", "iot:DeleteThingShadow"], "Resource": "arn:aws:iot:region:account:thing/*"	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre> }] }</pre> 5. Wählen Sie Erstellen aus. 6. Wählen Sie auf der AWS IoT IoT-Konsole im Navigationsbereich Manage, Things aus. 7. Wenn das Dialogfeld Sie haben noch nichts angezeigt wird, wählen Sie Etwas registrieren aus. Wählen Sie andernfalls Erstellen. 8. Wählen sie auf der Seite Creating AWS IoT things (AWS IoT-Objekte erstellen) den Eintrag Create a single thing (Einzelnes Objekt erstellen). 9. Geben Sie auf der Seite Add your device to the device registry (Ihr Gerät zur Geräteregistrierung hinzufügen) einen Namen für Ihr IoT-Objekt ein (z. B. `ClientDevice1`) und wählen Sie dann Next (Weiter).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Sie können den Namen eines Objekts nicht mehr ändern, nachdem Sie es erstellt haben. Um den Namen zu ändern, müssen Sie ein neues Ding erstellen, ihm den neuen Namen geben und dann das alte Ding löschen. 10. Wählen Sie auf der Seite Add a certificate for your thing (Fügen Sie ein Zertifikat für Ihr Objekt hinzu.) die Option Create certificate (Zertifikat erstellen). 11. Klicken Sie auf die Download-Links, um das Zertifikat, den privaten Schlüssel und das CA-Stammzertifikat herunterzuladen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Important Dies ist Ihre einzige Möglichkeit, Ihr Zertifikat und Ihren privaten Schlüssel herunterzuladen. 12. Wählen Sie Aktivieren aus, um Ihr Zertifikat zu aktivieren. Das Zertifikat muss aktiv sein, damit ein Gerät eine Verbindung zu AWS IoT herstellen kann. 13. Wählen Sie Attach a policy (Richtlinie anfügen) aus. 14. Wählen Sie unter Richtlinie für Ihr Ding hinzufügen die Option ClientDevicePolicy Ding registrieren aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das CA-Zertifikat vom Greengrass-Core-Gerät herunter.	Wenn Sie erwarten, dass das Greengrass-Core-Gerät in Offline-Umgebungen funktioniert, müssen Sie das Greengrass-Core-CA-Zertifikat für das Client-Gerät verfügbar machen, damit es das Zertifikat des MQTT-Brokers (das von der Greengrass Core CA ausgestellt wurde) verifizieren kann. Daher ist es wichtig, eine Kopie dieses Zertifikats zu erhalten. Verwenden Sie eine der folgenden Methoden, um das CA-Zertifikat herunterzuladen: • Wenn Sie von Ihrem PC aus Netzwerkzugriff auf das AWS IoT Greengrass-Gerät haben, geben Sie es `https://<device IP>:8883` in Ihrem Webbrowser ein und sehen Sie sich das MQTT-Broker-Zertifikat und das CA-Zertifikat an. Sie können das CA-Zertifikat auch auf dem Client-Gerät speichern. • Alternativ können Sie die OpenSSL-Befehlszeile verwenden:	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`openssl s_client -showcerts -connect <device IP>:8883`	
Kopieren Sie die Anmeldeinformationen auf den Client-Geräten.	Kopieren Sie das Greengrass Core CA-Zertifikat, das Gerätezertifikat und den privaten Schlüssel auf die Client-Geräte.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ordnen Sie Client-Geräte dem Kerngerät zu.	Ordnen Sie Client-Geräte einem Core-Gerät zu, sodass sie das Core-Gerät erkennen können. Die Client-Geräte können dann die Greengrass Discovery API verwenden, um Verbindungsinformationen und Zertifikate für ihre zugehörigen Kerngeräte abzurufen. Weitere Informationen finden Sie unter Client-Geräte zuordnen in der AWS IoT Greengrass-Dokumentation. 1. Wählen Sie auf der AWS IoT Greengrass-Konsole die Option Core-Geräte aus. 2. Wählen Sie das zu verwaltende Kerngerät aus. 3. Wählen Sie auf der Detailseite des Kerngeräts die Registerkarte Client-Ge räte aus. 4. Wählen Sie im Abschnitt Zugeordnete Client-Geräte die Option Client-Geräte zuordnen aus. 5. Gehen Sie im Modalmodus Client-Geräte mit Kerngerät verknüpfen für jedes zu verknüpfende Client-Gerät wie folgt vor: a. Geben Sie den Namen des AWS IoT ein, das als	AWS IoT Greengrass

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Client-Gerät verknüpft werden soll. b. Wählen Sie Hinzufügen aus. 6. Wählen Sie Associate aus. Die Client-Geräte, die Sie verknüpft haben, können jetzt die Greengrass Discovery API verwenden, um dieses Kerngerät zu erkennen.	

Daten senden und empfangen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie Daten von einem Client-Gerät an ein anderes Client-Gerät.	Verwenden Sie den MQTT-Client auf Ihrem Gerät, um eine Nachricht zu `dt/client 1/sensor` diesem Thema zu veröffentlichen.	Allgemeines AWS
Senden Sie Daten vom Client-Gerät an AWS IoT Core.	Verwenden Sie den MQTT-Client auf Ihrem Gerät, um eine Nachricht zu `dt/client 1/sensor` diesem Thema zu veröffentlichen. Abonnieren Sie im MQTT-Test client das Thema, zu dem das Gerät Nachrichten sendet, oder abonnieren Sie # für alle Themen (siehe Details).	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie Nachrichten von AWS IoT Core an Client-Geräte.	Geben Sie auf der MQTT-Testclient-Seite auf der Registerkarte In einem Thema veröffentlichen im Feld Themenname den Themennamen Ihrer Nachricht ein. Verwenden Sie in diesem Beispiel `cmd/client1` für das Thema.	Allgemeines AWS

Fehlerbehebung

Problem	Lösung
Fehler beim Serverzertifikat konnte nicht verifiziert werden	Dieser Fehler tritt auf, wenn der MQTT-Client das vom MQTT-Broker während des TLS-Handshakes vorgelegte Zertifikat nicht verifizieren kann. Der häufigste Grund ist, dass der MQTT-Client nicht über das CA-Zertifikat verfügt. Gehen Sie wie folgt vor, um sicherzustellen, dass das CA-Zertifikat dem MQTT-Client zur Verfügung gestellt wird. 1. Wenn Sie von Ihrem PC aus Netzwerkzugriff auf das AWS IoT Greengrass-Gerät haben, öffnen Sie `https://<device IP>:8883` ein Browserfenster, um das MQTT-Broker-Zertifikat und das CA-Zertifikat anzuzeigen. Sie können das CA-Zertifikat auch auf dem Client-Gerät speichern. Verwenden Sie alternativ die OpenSSL-Befehlszeile:

Problem	Lösung
	``` openssl s_client -showcerts -connect <device IP>:8883 ``` 2. Speichern Sie den Inhalt der Zertifikate Moquette CA und Greengrass Core CA in Dateien und zeigen Sie dann den dekodierten Inhalt mit dem folgenden Befehl an: ``` openssl x509 -in <Name of CA>.pem - text ``` Das Moquette CA-Zertifikat sollte das SAN-Feld wie in diesem Beispiel anzeigen: ``` X509v3 Subject Alternative Name: IP Address:XXX.XXX.XXX.XXX, IP Address:127.0.0.1, DNS:localhost ```
Fehler beim Überprüfen des Servernamens nicht möglich	Dieser Fehler tritt auf, wenn der MQTT-Client nicht überprüfen kann, ob er sich mit dem richtigen Server verbindet. Der häufigste Grund ist, dass die IP-Adresse des Greengrass-Geräts nicht im SAN-Feld des Zertifikats aufgeführt ist. Folgen Sie den Anweisungen in der vorherigen Lösung, um das MQTT-Broker-Zertifikat zu erhalten, und stellen Sie sicher, dass das SAN-Feld die IP-Adresse des AWS IoT Greengrass-Geräts enthält, wie im Abschnitt Zusätzliche Informationen erklärt. Falls nicht, stellen Sie sicher, dass die IP-Detektorkomponente korrekt installiert ist, und starten Sie das Kerngerät neu.

Problem	Lösung
Der Servername konnte nicht nur überprüft werden, wenn die Verbindung von einem eingebetteten Client-Gerät aus hergestellt wurde	Mbed TLS, eine beliebte TLS-Bibliothek, die in eingebetteten Geräten verwendet wird, unterstützt derzeit nur die DNS-Namen süberprüfung im SAN-Feld des Zertifikats, wie im Mbed TLS-Bibliothekscode gezeigt. Da das Kerngerät keinen eigenen Domainnamen hat und von der IP-Adresse abhängt, schlagen TLS-Clients, die Mbed TLS verwenden, die Überprüfung des Servernamens während des TLS-Handshakes fehl, was zu einem Verbindun gsfehler führt. Wir empfehlen, dass Sie die SAN-IP-Adressverifizierung über die Funktion x509_crt_check_san zu Ihrer Mbed-TLS-Bibliothek hinzufügen.

Zugehörige Ressourcen

- Dokumentation zu AWS IoT Greengrass
- Dokumentation zu AWS IoT Core
- MQTT-Broker-Komponente
- MQTT-Bridge-Komponente
- Authentifizierungskomponente für Client-Geräte
- Komponente des IP-Detektors
- AWS IoT IoT-Geräte-SDK s
- Implementierung lokaler Client-Geräte mit AWS IoT Greengrass (AWS-Blogbeitrag)
- RFC 5280 — Internet X.509-Infrastrukturzertifikat und CRL-Profil (Certificate Revocation List)

Zusätzliche Informationen

Dieser Abschnitt enthält zusätzliche Informationen zur Kommunikation zwischen den Client-Geräten und dem Core-Gerät.

Der MQTT-Broker wartet auf Port 8883 im Kerngerät auf einen Verbindungsversuch mit dem TLS-Client. Die folgende Abbildung zeigt ein Beispiel für ein Serverzertifikat des MQTT-Brokers.

Das Beispielzertifikat zeigt die folgenden Details an:

- Das Zertifikat wird von der AWS IoT Greengrass Core CA ausgestellt, die lokal und spezifisch für das Kerngerät ist. Das heißt, sie fungiert als lokale CA.
- Dieses Zertifikat wird automatisch jede Woche von der Client-Authentifizierungskomponente rotiert, wie in der folgenden Abbildung dargestellt. Sie können dieses Intervall in der Konfiguration der Client-Authentifizierungskomponente festlegen.

- Der alternative Subject Name (SAN) spielt eine entscheidende Rolle bei der Überprüfung des Servernamens auf der Seite des TLS-Clients. Damit kann der TLS-Client sicherstellen, dass er sich mit dem richtigen Server verbindet, und verhindert man-in-the-middle Angriffe bei der Einrichtung der TLS-Sitzung. Im Beispielzertifikat gibt das SAN-Feld an, dass dieser Server auf localhost (dem lokalen Unix-Domain-Socket) lauscht und die Netzwerkschnittstelle die IP-Adresse 192.168.1.12 hat.

Der TLS-Client verwendet das SAN-Feld im Zertifikat, um bei der Serververifizierung zu überprüfen, ob er eine Verbindung zu einem legitimen Server herstellt. Im Gegensatz dazu wird bei einem typischen TLS-Handshake zwischen einem HTTP-Server und einem Browser der Domainname im Feld Common Name (CN) oder SAN verwendet, um die Domain zu überprüfen, zu der der Browser während der Serververifizierung tatsächlich eine Verbindung herstellt. Wenn das Kerngerät keinen Domainnamen hat, dient die im SAN-Feld angegebene IP-Adresse demselben Zweck. Weitere Informationen finden Sie im Abschnitt „Alternativer Betreffname“ des Profils RFC 5280 — Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL).

Die IP-Detektorkomponente in AWS IoT Greengrass stellt sicher, dass die richtigen IP-Adressen im SAN-Feld des Zertifikats enthalten sind.

Das Zertifikat im Beispiel ist vom AWS IoT Greengrass-Gerät signiert, das als lokale Zertifizierungsstelle fungiert. Der TLS-Client (MQTT-Client) kennt diese CA nicht, daher müssen wir ein CA-Zertifikat bereitstellen, das wie folgt aussieht.

Mehr Muster

- Mit AWS IoT Greengrass IoT-Daten kostengünstig direkt in Amazon S3 aufnehmen

Migration und Modernisierung

Themen

- Migration
- Modernisierung
- Großrechner

Migration

Themen

- Erstellen Sie CloudFormation AWS-Vorlagen für AWS DMS-Aufgaben mit Microsoft Excel und Python
- Beginnen Sie mit der automatisierten Portfolioerkennung
- Migrieren Sie lokale Cloudera-Workloads zur Cloudera Data Platform auf AWS
- Verbindungsfehler nach der Migration von Microsoft SQL Server zur AWS-Cloud beheben
- Starten Sie den AWS Replication Agent SELinux nach dem Neustart eines RHEL-Quellservers automatisch neu, ohne ihn zu deaktivieren.
- Re-Architekt
- Erneut hosten
- Umziehen
- Plattformwechsel
- Migrationsmuster nach Arbeitslast
- Mehr Muster

Erstellen Sie CloudFormation AWS-Vorlagen für AWS DMS-Aufgaben mit Microsoft Excel und Python

Erstellt von Venkata Naveen Koppula (AWS)

Übersicht

Dieses Muster beschreibt die Schritte zur automatischen Erstellung von CloudFormation AWS-Vorlagen für AWS Database Migration Service (AWS DMS) mithilfe von Microsoft Excel und Python.

Die Migration von Datenbanken mithilfe von AWS DMS beinhaltet häufig die Erstellung von CloudFormation AWS-Vorlagen zur Bereitstellung von AWS DMS-Aufgaben. Bisher waren für die Erstellung von CloudFormation AWS-Vorlagen Kenntnisse der Programmiersprache JSON oder YAML erforderlich. Mit diesem Tool benötigen Sie nur Grundkenntnisse in Excel und in der Ausführung eines Python-Skripts über ein Terminal oder ein Befehlsfenster.

Als Eingabe verwendet das Tool eine Excel-Arbeitsmappe, die die Namen der zu migrierenden Tabellen, Amazon-Ressourcennamen (ARNs) von AWS-DMS-Endpunkten und AWS-DMS-Replikationsinstanzen enthält. Das Tool generiert dann CloudFormation AWS-Vorlagen für die erforderlichen AWS DMS-Aufgaben.

Ausführliche Schritte und Hintergrundinformationen finden Sie im Blogbeitrag CloudFormation AWS-Vorlagen für AWS-DMS-Aufgaben mithilfe von Microsoft Excel erstellen im AWS-Datenbank-Blog.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Microsoft Excel Version 2016 oder höher
- Python-Version 2.7 oder höher
- Das Python-Modul xlrd (installiert an einer Eingabeaufforderung mit dem Befehl: pip install xlrd)
- AWS-DMS-Quell- und Zielendpunkte und AWS-DMS-Replikationsinstanz

Einschränkungen

- Die Namen von Schemas, Tabellen und zugehörigen Spalten werden an den Zielendpunkten in Kleinbuchstaben umgewandelt.

- Dieses Tool befasst sich nicht mit der Erstellung von AWS DMS-Endpunkten und Replikationsinstanzen.
- Derzeit unterstützt das Tool nur ein Schema für jede AWS DMS-Aufgabe.

Architektur

Quelltechnologie-Stack

- Eine lokale Datenbank
- Microsoft Excel

Zieltechnologie-Stack

- CloudFormation AWS-Vorlagen
- Eine Datenbank in der AWS-Cloud

Architektur

Tools

- Pycharm IDE oder jede integrierte Entwicklungsumgebung (IDE), die Python Version 3.6 unterstützt
- Microsoft Office 2016 (für Microsoft Excel)

Epen

Konfiguration des Netzwerks, der AWS-DMS-Replikationsinstanz und der Endpunkte

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Falls erforderlich, fordern Sie eine Erhöhung der Servicequote an.	Fordern Sie bei Bedarf eine Erhöhung des Servicekontingents für die AWS DMS-Aufgaben an.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die AWS-Region, virtuelle private Clouds (VPCs), CIDR-Bereiche, Availability Zones und Subnetze.		Allgemeines AWS
Konfigurieren Sie die AWS DMS-Replikationsinstanz.	Die AWS DMS-Replikationsinstanz kann sich sowohl mit lokalen als auch mit AWS-Datenbanken verbinden.	Allgemeines AWS
Konfigurieren Sie AWS DMS-Endpunkte.	Konfigurieren Sie Endpunkte sowohl für die Quell- als auch für die Zieldatenbank.	Allgemeines AWS

Bereiten Sie die Arbeitsblätter für AWS DMS-Aufgaben und -Tags vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Tabellenliste.	Listet alle an der Migration beteiligten Tabellen auf.	Datenbank
Bereiten Sie das Arbeitsblatt mit den Aufgaben vor.	Bereiten Sie das Excel-Arbeitsblatt anhand der von Ihnen konfigurierten Tabellenliste vor.	Allgemein AWS, Microsoft Excel
Bereiten Sie das Tag-Arbeitsblatt vor.	Geben Sie die AWS-Ressourcen-Tags an, die an die AWS DMS-Aufgaben angehängt werden sollen.	Allgemein AWS, Microsoft Excel

Laden Sie das Tool herunter und führen Sie es aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das Tool zur Vorlagengenerierung herunter und extrahieren Sie es aus dem GitHub Repository.	GitHub Repositorium: https://github.com/aws-samples/dms-cloudformation-templates-generator/	
Führen Sie das Tool aus.	Folgen Sie den detaillierten Anweisungen im Blogbeitrag, der unter „Referenzen und Hilfe“ aufgeführt ist.	

Zugehörige Ressourcen

- CloudFormation AWS-Vorlagen für AWS DMS-Aufgaben mit Microsoft Excel erstellen (Blogbeitrag)
- Generator CloudFormation für DMS-Vorlagen (Repository) GitHub
- Python-Dokumentation
- XLRD-Beschreibung und Download
- AWS DMS-Dokumentation
- CloudFormation AWS-Dokumentation

Beginnen Sie mit der automatisierten Portfolioerkennung

Erstellt von Pratik Chunawala (AWS) und Rodolfo Jr. Geschlossen (AWS)

Übersicht

Die Bewertung des Portfolios und das Sammeln von Metadaten sind eine entscheidende Herausforderung bei der Migration von Anwendungen und Servern in die Amazon Web Services (AWS) Cloud, insbesondere bei großen Migrationen mit mehr als 300 Servern. Mithilfe eines automatisierten Portfolio-Discovery-Tools können Sie Informationen über Ihre Anwendungen sammeln, z. B. die Anzahl der Benutzer, die Nutzungshäufigkeit, Abhängigkeiten und Informationen über die Infrastruktur der Anwendung. Diese Informationen sind für die Planung von Migrationswellen unerlässlich, damit Sie Anwendungen mit ähnlichen Merkmalen richtig priorisieren und gruppieren können. Die Verwendung eines Discovery-Tools optimiert die Kommunikation zwischen dem Portfolio-Team und den Anwendungseigentümern, da das Portfolio-Team die Ergebnisse des Discovery-Tools validieren kann, anstatt die Metadaten manuell zu sammeln. In diesem Muster werden die wichtigsten Überlegungen zur Auswahl eines automatisierten Discovery-Tools sowie Informationen zur Bereitstellung und zum Testen eines Tools in Ihrer Umgebung erläutert.

Dieses Muster enthält eine Vorlage, die als Ausgangspunkt für die Erstellung Ihrer eigenen Checkliste mit Aktivitäten auf hoher Ebene dient. Neben der Checkliste befindet sich eine Vorlage für eine Matrix für verantwortungsvolle, rechenschaftspflichtige, konsultierte und informierte Informationen (RACI). Sie können diese RACI-Matrix verwenden, um zu bestimmen, wer für jede Aufgabe in Ihrer Checkliste verantwortlich ist.

Epen

Wählen Sie ein Discovery-Tool

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie fest, ob ein Discovery-Tool für Ihren Anwendungsfall geeignet ist.	Ein Discovery-Tool ist möglicherweise nicht die beste Lösung für Ihren Anwendung sfall. Berücksichtigen Sie den Zeitaufwand, der für die Auswahl, Beschaffung, Vorbereitung und Bereitste	Migrationsleiter, Migration singenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	llung eines Discovery-Tools erforderlich ist. Es kann 4 bis 8 Wochen dauern, die Scan-Appliance für ein agentenlo ses Erkennungstool in Ihrer Umgebung einzurichten oder Agenten für alle im Lieferumf ang enthaltenen Workloads zu installieren. Nach der Bereitstellung müssen Sie 4—12 Wochen einplanen , bis das Discovery-Tool Metadaten erfasst, indem es die Anwendungs-Workloads scannt und eine Anwendung s-Stack-Analyse durchführ t. Wenn Sie weniger als 100 Server migrieren, können Sie die Metadaten möglicher weise schneller manuell sammeln und Abhängigkeiten analysieren, als dies für die Bereitstellung und Erfassung von Metadaten mit einem automatisierten Erkennung stool erforderlich ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie ein Discovery-Tool aus.	Lesen Sie die Überlegungen zur Auswahl eines automatisierten Discovery-Tools im Abschnitt Zusätzliche Informationen. Ermitteln Sie die geeigneten Kriterien für die Auswahl eines Discovery-Tools für Ihren Anwendungsfall und bewerten Sie dann jedes Tool anhand dieser Kriterien. Eine umfassende Liste automatisierter Discovery-Tools finden Sie unter Tools für die Migration von Discovery, Planning und Recommendation.	Migrationsleiter, Migrationsingenieur

Bereiten Sie sich auf die Installation vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Checkliste vor der Bereitstellung vor.	Erstellen Sie eine Checkliste mit den Aufgaben, die Sie vor der Bereitstellung des Tools ausführen müssen. Ein Beispiel finden Sie in der Checkliste vor der Bereitstellung auf der Flexera Dokumentationswebsite.	Leiter der Entwicklung, Migrationsingenieur, Migrationsleiter, Netzwerkadministrator
Bereiten Sie die Netzwerkanforderungen vor.	Stellen Sie die Ports, Protokolle, IP-Adressen und das Routing bereit, die für die Ausführung des Tools und	Migrationsingenieur, Netzwerkadministrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den Zugriff auf die Zielserve r erforderlich sind. Weitere Informationen finden Sie in der Installationsanleitung für Ihr Discovery-Tool. Ein Beispiel finden Sie unter Deployment Requirements auf der Flexera-Dokumentationswebsite.	
Bereiten Sie die Anforderu ngen für das Konto und die Anmeldeinformationen vor.	Identifizieren Sie die Anmeldeinformationen, die Sie für den Zugriff auf die Zielserver und die Installation aller Komponenten des Tools benötigen.	Cloud-Administrator, AWS allgemein, Migrationsingenieu r, Migrationsleiter, Netzwerka dministrator, AWS-Admin istrator
Bereiten Sie die Appliances vor, auf denen Sie das Tool installieren werden.	Stellen Sie sicher, dass die Appliances, auf denen Sie die Toolkomponenten installie ren, die Spezifikationen und Plattformanforderungen für das Tool erfüllen.	Migrationsingenieur, Migration sleiter, Netzwerkadministrator
Bereiten Sie die Änderungs aufträge vor.	Bereiten Sie entsprechend dem Änderungsmanagemen tprozess in Ihrer Organisation alle erforderlichen Änderungs aufträge vor und stellen Sie sicher, dass diese Änderungs aufträge genehmigt werden.	Leitung aufbauen, Leitung für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie Anforderungen an die Beteiligten.	Senden Sie die Checkliste vor der Bereitstellung und die Netzwerkanforderungen an die Beteiligten. Die Beteiligt en sollten die erforderlichen Anforderungen überprüfen, bewerten und vorbereiten, bevor sie mit der Bereitste llung fortfahren.	Leitung aufbauen, Leitung Migration

Stellen Sie das Tool bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das Installat ionsprogramm herunter.	Laden Sie das Installat ionsprogramm oder das Image der virtuellen Maschine herunter. Images virtueller Maschinen werden normalerw eise im Open Virtualization Format (OVF) geliefert.	Führung beim Aufbau, Leitung bei der Migration
Extrahieren Sie die Dateien.	Wenn Sie ein Installat ionsprogramm verwenden , müssen Sie das Installat ionsprogramm herunterladen und auf einem lokalen Server ausführen.	Leiter für Aufbau, Migration
Stellen Sie das Tool auf den Servern bereit.	Stellen Sie das Discovery-Tool auf den lokalen Zielservern wie folgt bereit: • Wenn es sich bei Ihrer Quelldatei um ein VM-Image	Leiter für den Aufbau, Leiter der Migration, Netzwerka dministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	handelt, stellen Sie es in Ihrer VM-Umgebung bereit, z. B. VMware • Wenn es sich bei Ihrer Quelldatei um ein Installat ionsprogramm handelt, führen Sie das Installat ionsprogramm aus, um das Tool zu installieren und einzurichten.	
Melden Sie sich beim Discovery-Tool an.	Folgen Sie den Anweisung en auf dem Bildschirm und melden Sie sich an, um mit dem Tool zu beginnen.	Leiter der Migration, Leiter des Unternehmens
Aktivieren Sie das Produkt.	Geben Sie Ihren Lizenzsch lüssel ein.	Lead aufbauen, Lead Migration
Konfigurieren Sie das Tool.	Geben Sie alle Anmeldein formationen ein, die für den Zugriff auf die Zielserve r erforderlich sind, z. B. Anmeldeinformationen für Windows VMware, Simple Network Management Protocol (SNMP) und Secure Shell Protocol (SSH) oder Datenbanken.	Leitung beim Aufbau, Leitung bei der Migration

Testen Sie das Tool

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie Testserver aus.	Identifizieren Sie eine kleine Gruppe von Subnetzen oder IP-Adressen, die Sie verwenden können, um das Discovery-Tool zu testen. Auf diese Weise können Sie die Scans schnell validieren, Fehler schnell identifizieren und beheben und Ihre Tests von Produktionsumgebungen isolieren.	Leiter Aufbau, Leiter Migration, Netzwerkadministrator
Starten Sie das Scannen der ausgewählten Testserver.	Geben Sie bei einem Agentenlosen Discovery-Tool die Subnetze oder IP-Adress en für die ausgewählten Testserver in die Discovery-Tool-Konsole ein und starten Sie den Scan. Bei einem Agent-basierten Discovery-Tool installieren Sie den Agenten auf den ausgewählten Testservern.	Leiter für Aufbau, Migration, Netzwerkadministrator
Überprüfen Sie die Scanergeb nisse.	Überprüfen Sie die Scanergeb nisse für die Testserver. Wenn Fehler gefunden werden, führen Sie eine Fehlerbeh ebung durch und beheben Sie die Fehler. Dokumentieren Sie die Fehler und Lösungen. Sie verweisen in future auf diese Informationen und können	Leiter Aufbau, Leiter Migration, Netzwerkadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	diese Informationen zu Ihrem Portfolio-Runbook hinzufügen.	
Scannen Sie die Testserver erneut.	Sobald der erneute Scan abgeschlossen ist, wiederhol en Sie den Scan, bis keine Fehler mehr vorliegen.	Leiter für den Aufbau, Leiter der Migration, Netzwerka dministrator

Zugehörige Ressourcen

AWS Ressourcen

- Leitfaden zur Bewertung des Anwendungsportfolios für die AWS Cloud Migration
- Tools zur Erkennung, Planung und Empfehlung der Migration

Bereitstellungsleitfäden für häufig verwendete Discovery-Tools

- Stellen Sie die virtuelle Appliance RN15 0 bereit (Flexera-Dokumentation)
- Installation von Gatherer (ModelizeIT-Dokumentation)
- Installation des Analysis Servers vor Ort (ModelizeIT-Dokumentation)

Zusätzliche Informationen

Überlegungen zur Auswahl eines automatisierten Discovery-Tools

Jedes Discovery-Tool hat Vor- und Nachteile. Beachten Sie bei der Auswahl des geeigneten Tools für Ihren Anwendungsfall Folgendes:

- Wählen Sie ein Discovery-Tool aus, mit dem die meisten, wenn nicht sogar alle Metadaten erfasst werden können, die Sie zur Erreichung Ihres Portfoliobewertungsziels benötigen.
- Identifizieren Sie alle Metadaten, die Sie manuell sammeln müssen, da das Tool sie nicht unterstützt.
- Stellen Sie allen Beteiligten die Anforderungen an das Discovery-Tool zur Verfügung, damit sie das Tool anhand ihrer internen Sicherheits- und Compliance-Anforderungen, wie Server-, Netzwerk- und Anmeldeinformationen, überprüfen und bewerten können.

  - Erfordert das Tool, dass Sie einen Agenten für den Workload installieren, der im Leistungsumfang enthalten ist?
  - Erfordert das Tool, dass Sie eine virtuelle Appliance in Ihrer Umgebung einrichten?
- Ermitteln Sie Ihre Anforderungen an die Datenresidenz. Einige Unternehmen möchten ihre Daten nicht außerhalb ihrer Umgebung speichern. Um dieses Problem zu beheben, müssen Sie möglicherweise einige Komponenten des Tools in der lokalen Umgebung installieren.
- Stellen Sie sicher, dass das Tool das Betriebssystem (OS) und die Betriebssystemversion des Workloads unterstützt, der im Leistungsumfang enthalten ist.
- Stellen Sie fest, ob Ihr Portfolio Mainframe-, Midrange- und Legacy-Server umfasst. Die meisten Erkennungstools können diese Workloads als Abhängigkeiten erkennen, aber einige Tools sind möglicherweise nicht in der Lage, Gerätedetails wie Auslastung und Serverabhängigkeiten abzurufen. Die Discovery-Tools Device42 und ModernizeIT unterstützen sowohl Mainframe- als auch Midrange-Server.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Migrieren Sie lokale Cloudera-Workloads zur Cloudera Data Platform auf AWS

Erstellt von Battulga Purevragchaa (AWS), Nijjwol Lamsal (Partner) und Nidhi Gupta (AWS)

Übersicht

Dieses Muster beschreibt die allgemeinen Schritte für die Migration Ihrer lokalen Cloudera Distributed Hadoop (CDH), Hortonworks Data Platform (HDP) und Cloudera Data Platform (CDP) -Workloads zur CDP Public Cloud auf AWS. Wir empfehlen Ihnen, mit Cloudera Professional Services und einem Systemintegrator (SI) zusammenzuarbeiten, um diese Schritte umzusetzen.

Es gibt viele Gründe, warum Cloudera-Kunden ihre lokalen CDH-, HDP- und CDP-Workloads in die Cloud verlagern möchten. Zu den typischen Gründen gehören:

- Rationalisieren Sie die Einführung neuer Datenplattform-Paradigmen wie Data Lakehouse oder Data Mesh
- Erhöhen Sie die Flexibilität Ihres Unternehmens, demokratisieren Sie den Zugriff auf bestehende Datenbestände und die daraus resultierenden Rückschlüsse
- Senken Sie die Gesamtbetriebskosten (TCO)
- Verbessern Sie die Workload-Elastizität
- Ermöglichen Sie eine höhere Skalierbarkeit und reduzieren Sie den Zeitaufwand für die Bereitstellung von Datendiensten im Vergleich zu herkömmlichen Installationen vor Ort drastisch
- Legacy-Hardware außer Dienst stellen und Hardware-Aktualisierungszyklen deutlich reduzieren
- Nutzen Sie die pay-as-you-go Preisgestaltung, die mit dem Cloudera-Lizenzmodell (CCU) auf Cloudera-Workloads auf AWS ausgedehnt wird
- Nutzen Sie die Vorteile einer schnelleren Bereitstellung und einer verbesserten Integration mit Plattformen für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD)
- Verwenden Sie eine einzige einheitliche Plattform (CDP) für mehrere Workloads

Cloudera unterstützt alle wichtigen Workloads, einschließlich Machine Learning, Data Engineering, Data Warehouse, Operational Database, Stream Processing (CSP) sowie Datensicherheit und Governance. Cloudera bietet diese Workloads seit vielen Jahren vor Ort an, und Sie können diese Workloads in die AWS-Cloud migrieren, indem Sie CDP Public Cloud mit Workload Manager und Replication Manager verwenden.

Cloudera Shared Data Experience (SDX) bietet einen gemeinsamen Metadatenkatalog für diese Workloads, um eine konsistente Datenverwaltung und einen konsistenten Betrieb zu ermöglichen. SDX bietet außerdem umfassende, differenzierte Sicherheit zum Schutz vor Bedrohungen und eine einheitliche Steuerung für Prüf- und Suchfunktionen zur Einhaltung von Standards wie dem Payment Card Industry Data Security Standard (PCI DSS) und der DSGVO.

Die CDP-Migration auf einen Blick

Arbeitslast	Quell-Workload	CDH, HDP und CDP Private Cloud
	Quellumgebung	• Windows, Linux • Lokal, Colocation oder jede Umgebung außerhalb von AWS
	Ziel-Workload	CDP Public Cloud auf AWS
	Zielumgebung	• Bereitstellungsmodell: Kundenkonto • Betriebsmodell: Kunde/ClouderA-Steuerebene
Migration	Migrationsstrategie (7Rs)	Rehosten, Neuplattformen oder Refactoring
	Handelt es sich um ein Upgrade der Workload-Version?	Ja
	Dauer der Migration	• Bereitstellung: Ungefähr eine Woche, um ein Kundenkonto, eine vom Kunden verwaltete Virtual Private Cloud (VPC) und eine CDP Public Cloud-Umgebung zu erstellen.

- Migrationsdauer: 1—4 Monate, abhängig von der Komplexität und Größe der Arbeitslast.

Kosten	Kosten für die Ausführung des Workloads auf AWS	• Im Großen und Ganzen gehen die Kosten einer CDH-Workload-Migration zu AWS davon aus, dass Sie eine neue Umgebung auf AWS einrichten werden. Dazu gehören die Abrechnung von Zeit und Aufwand des Personals sowie die Bereitstellung von Rechenressourcen und die Lizenzierung von Software für die neue Umgebung. • Das auf der Cloud-Nutzung basierende Preismodell von Cloudera bietet Ihnen die Flexibilität, die Vorteile von Bursting- und automatischen Skalierungsfunktionen zu nutzen. Weitere Informati onen finden Sie unter CDP Public Cloud-Servicetarife auf der Cloudera-Website. • Cloudera Enterprise Data Hub basiert auf Amazon Elastic Compute Cloud (Amazon EC2) und bildet traditionelle Cluster eng ab. Data Hub kann angepasst werden, was sich jedoch auf die Kosten auswirken wird. • CDP Public Cloud Data Warehouse, Cloudera Machine Learning und Cloudera Data Engineering (CDE) sind containerbasiert

		und können so konfiguriert werden, dass sie automatisch skalieren.
	Systemanforderungen	Weitere Informationen finden Sie im Abschnitt Voraussetzungen.
Infrastrukturvereinbarungen und Rahmenbedingungen	SLA	Weitere Informationen finden Sie unter Cloudera Service Level Agreement für CDP Public Cloud.
	DR	Weitere Informationen finden Sie in der Cloudera-Dokumentation unter Disaster Recovery.
	Lizenz- und Betriebsmodell (für AWS-Zielkonto)	Modell „Bring Your Own License“ (BYOL)
Compliance	Anforderungen an Sicherheit	Weitere Informationen finden Sie in der Cloudera-Dokumentation im Überblick über die Cloudera-Sicherheit.
	Andere Compliance-Zertifizierungen	Informationen zur Einhaltung der Allgemeinen Datenschutzverordnung (DSGVO) und zum CDP Trust Center finden Sie auf der Cloudera-Website.

Voraussetzungen und Einschränkungen

Voraussetzungen

- AWS-Kontoanforderungen, einschließlich Konten, Ressourcen, Services und Berechtigungen, z. B. Einrichtung von Rollen und Richtlinien für AWS Identity and Access Management (IAM)

- Voraussetzungen für die Bereitstellung von CDP über die Cloudera-Website

Die Migration erfordert die folgenden Rollen und Fachkenntnisse:

Rolle	Fähigkeiten und Verantwortlichkeiten
Führung im Bereich Migration	Sorgt für die Unterstützung der Geschäfts leitung, die Zusammenarbeit, Planung, Implementierung und Bewertung im Team
Cloudera KMU	Fachkenntnisse in den Bereichen CDH-, HDP- und CDP-Administration, Systemadministration und Architektur
AWS-Architekt	Kenntnisse in AWS-Services, Netzwerken, Sicherheit und Architekturen

Architektur

Der Aufbau der geeigneten Architektur ist ein entscheidender Schritt, um sicherzustellen, dass Migration und Leistung Ihren Erwartungen entsprechen. Damit Ihre Migrationsbemühungen die Annahmen dieses Playbooks erfüllen, muss Ihre Zieldatenumgebung in der AWS-Cloud, entweder auf gehosteten Virtual Private Cloud (VPC) -Instances oder CDP, in Bezug auf Betriebssystem- und Softwareversionen sowie wichtige Maschinenspezifikationen Ihrer Quellumgebung entsprechen.

Das folgende Diagramm (mit freundlicher Genehmigung aus dem Cloudera Shared Data Experience-Datenblatt wiedergegeben) zeigt die Infrastrukturkomponenten für die CDP-Umgebung und wie die Stufen oder Infrastrukturkomponenten interagieren.

Die Architektur umfasst die folgenden CDP-Komponenten:

- Data Hub ist ein Dienst zum Starten und Verwalten von Workload-Clustern, der von Cloudera Runtime unterstützt wird. Sie können die Clusterdefinitionen in Data Hub verwenden, um Workload-Cluster für benutzerdefinierte Anwendungsfälle bereitzustellen und auf sie zuzugreifen und benutzerdefinierte Clusterkonfigurationen zu definieren. Weitere Informationen finden Sie auf der Cloudera-Website.

- Data Flow and Streaming befasst sich mit den wichtigsten Herausforderungen, mit denen Unternehmen bei der Übertragung von Daten konfrontiert sind. Es verwaltet Folgendes:
  - Verarbeitung von Echtzeit-Datenstreaming mit hohem Volumen und großem Umfang
  - Verfolgung der Herkunft und Herkunft von Streaming-Daten
  - Verwaltung und Überwachung von Edge-Anwendungen und Streaming-Quellen

  Weitere Informationen finden Sie unter Cloudera DataFlow und CSP auf der Cloudera-Website.
- Data Engineering umfasst Datenintegration, Datenqualität und Datenverwaltung, die Unternehmen beim Aufbau und der Pflege von Daten-Pipelines und Workflows unterstützen. Weitere Informationen finden Sie auf der Cloudera-Website. Erfahren Sie mehr über die Unterstützung für Spot-Instances, um Kosteneinsparungen bei AWS for Cloudera Data Engineering-Workloads zu ermöglichen.
- Mit Data Warehouse können Sie unabhängige Data Warehouses und Data Marts einrichten, die automatisch skaliert werden, um den Workload-Anforderungen gerecht zu werden. Dieser Service bietet isolierte Recheninstanzen und automatisierte Optimierungen für jedes Data Warehouse und jeden Data Mart und hilft Ihnen, während der Besprechung SLAs Kosten zu sparen. Weitere Informationen finden Sie auf der Cloudera-Website. Erfahren Sie mehr über Kostenmanagement und auto-scaling für Cloudera Data Warehouse auf AWS.
- Die Betriebsdatenbank in CDP bietet eine zuverlässige und flexible Grundlage für skalierbare Hochleistungsanwendungen. Sie bietet eine jederzeit verfügbare, skalierbare Echtzeitdatenbank, die traditionelle strukturierte Daten zusammen mit neuen, unstrukturierten Daten auf einer einheitlichen Betriebs- und Warehousing-Plattform bereitstellt. Weitere Informationen finden Sie auf der Cloudera-Website.
- Machine Learning ist eine Cloud-native Plattform für maschinelles Lernen, die Self-Service-Funktionen für Datenwissenschaft und Datentechnik zu einem einzigen, portablen Service innerhalb einer Unternehmensdatencloud zusammenführt. Sie ermöglicht den skalierbaren Einsatz von maschinellem Lernen und künstlicher Intelligenz (KI) für Daten an jedem beliebigen Ort. Weitere Informationen finden Sie auf der Cloudera-Website.

CDP auf AWS

Das folgende Diagramm (mit freundlicher Genehmigung der Cloudera-Website angepasst) zeigt die High-Level-Architektur von CDP auf AWS. CDP implementiert ein eigenes Sicherheitsmodell, um sowohl Konten als auch den Datenfluss zu verwalten. Diese werden mithilfe von kontenübergreifenden Rollen in IAM integriert.

Die CDP-Steuerebene befindet sich in einem Cloudera-Master-Konto in einer eigenen VPC. Jedes Kundenkonto hat sein eigenes Unterkonto und eine eigene VPC. Kontoübergreifende IAM-Rollen und SSL-Technologien leiten den Verwaltungsdatenverkehr zur und von der Steuerungsebene an Kundenservices weiter, die sich in öffentlichen Subnetzen befinden, die über das Internet routbar sind, innerhalb jeder Kunden-VPC. Auf der VPC des Kunden bietet die Cloudera Shared Data Experience (SDX) unternehmensweite Sicherheit mit einheitlicher Governance und Compliance, sodass Sie schneller Erkenntnisse aus Ihren Daten gewinnen können. SDX ist eine Designphilosophie, die in alle Cloudera-Produkte integriert ist. Weitere Informationen zu SDX und der CDP Public Cloud-Netzwerkarchitektur für AWS finden Sie in der Cloudera-Dokumentation.

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Elastic Kubernetes Service (Amazon EKS) hilft Ihnen, Kubernetes auf AWS auszuführen, ohne Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten zu müssen.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der AWS-Cloud.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Automatisierung und Tools

- Für zusätzliche Tools können Sie Cloudera Backup Data Recovery (BDR), AWS Snowball und AWS Snowmobile verwenden, um Daten von lokalen CDH, HDP und CDP auf AWS-gehostete CDP zu migrieren.
- Für neue Bereitstellungen empfehlen wir, die AWS-Partnerlösung für CDP zu verwenden.

Epics

Bereiten Sie sich auf die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Binden Sie das Cloudera-Team ein.	Cloudera verfolgt ein standardisiertes Kooperationsmodell mit seinen Kunden und kann mit Ihrem Systemintegrator (SI) zusammenarbeiten, um denselben Ansatz zu fördern. Wenden Sie sich an das Cloudera-Kundenteam, damit es Ihnen mit Rat und Tat zur Seite steht und Ihnen die notwendigen technischen Ressourcen für den Start des Projekts zur Verfügung stellt. Durch die Kontaktaufnahme mit dem Cloudera-Team wird sichergestellt, dass sich alle erforderlichen Teams auf die Migration vorbereiten können, wenn der Termin näher rückt. Sie können sich an Cloudera Professional Services wenden, um Ihre Cloudera-Implementierung schnell, zu geringeren Kosten und mit Spitzenleistung von der Pilotphase zur Produktion zu überführen. Eine vollständige Liste der Angebote finden Sie auf der Cloudera-Website.	Leiter der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CDP Public Cloud-Umgebung auf AWS für Ihre VPC.	Arbeiten Sie mit Cloudera Professional Services oder Ihrem SI zusammen, um CDP Public Cloud in einer VPC auf AWS zu planen und bereitzustellen.	Cloud-Architekt, Cloudera SME

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Priorisieren und bewerten Sie die zu migrierenden Workloads.	Bewerten Sie alle Ihre lokalen Workloads, um herauszufinden, welche Workloads am einfachsten zu migrieren sind. Anwendungen, die nicht geschäftskritisch sind, sollten am besten zuerst verschoben werden, da sie nur minimale Auswirkungen auf Ihre Kunden haben werden. Speichern Sie die geschäftskritischen Workloads bis zum Schluss, nachdem Sie andere Workloads erfolgreich migriert haben. **Note** Transiente Workloads (CDP Data Engineering) lassen sich einfacher migrieren als persistente Workloads (CDP Data Warehouse). Es ist auch wichtig, bei der Migration das Datenvolumen und die Standorte zu berücksichtigen. Zu den Herausforderungen können die kontinuierliche Replikation von Daten aus einer lokalen Umgebung	Leitung der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in die Cloud und die Änderung der Datenerfassungspip elines gehören, um Daten direkt in die Cloud zu importieren.	
Erörtern Sie Aktivitäten zur Migration von CDH, HDP, CDP und Legacy-An wendungen.	Erwägen Sie mit Cloudera Workload Manager die folgenden Aktivitäten und beginnen Sie mit der Planung: • Daten und Workloads zum Kopieren in Ihre AWS-Umgebung • Cloud-fähige Daten • Laute Nachbarn, die Ressourcen verbrauch en und anderen Mietern Probleme bereiten • Elastische Workloads • Kleine Cluster mit hohem Betriebsaufwand	Leitung der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erfüllen Sie die Anforderungen und Empfehlungen von Cloudera Replication Manager.	Arbeiten Sie mit Cloudera Professional Services und Ihrem SI zusammen, um die Migration von Workloads in Ihre CDP Public Cloud-Umgebung auf AWS vorzubereiten. Wenn Sie die folgenden Anforderungen und Empfehlungen kennen, können Sie häufig auftretende Probleme während und nach der Installation des Replication Manager-Service vermeiden. • Überprüfen Sie anhand der Begleitdokumente zu Replication Manager, ob Sie die Umgebungs- und Systemanforderungen erfüllen. Weitere Informationen finden Sie unter Supportmatrix für CDP Public Cloud Replication Manager auf der Cloudera-Website. • Sie benötigen keinen Root-Zugriff auf die Knoten, auf denen die Replication Manager App und die Data Lifecycle Manager (DLM) -Engine installiert werden. • Installieren Sie Apache Hive während der Erstinstallation von Replication Manager,	Leiter der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	sofern Sie nicht sicher sind, dass Sie die Hive-Replikation in future nicht mehr verwenden werden. Wenn Sie Hive installieren möchten, nachdem Sie HDFS-Replikationsrichtlinien in Replication Manager erstellt haben, müssen Sie alle HDFS-Replikationsrichtlinien löschen und anschließend neu erstellen, nachdem Sie Hive hinzugefügt haben. • In Replication Manager verwendete Cluster müssen symmetrische Konfigurationen haben. Jeder Cluster in einer Replikationsbeziehung muss in Bezug auf Sicherheit (Kerberos), Benutzerverwaltung (LDAP/AD) und Knox Proxy exakt gleich konfiguriert sein. Clusterdienste wie Hadoop Distributed File System (HDFS), Apache Hive, Apache Knox, Apache Ranger und Apache Atlas können unterschiedliche Konfigurationen für Hochverfügbarkeit (HA) haben. Quell- und Zielcluster können beispielsweise	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	separate HA- und Nicht-HA-Konfigurationen haben.	

CDP zu AWS migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie den ersten Workload für Entwicklungs-/Testumgebungen mithilfe von Cloudera Workload Manager.	Ihr SI kann Ihnen helfen, Ihren ersten Workload in die AWS-Cloud zu migrieren. Dabei sollte es sich um eine Anwendung handeln, die nicht kundenorientiert oder geschäftskritisch ist. Ideale Kandidaten für die Dev/Test-Migration sind Anwendungen mit Daten, die die Cloud problemlos aufnehmen kann, wie z. B. CDP Data Engineering-Workloads. Dabei handelt es sich um eine vorübergehende Arbeitslast, auf die in der Regel weniger Benutzer zugreifen, verglichen mit einer persistenten Arbeitslast wie einer CDP Data Warehouse-Arbeitslast, auf die viele Benutzer ununterbrochenen Zugriff benötigen. Data Engineering-Workloads sind nicht dauerhaft, wodurch die Auswirkungen auf das Geschäft minimiert werden, falls etwas schief geht. Diese	Leiter der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Aufgaben können jedoch für die Produktionsbericht erstattung von entscheidender Bedeutung sein. Priorisieren Sie daher zunächst Datenvera rbeitungs-Workloads mit geringen Auswirkungen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wiederholen Sie die Migrationsschritte nach Bedarf.	Cloudera Workload Manager hilft bei der Identifizierung von Workloads, die sich am besten für die Cloud eignen. Er bietet Kennzahlen wie Cloud-Leistungsbewertungen, Größen-/Kapazitätspläne für die Zielumgebung und Replikationspläne. Die besten Kandidaten für eine Migration sind saisonale Workloads, Ad-hoc-Berichte und zeitweilige Jobs, die nicht viele Ressourcen verbrauchen. Cloudera Replication Manager verschiebt Daten von lokalen Standorten in die Cloud und von der Cloud in lokale Umgebungen. Optimieren Sie mithilfe von Workload Manager proaktiv Workloads, Anwendungen, Leistung und Infrastrukturkapazität für Data Warehousing, Data Engineering und maschinelles Lernen. Eine vollständige Anleitung zur Modernisierung eines Data Warehouse finden Sie auf der Cloudera-Website.	Cloudera SME

Zugehörige Ressourcen

Cloudera-Dokumentation:

- Registrierung klassischer Cluster bei CDP, Cloudera Manager und Replication Manager:
  - Management-Konsole
  - Replication Manager: Hive-Replikation
- Sentry-Replikation
- Sentry-Berechtigungen
- Checkliste für die Planung von Data Hub-Clustern
- Workload Manager-Architektur
- Anforderungen für Replication Manager
- Beobachtbarkeit der Cloudera-Datenplattform
- AWS-Anforderungen

AWS-Dokumentation:

- Cloud-Datenmigration

Verbindungsfehler nach der Migration von Microsoft SQL Server zur AWS-Cloud beheben

Erstellt von Premkumar Chelladurai (AWS)

Übersicht

Nachdem Sie Microsoft SQL Server, der unter Windows Server 2008 R2, 2012 oder 2012 R2 ausgeführt wird, zu Amazon Elastic Compute Cloud (Amazon EC2) -Instances in der Amazon Web Services (AWS) -Cloud migriert haben, schlägt die Verbindung zu SQL Server fehl und die folgenden Fehler werden angezeigt:

- `[Microsoft][ODBC SQL Server Driver][DBNETLIB] General Network error`
- `ERROR [08S01] [Microsoft][SQL Native Client]Communication link failure. System.Data.SqlClient.SqlException: A transport-level error has occurred when sending the request to the server. (provider: TCP Provider, error: 0 - An existing connection was forcibly closed by the remote host.)`
- `TCP Provider: The semaphore timeout period has expired`

Dieses Muster beschreibt, wie Sie diese Fehler beheben können, indem Sie die Windows Scalable Networking Pack (SNP) -Features auf Betriebssystem- (OS) und Netzwerkschnittstellenebene für SQL Server deaktivieren, der unter Windows Server 2008 R2, 2012 oder 2012 R2 ausgeführt wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Administratorrechte für Windows Server.
- Wenn Sie AWS Application Migration Service als Migrationstool verwendet haben, benötigen Sie eine der folgenden Windows Server-Versionen:
  - Windows Server 2008 R2 Service Pack 1, 2012 oder 2012 R2
- Wenn Sie CloudEndure Migration als Migrationstool verwendet haben, benötigen Sie eine der folgenden Windows Server-Versionen:
  - Windows Server 2003 R2 Service Pack 3, 2008, 2008 R2 Service Pack 1, 2012 oder 2012 R2

Tools

- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können Amazon verwenden EC2 , um so viele oder so wenige virtuelle Server zu starten, wie Sie benötigen, und Sie können nach oben oder unten skalieren.
- Windows Server — Windows Server ist eine Plattform für den Aufbau einer Infrastruktur aus verbundenen Anwendungen, Netzwerken und Webdiensten.

Epen

Schalten Sie die SNP-Funktionen auf Betriebssystem- und elastic network interface Network-Schnittstellenebene aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schalten Sie die SNP-Funktionen auf Betriebssystemebene aus.	1. Melden Sie sich bei Windows Server an und öffnen Sie als Administrator eine Eingabeaufforderung. 2. Führen Sie den Befehl `netsh int tcp show global` aus. 3. Überprüfen Sie in der Ausgabe, ob sich entweder `Receive-Side Scaling` oder im `enabled` Modus `Chimney Offload` befindet. Wenn einer von ihnen der Fall ist`enabled`, führen Sie die folgenden Befehle aus: • `netsh int tcp set global chimney=disabled`	AWS-Administrator, AWS-Systemadministrator, Migrationsingenieur, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `netsh int tcp set global rss=disabled`	
Schalten Sie die SNP-Funktionen auf der Ebene der elastic network interface aus.	1. Wählen Sie Start, geben Sie die Eingabetaste ein `ncpa.cpl`, und drücken Sie dann die EINGABETASTE. 2. Rechtsklicken Sie auf Elastic Network Adapter. 3. Wählen Sie im Popup-Menü Eigenschaften. 4. Wählen Sie im Fenster mit den Eigenschaften des Ethernet-Adapters die Option Konfigurieren aus. 5. Wählen Sie im Popup-Fenster mit den Eigenschaften des Amazon Elastic Network Adapters die Registerkarte Erweitert aus. 6. Deaktivieren Sie im Bereich Property alle Offloads und RSS.	AWS-Administrator, Cloud-Administrator, AWS-Systemadministrator

Zugehörige Ressourcen

- Wie behebt man Probleme mit erweiterten Netzwerkleistungsfunktionen wie RSS und NetDMA

Starten Sie den AWS Replication Agent SELinux nach dem Neustart eines RHEL-Quellservers automatisch neu, ohne ihn zu deaktivieren.

Erstellt von Anil Kunapareddy (AWS), Shanmugam Shanker (AWS) und Venkatramana Chintha (AWS)

Übersicht

Der AWS Application Migration Service hilft Ihnen dabei, die Migration Ihres Red Hat Enterprise Linux (RHEL) -Workloads zur Amazon Web Services (AWS) Cloud zu vereinfachen, zu beschleunigen und zu automatisieren. Um Quellserver zu Application Migration Service hinzuzufügen, installieren Sie den AWS Replication Agent auf den Servern.

Der Application Migration Service bietet asynchrone Replikation auf Blockebene in Echtzeit. Das bedeutet, dass Sie während des gesamten Replikationsprozesses den normalen IT-Betrieb fortsetzen können. Diese IT-Operationen erfordern möglicherweise, dass Sie Ihren RHEL-Quellserver während der Migration neu starten oder neu starten. In diesem Fall wird der AWS Replication Agent nicht automatisch neu gestartet und Ihre Datenreplikation wird gestoppt. In der Regel können Sie Security-Enhanced Linux (SELinux) auf den deaktivierten oder permissiven Modus setzen, um den AWS Replication Agent automatisch neu zu starten. Die Sicherheitsrichtlinien Ihres Unternehmens verbieten jedoch möglicherweise die Deaktivierung SELinux, und Sie müssen Ihre Dateien möglicherweise auch neu kennzeichnen.

Dieses Muster beschreibt, wie Sie den AWS Replication Agent automatisch neu starten, ohne ihn auszuschalten, SELinux wenn Ihr RHEL-Quellserver neu gestartet wird oder während einer Migration neu gestartet wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein lokaler RHEL-Workload, den Sie in die AWS-Cloud migrieren möchten.
- Der Application Migration Service wurde über die Application Migration Service-Konsole initialisiert. Die Initialisierung ist nur erforderlich, wenn Sie diesen Dienst zum ersten Mal verwenden. Anweisungen finden Sie in der Dokumentation zum Application Migration Service.

- Eine bestehende AWS Identity and Access Management (IAM) -Richtlinie für den Application Migration Service. Weitere Informationen finden Sie in der Dokumentation zum Application Migration Service.

Versionen

- RHEL Version 7 oder höher

Tools

AWS-Services

- AWS Application Migration Service ist eine hochautomatisierte lift-and-shift (Rehost-) Lösung, die die Migration von Anwendungen zu AWS vereinfacht, beschleunigt und die Kosten senkt.

Linux-Befehle

Die folgende Tabelle enthält eine Liste der Linux-Befehle, die Sie auf Ihrem RHEL-Quellserver ausführen werden. Diese werden auch in den Epen und Geschichten zu diesem Muster beschrieben.

Befehl	Beschreibung
`#systemctl –version`	Identifiziert die Systemversion.
`#systemctl list-units --type=service`	Listet alle aktiven Dienste auf, die auf dem RHEL-Server verfügbar sind.
`#systemctl list-units --type=service | grep running`	Listet alle Dienste auf, die derzeit auf dem RHEL-Server ausgeführt werden.
`#systemctl list-units --type=service | grep failed`	Listet alle Dienste auf, die nach dem Neustart oder Neustart des RHEL-Servers nicht geladen werden konnten.
`restorecon -Rv /etc/rc.d/init.d/aws-replication-service`	Ändert den Kontext zu. `aws-replication-service`

`yum install policycoreutils*`	Installiert die wichtigsten Richtliniendienstp rogramme, die für den Betrieb des SELinux Systems erforderlich sind.
`ausearch -c "insmod" --raw | audit2allow -M my-modprobe`	Durchsucht das Auditprotokoll und erstellt ein Modul für Richtlinien.
`semodule -i my-modprobe.pp`	Aktiviert die Richtlinie.
`cat my-modprobe.te`	Zeigt den Inhalt der `my-modprobe.te` Datei an.
`semodule -l | grep my-modprobe`	Überprüft, ob die Richtlinie in das SELinux Modul geladen wurde.

Epen

Installieren Sie den AWS Replication Agent und starten Sie den RHEL-Quellserver neu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Application Migration Service-Benutzer mit einem Zugriffsschlüssel und einem geheimen Zugriffsschlüssel.	Um den AWS Replication Agent zu installieren, müssen Sie einen Application Migration Service-Benutzer mit den erforderlichen AWS-Anmeldeinformationen erstellen. Anweisungen finden Sie in der Dokumentation zum Application Migration Service.	Migrationsingenieur
Installieren Sie den AWS Replication Agent.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS Migration Service-Konsole zu https://console.aws.amazon.com/mgn/Hause.	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Konfigurieren Sie die Replikationseinstellungen, indem Sie den Anweisungen in der Dokumentation zum Application Migration Service folgen. 3. Installieren Sie den AWS Replication Agent, indem Sie den Anweisungen in der Dokumentation zum Application Migration Service folgen. 4. Wählen Sie auf der Seite Quellserver den RHEL-Quellserver und anschließend Replikation aus, um die erste Replikation zu starten. Weitere Informationen finden Sie in der Dokumentation zum Application Migration Service.	
Starten Sie den RHEL-Quellserver neu oder starten Sie ihn neu.	Starten Sie Ihren RHEL-Quellserver neu oder starten Sie ihn neu, wenn der Datenreplikationsstatus im Migrations-DashboardBlockiert angezeigt wird.	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Status der Datenreplikation.	Warten Sie eine Stunde und überprüfen Sie dann erneut den Status der Datenrepl ikation im Migrations-Dashboa rd. Es sollte sich im Status Fehlerfrei befinden.	Ingenieur für Migration

Überprüfen Sie den Status des AWS Replication Agents auf dem RHEL-Quellserver

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Systemversion.	Öffnen Sie die Befehlsze ilenschnittstelle für Ihren RHEL-Quellserver und führen Sie den folgenden Befehl aus, um die Systemversion zu identifizieren: `#systemctl –version`	Migrationsingenieur
Listet alle aktiven Dienste auf.	Führen Sie den folgenden Befehl aus, um alle aktiven Dienste aufzulisten, die auf dem RHEL-Server verfügbar sind: `#systemctl list-unit s --type=service`	Ingenieur für Migration
Listet alle laufenden Dienste auf.	Verwenden Sie den folgenden Befehl, um alle Dienste aufzulisten, die derzeit auf dem RHEL-Server ausgeführt werden:	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`#systemctl list-units --type=service | grep running`	
Listet alle Dienste auf, die nicht geladen werden konnten.	Um alle Dienste aufzulisten, die nach dem Neustart oder Neustart des RHEL-Servers nicht geladen werden konnten, führen Sie den folgenden Befehl aus: `#systemctl list-units --type=service | grep failed`	Ingenieur für Migration

Erstellen Sie das SELinux Modul und führen Sie es aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie den Sicherheitskontext.	Führen Sie in der Befehlszeilenschnittstelle für Ihren RHEL-Quellserver den folgenden Befehl aus, um den Sicherheitskontext auf den AWS-Replikationsservice zu ändern: `restorecon -Rv /etc/rc.d/init.d/aws-replication-service`	Migrationsingenieur
Installieren Sie die wichtigsten Dienstprogramme.	Führen Sie den folgenden Befehl aus, um die Kerndienstprogramme zu installieren, die für den Betrieb des SELinux	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Systems und seiner Richtlinien erforderlich sind: `yum install policycoreutils*`	
Durchsuchen Sie das Audit-Protokoll und erstellen Sie ein Modul für Richtlinien.	Führen Sie den Befehl aus: `ausearch -c "insmod" --raw | audit2allow -M my-modprobe`	Ingenieur für Migration
Zeigt den Inhalt der my-modprobe-te Datei an.	Die `my-modprobe.te` Datei wird mit dem Befehl audit2allow generiert. Sie umfasst die SELinux Domänen, das Quellverzeichnis der Richtlinie und die Unterverzeichnisse und spezifiziert die Zugriffsvektorregeln und Übergänge, die den Domänen zugeordnet sind. Führen Sie den folgenden Befehl aus, um den Inhalt der Datei anzuzeigen: `cat my modprobe.te`	Ingenieur für Migration
Aktivieren Sie die Richtlinie.	Führen Sie den folgenden Befehl aus, um das Modul einzufügen und das Richtlinienpaket zu aktivieren: `semodule -i my-modprobe.pp`	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Prüfen Sie, ob das Modul geladen wurde.	Führen Sie den Befehl aus: `semodule -l | grep my-modprobe` Nachdem das SELinux Modul geladen wurde, müssen Sie während Ihrer Migration nicht mehr in SELinux den deaktivierten oder permissiven Modus wechseln.	Ingenieur für Migration
Starten Sie den RHEL-Quellserver neu oder starten Sie ihn neu und überprüfen Sie den Status der Datenreplikation.	Öffnen Sie die AWS Migration Service Service-Konsole, navigieren Sie zu Status der Datenreplikation und starten Sie dann Ihren RHEL-Quellserver neu oder starten Sie ihn neu. Die Datenreplikation sollte jetzt automatisch fortgesetzt werden, nachdem der RHEL-Quellserver neu gestartet wurde.	Ingenieur für Migration

Zugehörige Ressourcen

- Dokumentation zum Service für die Anwendungsmigration
- Technisches Schulungsmaterial
- Behebung von Problemen mit dem AWS Replication Agent
- Richtlinien für den Service zur Anwendungsmigration

Re-Architekt

Themen

- Konvertiert VARCHAR2 (1) den Datentyp für Oracle in den booleschen Datentyp für Amazon Aurora PostgreSQL
- Anwendungsbenutzer und Rollen in Aurora PostgreSQL-Compatible erstellen
- Emulieren Sie Oracle DR mithilfe einer PostgreSQL-kompatiblen globalen Aurora-Datenbank
- Implementieren Sie SHA1 Hashing für PII-Daten bei der Migration von SQL Server zu PostgreSQL
- Schrittweise Migration von Amazon RDS for Oracle zu Amazon RDS for PostgreSQL mithilfe von Oracle SQL Developer und AWS SCT
- Laden Sie BLOB-Dateien in TEXT, indem Sie die Dateikodierung in Aurora PostgreSQL-kompatibel verwenden
- Migrieren Sie Amazon RDS for Oracle zu Amazon RDS for PostgreSQL mit AWS SCT und unter Verwendung von und AWS DMSAWS CLIAWS CloudFormation
- Migrieren Sie Amazon RDS for Oracle zu Amazon RDS for PostgreSQL im SSL-Modus mithilfe von AWS DMS
- Migrieren Sie Oracle SERIALLY_REUSABLE Pragma-Pakete nach PostgreSQL
- Migrieren Sie externe Oracle-Tabellen zu Amazon Aurora PostgreSQL-kompatibel
- Migrieren Sie funktionsbasierte Indizes von Oracle nach PostgreSQL
- Migrieren Sie native Oracle-Funktionen mithilfe von Erweiterungen zu PostgreSQL
- Migrieren Sie mithilfe von AWS DMS eine Db2-Datenbank von Amazon EC2 zu Aurora MySQL-kompatibel
- Migrieren Sie mithilfe von AWS DMS eine Microsoft SQL Server-Datenbank von Amazon EC2 zu Amazon DocumentDB
- Migrieren Sie eine lokale ThoughtSpot Falcon-Datenbank zu Amazon Redshift
- Migrieren Sie eine Oracle-Datenbank mit AWS DMS zu Amazon DynamoDB
- Migrieren Sie eine partitionierte Oracle-Tabelle mithilfe von AWS DMS zu PostgreSQL
- Migrieren Sie von Amazon RDS for Oracle zu Amazon RDS for MySQL
- Migrieren Sie mithilfe von AWS DMS und AWS SCT von IBM Db2 auf Amazon EC2 zu Aurora PostgreSQL-kompatibel
- Migrieren Sie mithilfe von AWS DMS von Oracle 8i oder 9i zu Amazon RDS for PostgreSQL SharePlex

- Migrieren Sie mithilfe von Materialized Views und AWS DMS von Oracle 8i oder 9i zu Amazon RDS for PostgreSQL
- Migrieren Sie mithilfe von AWS DMS und AWS SCT von Oracle auf Amazon EC2 zu Amazon RDS for MySQL
- Migrieren Sie mit AWS DMS von Oracle zu Amazon DocumentDB
- Migrieren Sie mithilfe von AWS DMS und AWS SCT eine Oracle-Datenbank von Amazon EC2 zu Amazon RDS for MariaDB
- Migrieren Sie eine lokale Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon RDS for MySQL
- Migrieren Sie eine lokale Oracle-Datenbank mithilfe eines Oracle-Bystanders und AWS DMS zu Amazon RDS for PostgreSQL
- Migrieren Sie mithilfe von Oracle von Oracle Database zu Amazon RDS for PostgreSQL GoldenGate
- Migrieren Sie eine Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon Redshift
- Migrieren Sie eine Oracle-Datenbank mit AWS DMS und AWS SCT zu Aurora PostgreSQL
- Migrieren Sie Daten von einer lokalen Oracle-Datenbank zu Aurora PostgreSQL
- Migrieren Sie mithilfe von AWS DMS von SAP ASE zu Amazon RDS for SQL Server
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mit AWS DMS zu Amazon Redshift
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mithilfe von AWS SCT-Datenextraktionsagenten zu Amazon Redshift
- Migrieren Sie eine Teradata-Datenbank mithilfe von AWS SCT-Datenextraktionsagenten zu Amazon Redshift
- Migrieren Sie eine lokale Vertica-Datenbank mithilfe von AWS SCT-Datenextraktionsagenten zu Amazon Redshift
- Migrieren Sie Legacy-Anwendungen von Oracle Pro*C zu ECPG
- Migrieren Sie virtuell generierte Spalten von Oracle nach PostgreSQL
- Richten Sie die Oracle UTL_FILE-Funktionalität auf Aurora PostgreSQL-Compatible ein
- Datenbankobjekte nach der Migration von Oracle zu Amazon Aurora PostgreSQL validieren

Konvertiert VARCHAR2 (1) den Datentyp für Oracle in den booleschen Datentyp für Amazon Aurora PostgreSQL

Erstellt von Naresh Damera (AWS)

Übersicht

Während einer Migration von Amazon Relational Database Service (Amazon RDS) for Oracle zu Amazon Aurora PostgreSQL-Compatible Edition kann es bei der Validierung der Migration in () zu einem Datenkonflikt kommen. AWS Database Migration Service AWS DMS Um diese Diskrepanz zu vermeiden, können Sie den Datentyp VARCHAR2 (1) in den booleschen Datentyp konvertieren.

VARCHAR2 Der Datentyp speichert Textzeichenfolgen variabler Länge, und VARCHAR2 (1) gibt an, dass die Zeichenfolge 1 Zeichen lang oder 1 Byte lang ist. Weitere Informationen zu VARCHAR2 finden Sie unter Integrierte Oracle-Datentypen (Oracle-Dokumentation).

In diesem Muster sind die Daten VARCHAR2 (1) in der Spalte der Beispielquellendatentabelle entweder Y für Ja oder N für Nein. Dieses Muster enthält Anweisungen zur Verwendung von AWS DMS und AWS Schema Conversion Tool (AWS SCT) zur Konvertierung dieses Datentyps von den Y - und N-Werten in VARCHAR2 (1) in die Werte Wahr oder Falsch in Boolean.

Beabsichtigte Zielgruppe

Dieses Muster wird für Benutzer empfohlen, die Erfahrung mit der Migration von Oracle-Datenbanken auf Aurora PostgreSQL-Compatible haben. AWS DMS Halten Sie sich beim Abschluss der Migration an die Empfehlungen unter Converting Oracle to Amazon RDS for PostgreSQL oder Amazon Aurora PostgreSQL (Dokumentation).AWS SCT

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver. AWS-Konto
- Vergewissern Sie sich, dass Ihre Umgebung für Aurora vorbereitet ist, einschließlich der Einrichtung von Anmeldeinformationen, Berechtigungen und einer Sicherheitsgruppe. Weitere Informationen finden Sie unter Einrichten Ihrer Umgebung für Amazon Aurora (Aurora-Dokumentation).
- Eine Amazon RDS for Oracle Oracle-Quelldatenbank, die eine Tabellenspalte mit VARCHAR2 (1) Daten enthält.

- Eine mit Amazon Aurora PostgreSQL kompatible Zieldatenbank-Instance. Weitere Informationen finden Sie unter Einen Datenbank-Cluster erstellen und eine Verbindung zu einer Datenbank auf einem Aurora PostgreSQL-Datenbank-Cluster herstellen (Aurora-Dokumentation).

Produktversionen

- Amazon RDS for Oracle Version 12.1.0.2 oder höher.
- AWS DMS Version 3.1.4 oder höher. Weitere Informationen finden Sie unter Verwenden einer Oracle-Datenbank als Quelle für AWS DMS und Verwenden einer PostgreSQL-Datenbank als Ziel für AWS DMS (AWS DMS Dokumentation). Wir empfehlen Ihnen, die neueste Version von zu verwenden, um die umfassendste AWS DMS Versions- und Funktionsunterstützung zu erhalten.
- AWS Schema Conversion Tool (AWS SCT) Version 1.0.632 oder höher. Wir empfehlen Ihnen, die neueste Version von zu verwenden, um die umfassendste AWS SCT Versions- und Funktionsunterstützung zu erhalten.
- Aurora unterstützt die PostgreSQL-Versionen, die unter Database Engine Versions for Aurora PostgreSQL-compatible (Aurora-Dokumentation) aufgeführt sind.

Architektur

Quelltechnologie-Stack

Amazon RDS for Oracle Oracle-Datenbank-Instance

Zieltechnologie-Stack

Amazon Aurora PostgreSQL-kompatible Datenbank-Instance

Quell- und Zielarchitektur

Tools

AWS-Services

- Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt.
- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die oder zwischen Kombinationen von Cloud- und lokalen Setups. AWS Cloud

- Amazon Relational Database Service (Amazon RDS) für Oracle unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Oracle-Datenbank in der. AWS Cloud
- AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein mit der Zieldatenbank kompatibles Format konvertiert werden.

Andere Dienste

- Oracle SQL Developer ist eine integrierte Entwicklungsumgebung, die die Entwicklung und Verwaltung von Oracle-Datenbanken sowohl in herkömmlichen als auch in Cloud-basierten Bereitstellungen vereinfacht. In diesem Muster verwenden Sie dieses Tool, um eine Verbindung zur Amazon RDS for Oracle Oracle-Datenbank-Instance herzustellen und die Daten abzufragen.
- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL. Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, verwalten und verwenden können. In diesem Muster verwenden Sie dieses Tool, um eine Verbindung zur Aurora-Datenbank-Instance herzustellen und die Daten abzufragen.

Epen

Bereite dich auf die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Datenbank migrationsbericht.	1. Erstellen Sie AWS SCT unter einen Bewertung sbericht zur Datenbank migration. Weitere Informati onen finden Sie unter Bewertungsberichte zur Migration erstellen. 2. Überprüfen Sie die Aktionspunkte im Bericht zur Migrationsbewertun g und führen Sie sie aus. Weitere Informationen finden Sie unter Aktionspu	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	nkte des Bewertung sberichts.	
Deaktivieren Sie Fremdschl üsseleinschränkungen für die Zieldatenbank.	In PostgreSQL werden Fremdschlüssel mithilfe von Triggern implementiert. AWS DMS Lädt während der Vollladephase jede Tabelle einzeln. Es wird dringend empfohlen, Fremdschl üsseleinschränkungen während des Vollladens zu deaktivieren, indem Sie eine der folgenden Methoden verwenden: • Deaktivieren Sie vorüberge hend alle Auslöser aus der Instance und beenden Sie den vollständigen Ladevorgang. • Verwenden Sie den `session_replicatio n_role` -Parameter in PostgreSQL. Wenn das Deaktivieren von Fremdschlüsseleinschränkung en nicht möglich ist, erstellen Sie eine AWS DMS Migration saufgabe für die Primärdat en, die für die übergeordnete Tabelle und die untergeor dnete Tabelle spezifisch ist.	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Deaktivieren Sie die Primärschlüssel und eindeutigen Schlüssel in der Zieldatenbank.	Deaktivieren Sie mit den folgenden Befehlen die Primärschlüssel und Einschränkungen in der Zieldatenbank. Dies trägt dazu bei, die Leistung der ersten Ladeaufgabe zu verbessern.
	`ALTER TABLE <table> DISABLE PRIMARY KEY;`
	`ALTER TABLE <table> DISABLE CONSTRAINT <constraint_name>;`
		DBA, Entwickler

Erstellen Sie die erste Ladeaufgabe.	Erstellen Sie unter die Migrationsaufgabe für das erste Laden. AWS DMS Anweisungen finden Sie unter Aufgabe erstellen. Wählen Sie für die Migrationsmethode die Option Bestehende Daten migrieren aus. Diese Migrationsmethode wird `Full Load` in der API aufgerufen. Starten Sie diese Aufgabe noch nicht.	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bearbeiten Sie die Aufgabene instellungen für die erste Ladeaufgabe.	Bearbeiten Sie die Aufgabene instellungen, um eine Datenvalidierung hinzuzufü gen. Diese Validierungseinste llungen müssen in einer JSON-Datei erstellt werden. Anweisungen und Beispiele finden Sie unter Aufgabene instellungen angeben. Fügen Sie die folgenden Validieru ngen hinzu: • Um zu überprüfen, ob die VARCHAR2 (1) -Daten in der Zieldatenbank korrekt in boolesche Werte konvertiert wurden, fügen Sie den Code im Datenüber prüfungsskript im Abschnitt Zusätzliche Informationen dieses Musters hinzu. Das Überprüfungsskript konvertiert die boolesche n Werte von 1 in Y und 0 in N in der Zieltabelle und vergleicht dann die Werte in der Zieltabelle mit der Quelltabelle. Um den Rest der Datenmigr ation zu validieren, aktiviere n Sie die Datenvalidierung in der Aufgabe. Weitere Informationen finden Sie unter	AWS-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Einstellungen für die Datenvalidierungsaufgabe.	
Erstellen Sie die laufende Replikationsaufgabe.	Erstellen Sie in AWS DMS die Migrationsaufgabe, die dafür sorgt, dass die Zieldatenbank mit der Quelldatenbank synchronisiert wird. Anweisungen finden Sie unter Aufgabe erstellen. Wählen Sie als Migrationsmethode die Option Nur Datenänderungen replizieren aus. Starten Sie diese Aufgabe noch nicht.	DBA

Testen Sie die Migrationsaufgaben

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Beispieldaten zum Testen.	Erstellen Sie in der Quelldatenbank eine Beispieltabelle mit Daten für Testzwecke.	Developer
Vergewissern Sie sich, dass keine widersprüchlichen Aktivitäten vorliegen.	Verwenden Sie denpg_stat_activity , um nach Aktivitäten auf dem Server zu suchen, die sich auf die Migration auswirken könnten. Weitere Informationen finden Sie unter The Statistics Collector (PostgreSQL-Dokumentation).	AWS-Administrator
Starten Sie die AWS DMS Migrationsaufgaben.	Starten Sie in der AWS DMS Konsole auf der Dashboard-	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Seite die Aufgaben zum ersten Laden und zur laufenden Replikation, die Sie im vorherigen Epic erstellt haben.	
Überwachen Sie die Aufgaben und den Ladestatus der Tabelle.	Überwachen Sie während der Migration den Aufgabenstatus und den Tabellenstatus. Wenn die erste Ladeaufgabe abgeschlossen ist, gehen Sie auf der Registerkarte Tabellenstatistiken wie folgt vor: • Der Ladestatus sollte „Tabelle abgeschlossen“ lauten. • Der Status „Validierung“ sollte „Validiert“ lauten.	AWS-Administrator
Überprüfen Sie die Migrationsergebnisse.	Fragen Sie mit pgAdmin die Tabelle in der Zieldatenbank ab. Eine erfolgreiche Abfrage zeigt an, dass die Daten erfolgreich migriert wurden.	Developer
Fügen Sie Primärschlüssel und Fremdschlüssel zur Zieldatenbank hinzu.	Erstellen Sie den Primärschlüssel und den Fremdschlüssel in der Zieldatenbank. Weitere Informationen finden Sie unter ALTER TABLE (PostgreSQL-Website).	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen Sie die Testdaten.	Bereinigen Sie in den Quell- und Zieldatenbanken Daten, die für Komponententests erstellt wurden.	Developer

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schließen Sie die Migration ab.	Wiederholen Sie das vorherige Epic, Testen Sie die Migration saufgaben, und verwenden Sie dabei die echten Quelldaten. Dadurch werden die Daten von der Quell- zur Zieldatenbank migriert.	Developer
Stellen Sie sicher, dass die Quell- und Zieldatenbanken synchron sind.	Stellen Sie sicher, dass die Quell- und Zieldatenbanken synchron sind. Weitere Informationen und Anweisungen finden Sie unter AWS DMS Datenvalidierung.	Developer
Stoppen Sie die Quelldatenbank.	Stoppen Sie die Amazon RDS for Oracle Oracle-Datenbank. Anweisungen finden Sie unter Vorübergehendes Stoppen einer Amazon RDS-DB-Instance. Wenn Sie die Quelldatenbank beenden, werden das anfängliche Laden und die laufenden Replikationsaufgaben in AWS DMS automatisch gestoppt.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Es sind keine zusätzlichen Maßnahmen erforderlich, um diese Aufgaben zu beenden.	

Zugehörige Ressourcen

AWS Verweise

- Migrieren Sie eine Oracle-Datenbank mit AWS DMS und zu Aurora PostgreSQL AWS SCT (AWS Prescriptive Guidance)
- Konvertierung von Oracle zu Amazon RDS for PostgreSQL oder Amazon Aurora PostgreSQL (Dokumentation)AWS SCT
- Wie funktioniert AWS DMS (Dokumentation)AWS DMS

Andere Referenzen

- Boolescher Datentyp (PostgreSQL-Dokumentation)
- Integrierte Oracle-Datentypen (Oracle-Dokumentation)
- pgAdmin (pgAdmin-Webseite)
- SQL-Entwickler (Oracle-Website)

Tutorials und Videos

- Erste Schritte mit AWS DMS
- Erste Schritte mit Amazon RDS
- Einführung in AWS DMS (Video)
- Amazon RDS verstehen (Video)

Zusätzliche Informationen

Skript zur Datenvalidierung

Das folgende Datenüberprüfungsskript konvertiert 1 in Y und 0 in N. Dies hilft der AWS DMS Aufgabe, die Tabellenüberprüfung erfolgreich abzuschließen und zu bestehen.

```
{
"rule-type": "validation",
"rule-id": "5",
"rule-name": "5",
"rule-target": "column",
"object-locator": {
"schema-name": "ADMIN",
"table-name": "TEMP_CHRA_BOOL",
"column-name": "GRADE"
},
"rule-action": "override-validation-function",
"target-function": "case grade when '1' then 'Y' else 'N' end"
        }
```

Die `case` Anweisung im Skript führt die Validierung durch. Wenn die Validierung fehlschlägt, wird ein Datensatz in die Tabelle public.awsdms_validation_failures_v1 auf der Zieldatenbankinstanz AWS DMS eingefügt. Dieser Datensatz enthält den Tabellennamen, die Fehlerzeit und Details zu den nicht übereinstimmenden Werten in der Quell- und Zieltabelle.

Wenn Sie dieses Datenüberprüfungsskript nicht zur AWS DMS Aufgabe hinzufügen und die Daten in die Zieltabelle eingefügt werden, zeigt die AWS DMS Aufgabe den Validierungsstatus als Nicht übereinstimmende Datensätze an.

Während der AWS SCT Konvertierung ändert die AWS DMS Migrationsaufgabe den Datentyp des Datentyps VARCHAR2 (1) in Boolean und fügt der Spalte eine Primärschlüsseleinschränkung hinzu. `"N0"`

Anwendungsbenutzer und Rollen in Aurora PostgreSQL-Compatible erstellen

Erstellt von Abhishek Verma (AWS)

Übersicht

Wenn Sie zu Amazon Aurora PostgreSQL-Compatible Edition migrieren, müssen die Datenbankbenutzer und Rollen, die in der Quelldatenbank vorhanden sind, in der Aurora PostgreSQL-kompatiblen Datenbank erstellt werden. Sie können die Benutzer und Rollen in Aurora PostgreSQL-kompatibel erstellen, indem Sie zwei verschiedene Ansätze verwenden:

- Verwenden Sie in der Zieldatenbank ähnliche Benutzer und Rollen wie in der Quelldatenbank. Bei diesem Ansatz werden die Datendefinitionssprachen (DDLs) für Benutzer und Rollen aus der Quelldatenbank extrahiert. Anschließend werden sie transformiert und auf die Aurora PostgreSQL-kompatible Zieldatenbank angewendet. Der Blogbeitrag Verwenden Sie SQL, um Benutzer, Rollen und Zuschüsse von Oracle zu PostgreSQL zuzuordnen, behandelt beispielsweise die Verwendung der Extraktion aus einer Oracle-Quelldatenbank-Engine.
- Verwenden Sie standardisierte Benutzer und Rollen, die häufig bei der Entwicklung, Verwaltung und Durchführung anderer verwandter Operationen in der Datenbank verwendet werden. Dazu gehören Schreibschutz, Lese-/Schreibvorgänge, Entwicklungs-, Verwaltungs- und Bereitstellungsvorgänge, die von den jeweiligen Benutzern ausgeführt werden.

Dieses Muster enthält die Grants, die für die Erstellung von Benutzern und Rollen in Aurora PostgreSQL-kompatibel erforderlich sind und für den standardisierten Benutzer- und Rollenansatz erforderlich sind. Die Schritte zur Benutzer- und Rollenerstellung orientieren sich an der Sicherheitsrichtlinie, den Datenbankbenutzern die geringsten Rechte zu gewähren. In der folgenden Tabelle sind die Benutzer, ihre entsprechenden Rollen und ihre Details in der Datenbank aufgeführt.

Benutzer	Rollen	Zweck
`APP_read`	`APP_RO`	Wird für den schreibgeschützten Zugriff auf das Schema verwendet `APP`
`APP_WRITE`	`APP_RW`	Wird für Schreib- und Lesevorgänge auf dem Schema verwendet `APP`

`APP_dev_user`	`APP_DEV`	Wird für Entwicklungszwecke im Schema verwendet `APP_DEV`, mit schreibgeschütztem Zugriff auf das Schema `APP`
`Admin_User`	`rds_superuser`	Wird für die Ausführung von Administratoroperationen an der Datenbank verwendet
`APP`	`APP_DEP`	Wird für die Erstellung der Objekte unter dem `APP` Schema und für die Bereitstellung von Objekten im `APP` Schema verwendet

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS) -Konto
- Eine PostgreSQL-Datenbank, Amazon Aurora PostgreSQL-Compatible Edition-Datenbank oder Amazon Relational Database Service (Amazon RDS) für PostgreSQL-Datenbank

Produktversionen

- Alle Versionen von PostgreSQL

Architektur

Quelltechnologie-Stack

- Beliebige Datenbank

Zieltechnologie-Stack

- Amazon Aurora PostgreSQL-kompatibel

Zielarchitektur

Das folgende Diagramm zeigt Benutzerrollen und die Schemaarchitektur in der Aurora PostgreSQL-kompatiblen Datenbank.

Automatisierung und Skalierung

Dieses Muster enthält die Benutzer, Rollen und das Skript zur Schemaerstellung, das Sie mehrfach ausführen können, ohne dass dies Auswirkungen auf bestehende Benutzer der Quell- oder Zieldatenbank hat.

Tools

AWS-Services

- Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt.

Andere Dienste

- psql ist ein terminalbasiertes Frontend-Tool, das bei jeder PostgreSQL-Datenbankinstallation installiert wird. Es verfügt über eine Befehlszeilenschnittstelle zum Ausführen von SQL-, PL-PGSQL- und Betriebssystembefehlen.
- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL. Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, verwalten und verwenden können.

Epen

Erstellen Sie die Benutzer und Rollen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Deployment-Benutzer.	Der Deployment-Benutzer APP wird verwendet, um die Datenbankobjekte während	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	der Bereitstellung zu erstellen und zu ändern. Verwenden Sie die folgenden Skripts, um die Deployment-Benutzerrolle APP_DEP im Schema APP zu erstellen. Überprüfen Sie die Zugriffsrechte, um sicherzustellen, dass dieser Benutzer nur berechtigt ist, Objekte im erforderlichen Schema zu erstellenAPP.
	
	1. Stellen Sie eine Verbindung mit dem Admin-Benutzer her und erstellen Sie das Schema.
	
	`CREATE SCHEMA APP;`
	
	2. Erstellen Sie den Benutzer.
	
	`CREATE USER APP WITH PASSWORD <password> ;`
	
	3. Erstellen Sie die -Rolle.
	
	`CREATE ROLE APP_DEP ;`
	`GRANT all on schema APP to APP_DEP ;`
	`GRANT USAGE ON SCHEMA APP to APP_DEP ;`
	`GRANT connect on database <db_name> to APP_DEP ;`
	`GRANT APP_DEP to APP;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	4. Um die Rechte zu testen, stellen Sie eine Verbindung zu den Tabellen her APP und erstellen Sie sie.
	
	`set search_path to APP;`
	`SET`
	`CREATE TABLE test(id integer ) ;`
	`CREATE TABLE`
	
	5. Überprüfen Sie die Rechte.
	
	`select schemaname , tablename , tableowner from pg_tables where tablename like 'test' ;`
	`schemaname | tablename | tableowner`
	`APP | test | APP`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den schreibge schützten Benutzer.	Der schreibgeschützte Benutzer APP_read wird für die Ausführung des schreibge schützten Vorgangs im Schema verwendet. APP Verwenden Sie die folgenden Skripten, um den schreibge schützten Benutzer zu erstellen. Überprüfen Sie die Zugriffsrechte, um sicherzus tellen, dass dieser Benutzer nur berechtigt ist, die Objekte im Schema zu lesen APP und allen neuen Objekten, die im Schema erstellt wurden, automatisch Lesezugriff zu gewähren. APP
	
	1. Erstellen Sie den BenutzerAPP_read.
	
	`create user APP_read ;`
	`alter user APP_read`
	`with password`
	`'your_password' ;`
	
	2. Erstellen Sie die -Rolle.
	
	`CREATE ROLE APP_ro ;`
	`GRANT SELECT ON ALL`
	`TABLES IN SCHEMA APP`
	`TO APP_RO ;`
	`GRANT USAGE ON SCHEMA`
	`APP TO APP_RO`
	`GRANT CONNECT ON`
	`DATABASE testdb TO`
	`APP_RO ;`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`GRANT APP_RO TO APP_read;`
	3. Um die Rechte zu testen, melden Sie sich mit dem `APP_read` Benutzer an.
	`set search_path to APP ;`
	`create table test1( id integer) ;`
	`ERROR: permission denied for schema APP`
	`LINE 1: create table test1( id integer) ;`
	`insert into test values (34) ;`
	`ERROR: permission denied for table test SQL state: 42501`
	`select from test`
	`no rows selected`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den Benutzer mit Lese-/Schreibzugriff.	Der Benutzer mit Lese-/Schreibzugriff `APP_WRITE` wird verwendet, um Lese- und Schreiboperationen im Schema auszuführen. `APP` Verwenden Sie die folgenden Skripten, um den Lese-/Schreibbenutzer zu erstellen und ihm die Rolle zuzuweisen. `APP_RW` Überprüfen Sie die Zugriffsrechte, um sicherzustellen, dass dieser Benutzer nur Lese- und Schreibrechte für die Objekte im Schema hat, `APP` und um jedem neuen Objekt, das im Schema erstellt wurde, automatisch Lese- und Schreibzugriff zu gewähren. `APP`
	
	1. Erstellen Sie den Benutzer.
	
	`CREATE USER APP_WRITE ; alter user APP_WRITE with password 'your_password' ;`
	
	2. Erstellen Sie die -Rolle.
	
	`CREATE ROLE APP_RW; GRANT SELECT, INSERT, UPDATE, DELETE ON ALL TABLES IN SCHEMA APP TO APP_RW ;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>GRANT CONNECT ON
	 DATABASE postgres to
	 APP_RW ;
	GRANT USAGE ON SCHEMA
	 APP to APP_RW ;
	ALTER DEFAULT
	 PRIVILEGES IN SCHEMA
	 APP
	GRANT SELECT, INSERT,
	 UPDATE, DELETE ON
	 TABLES TO APP_RW ;
	GRANT APP_RW to
	 APP_WRITE</pre>	

	3. Um die Rechte zu testen, melden Sie sich mit dem `APP_WRITE` Benutzer an.
	<pre>SET SEARCH_PATH to
	 APP;
	CREATE TABLE
	 test1(id integer) ;
	ERROR: permission
	 denied for schema APP
	LINE 1: create table
	 test1(id integer) ;
	SELECT * FROM test ;
	id
	---- 	
	12
	INSERT INTO test
	 values (31) ;
	INSERT 0 1</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den Admin-Benutzer.	Der Admin-Benutzer `Admin_User` wird verwendet, um Admin-Operationen an der Datenbank durchzuführen. Beispiele für diese Operationen sind `CREATE ROLE` und`CREATE DATABASE`. `Admin_User` verwendet die integrierte Rolle`rds_superuser`, um Admin-Operationen in der Datenbank durchzuführen. Verwenden Sie die folgenden Skripts, um die Rechte für den Admin-Benutzer `Admin_User` in der Datenbank zu erstellen und zu testen.
	1. Erstellen Sie den Benutzer und gewähren Sie ihm die Rolle.
	`create user Admin_User WITH PASSWORD ‘Your password’`
	`ALTER user Admin_user CREATEDB;`
	`ALTER user Admin_user CREATEROLE;`
	2. Um das Recht zu testen, melden Sie sich vom `Admin_User` Benutzer aus an.
	`SELECT * FROM APP.test ;`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> id
	  ---- 	
	   31
	CREATE ROLE TEST ;
	CREATE DATABASE
	 test123 ;</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den Entwicklungsbenutzer.	Der Entwicklungsbenutzer `APP_dev_user` erhält die Rechte, die Objekte in seinem lokalen Schema zu erstellen `APP_DEV` und über Lesezugriff im Schema zu verfügen`APP`. Verwenden Sie die folgenden Skripten, um die Rechte des Benutzers `APP_dev_user` in der Datenbank zu erstellen und zu testen.
	1. Erstellen Sie den Benutzer.
	`CREATE USER APP1_dev_user with password ‘your password’;`
	2. Erstellen Sie das `APP_DEV` Schema für die`App_dev_user` .
	`CREATE SCHEMA APP1_DEV ;`
	3. Erstellen Sie die `APP_DEV`-Rolle.
	`CREATE ROLE APP1_DEV ;`
	`GRANT APP1_RO to APP1_DEV ;`
	`GRANT SELECT ON ALL TABLES IN SCHEMA APP1_DEV to APP1_dev_user`
	`GRANT USAGE, CREATE ON SCHEMA APP1_DEV to APP1_DEV_USER`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`GRANT APP1_DEV to APP1_DEV_USER ;`
	4. Um die Rechte zu testen, melden Sie sich von an`APP_dev_user` .
	`CREATE TABLE APP1_dev.test1( id integer ) ;`
	`CREATE TABLE`
	`INSERT into APP1_dev.test1 ( select * from APP1.test );`
	`INSERT 0 1`
	`CREATE TABLE APP1.test4 ( id int) ;`
	`ERROR: permission denied for schema APP1`
	`LINE 1: create table APP1.test4 ( id int) ;`	

Zugehörige Ressourcen

PostgreSQL-Dokumentation

- ROLLE ERSTELLEN
- BENUTZER ERSTELLEN
- Vordefinierte Rollen

Zusätzliche Informationen

Erweiterung von PostgreSQL 14

PostgreSQL 14 bietet eine Reihe vordefinierter Rollen, die den Zugriff auf bestimmte häufig benötigte, privilegierte Funktionen und Informationen ermöglichen. Administratoren (einschließlich Rollen mit entsprechenden Rechten`CREATE ROLE`) können Benutzern diese Rollen oder andere Rollen in ihrer Umgebung zuweisen und ihnen so Zugriff auf die angegebenen Funktionen und Informationen gewähren.

Administratoren können Benutzern mithilfe des `GRANT` Befehls Zugriff auf diese Rollen gewähren. Um beispielsweise die `pg_signal_backend` Rolle zu erteilen`Admin_User`, können Sie den folgenden Befehl ausführen.

```
GRANT pg_signal_backend TO Admin_User;
```

Die `pg_signal_backend` Rolle soll es Administratoren ermöglichen, vertrauenswürdigen Rollen ohne Superuser das Senden von Signalen an andere Back-Ends zu ermöglichen. Weitere Informationen finden Sie unter PostgreSQL 14-Erweiterung.

Feinabstimmung des Zugriffs

In einigen Fällen kann es erforderlich sein, den Benutzern einen detaillierteren Zugriff zu gewähren (z. B. tabellenbasierter Zugriff oder spaltenbasierter Zugriff). In solchen Fällen können zusätzliche Rollen erstellt werden, um den Benutzern diese Rechte zu gewähren. Weitere Informationen finden Sie unter PostgreSQL Grants.

Emulieren Sie Oracle DR mithilfe einer PostgreSQL-kompatiblen globalen Aurora-Datenbank

Erstellt von HariKrishna Boorgadda (AWS)

Übersicht

Bewährte Methoden für Disaster Recovery (DR) in Unternehmen bestehen im Wesentlichen darin, fehlertolerante Hardware- und Softwaresysteme zu entwickeln und zu implementieren, die einen Notfall überstehen (Geschäftskontinuität) und den normalen Betrieb wieder aufnehmen können (Wiederaufnahme des Geschäftsbetriebs), und zwar mit minimalen Eingriffen und idealerweise ohne Datenverlust. Der Aufbau fehlertoleranter Umgebungen zur Erfüllung der DR-Ziele von Unternehmen kann teuer und zeitaufwändig sein und erfordert ein starkes Engagement des Unternehmens.

Oracle Database bietet drei verschiedene Ansätze für DR, die im Vergleich zu anderen Ansätzen zum Schutz von Oracle-Daten das höchste Maß an Datenschutz und Verfügbarkeit bieten.

- Oracle Zero Data Loss Recovery Appliance
- Oracle Active Data Guard
- Oracle GoldenGate

Dieses Muster bietet eine Möglichkeit, Oracle GoldenGate DR mithilfe einer globalen Amazon Aurora Aurora-Datenbank zu emulieren. Die Referenzarchitektur verwendet Oracle GoldenGate für DR in drei AWS-Regionen. Das Muster führt durch die Umstellung der Quellarchitektur auf die Cloud-native globale Aurora-Datenbank, die auf der Amazon Aurora PostgreSQL-Compatible Edition basiert.

Die globalen Aurora-Datenbanken sind für Anwendungen mit globaler Präsenz konzipiert. Eine einzelne Aurora-Datenbank umfasst mehrere AWS-Regionen mit bis zu fünf sekundären Regionen. Die globalen Aurora-Datenbanken bieten die folgenden Funktionen:

- Replizierung auf physischer Speicherebene
- Globale Lesevorgänge mit geringer Latenz
- Schnelle Notfallwiederherstellung nach Ausfällen in der gesamten Region
- Schnelle regionsübergreifende Migrationen
- Geringe Replikationsverzögerung zwischen Regionen
- Little-to-no Auswirkung auf die Leistung Ihrer Datenbank

Weitere Informationen zu den Funktionen und Vorteilen der globalen Aurora-Datenbank finden Sie unter Verwenden globaler Amazon Aurora Aurora-Datenbanken. Weitere Informationen zu ungeplanten und verwalteten Failovers finden Sie unter Verwenden von Failover in einer globalen Amazon Aurora Aurora-Datenbank.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Java Database Connectivity (JDBC) PostgreSQL-Treiber für Anwendungskonnektivität
- Eine globale Aurora-Datenbank, die auf der Amazon Aurora PostgreSQL-kompatiblen Edition basiert
- Eine Oracle Real Application Clusters (RAC) -Datenbank wurde auf die globale Aurora-Datenbank migriert, die auf Aurora PostgreSQL-kompatibel ist

Einschränkungen der globalen Aurora-Datenbanken

- Die globalen Aurora-Datenbanken sind nicht in allen AWS-Regionen verfügbar. Eine Liste der unterstützten Regionen finden Sie unter Globale Aurora-Datenbanken mit Aurora PostgreSQL.
- Informationen zu Funktionen, die nicht unterstützt werden, und zu anderen Einschränkungen der globalen Aurora-Datenbanken finden Sie unter Einschränkungen der globalen Amazon Aurora Aurora-Datenbanken.

Produktversionen

- Amazon Aurora PostgreSQL — Compatible Edition Version 10.14 oder höher

Architektur

Quelltechnologie-Stack

- Oracle RAC-Datenbank mit vier Knoten
- Oracle GoldenGate

Quellarchitektur

Das folgende Diagramm zeigt drei Cluster mit Oracle RAC mit vier Knoten in verschiedenen AWS-Regionen, die mit Oracle repliziert wurden. GoldenGate

Zieltechnologie-Stack

- Eine globale Amazon Aurora Aurora-Datenbank mit drei Clustern, die auf Aurora PostgreSQL basiert — kompatibel, mit einem Cluster in der primären Region, zwei Clustern in verschiedenen sekundären Regionen

Zielarchitektur

Tools

AWS-Services

- Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt.
- Die globalen Datenbanken von Amazon Aurora erstrecken sich über mehrere AWS-Regionen und bieten globale Lesevorgänge mit geringer Latenz und eine schnelle Wiederherstellung nach dem seltenen Ausfall, der eine gesamte AWS-Region betreffen kann.

Epen

Fügen Sie Regionen mit Reader-DB-Instances hinzu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Hängen Sie einen oder mehrere sekundäre Aurora-Cluster an.	Wählen Sie in der AWS-Managementkonsole Amazon Aurora aus. Wählen Sie den primären Cluster aus, wählen Sie Aktionen und dann Region hinzufügen aus der Drop-down-Liste aus.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie die Instanzklasse aus.	Sie können die Instanzklasse des sekundären Clusters ändern. Wir empfehlen jedoch, dieselbe wie die Instance-Klasse des primären Clusters beizubehalten.	DBA
Fügen Sie die dritte Region hinzu.	Wiederhole die Schritte in diesem Epos, um einen Cluster in der dritten Region hinzuzufügen.	DBA

Failover der globalen Aurora-Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie den primären Cluster aus der globalen Aurora-Datenbank.	1. Wählen Sie auf der Seite Datenbanken den primären Cluster aus. 2. Wählen Sie Aus Global entfernen, um ein Failover zu einem sekundären Cluster durchzuführen.	DBA
Konfigurieren Sie Ihre Anwendung neu, um den Schreibdatenverkehr an den gerade hochgestuften Cluster weiterzuleiten.	Ändern Sie den Endpunkt in der Anwendung mit dem Endpunkt des neu hochgestuften Clusters.	DBA
Beenden Sie die Ausführung von Schreibvorgängen für den nicht verfügbaren Cluster.	Beenden Sie die Anwendung und jegliche DML-Aktivitäten (Data Manipulation Language)	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	für den Cluster, den Sie entfernt haben.	
Erstellen Sie eine neue globale Aurora-Datenbank.	Jetzt können Sie eine globale Aurora-Datenbank mit dem neu beworbenen Cluster als primärem Cluster erstellen.	DBA

Starten Sie den primären Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie den primären Cluster aus, der aus der globalen Datenbank gestartet werden soll.	Wählen Sie auf der Amazon Aurora Aurora-Konsole im Global Database-Setup den primären Cluster aus.	DBA
Starten Sie den Cluster.	Wählen Sie in der Dropdownl iste Aktionen die Option Start aus. Dieser Vorgang kann einige Zeit in Anspruch nehmen. Aktualisieren Sie den Bildschirm, um den Status zu sehen, oder überprüfen Sie nach Abschluss des Vorgangs in der Spalte Status den aktuellen Status des Clusters.	DBA

Säubere die Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die verbleibenden sekundären Cluster.	Entfernen Sie nach Abschluss des Failover-Pilotprojekts die	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	sekundären Cluster aus der globalen Datenbank.	
Löschen Sie den primären Cluster.	Entfernen Sie den Cluster.	DBA

Zugehörige Ressourcen

- Verwenden von Amazon Aurora Global Databases
- Aurora PostgreSQL Disaster Recovery-Lösungen mit Amazon Aurora Global Database (Blogbeitrag)

Implementieren Sie SHA1 Hashing für PII-Daten bei der Migration von SQL Server zu PostgreSQL

Erstellt von Rajkumar Raghuwanshi (AWS) und Jagadish Kantubugata (AWS)

Übersicht

Dieses Muster beschreibt, wie Secure Hash Algorithm 1 (SHA1) -Hashing für E-Mail-Adressen implementiert wird, wenn von SQL Server zu Amazon RDS for PostgreSQL oder Amazon Aurora PostgreSQL-kompatibel migriert wird. Eine E-Mail-Adresse ist ein Beispiel für persönlich identifizierbare Informationen (PII). PII sind Informationen, die, wenn sie direkt betrachtet oder mit anderen verwandten Daten kombiniert werden, verwendet werden können, um vernünftige Rückschlüsse auf die Identität einer Person zu ziehen.

Dieses Muster deckt die Herausforderungen ab, die mit der Aufrechterhaltung konsistenter Hashwerte für verschiedene Datenbankkollationen und Zeichenkodierungen verbunden sind, und bietet eine Lösung mithilfe von PostgreSQL-Funktionen und -Triggern. Dieses Muster konzentriert sich zwar auf SHA1 Hashing, kann aber für andere Hashing-Algorithmen angepasst werden, die vom PostgreSQL-Modul unterstützt werden. `pgcrypto` Berücksichtigen Sie immer die Auswirkungen Ihrer Hashing-Strategie auf die Sicherheit und wenden Sie sich beim Umgang mit sensiblen Daten an Sicherheitsexperten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Quell-SQL Server-Datenbank
- PostgreSQL-Zieldatenbank (Amazon RDS für PostgreSQL oder Aurora PostgreSQL-kompatibel)
- Erfahrung in der PL/PGSQL-Codierung

Einschränkungen

- Dieses Muster erfordert je nach Anwendungsfall Änderungen der Sortierung auf Datenbankebene.
- Die Auswirkungen auf die Leistung großer Datensätze wurden nicht bewertet.
- Einige AWS-Services sind nicht in allen AWS-Regionen verfügbar. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie unter AWS Dienste nach Regionen. Informationen zu

bestimmten Endpunkten finden Sie unter Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Produktversionen

- Microsoft SQL Server 2012 oder höher

Architektur

Quelltechnologie-Stack

- SQL Server
- .NET Framework.

Zieltechnologie-Stack

- PostgreSQL
- `pgcrypto`Erweiterung

Automatisierung und Skalierung

- Erwägen Sie die Implementierung der Hashing-Funktion als gespeicherte Prozedur, um die Wartung zu vereinfachen.
- Bei großen Datensätzen sollten Sie die Leistung bewerten und Strategien zur Stapelverarbeitung oder Indizierung in Betracht ziehen.

Tools

AWS-Services

- Amazon Aurora PostgreSQL-Compatible ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt.
- AWS Database Migration Service (AWS DMS) hilft Ihnen bei der Migration von Datenspeichern in die oder zwischen Kombinationen von Cloud- und lokalen Setups. AWS Cloud

- Amazon Relational Database Service Amazon RDS for PostgreSQL unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen PostgreSQL-Datenbank in der. AWS Cloud
- AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist.

Andere Tools

- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL. Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, verwalten und verwenden können.
- SQL Server Management Studio (SSMS) ist eine integrierte Umgebung für die Verwaltung beliebiger SQL-Infrastrukturen.

Bewährte Methoden

- Verwenden Sie die entsprechenden Sortierungseinstellungen für die Behandlung von Sonderzeichen auf der Zieldatenbankseite.
- Testen Sie gründlich mit einer Vielzahl von E-Mail-Adressen, einschließlich Adressen mit Nicht-ASCII-Zeichen.
- Achten Sie bei der Verarbeitung von Groß- und Kleinbuchstaben auf Anwendungs- und Datenbankebene auf Konsistenz.
- Vergleichen Sie die Leistung von Abfragen anhand der Hash-Werte.

Epen

Analysieren Sie die Implementierung des Quell-Hashings

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den SQL Server-Code.	Gehen Sie wie folgt vor, um den SQL Server-Code zu überprüfen, der SHA1 Hashes generiert:	Dateningenieur, DBA, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Analysieren Sie die bestehende SQL Server-Implementierung von SHA1 Hashing. • Identifizieren Sie die genauen Methoden, die für die Hash-Generierung verwendet werden. • Dokumentieren Sie die Eingabeparameter und das Ausgabeformat. • Überprüfen Sie alle Konvertierungen oder Transformationen von Datentypen. • Untersuchen Sie die Sortierungseinstellungen und ihre Auswirkungen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Dokumentieren Sie den Hash-Algorithmus und die Datentransformationen.	Gehen Sie wie folgt vor, um den genauen Hash-Algorithmus und die Datentransformationen zu dokumentieren: • Erstellen Sie eine detaillierte technische Dokumentation des Hashing-Prozesses. • Dokumentieren Sie die step-by-step Transformationslogik. • Geben Sie Eingabe- und Ausgabeformate und Datentypen an. • Schließen Sie Sonderfälle und die Behandlung von Sonderzeichen mit ein.	App-Entwickler, Dateningenieur, DBA

PostgreSQL-Hashing-Funktion erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
`pgcrypto`Erweiterung erstellen.	Führen Sie den folgenden Befehl aus, `pgAdmin/psql` um die `pgcrypto` Erweiterung zu erstellen: `CREATE EXTENSION pgcrypto;`	DBA, Dateningenieur
Implementieren Sie eine PostgreSQL-Funktion.	Implementieren Sie die folgende PostgreSQL-Funktion, um die SQL Server-Ha	Dateningenieur, DBA, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	shing-Logik zu replizieren. Auf hoher Ebene verwendet diese Funktion die folgenden Schritte: 1. Konvertiert die Eingabe optional in Großbuchs taben. 2. Erzeugt einen SHA1 Hash der Eingabe. 3. Nimmt die letzten 10 Byte (80 Bit) dieses Hashs. 4. Konvertiert diese Byte in eine 64-Bit-Ganzzahl. `CREATE OR REPLACE FUNCTION utility.hex_to_bigint (par_val character varying, par_upper character varying DEFAULT 'lower'::character varying) RETURNS bigint LANGUAGE 'plpgsql' AS $BODY$ DECLARE retnumber bigint; digest_bytes bytea; BEGIN if lower(par_upper) = 'upper' then digest_bytes := digest(upper(par_val), 'sha1'); else`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>digest_bytes := digest((par_val), 'sha1');
	end if;
	retnumber := ('x' || encode(substring(digest_bytes, length(digest_bytes)-10+1), 'hex'))::bit(64)::bigint;
	RETURN retnumber;
	END;
	$BODY$;</pre>	

Testen der Funktion.	Verwenden Sie zum Testen der Funktion Beispieldaten von SQL Server, um die übereinstimmenden Hashwerte zu überprüfen. Führen Sie den folgenden Befehl aus:
	<pre>select 'alejandro_rosalez@example.com' as Email,
	utility.hex_to_bigint('alejandro_rosalez@example.com', 'upper') as HashValue;
	
	--OUTPUT
	/*
	email
	hashvalue
	"alejandro_rosalez@example.com" 451397011176045063
	*/</pre>
		App-Entwickler, DBA, Dateningenieur

Implementieren Sie Auslöser für automatisches Hashing

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie Trigger für relevante Tabellen.	Um Trigger für relevante Tabellen zu erstellen, die beim Einfügen oder Aktualisieren automatisch Hashwerte generieren, führen Sie den folgenden Befehl aus:
	`CREATE OR REPLACE FUNCTION update_email_hash() RETURNS TRIGGER AS $$ BEGIN NEW.email_hash = utility.hex_to_bigint(NEW.email, 'upper'); RETURN NEW; END; $$ LANGUAGE plpgsql;`
	`CREATE TRIGGER email_hash_trigger BEFORE INSERT OR UPDATE ON users FOR EACH ROW EXECUTE FUNCTION update_email_hash();`
		App-Entwickler, Dateningenieur, DBA

Migrieren Sie vorhandene Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entwickeln Sie ein Migration sskript oder verwenden Sie es AWS DMS.	Entwickeln Sie ein Migration sskript oder verwenden Sie es, AWS DMS um Hashwerte für bestehende Daten aufzufüll en (einschließlich Hashwerte , die `BIGINT` im Quellsystem gespeichert sind). Führen Sie die folgenden Schritte aus: • Erstellen Sie Migration sskripten für die Datenüber tragung mit Hashwerten. • Konfigurieren Sie AWS DMS Aufgaben mit entsprechenden Transform ationsregeln. • Richten Sie Quell- und Zielendpunkte in AWS DMS ein. • Implementieren Sie Mechanismen zur Fehlerbeh andlung und Protokoll ierung. • Entwerfen Sie eine Strategie zur Stapelverarbeitung für große Datensätze. • Erstellen Sie Validieru ngsabfragen für die Datenüberprüfung.	Dateningenieur, App-Entwi ckler, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie die neue PostgreSQL-Hashing-Funktion .	Gehen Sie wie folgt vor, um die neue PostgreSQL-Hashing -Funktion zur Sicherstellung der Konsistenz zu verwenden: • Implementieren Sie Validierungsverfahren, um die Hash-Konsistenz zu überprüfen. • Erstellen Sie Vergleich sskripten zwischen Quell- und Zielsystem. • Richten Sie automatisierte Tests zur Überprüfung des Hashwerts ein. • Dokumentieren Sie alle Unstimmigkeiten und Lösungsschritte.	App-Entwickler, DBA, Ingenieur DevOps

Anwendungsabfragen aktualisieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Anwendung sanfragen.	Gehen Sie wie folgt vor, um Anwendungsabfragen zu identifizieren, die Hashwerte verwenden: • Analysieren Sie die Anwendungscodebasis für Abfragen, die Hashwerte verwenden. • Überprüfen Sie gespeiche rte Prozeduren und	App-Entwickler, DBA, Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Funktionen, die auf Hash-Operationen verweisen. • Dokumentieren Sie Leistungskennzahlen und Ausführungspläne für Abfragen. • Identifizieren Sie Abhängigkeiten von Hash-basierten Suchvorgängen. • Ordnen Sie die betroffenen Anwendungskomponenten zu.	
Abfragen ändern.	Ändern Sie bei Bedarf Abfragen, um die neue PostgreSQL-Hashing-Funktion zu verwenden. Gehen Sie wie folgt vor: • Refaktorieren Sie bestehende Abfragen, um die PostgreSQL-Hashing-Funktion zu verwenden. • Aktualisieren Sie gespeicherte Prozeduren und Funktionen. • Implementieren und testen Sie neue Abfragemuster. • Optimieren Sie geänderte Abfragen im Hinblick auf die Leistung.	App-Entwickler, DBA, Dateningenieur

Testen und validieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie Tests durch.	Gehen Sie wie folgt vor, um gründliche Tests mit einer Teilmenge von Produktio nsdaten durchzuführen: • Erstellen Sie einen Testplan für die Validierung von Datenteilmengen. • Extrahieren Sie eine repräsentative Stichprobe von Produktionsdaten. • Richten Sie eine Testumgeb ung mit den richtigen Konfigurationen ein. • Führen Sie Tests zum Laden und Transformieren von Daten durch. • Führen Sie Volumen- und Stresstests durch.	App-Entwickler, Dateninge nieur, DBA
Stellen Sie sicher, dass die Hashwerte übereinstimmen.	Gehen Sie wie folgt vor, um zu überprüfen, ob die Hashwerte zwischen SQL Server und PostgreSQL übereinstimmen: • Entwickeln Sie Vergleich sskripten für Hashwerte. • Erstellen Sie Validieru ngsberichte für den Hash-Abgleich.	App-Entwickler, Dateninge nieur, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Implementieren Sie automatisierte Überprüfungsverfahren. • Dokumentieren Sie alle festgestellten Unstimmigkeiten. • Analysieren und beheben Sie Hash-Inkongruenzen.	
Überprüfen Sie die Funktionalität der Anwendung.	Gehen Sie wie folgt vor, um die Anwendungsfunktionalität anhand der migrierten Daten und der neuen Hashing-Implementierung zu überprüfen: • Führen Sie end-to-end Anwendungstests durch. • Überprüfen Sie alle Anwendungsfunktionen mithilfe von Hash-Daten. • Testen Sie die Anwendungsleistung mit der neuen Implementierung. • Überprüfen Sie die API-Integrationen und Abhängigkeiten.	App-Entwickler, DBA, Dateningenieur

Fehlerbehebung

Problem	Lösung
Hashwerte stimmen nicht überein.	Überprüfen Sie die Zeichenkodierungen und Kollationen zwischen Quelle und Ziel. Weitere

Problem	Lösung
	Informationen finden Sie unter Sortierungsänderungen in PostgreSQL auf Amazon Aurora und Amazon RDS verwalten (AWS Blog).

Zugehörige Ressourcen

AWS Blogs

- Sortierungsänderungen in PostgreSQL auf Amazon Aurora und Amazon RDS verwalten
- Migrieren Sie SQL Server zu Amazon Aurora PostgreSQL mithilfe von Best Practices und Erfahrungen aus der Praxis

Sonstige Ressourcen

- PostgreSQL-Pgcrypto-Modul (PostgreSQL-Dokumentation)
- PostgreSQL-Triggerfunktionen (PostgreSQL-Dokumentation)
- SQL Server-HASHBYTES-Funktion (Microsoft-Dokumentation)

Schrittweise Migration von Amazon RDS for Oracle zu Amazon RDS for PostgreSQL mithilfe von Oracle SQL Developer und AWS SCT

Erstellt von Pinesh Singal (AWS)

Übersicht

Viele Migrationsstrategien und -ansätze laufen in mehreren Phasen ab, die von einigen Wochen bis zu mehreren Monaten dauern können. Während dieser Zeit kann es aufgrund von Patches oder Upgrades in den Oracle-Quell-DB-Instances, die Sie zu PostgreSQL-DB-Instances migrieren möchten, zu Verzögerungen kommen. Um diese Situation zu vermeiden, empfehlen wir, den verbleibenden Oracle-Datenbankcode inkrementell zum PostgreSQL-Datenbankcode zu migrieren.

Dieses Muster bietet eine inkrementelle Migrationsstrategie ohne Ausfallzeiten für eine Oracle-DB-Instance mit mehreren Terabyte, bei der nach Ihrer ersten Migration eine hohe Anzahl von Transaktionen ausgeführt wurde und die in eine PostgreSQL-Datenbank migriert werden muss. Sie können den step-by-step Ansatz dieses Musters verwenden, um eine Amazon Relational Database Service (Amazon RDS) für Oracle-DB-Instance schrittweise zu einer Amazon RDS for PostgreSQL PostgreSQL-DB-Instance zu migrieren, ohne sich bei der Amazon Web Services (AWS) Management Console anzumelden.

Das Muster verwendet Oracle SQL Developer, um die Unterschiede zwischen zwei Schemas in der Oracle-Quelldatenbank zu ermitteln. Anschließend verwenden Sie das AWS Schema Conversion Tool (AWS SCT), um die Datenbankschemaobjekte von Amazon RDS for Oracle in Amazon RDS for PostgreSQL PostgreSQL-Datenbankschemaobjekte zu konvertieren. Anschließend können Sie in der Windows-Befehlszeile ein Python-Skript ausführen, um AWS-SCT-Objekte für die inkrementellen Änderungen an den Quelldatenbankobjekten zu erstellen.

> **Note**
>
> Bevor Sie Ihre Produktions-Workloads migrieren, empfehlen wir Ihnen, einen Machbarkeitsnachweis (PoC) für den Ansatz dieses Musters in einer Test- oder Nicht-Produktionsumgebung durchzuführen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine bestehende Amazon RDS for Oracle Oracle-DB-Instance.
- Eine bestehende Amazon RDS for PostgreSQL PostgreSQL-DB-Instance.
- AWS SCT, installiert und konfiguriert mit JDBC-Treibern für Oracle- und PostgreSQL-Datenbank-Engines. Weitere Informationen dazu finden Sie unter Installation von AWS SCT und Installation der erforderlichen Datenbanktreiber in der AWS SCT-Dokumentation.
- Oracle SQL Developer, installiert und konfiguriert. Weitere Informationen dazu finden Sie in der Oracle SQL Developer-Dokumentation.
- Die `incremental-migration-sct-sql.zip` Datei (angehängt) wurde auf Ihren lokalen Computer heruntergeladen.

Einschränkungen

- Die Mindestanforderungen für Ihre Amazon RDS for Oracle DB-Quell-Instance sind:
  - Oracle-Versionen 10.2 und höher (für Versionen 10.x), 11g (Versionen 11.2.0.3.v1 und höher) und bis zu 12.2 und 18c für die Editionen Enterprise, Standard, Standard One und Standard Two
- Die Mindestanforderungen für Ihre Amazon RDS for PostgreSQL PostgreSQL-DB-Ziel-Instance sind:
  - PostgreSQL-Versionen 9.4 und höher (für Versionen 9.x), 10.x und 11.x
- Dieses Muster verwendet Oracle SQL Developer. Ihre Ergebnisse können variieren, wenn Sie andere Tools verwenden, um Schemaunterschiede zu finden und zu exportieren.
- Die von Oracle SQL Developer generierten SQL-Skripten können zu Transformationsfehlern führen, was bedeutet, dass Sie eine manuelle Migration durchführen müssen.
- Wenn die AWS SCT-Quell- und Zieltestverbindungen fehlschlagen, stellen Sie sicher, dass Sie die JDBC-Treiberversionen und eingehenden Regeln für die Sicherheitsgruppe der Virtual Private Cloud (VPC) so konfigurieren, dass sie eingehenden Datenverkehr akzeptiert.

Produktversionen

- Amazon RDS for Oracle Oracle-DB-Instance Version 12.1.0.2 (Version 10.2 und höher)
- Amazon RDS for PostgreSQL PostgreSQL-DB-Instance Version 11.5 (Version 9.4 und höher)
- Oracle SQL Developer Version 19.1 und höher
- AWS SCT Version 1.0.632 und höher

Architektur

Quelltechnologie-Stack

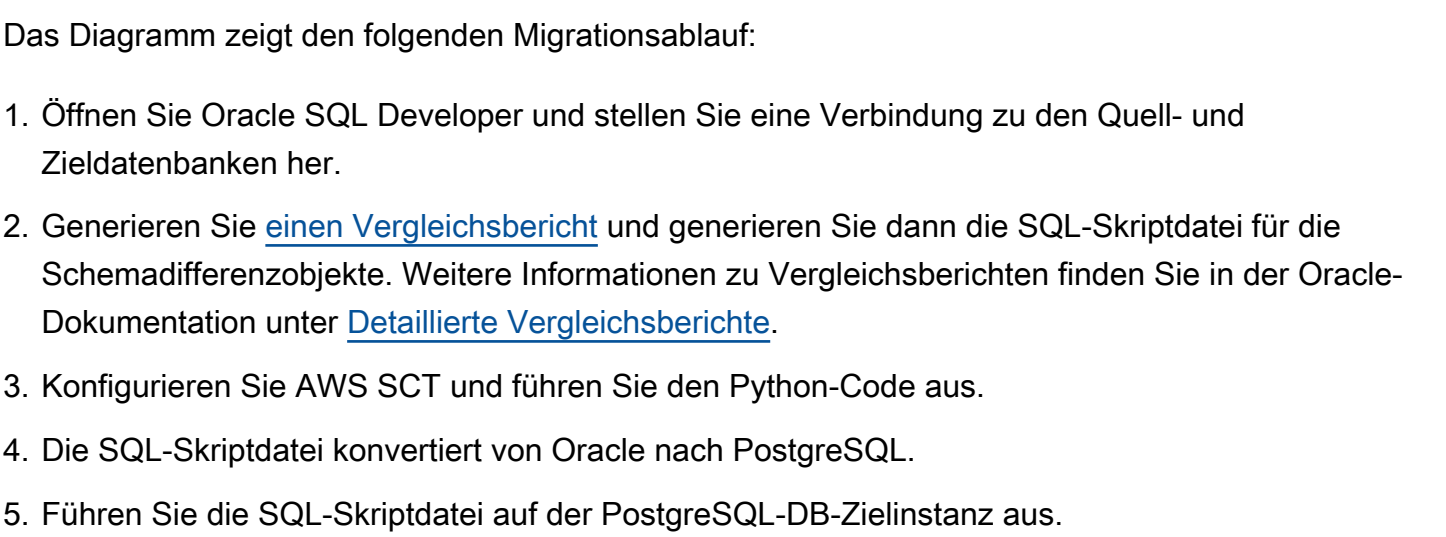
- Amazon RDS for Oracle Oracle-DB-Instance

Zieltechnologie-Stack

- Amazon RDS for PostgreSQL PostgreSQL-DB-Instance

Quell- und Zielarchitektur

Das folgende Diagramm zeigt die Migration einer Amazon RDS for Oracle DB-Instance zu einer Amazon RDS for PostgreSQL DB-Instance.



Das Diagramm zeigt den folgenden Migrationsablauf:

1. Öffnen Sie Oracle SQL Developer und stellen Sie eine Verbindung zu den Quell- und Zieldatenbanken her.
2. Generieren Sie einen Vergleichsbericht und generieren Sie dann die SQL-Skriptdatei für die Schemadifferenzobjekte. Weitere Informationen zu Vergleichsberichten finden Sie in der Oracle-Dokumentation unter Detaillierte Vergleichsberichte.
3. Konfigurieren Sie AWS SCT und führen Sie den Python-Code aus.
4. Die SQL-Skriptdatei konvertiert von Oracle nach PostgreSQL.
5. Führen Sie die SQL-Skriptdatei auf der PostgreSQL-DB-Zielinstanz aus.

Automatisierung und Skalierung

Sie können diese Migration automatisieren, indem Sie Ihrem Python-Skript zusätzliche Parameter und sicherheitsrelevante Änderungen für mehrere Funktionen in einem einzigen Programm hinzufügen.

Tools

- AWS SCT — Das AWS Schema Conversion Tool (AWS SCT) konvertiert Ihr vorhandenes Datenbankschema von einer Datenbank-Engine in eine andere.

- Oracle SQL Developer — Oracle SQL Developer ist eine integrierte Entwicklungsumgebung (IDE), die die Entwicklung und Verwaltung von Oracle-Datenbanken sowohl in herkömmlichen als auch in Cloud-basierten Bereitstellungen vereinfacht.

Code

Die `incremental-migration-sct-sql.zip` Datei (angehängt) enthält den vollständigen Quellcode für dieses Muster.

Epen

Erstellen Sie die SQL-Skriptdatei für die Schemaunterschiede in der Quelldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie Database Diff in Oracle SQL Developer aus.	1. Melden Sie sich bei Ihrer Oracle-DB-Quellinstanz an, wählen Sie Tools und dann Database Diff. 2. Wählen Sie Ihre Quelldatenbank unter Source Connection aus. 3. Wählen Sie die aktualisierte oder gepatchte Quelldatenbank unter Destination Connection aus. 4. Konfigurieren Sie die übrigen Optionen Ihren Anforderungen entsprechend, wählen Sie Weiter und anschließend Fertig stellen, um den Vergleichsbericht zu erstellen.	DBA
Generieren Sie die SQL-Skripdatei.	Wählen Sie Generate Script, um die Unterschiede in den SQL-Dateien zu generieren.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dadurch wird die SQL-Skrip tdatei generiert, die AWS SCT verwendet, um Ihre Datenbank von Oracle nach PostgreSQL zu konvertieren.	

Verwenden Sie das Python-Skript, um die Ziel-DB-Objekte in AWS SCT zu erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie AWS SCT mit der Windows-Eingabeauf forderung.	1. Kopieren Sie die `AWSSchemaConversionToolBatch.jar` Datei aus Ihrem vorinstal lierten AWS SCT-Ordne r und fügen Sie sie in Ihr Arbeitsverzeichnis ein. 2. Stellen Sie den Python-Code aus der `run_aws_sct_sql.py` Datei aus dem `incremental-migration-sct-sql.zip` Ordner (angehängt) bereit. Dadurch werden XML- und SCT-Dateien im `projects` Verzeichnis mit den Konfigurationsdetails Ihrer Quell- und Zieldaten bankumgebung erstellt. Es liest auch die SQL-Skrip tdatei, die Sie in Oracle SQL Developer generiert haben. Schließlich erstellt	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	es .sql-Dateiobjekte im `output` Verzeichnis.
	3. Konfigurieren Sie die Konfigurationsdetails der Quell- und Zielumgeb ung in der `database_ migration.txt` Datei, indem Sie das folgende Format verwenden:
	`#source_vendor,sou rce_hostname,sourc e_dbname,source_us er,source_pwd,sour ce_schema,source_p ort,source_sid,tar get_vendor,target_ hostname,target_us er,target_pwd,targ et_dbname,target_port`
	`ORACLE,myoracledb.cokm vis0v46q.us-east-1 .rds.amazonaws.com ,ORCL,orcl,orcl123 4,orcl,1521,ORCL,P OSTGRESQL,mypgdbin stance.cokmvis0v46 q.us-east-1.rds.am azonaws.com,pguser ,pgpassword,pgdb,5432`
	4. Ändern Sie die AWS SCT-Konfigurationsparameter gemäß Ihren Anforderu ngen und kopieren Sie dann die SQL-Skriptdatei in Ihr	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Arbeitsverzeichnis im `input` Unterverzeichnis.	
Führen Sie das Python-Skript aus.	1. Führen Sie das Python-Skript mit dem folgenden Befehl aus: `$ python run_aws_sct_sql.py database_migration.txt` 2. Dadurch wird die SQL-Datei für DB-Objekte erstellt. Nicht konvertierte Codes mit Transformationsfehlern können manuell konvertiert werden.	DBA
Erstellen Sie die Objekte in Amazon RDS for PostgreSQL	Führen Sie die SQL-Dateien aus und erstellen Sie Objekte in Ihrer Amazon RDS for PostgreSQL PostgreSQL-DB-Instance.	DBA

Zugehörige Ressourcen

- Oracle auf Amazon RDS
- PostgreSQL auf Amazon RDS
- Verwenden der AWS SCT-Benutzeroberfläche
- Verwenden von Oracle als Quelle für AWS SCT

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Laden Sie BLOB-Dateien in TEXT, indem Sie die Dateikodierung in Aurora PostgreSQL-kompatibel verwenden

Erstellt von Bhanu Ganesh Gudivada (AWS) und Jeevan Shetty (AWS)

Übersicht

Während der Migration gibt es häufig Fälle, in denen Sie unstrukturierte und strukturierte Daten verarbeiten müssen, die aus Dateien in einem lokalen Dateisystem geladen werden. Die Daten können sich auch in einem Zeichensatz befinden, der sich vom Zeichensatz der Datenbank unterscheidet.

Diese Dateien enthalten die folgenden Datentypen:

- Metadaten — Diese Daten beschreiben die Dateistruktur.
- Semistrukturierte Daten — Dies sind Textzeichenfolgen in einem bestimmten Format wie JSON oder XML. Möglicherweise können Sie Aussagen zu solchen Daten treffen, z. B. „beginnt immer mit '<'“ oder „enthält keine Zeilenumbruchzeichen“.
- Volltext — Diese Daten enthalten normalerweise alle Arten von Zeichen, einschließlich Zeilenumbruch- und Anführungszeichen. Sie können auch aus Multibyte-Zeichen in UTF-8 bestehen.
- Binärdaten — Diese Daten können Bytes oder Kombinationen von Bytes enthalten, einschließlich Nullen und Markierungen. end-of-file

Das Laden einer Mischung dieser Datentypen kann eine Herausforderung sein.

Das Muster kann mit lokalen Oracle-Datenbanken, Oracle-Datenbanken, die sich auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances in der Amazon Web Services (AWS) -Cloud befinden, und Amazon Relational Database Service (Amazon RDS) für Oracle-Datenbanken verwendet werden. Als Beispiel verwendet dieses Muster Amazon Aurora PostgreSQL-Compatible Edition.

In Oracle Database können Sie mithilfe eines `BFILE` (binären Datei-) Zeigers, des `DBMS_LOB` Pakets und der Oracle-Systemfunktionen Daten aus einer Datei laden und mit Zeichenkodierung in CLOB konvertieren. Da PostgreSQL den BLOB-Datentyp bei der Migration zu einer Amazon Aurora PostgreSQL-Compatible Edition-Datenbank nicht unterstützt, müssen diese Funktionen in PostgreSQL-kompatible Skripten konvertiert werden.

Dieses Muster bietet zwei Ansätze für das Laden einer Datei in eine einzelne Datenbankspalte in einer Amazon Aurora PostgreSQL-kompatiblen Datenbank:

- Ansatz 1 — Sie importieren Daten aus Ihrem Amazon Simple Storage Service (Amazon S3) -Bucket, indem Sie die `table_import_from_s3` Funktion der `aws_s3` Erweiterung mit der Kodierungsoption verwenden.
- Ansatz 2 — Sie kodieren außerhalb der Datenbank hexadezimal und dekodieren dann, um sie innerhalb der Datenbank anzuzeigen. `TEXT`

Wir empfehlen die Verwendung von Approach 1, da Aurora PostgreSQL-Compatible direkt in die Erweiterung integriert ist. `aws_s3`

Dieses Muster verwendet das Beispiel des Ladens einer Flat-Datei, die eine E-Mail-Vorlage mit Multibyte-Zeichen und unterschiedlicher Formatierung enthält, in eine Amazon Aurora PostgreSQL-kompatible Datenbank.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Amazon RDS-Instance oder eine Aurora PostgreSQL-kompatible Instance
- Ein grundlegendes Verständnis von SQL und dem relationalen Datenbankmanagementsystem (RDBMS)
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket.
- Kenntnisse der Systemfunktionen in Oracle und PostgreSQL
- RPM-Paket HexDump -XXD-0.1.1 (in Amazon Linux 2 enthalten)

> **Note**
>
> Amazon Linux 2 nähert sich dem Ende des Supports. Weitere Informationen finden Sie unter Amazon Linux FAQs 2.

Einschränkungen

- Für den `TEXT` Datentyp beträgt die längste mögliche Zeichenfolge, die gespeichert werden kann, etwa 1 GB.

Versionen der Produkte

- Aurora unterstützt die PostgreSQL-Versionen, die in Amazon Aurora PostgreSQL-Updates aufgeführt sind.

Architektur

Zieltechnologie-Stack

- Aurora PostgreSQL-kompatibel

Zielarchitektur

Ansatz 1 — Verwendung von aws_s3.table_import_from_s3

Von einem lokalen Server wird eine Datei, die eine E-Mail-Vorlage mit Multibyte-Zeichen und benutzerdefinierter Formatierung enthält, an Amazon S3 übertragen. Die durch dieses Muster bereitgestellte benutzerdefinierte Datenbankfunktion verwendet die `aws_s3.table_import_from_s3` Funktion mit`file_encoding`, um Dateien in die Datenbank zu laden und Abfrageergebnisse als `TEXT` Datentyp zurückzugeben.

1. Dateien werden in den Staging-S3-Bucket übertragen.
2. Dateien werden in die Amazon Aurora PostgreSQL-kompatible Datenbank hochgeladen.
3. Mit dem pgAdmin-Client `load_file_into_clob` wird die benutzerdefinierte Funktion in der Aurora-Datenbank bereitgestellt.
4. Die benutzerdefinierte Funktion wird intern `table_import_from_s3` mit file_encoding verwendet. Die Ausgabe der Funktion wird durch die Verwendung von `array_to_string` und `array_agg` als `TEXT` Ausgabe abgerufen.

Ansatz 2 — Hexadezimale Kodierung außerhalb der Datenbank und Dekodierung zur Anzeige von TEXT innerhalb der Datenbank

Eine Datei von einem lokalen Server oder einem lokalen Dateisystem wird in einen Hex-Dump konvertiert. Dann wird die Datei als Feld in PostgreSQL importiert. `TEXT`

1. Konvertieren Sie die Datei in der Befehlszeile mit der Option in einen Hex-Dump. `xxd -p`

2. Laden Sie die Hex-Dump-Dateien mithilfe der `\copy` Option in das Aurora PostgreSQL-kompatible Format hoch und dekodieren Sie dann die Hex-Dump-Dateien in Binärdateien.
3. Kodieren Sie die Binärdaten, die zurückgegeben werden sollen als. `TEXT`

Tools

AWS-Services

- Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

Andere Tools

- pgAdmin4 ist eine Open-Source-Verwaltungs- und Entwicklungsplattform für PostgreSQL. pgAdmin4 kann unter Linux, Unix, Mac OS und Windows zur Verwaltung von PostgreSQL verwendet werden.

Epen

Ansatz 1: Daten von Amazon S3 nach Aurora PostgreSQL-kompatibel importieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie eine EC2 Instanz.	Anweisungen zum Starten einer Instance finden Sie unter Starten Sie Ihre Instance.	DBA
Installieren Sie das PostgreSQL-Client-Tool pgAdmin.	Laden Sie pgAdmin herunter und installieren Sie es.	DBA
Erstellen Sie eine IAM-Richtlinie.	Erstellen Sie eine AWS Identity and Access Management (IAM) -Richtlinie mit dem Name`aurora-s3`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`-access-pol` , die Zugriff auf den S3-Bucket gewährt, in dem die Dateien gespeicherte werden. Verwenden Sie den folgenden Code und `<bucket-name>` ersetzen Sie ihn durch den Namen Ihres S3-Buckets. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "s3:GetObject", "s3:AbortMultipartUpload", "s3:DeleteObject", "s3:ListMultipartUploadParts", "s3:PutObject", "s3:ListBucket" ], "Resource": [ "arn:aws:s3:::<bucket-name>/*", "arn:aws:s3:::<bucket-name>"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>]
	        }
	    ]
	}</pre>	

Erstellen Sie eine IAM-Rolle für den Objektimport von Amazon S3 nach Aurora PostgreSQL-kompatibel.	Verwenden Sie den folgenden Code, um eine IAM-Rolle mit dem Namen der Vertrauen sbeziehung zu erstellen. `aurora-s3-import-role` AssumeRole `AssumeRole` ermöglich t Aurora, in Ihrem Namen auf andere AWS-Services zuzugreifen.
	<pre>{
	  "Version": "2012-10-17",
	  "Statement": [
	    {
	      "Effect": "Allow","Principal": {
	        "Service": "rds.amazonaws.com"
	      },"Action": "sts:AssumeRole"
	    }
	  ]
	}</pre>
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ordnen Sie die IAM-Rolle dem Cluster zu.	Um die IAM-Rolle dem Aurora PostgreSQL-kompatiblen Datenbank-Cluster zuzuordnen, führen Sie den folgenden AWS-CLI-Befehl aus. Ändern Sie `<Account-ID>` die ID des AWS-Kontos, das die Aurora PostgreSQL-kompatible Datenbank hostet. Dadurch kann die Aurora PostgreSQL-kompatible Datenbank auf den S3-Bucket zugreifen. `aws rds add-role-to-db-cluster --db-cluster-identifier aurora-postgres-cl --feature-name s3Import --role-arn arn:aws:iam::<Account-ID>:role/aurora-s3-import-role`	DBA
Laden Sie das Beispiel auf Amazon S3 hoch.	1. Kopieren Sie im Abschnitt Zusätzliche Informationen dieses Musters den E-Mail-Vorlagencode in eine Datei mit dem Namen `salary.event.notification.email.vm` . 2. Laden Sie die Datei in den S3-Bucket hoch.	DBA, Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die benutzerd efinierte Funktion bereit.	1. Kopieren Sie im Abschnitt Zusätzliche Informationen den Inhalt der `load_file _into_clob` SQL-Datei mit der benutzerdefinierten Funktion in eine temporäre Tabelle. 2. Melden Sie sich bei der Aurora PostgreSQL-kompatiblen Datenbank an und stellen Sie sie mithilfe des pgAdmin-Clients im Datenbankschema bereit.	Besitzer der App, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Führen Sie die benutzerd efinierte Funktion zum Importieren der Daten in die Datenbank aus.	Führen Sie den folgenden SQL-Befehl aus und ersetzen Sie die Elemente in spitzen Klammern durch die entsprech enden Werte.
	`select load_file _into_clob('aws-s3 -import-test'::tex t,'us-west-1'::tex t,'employee.salary .event.notificatio n.email.vm'::text);`
	Ersetzen Sie die Elemente in spitzen Klammern durch die entsprechenden Werte, wie im folgenden Beispiel gezeigt, bevor Sie den Befehl ausführen.
	`Select load_file _into_clob('aws-s3 -import-test'::tex t,'us-west-1'::tex t,'employee.salary .event.notificatio n.email.vm'::text);`
	Der Befehl lädt die Datei aus Amazon S3 und gibt die Ausgabe als zurück`TEXT`.
		Besitzer der App, DBA

Ansatz 2: Konvertieren Sie die Vorlagendatei in einen Hex-Dump in einem lokalen Linux-System

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konvertiert die Vorlagendatei in einen Hex-Dump.	**Note** Das Hexdump-Hilfsprogramm zeigt den Inhalt von Binärdateien in Hexadezimal, Dezimal, Oktal oder ASCII an. Der `hexdump` Befehl ist Teil des `util-linux` Pakets und in Linux-Distributionen vorinstalliert. Das Hexdump RPM-Paket ist ebenfalls Teil von Amazon Linux 2. (: Amazon Linux 2 nähert sich dem Ende der Unterstützung. Weitere Informationen finden Sie unter Amazon Linux FAQs 2.) Um den Dateiinhalt in einen Hex-Dump zu konvertieren, führen Sie den folgenden Shell-Befehl aus. `xxd -p </path/file.vm> | tr -d '\n' > </path/file.hex>`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ersetzen Sie den Pfad und die Datei durch die entsprechenden Werte, wie im folgenden Beispiel gezeigt. `xxd -p employee.salary.event.notification.email.vm | tr -d '\n' > employee.salary.event.notification.email.vm.hex`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Laden Sie die Hexdump-Datei in das Datenbankschema.	Verwenden Sie die folgenden Befehle, um die Hexdump-Datei in die Aurora PostgreSQL-kompatible Datenbank zu laden.
	
	1. Melden Sie sich bei der Aurora PostgreSQL-Datenbank an und erstellen Sie eine neue Tabelle mit dem Namen. `email_template_hex`
	
	`CREATE TABLE email_template_hex(hex_data TEXT);`
	
	2. Laden Sie die Dateien mit dem folgenden Befehl aus dem lokalen Dateisystem in das DB-Schema.
	
	`\copy email_template_hex FROM '/path/file.hex';`
	
	Ersetzen Sie den Pfad durch den Speicherort in Ihrem lokalen Dateisystem.
	
	`\copy email_template_hex FROM '/tmp/employee.salary.event.notification.email.vm.hex';`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	3. Erstellen Sie eine weitere Tabelle mit dem Namen`email_template_bytea` .
	`CREATE TABLE email_template_bytea(hex_data bytea);`
	4. Fügen Sie die Daten von `email_template_hex` in ein`email_template_bytea` .
	`INSERT INTO email_template_bytea (hex_data)`
	`(SELECT decode(hex_data, 'hex') FROM email_template_hex limit 1);`
	5. Um Hex-Bytea-Code als TEXT Daten zurückzugeben, führen Sie den folgenden Befehl aus.
	`SELECT encode(hex_data::bytea, 'escape') FROM email_template_bytea;`	

Zugehörige Ressourcen

Referenzen

- Verwenden einer PostgreSQL-Datenbank als Ziel für den AWS Database Migration Service
- Playbook zur Migration von Oracle Database 19c zu Amazon Aurora mit PostgreSQL-Kompatibilität (12.4)
- IAM-Richtlinien erstellen
- Zuordnen einer IAM-Rolle zu einem Amazon Aurora MySQL-DB-Cluster
- pgAdmin

Tutorials

- Erste Schritte mit Amazon RDS
- Migrieren Sie von Oracle zu Amazon Aurora

Zusätzliche Informationen

benutzerdefinierte Funktion load_file_into_clob

```
CREATE OR REPLACE FUNCTION load_file_into_clob(
    s3_bucket_name text,
    s3_bucket_region text,
    file_name text,
    file_delimiter character DEFAULT '&'::bpchar,
    file_encoding text DEFAULT 'UTF8'::text)
    RETURNS text
    LANGUAGE 'plpgsql'
    COST 100
    VOLATILE PARALLEL UNSAFE
AS $BODY$
DECLARE
    blob_data BYTEA;
    clob_data TEXT;
    l_table_name CHARACTER VARYING(50) := 'file_upload_hex';
    l_column_name CHARACTER VARYING(50) := 'template';
    l_return_text TEXT;
    l_option_text CHARACTER VARYING(150);
    l_sql_stmt CHARACTER VARYING(500);

BEGIN

    EXECUTE format ('CREATE TEMPORARY TABLE %I (%I text, id_serial serial)',
 l_table_name, l_column_name);
```

```
    l_sql_stmt := 'select ''(format text, delimiter ''''' || file_delimiter || ''''',
 encoding ''''' || file_encoding ||  ''''')'' ';

    EXECUTE FORMAT(l_sql_stmt)
    INTO l_option_text;

    EXECUTE FORMAT('SELECT aws_s3.table_import_from_s3($1,$2,$6,
 aws_commons.create_s3_uri($3,$4,$5))')
    INTO l_return_text
    USING l_table_name, l_column_name, s3_bucket_name,
 file_name,s3_bucket_region,l_option_text;

    EXECUTE format('select array_to_string(array_agg(%I order by id_serial),E''\n'')
 from %I', l_column_name, l_table_name)
    INTO clob_data;

    drop table file_upload_hex;

    RETURN clob_data;
END;
$BODY$;
```

E-Mail-Vorlage

```
##############################################################################################
##
 ##
##    johndoe Template Type: email
 ##
##    File: johndoe.salary.event.notification.email.vm
 ##
##    Author: Aimée Étienne    Date 1/10/2021
      ##
##  Purpose: Email template used by EmplmanagerEJB to inform a johndoe they         ##
##        have been given access to a salary event
 ##
##    Template Attributes:
 ##
##        invitedUser - PersonDetails object for the invited user
  ##
```

```
##        salaryEvent - OfferDetails object for the event the user was given access
 ##
##        buyercollege - CompDetails object for the college owning the salary event
 ##
##        salaryCoordinator - PersonDetails of the salary coordinator for the event
 ##
##        idp - Identity Provider of the email recipient
 ##
##        httpWebRoot - HTTP address of the server
 ##
##
 ##
#################################################################################

$!invitedUser.firstname $!invitedUser.lastname,

Ce courriel confirme que vous avez ete invite par $!salaryCoordinator.firstname $!
salaryCoordinator.lastname de $buyercollege.collegeName a participer a l'evenement
 "$salaryEvent.offeringtitle" sur johndoeMaster Sourcing Intelligence.

Votre nom d'utilisateur est $!invitedUser.username

Veuillez suivre le lien ci-dessous pour acceder a l'evenement.

${httpWebRoot}/myDashboard.do?idp=$!{idp}

Si vous avez oublie votre mot de passe, utilisez le lien "Mot de passe oublie" situe
 sur l'ecran de connexion et entrez votre nom d'utilisateur ci-dessus.

Si vous avez des questions ou des preoccupations, nous vous invitons a
 communiquer avec le coordonnateur de l'evenement $!salaryCoordinator.firstname $!
salaryCoordinator.lastname au ${salaryCoordinator.workphone}.

*******

johndoeMaster Sourcing Intelligence est une plateforme de soumission en ligne pour les
 equipements, les materiaux et les services.

Si vous avez des difficultes ou des questions, envoyez un courriel a
 support@johndoeMaster.com pour obtenir de l'aide.
```

Migrieren Sie Amazon RDS for Oracle zu Amazon RDS for PostgreSQL mit AWS SCT und unter Verwendung von und AWS DMSAWS CLIAWS CloudFormation

Erstellt von Pinesh Singal (AWS)

Übersicht

Dieses Muster zeigt, wie Sie mithilfe von () eine Amazon Relational Database Service (Amazon RDS) für Oracle-DB-Instance mit mehreren Terabyte zu einer Amazon RDS for PostgreSQL PostgreSQL-DB-Instance migrieren. AWS Command Line Interface AWS CLI Dieser Ansatz bietet minimale Ausfallzeiten und erfordert keine Anmeldung bei. AWS Management Console

Dieses Muster trägt dazu bei, manuelle Konfigurationen und individuelle Migrationen mithilfe der Konsolen AWS Schema Conversion Tool (AWS SCT) und AWS Database Migration Service (AWS DMS) zu vermeiden. Die Lösung richtet eine einmalige Konfiguration für mehrere Datenbanken ein und führt die Migrationen mithilfe AWS SCT von und in der durch. AWS DMS AWS CLI

Das Muster wird verwendet AWS SCT , um Datenbankschemaobjekte von Amazon RDS for Oracle in Amazon RDS for PostgreSQL zu konvertieren, und verwendet es dann, um die Daten AWS DMS zu migrieren. Mithilfe von AWS CLI Python-Skripten in erstellen Sie AWS SCT Objekte und AWS DMS Aufgaben mit einer AWS CloudFormation Vorlage.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto.
- Eine bestehende Amazon RDS for Oracle Oracle-DB-Instance.
- Eine bestehende Amazon RDS for PostgreSQL PostgreSQL-DB-Instance.
- Eine Amazon Elastic Compute Cloud (Amazon EC2) -Instanz oder ein lokaler Computer mit Windows- oder Linux-Betriebssystem zum Ausführen von Skripten.
- Ein Verständnis der folgenden Arten von AWS DMS Migrationsaufgaben:`full-load`,`cdc`,`full-load-and-cdc`. Weitere Informationen finden Sie in der AWS DMS Dokumentation unter Aufgabe erstellen.
- AWS SCT, installiert und konfiguriert mit Java Database Connectivity (JDBC) -Treibern für Oracle- und PostgreSQL-Datenbank-Engines. Weitere Informationen finden Sie in der Dokumentation unter Installation und Konfiguration AWS SCT. AWS SCT
- Die `AWSSchemaConversionToolBatch.jar` Datei aus dem installierten AWS SCT Ordner wurde in Ihr Arbeitsverzeichnis kopiert.

- Die `cli-sct-dms-cft.zip` Datei (angehängt), heruntergeladen und in Ihr Arbeitsverzeichnis extrahiert.
- Die neueste Version der AWS DMS Replication Instance Engine. Weitere Informationen finden Sie in der AWS -Support Dokumentation und in den AWS DMS Versionshinweisen unter Wie erstelle ich eine AWS DMS Replikationsinstanz.
- AWS CLI Version 2, installiert und konfiguriert mit Ihrer Zugriffsschlüssel-ID, Ihrem geheimen Zugriffsschlüssel und dem AWS-Region Standardnamen für die EC2 Instanz oder das Betriebssystem, auf dem die Skripts ausgeführt werden. Weitere Informationen finden Sie in der AWS CLI Dokumentation unter Installation oder Aktualisierung auf die neueste Version von AWS CLI und Konfiguration AWS CLI der Einstellungen für.
- Vertrautheit mit AWS CloudFormation Vorlagen. Weitere Informationen finden Sie in der AWS CloudFormation Dokumentation unter So AWS CloudFormation funktioniert es.
- Python Version 3, installiert und konfiguriert auf der EC2 Instanz oder dem Betriebssystem, auf dem die Skripts ausgeführt werden. Weitere Informationen finden Sie in der Python-Dokumentation.

Einschränkungen

- Die Mindestanforderungen für Ihre Amazon RDS for Oracle DB-Quell-Instance sind:
  - Oracle-Versionen 12c (12.1.0.2, 12.2.0.1), 18c (18.0.0.0) und 19c (19.0.0.0) für die Editionen Enterprise, Standard, Standard One und Standard Two.
  - Obwohl Amazon RDS Oracle 18c (18.0.0.0) unterstützt, ist diese Version veraltet, da Oracle nach diesem Datum keine Patches mehr für 18c bereitstellt. end-of-support Weitere Informationen finden Sie unter Amazon RDS for Oracle in der Amazon RDS-Dokumentation.
  - Amazon RDS for Oracle 11g wird nicht mehr unterstützt.
- Die Mindestanforderungen für Ihre Amazon RDS for PostgreSQL PostgreSQL-DB-Ziel-Instance sind:
  - PostgreSQL-Versionen 9 (9.5 und 9.6), 10.x, 11.x, 12.x und 13.x

Produktversionen

- Amazon RDS for Oracle Oracle-DB-Instance Version 12.1.0.2 und höher
- Amazon RDS for PostgreSQL PostgreSQL-DB-Instance Version 11.5 und höher
- AWS CLI Version 2

- Die neueste Version von AWS SCT
- Die neueste Version von Python 3

Architektur

Quelltechnologie-Stack

- Amazon RDS für Oracle

Zieltechnologie-Stack

- Amazon RDS für PostgreSQL

Quell- und Zielarchitektur

Das folgende Diagramm zeigt die Migration einer Amazon RDS for Oracle DB-Instance zu einer Amazon RDS for PostgreSQL DB-Instance mithilfe von AWS DMS Python-Skripten.

Das Diagramm zeigt den folgenden Migrationsablauf:

1. Das Python-Skript wird verwendet AWS SCT , um eine Verbindung zu den Quell- und Ziel-DB-Instances herzustellen.
2. Der Benutzer beginnt AWS SCT mit dem Python-Skript, konvertiert den Oracle-Code in PostgreSQL-Code und führt ihn auf der Ziel-DB-Instance aus.
3. Das Python-Skript erstellt AWS DMS Replikationsaufgaben für die Quell- und Ziel-DB-Instances.
4. Der Benutzer stellt Python-Skripts bereit, um die AWS DMS Aufgaben zu starten, und stoppt die Aufgaben dann, nachdem die Datenmigration abgeschlossen ist.

Automatisierung und Skalierung

Sie können diese Migration automatisieren, indem Sie Ihrem Python-Skript Parameter und sicherheitsrelevante Änderungen hinzufügen, um zusätzliche Funktionen bereitzustellen.

Tools

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS CloudFormationhilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend AWS-Konten zu verwalten. Dieses Muster konvertiert die `.csv` `.json` Eingabedatei mithilfe eines Python-Skripts in eine Eingabedatei. Die `.json` Datei wird in AWS CLI Befehlen verwendet, um einen AWS CloudFormation Stack zu erstellen, der mehrere AWS DMS Replikationsaufgaben mit Amazon-Ressourcennamen (ARNs), Migrationstypen, Aufgabeneinstellungen und Tabellenzuordnungen erstellt.
- AWS Database Migration Service (AWS DMS) hilft Ihnen bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen von Cloud- und lokalen Setups. Dieses Muster wird verwendet, AWS DMS um Aufgaben mit einem Python-Skript, das in der Befehlszeile ausgeführt wird, zu erstellen, zu starten und zu beenden und die AWS CloudFormation Vorlage zu erstellen.
- AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist. Für dieses Muster ist die `AWSSchemaConversionToolBatch.jar` Datei aus dem installierten Verzeichnis erforderlich. AWS SCT

Code

Die `cli-sct-dms-cft.zip` Datei (angehängt) enthält den kompletten Quellcode für dieses Muster.

Epen

Konfigurieren AWS SCT und erstellen Sie Datenbankobjekte in AWS CLI

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie AWS SCT es so, dass es von der ausgeführt wird AWS CLI.	1. Konfigurieren Sie die Konfigurationsdetails der Quell- und Zielumgeb ung in der `database_ migration.txt` Datei im folgenden Format:	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>#source_vendor,source_hostname,source_dbname,source_user,source_pwd,source_schema,source_port,source_sid,target_vendor,target_hostname,target_user,target_pwd,target_dbname,target_port
	ORACLE,myoracledb.cokmvis0v46q.us-east-1.rds.amazonaws.com,ORCL,orcl,orcl1234,orcl,1521,ORCL,POSTGRESQL,mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com,pguser,pgpassword,pgdb,5432</pre> 2. Ändern Sie die AWS SCT Konfigurationsparameter gemäß Ihren Anforderungen in den folgenden Dateien: `project_settings.xml` `Oracle_PG_Test_Batch.xml` , und`ORACLE-orcl-to-POSTGRESQL.xml` .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das `run_aws_sct.py` Python-Skript aus.	Führen Sie das `run_aws_sct.py` Python-Skript mit dem folgenden Befehl aus: `$ python run_aws_sct.py database_migration.txt` Das Python-Skript konvertiert die Datenbankobjekte von Oracle nach PostgreSQL und erstellt SQL-Dateien im PostgreSQL-Format. Das Skript erstellt auch die PDF-Datei`Database migration assessment report` , die Ihnen detaillierte Empfehlungen und Konvertierungsstatistiken für Datenbankobjekte bietet.	DBA
Erstellen Sie Objekte in Amazon RDS for PostgreSQL.	1. Ändern Sie die von generierten SQL-Dateien manuell AWS SCT, falls erforderlich. 2. Führen Sie die SQL-Dateien aus und erstellen Sie Objekte in Ihrer Amazon RDS for PostgreSQL PostgreSQL-DB-Instance.	DBA

Konfigurieren und erstellen Sie AWS DMS Aufgaben mithilfe von und AWS CLIAWS CloudFormation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS DMS Replikationsinstanz.	Melden Sie sich bei der an AWS Management Console, öffnen Sie die AWS DMS Konsole und erstellen Sie eine Replikationsinstanz, die Ihren Anforderungen entsprechend konfiguriert ist. Weitere Informationen finden Sie in der Dokumentation unter Erstellen einer Replikationsinstanz und in der AWS DMS Dokumentation unter Wie erstelle ich eine AWS DMS Replikationsinstanz. AWS -Support	DBA
Erstellen Sie den Quellendpunkt.	Wählen Sie in der AWS DMS Konsole Endpoints aus und erstellen Sie dann einen Quellendpunkt für die Oracle-Datenbank entsprechend Ihren Anforderungen. **Note** Das zusätzliche Verbindungsattribut muss `numberDataTypeScale` einen `-2` Wert haben.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie in der AWS DMS Dokumentation unter Quell- und Zielendpunkte erstellen.	
Erstellen Sie den Zielendpunkt.	Wählen Sie in der AWS DMS Konsole Endpoints aus und erstellen Sie dann einen Zielendpunkt für die PostgreSQL-Datenbank gemäß Ihren Anforderungen. Weitere Informationen finden Sie in der Dokumentation unter Quell- und Zielendpunkte erstellen. AWS DMS	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie die AWS DMS Replikationsdetails so, dass sie von der aus ausgeführt AWS CLI werden sollen.	Konfigurieren Sie die AWS DMS Quell- und Zielendpunkte sowie die Replikationsdetails in der `dms-arn-list.txt` Datei mit dem Quellendpunkt-ARN, dem Zielendpunkt-ARN und dem Replizierungsinstanz-ARN im folgenden Format:
	`#sourceARN,targetARN,repARN`
	`arn:aws:dms:us-east-1:123456789012:endpoint:EH7AINRUDZ5GOYIY6HVMXECMCQ`
	`arn:aws:dms:us-east-1:123456789012:endpoint:HHJVUV57N7O3CQF4PJZKGIOYY5`
	`arn:aws:dms:us-east-1:123456789012:rep:LL57N77AQQAHHJF4PJFHNEDZ5G`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das `dms-create-task.py` Python-Skript aus, um die AWS DMS Aufgaben zu erstellen.	1. Führen Sie das `dms-create-task.py` Python-Skript mit dem folgenden Befehl aus: `$ python dms-create-task.py database_migration.txt dms-arn-list.txt <cft-stack-name> <migration-type>` Wobei: • `database_migration.txt` ist die Textdatei für die Datenbankmigration. • `dms-arn-list.txt` ist die ARN-Liste für AWS DMS. • `<cft-stack-name>` ist der benutzerdefinierte AWS CloudFormation Stack-Name. • `<migration-type>` ist `full-load` , `cdc` oder `full-load-and-cdc` . 2. Abhängig von Ihrem Migrationstyp können Sie die folgenden Befehle verwenden, um drei Arten von AWS DMS Aufgaben zu erstellen: • `$ python dms-create-task.py`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`database_migration .txt dms-arn-l ist.txt dms-cli-c ft-stack full-load` • `$ python dms- create-task.py database_migration .txt dms-arn-l ist.txt dms-cli-c ft-stack cdc` • `$ python dms- create-task.py database_migration .txt dms-arn-l ist.txt dms-cli-c ft-stack full-load -and-cdc`	
Stellen Sie sicher, dass die AWS DMS Aufgaben bereit sind.	Überprüfen Sie auf der AWS DMS Konsole im Abschnitt `Ready` Status, ob Ihre AWS DMS Aufgaben den Status haben.	DBA

Starten und beenden Sie die AWS DMS Aufgaben mit dem AWS CLI

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starte die AWS DMS Aufgaben.	Führen Sie das `dms-start -task.py` Python-Skript mit dem folgenden Befehl aus:	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`$ python dms-start-task.py start '<cdc-start-datetime>'` **Note** Das Startdatum und die Startzeit müssen im `'YYYY-MM-DDTHH:MI:SS'` Format `'DD-MON-YYYY'` oder angegeben werden (z. B. `'01-Dec-2019'` oder`'2018-03-08T12:12:12'`). Sie können den Status der AWS DMS Aufgabe auf der Registerkarte Tabellens tatistiken auf der Seite Aufgaben der AWS DMS Konsole überprüfen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Daten.	1. Nach Abschluss der Volllastmigration wird die Aufgabe kontinuierlich für CDC ausgeführt. 2. Wenn CDC abgeschlossen ist oder keine Änderungen mehr migriert werden müssen, überprüfen und validieren Sie die Ergebnisse und Daten der Migrationsaufgaben in Ihren Oracle- und PostgreSQL-Datenbanken. Sie können Ihre Daten überprüfen, indem Sie die Status- und Zählspalten (`Validation state`, `Validation pending`, `Validation failed`, `Validation suspended`, und `Validation details`) auf der Registerkarte Tabellenstatistiken Ihrer Datenbankmigrationsaufgabe auf der Seite Aufgaben der Konsole überprüfen. AWS DMS Weitere Informationen finden Sie in der AWS DMS Dokumentation unter AWS DMS Datenvalidierung.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stoppen Sie die AWS DMS Aufgaben.	Führen Sie das Python-Skript mit dem folgenden Befehl aus: `$ python dms-start-task.py stop` **Note** AWS DMS Aufgaben werden je nach `failed` Validieru ngsstatus möglicher weise mit einem Status beendet. Weitere Informati onen finden Sie im folgenden Abschnitt.	DBA

Fehlerbehebung

Problem	Lösung
AWS SCT Quell- und Zieltestverbindungen schlagen fehl.	Konfigurieren Sie die JDBC-Treiberversionen und die Regeln für den eingehenden Datenverk ehr der VPC-Sicherheitsgruppe so, dass sie den eingehenden Datenverkehr akzeptieren.
Der Testlauf am Quell- oder Zielendpunkt schlägt fehl.	Überprüfen Sie, ob sich die Endpunkte instellungen und die Replikationsinstanz im `Available` Status befinden. Überprüfen Sie, ob der Status der Endpunktverbindung lautet`Successful` .

Problem	Lösung
	Weitere Informationen finden Sie in der AWS -Support Dokumentation unter Wie behebe ich Fehler bei der AWS DMS-Endpunktkonnektivität?.
Der Volllastlauf schlägt fehl.	Überprüfen Sie, ob die Quell- und Zieldatenbanken übereinstimmende Datentypen und Größen haben. Weitere Informationen finden Sie in der AWS DMS Dokumentation unter Problembehandlung AWS DMS bei Migrationsaufgaben.
Es treten Fehler beim Validierungslauf auf.	Prüfen Sie, ob die Tabelle einen Primärschlüssel hat, da Tabellen, die keine Primärschlüssel sind, nicht validiert werden. Wenn die Tabelle einen Primärschlüssel enthält und Fehler auftreten, überprüfen Sie, ob das zusätzliche Verbindungsattribut im Quellendpunkt einen hat`numberDataTypeScale=-2` . Weitere Informationen finden Sie in der AWS DMS Dokumentation unter Endpunkteinstellungen bei Verwendung von Oracle als Quelle für AWS DMSOracleSettings, und Problembehandlung.

Zugehörige Ressourcen

- Installation und Konfiguration AWS SCT
- Einführung in AWS DMS (Video)
- Beispiele für CloudFormation Stack-Operationsbefehle für AWS CLI und PowerShell
- Navigieren in der Benutzeroberfläche des AWS SCT
- Verwenden einer Oracle-Datenbank als Quelle für AWS DMS

- Verbindung zu Oracle-Datenbanken herstellen mit AWS SCT
- Verwendung einer PostgreSQL-Datenbank als Ziel für AWS DMS
- Quellen für die Datenmigration
- Ziele für die Datenmigration
- Cloudformation (AWS CLI Dokumentation)
- create-stack (Dokumentation)AWS CLI
- dms (Dokumentation)AWS CLI

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Migrieren Sie Amazon RDS for Oracle zu Amazon RDS for PostgreSQL im SSL-Modus mithilfe von AWS DMS

Erstellt von Pinesh Singal (AWS)

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer Amazon Relational Database Service (Amazon RDS) für Oracle-Datenbank-Instance zu einer Amazon RDS for PostgreSQL PostgreSQL-Datenbank in der Amazon Web Services (AWS) -Cloud. Um Verbindungen zwischen den Datenbanken zu verschlüsseln, verwendet das Muster die Zertifizierungsstelle (CA) und den SSL-Modus in Amazon RDS und AWS Database Migration Service (AWS DMS).

Das Muster beschreibt eine Online-Migrationsstrategie mit geringen oder keinen Ausfallzeiten für eine Oracle-Quelldatenbank mit mehreren Terabyte und einer hohen Anzahl von Transaktionen. Aus Gründen der Datensicherheit verwendet das Muster SSL bei der Übertragung der Daten.

Dieses Muster verwendet das AWS Schema Conversion Tool (AWS SCT), um das Amazon RDS for Oracle Oracle-Datenbankschema in ein Amazon RDS for PostgreSQL PostgreSQL-Schema zu konvertieren. Anschließend verwendet das Muster AWS DMS, um Daten von der Amazon RDS for Oracle Oracle-Datenbank zur Amazon RDS for PostgreSQL PostgreSQL-Datenbank zu migrieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Amazon RDS-Datenbankzertifizierungsstelle (CA), konfiguriert nur mit rds-ca-rsa2048-g1
  - Das rds-ca-2019-Zertifikat ist im August 2024 abgelaufen.
  - Das rds-ca-2015-Zertifikat ist am 5. März 2020 abgelaufen.
- AWS SCT
- AWS DMS
- pgAdmin
- SQL-Tools (z. B. SQL Developer oder SQL*Plus)

Einschränkungen

- Amazon RDS for Oracle Oracle-Datenbank — Die Mindestanforderung gilt für die Oracle-Versionen 19c für die Enterprise- und Standard Two-Editionen.
- Amazon RDS for PostgreSQL PostgreSQL-Datenbank — Die Mindestanforderung gilt für PostgreSQL Version 12 und höher (für Versionen 9.x und höher).

Produktversionen

- Amazon RDS for Oracle Oracle-Datenbank-Instance Version 12.1.0.2
- Amazon RDS for PostgreSQL PostgreSQL-Datenbank-Instance Version 11.5

Architektur

Quelltechnologie-Stack

- Eine Amazon RDS for Oracle Oracle-Datenbank-Instance mit Version 12.1.0.2.v18.

Zieltechnologie-Stack

- AWS DMS
- Eine Amazon RDS for PostgreSQL PostgreSQL-Datenbank-Instance mit Version 11.5.

Zielarchitektur

Das folgende Diagramm zeigt die Architektur für die Datenmigrationsarchitektur zwischen Oracle-Datenbanken (Quell-) und PostgreSQL-Datenbanken (Ziel). Die Architektur umfasst Folgendes:

- Eine virtuelle private Cloud (VPC)
- Eine Verfügbarkeitszone
- Ein privates Subnetz
- Eine Amazon RDS for Oracle Oracle-Datenbank
- Eine AWS-DMS-Replikationsinstanz
- Eine RDS-Datenbank für PostgreSQL

Um Verbindungen für Quell- und Zieldatenbanken zu verschlüsseln, müssen der CA- und SSL-Modus in Amazon RDS und AWS DMS aktiviert sein.

Tools

AWS-Services

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS-Cloud oder zwischen Kombinationen von Cloud- und lokalen Setups.
- Amazon Relational Database Service (Amazon RDS) für Oracle unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Oracle-Datenbank in der AWS-Cloud.
- Amazon Relational Database Service (Amazon RDS) für PostgreSQL unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen PostgreSQL-Datenbank in der AWS-Cloud.
- Das AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist.

Andere Dienste

- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL. Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, verwalten und verwenden können.

Bewährte Methoden

Amazon RDS stellt neue CA-Zertifikate als eine bewährte Methode für die AWS-Sicherheit bereit. Informationen zu den neuen Zertifikaten und den unterstützten AWS-Regionen finden Sie unter SSL/TLS zum Verschlüsseln einer Verbindung zu einer DB-Instance oder einem DB-Cluster verwenden.

Wenn Ihre RDS-Instance derzeit über ein CA-Zertifikat `rds-ca-2019` verfügt und Sie ein Upgrade durchführen möchten`rds-ca-rsa2048-g1`, folgen Sie den Anweisungen unter Aktualisieren Ihres CA-Zertifikats durch Ändern Ihrer DB-Instance oder Ihres Clusters oder Aktualisieren Ihres CA-Zertifikats durch Wartung.

Epen

Amazon RDS for Oracle Oracle-Instance konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Oracle-Datenbankinstanz.	Melden Sie sich bei Ihrem AWS-Konto an, öffnen Sie die AWS-Managementkonsole und navigieren Sie zur Amazon RDS-Konsole. Wählen Sie in der Konsole Create database und dann Oracle aus.	Allgemein AWS, DBA
Konfigurieren Sie Sicherheitsgruppen.	Konfigurieren Sie Sicherheitsgruppen für eingehenden und ausgehenden Datenverkehr.	Allgemeines AWS
Erstellen Sie eine Optionsgruppe.	Erstellen Sie eine Optionsgruppe in derselben VPC und Sicherheitsgruppe wie die Amazon RDS for Oracle Oracle-Datenbank. Wählen Sie für Option die Option SSL aus. Wählen Sie für Port 2484 (für SSL-Verbindungen) aus.	Allgemeines AWS
Konfigurieren Sie die Optionseinstellungen.	Verwenden Sie die folgenden Einstellungen: • `SQLNET.CIPHER_SUITE : SSL_RSA_WITH_AES_256_CBC_SHA` • `SQLNET.SSL_VERSION : 1.2 or 1.0`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die RDS für Oracle-DB-Instance.	Legen Sie das CA-Zertifikat auf rds-ca-rsa2048-g1 fest. Fügen Sie unter Optionsgruppe die zuvor erstellte Optionsgruppe hinzu.	DBA, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Vergewissern Sie sich, dass die RDS for Oracle DB-Instance verfügbar ist.	Stellen Sie sicher, dass die Amazon RDS for Oracle Oracle-Datenbank-Instance betriebsbereit ist und dass auf das Datenbankschema zugegriffen werden kann.
	
	Verwenden Sie den Befehl von der `sqlplus` Befehlszeile aus, um eine Verbindung zur RDS for Oracle-DB herzustellen.
	
	`$ sqlplus orcl/**** @myoracledb.cokmvis0v46q.us-east-1.rds.amazonaws.com:1521/ORCL`
	`SQL*Plus: Release 12.1.0.2.0 Production on Tue Oct 15 18:11:07 2019`
	`Copyright (c) 1982, 2016, Oracle. All rights reserved.`
	`Last Successful login time: Mon Dec 16 2019 23:17:31 +05:30`
	`Connected to:`
	`Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production`
	`With the Partitioning, OLAP, Advanced Analytics and Real Application Testing options`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`SQL>`	
Erstellen Sie Objekte und Daten in der Datenbank RDS for Oracle.	Erstellen Sie Objekte und fügen Sie Daten in das Schema ein.	DBA

Amazon RDS for PostgreSQL PostgreSQL-Instance konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Datenbank RDS für PostgreSQL.	Wählen Sie auf der Seite Datenbank erstellen der Amazon RDS-Konsole PostgreSQL aus, um eine Amazon RDS for PostgreSQL PostgreSQL-Datenbank-Instanz zu erstellen.	DBA, Allgemeines AWS
Konfigurieren Sie Sicherheitsgruppen.	Konfigurieren Sie Sicherheitsgruppen für eingehenden und ausgehenden Datenverkehr.	Allgemeines AWS
Erstellen Sie eine Parametergruppe.	Wenn Sie PostgreSQL Version 11.x verwenden, erstellen Sie eine Parametergruppe, um SSL-Parameter festzulegen. In PostgreSQL Version 12 ist die SSL-Parametergruppe standardmäßig aktiviert.	Allgemeines AWS
Parameter bearbeiten.	Ändern Sie den `rds.force_ssl` Parameter auf 1 (ein).	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Standardmäßig ist der `ssl` Parameter 1 (on). Wenn Sie den `rds.force_ssl` Parameter auf setzen1, zwingen Sie, dass alle Verbindungen nur im SSL-Modus eine Verbindung herstellen.	
Ändern Sie die DB-Instance RDS für PostgreSQL.	Legen Sie das CA-Zertifikat auf 2048-g1 fest. rds-ca-rsa Hängen Sie je nach Ihrer PostgreSQL-Version die Standardparametergruppe oder die zuvor erstellte Parametergruppe an.	DBA, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vergewissern Sie sich, dass die RDS for PostgreSQL-DB-Instance verfügbar ist.	Stellen Sie sicher, dass die Amazon RDS for PostgreSQ L PostgreSQL-Datenbank betriebsbereit ist. Der `psql` Befehl stellt eine SSL-Verbindung her, die über die Befehlszeile `sslmode` festgelegt wurde. Eine Möglichkeit besteht darin, die Parametergruppe festzulegen `sslmode=1` und eine `psql` Verbindun g zu verwenden, ohne den `sslmode` Parameter in den Befehl aufzunehmen. Die folgende Ausgabe zeigt, dass die SSL-Verbindung hergestellt wurde. `$ psql -h mypgdbins tance.cokmvis0v46q .us-east-1.rds.ama zonaws.com -p 5432 "dbname=pgdb user=pgus er" Password for user pguser: psql (11.3, server 11.5) SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compressi on: off)`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`Type "help" for help.`
	`pgdb=>`
	
	Eine zweite Option besteht darin, die Parametergruppe festzulegen `sslmode=1` und den `sslmode` Parameter in den `psql` Befehl aufzunehmen.
	
	Die folgende Ausgabe zeigt, dass die SSL-Verbindung hergestellt wurde.
	
	`$ psql -h mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com -p 5432 "dbname=pgdb user=pguser sslmode=require"`
	`Password for user pguser:`
	`psql (11.3, server 11.5)`
	`SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)`
	`Type "help" for help.`
	`pgdb=>`	

AWS SCT konfigurieren und ausführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie AWS SCT.	Installieren Sie die neueste Version der AWS SCT-Anwendung.	Allgemeines AWS
Konfigurieren Sie AWS SCT mit JDBC-Treibern.	Laden Sie die Java Database Connectivity (JDBC) -Treiber für Oracle (ojdbc8.jar) und PostgreSQL (postgresql-42.2.5.jar) herunter. Um die Treiber in AWS SCT zu konfigurieren, wählen Sie Einstellungen, Globale Einstellungen, Treiber.	Allgemeines AWS
Erstellen Sie das AWS SCT-Projekt.	Erstellen Sie das AWS SCT-Projekt und den Bericht mit Oracle als Quell-DB-Engine und Amazon RDS for PostgreSQL als Ziel-DB-Engine: 1. Testen Sie Verbindungen zur Oracle-Quelldatenbank und zur Zieldatenbank Amazon RDS for PostgreSQL, indem Sie Verbindungsdetails angeben. Für die Oracle-Quelldatenbank sind die folgenden Berechtigungen oder Privilegien erforderlich:	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `CONNECT` • `SELECT_CATALOG_ROLE` • `SELECT ANY DICTIONARY` • `SELECT on SYS.USER$ TO <sct_user>` Weitere Informationen finden Sie unter Verwenden von Oracle Database als Quelle für AWS SCT. Sowohl Quell- als auch Zielverbindungen müssen erfolgreich sein, bevor AWS SCT den Migrationsbericht starten kann. 2. Geben Sie nach dem Bericht das zu konvertierende Schema ein und wählen Sie Fertig stellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie Datenbank objekte.	1. Wählen Sie Schema laden. AWS SCT zeigt die Quell- und die konvertierten Zielobjekte an, einschlie ßlich fehlerhafter Objekte. Aktualisieren Sie alle falschen Objekte in der Zieldatenbank. 2. Überprüfen Sie die Fehler und beheben Sie sie durch manuelles Eingreifen. 3. Nachdem alle Fehler behoben wurden, wählen Sie erneut Schema laden. 4. Wählen Sie Auf Datenbank anwenden. 5. Stellen Sie eine Connect zu pgAdmin oder einem anderen Tool her, das eine PostgreSQL-DB-Verb indung unterstützt, und überprüfen Sie das Schema und die Objekte.	DBA, Allgemeines AWS

AWS DMS konfigurieren und ausführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Replikati onsinstanz.	1. Melden Sie sich bei Ihrem Konto an, öffnen Sie die AWS-Managementkonsole	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und navigieren Sie zur AWS DMS-Konsole. 2. Erstellen Sie eine Replizierungsinstanz mit gültigen Einstellungen für die VPC, die Sicherheitsgruppe, die Availability Zone und zusätzliche Verbindungsattribute.	
Importieren Sie das Zertifikat.	Laden Sie das Zertifikatspaket (PEM) für Ihre AWS-Region herunter. Das Paket enthält sowohl die `rds-ca-2019` Zwischen- als auch die Stammzertifikate. Das Paket enthält auch die `rds-ca-ecc384-g1` CA-Stammzertifikate `rds-ca-rsa2048-g1` `rds-ca-rsa4096-g1` , und. Ihr Anwendungs-Trustspeicher muss nur das Root-CA-Zertifikat registrieren.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Quellendpunkt.	1. Erstellen Sie einen Quellendpunkt für Amazon RDS for Oracle, indem Sie Select RDS DB-Instance und dann die RDS for Oracle DB-Instance auswählen, die Sie erstellt haben. Die Details zur Endpunktkonfiguration werden automatisch ausgefüllt. 2. Wählen Sie Zugangsinformationen manuell bereitstellen aus. Stellen Sie sicher, dass Sie für Port 2484 eingeben. 3. Wählen Sie im Secure Socket Layer (SSL) -Modus das CA-Zertifikat aus `verify-ca` , das Sie zuvor erstellt haben, und wählen Sie es anschließend aus. 4. Fügen Sie unter Endpunkteinstellungen das zusätzliche Verbindungsattribut hinzu `NumberDataTypeScale=-2` , um den `NUMBER` Datentyp ohne Größe zu unterstützen. Weitere Informationen finden Sie unter Verwenden einer	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Oracle-Datenbank als Quelle für den AWS Database Migration Service.	
Erstellen Sie den Zielendpunkt.	1. Erstellen Sie einen Zielendpunkt für Amazon RDS for PostgreSQL, indem Sie Select RDS DB-Instance und dann Ihre RDS for PostgreSQL DB-Instance auswählen. Die Details zur Endpunktkonfiguration werden automatisch ausgefüllt. 2. Wählen Sie Zugangsinformationen manuell bereitstellen aus. Stellen Sie sicher, dass Sie für Port 2484 eingeben. Weitere Informationen finden Sie unter Verwenden einer PostgreSQL-Datenbank als Ziel für den AWS Database Migration Service.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Endpunkte.	1. Testen Sie die Quell- und Zielendpunkte, um sicherzustellen, dass beide erfolgreich und verfügbar sind. 2. Wenn ein Test fehlschlägt, stellen Sie sicher, dass die Regeln für eingehende Zugriffe in der Sicherheitsgruppe gültig sind.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Migration saufgaben.	Gehen Sie wie folgt vor, um eine Migrationsaufgabe für Volllast und Change Data Capture (CDC) oder für die Datenvalidierung zu erstellen: 1. Um eine Datenbank migrationsaufgabe zu erstellen, wählen Sie die Replikationsinstanz, den Quelldatenbankendp unkt und den Zieldaten bankendpunkt aus. Geben Sie den Migrationstyp als einen der folgenden an: • Migrieren Sie vorhandene Daten (Volllast) • Nur Datenänderungen replizieren (CDC) • Migrieren Sie vorhanden e Daten und replizieren Sie laufende Änderungen (Volllast und CDC) 2. Unter Tabellenzuordnungen können Sie Auswahlregeln und Transformationsregeln im GUI- oder JSON-Format konfigurieren: • Wählen Sie unter Auswahlregeln das Schema aus, geben Sie den Tabellennamen ein und wählen Sie die Aktion (Einschließen oder	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ausschließen) aus, die konfiguriert werden soll, z. B. Schema ORCL, Tabellenname%, Aktion Einschließen. • Führen Sie unter Transformationsregeln einen der folgenden Schritte aus: • Wählen Sie das Schema und dann die Aktion (Groß- und Kleinschreibung, Präfix, Suffix) aus, z. B. Zielschema ORCL, Aktion Kleinbuchstaben erstellen. • Wählen Sie das Schema aus, geben Sie den Tabellenn amen ein und wählen Sie die Aktion aus (Groß- und Kleinschr eibung, Präfix, Suffix), z. B. Zielschema ORCL, Tabelle%, Action Make kleingesc hrieben. 3. Aktivieren Sie die Amazon CloudWatch Logs-Über wachung. 4. Fügen Sie für die Zuordnungsregeln den	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	folgenden JSON-Code hinzu. `{ "rules": [{ "rule-type": "transformation", "rule-id": "1", "rule-name": "1", "rule-target": "table", "object-locator": { "schema-name": "%", "table-name": "%" }, "rule-action": "convert-lowercase", "value": null, "old-value": null }, { "rule-type": "transformation", "rule-id": "2", "rule-name": "2", "rule-target": "schema",`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	"object-locator": {
	"schema-name": "ORCL",
	"table-name": "%"
	},
	"rule-action": "convert-lowercase",
	"value": null,
	"old-value": null
	},
	{
	"rule-type": "selection",
	"rule-id": "3",
	"rule-name": "3",
	"object-locator": {
	"schema-name": "ORCL",
	"table-name": "DEPT"
	},
	"rule-action": "include",
	"filters": []
	}
	]
	}	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Planen Sie den Produktionslauf.	Bestätigen Sie Ausfallzeiten mit Stakeholdern wie Anwendungsbesitzern, um AWS DMS in Produktionssystemen auszuführen.	Leiter der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die -Migratio nsaufgabe aus.	1. Starten Sie die AWS-DMS-Aufgabe mit dem Status Bereit und überwachen Sie die Protokolle der Migration saufgaben in Amazon CloudWatch auf Fehler. Wenn Sie als Migration styp Bestehende Daten migrieren und laufende Änderungen replizieren wählen und der Status Load complete running replication lautet, ist der vollständige Ladevorgang mit der CDC-Datenmigration abgeschlo ssen und die Validierung läuft. 2. Nachdem Sie die Migration gestartet haben, finden Sie weitere Informationen zur SSL-Verbindung unter. CloudWatch CloudWatc h Zeigt für Oracle die folgende Verbindun gszeichenfolge an. `2019-12-17T09:15:1 1 [SOURCE_U NLOAD ]I: Connectin g to Oracle: Beginning session (oracle_endpoint_c onn.c:834)`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Die PostgreSQL-Verbindungszeichenfolge wird dem folgenden Beispiel ähneln. `2019-12-17T09:15:11 [TARGET_LOAD ]I: Going to connect to ODBC connection string: PROTOCOL=7.4-0;DRIVER={PostgreSQL};SERVER=mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com;DATABASE=pgdb;PORT=5432;sslmode=require;UID=pguser; (odbc_endpoint_imp.c:2218)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Daten.	Überprüfen Sie die Ergebnisse und Daten der Migrationsaufgaben in den Oracle-Quelldatenbanken und den PostgreSQL-Zieldatenbanken: 1. Connect zu pgAdmin her und überprüfen Sie die Daten in Ihrer PostgreSQL-Datenbank mit Schema. `ORCL` 2. Überprüfen Sie für CDC die laufenden Änderungen, indem Sie Daten in die Oracle-Quelldatenbank einfügen oder aktualisieren.	DBA
Beenden Sie die Migrationsaufgabe.	Nachdem Sie die Datenüberprüfung erfolgreich abgeschlossen haben, beenden Sie die Migrationsaufgabe.	Allgemeines AWS

Säubere die Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die AWS DMS-Aufgaben.	1. Navigieren Sie in der AWS DMS-Konsole zu Datenbankmigrationsaufgaben und beenden Sie alle laufenden oder laufenden AWS DMS-Aufgaben.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie die Aufgabe oder die Aufgaben aus, klicken Sie auf Aktionen und dann auf Löschen.	
Löschen Sie die AWS DMS-Endpunkte.	Wählen Sie die Quell- und Zielendpunkte aus, die Sie erstellt haben, wählen Sie Aktionen und dann Löschen aus.	Allgemeines AWS
Löschen Sie die AWS DMS-Replikationsinstanz.	Wählen Sie die Replikati onsinstanz aus, klicken Sie auf Aktionen und dann auf Löschen.	Allgemeines AWS
Löschen Sie die PostgreSQL-Datenbank.	1. Wählen Sie auf der Amazon RDS-Konsole Datenbanken aus. 2. Wählen Sie die PostgreSQ L-Datenbankinstanz aus, die Sie erstellt haben, klicken Sie auf Aktionen und dann auf Löschen.	Allgemeines AWS
Löschen Sie die Oracle-Da tenbank.	Wählen Sie in der Amazon RDS-Konsole die Oracle-Da tenbank-Instance aus, klicken Sie auf Actions und anschließ end auf Delete.	Allgemeines AWS

Fehlerbehebung

Problem	Lösung
Die Quell- und Zieltestverbindungen von AWS SCT schlagen fehl.	Konfigurieren Sie JDBC-Treiberversionen und eingehende VPC-Sicherheitsgruppenregeln, um den eingehenden Datenverkehr zu akzeptieren.
Der Testlauf für den Oracle-Quellendpunkt schlägt fehl.	Überprüfen Sie die Endpunkteinstellungen und ob die Replikationsinstanz verfügbar ist.
Der Volllastlauf der AWS DMS-Aufgabe schlägt fehl.	Prüfen Sie, ob die Quell- und Zieldatenbanken übereinstimmende Datentypen und Größen haben.
Die AWS DMS-Validierungs-Migrationsaufgabe gibt Fehler zurück.	1. Prüfen Sie, ob die Tabelle einen Primärschlüssel hat. Tabellen ohne Primärschlüssel werden nicht validiert. 2. Wenn die Tabelle einen Primärschlüssel hat, aber Fehler zurückgibt, überprüfen Sie das zusätzliche Verbindungsattribut im Quellendpunkt. Das zusätzliche Verbindungsattribut `numberDataTypeScale=-2` muss den `NUMBER` Datentyp ohne Größe dynamisch auf der Grundlage der in der Tabelle verfügbaren Daten unterstützen.

Zugehörige Ressourcen

Datenbanken

- Amazon RDS für Oracle
- Amazon RDS für PostgreSQL

SSL-DB-Verbindung

- Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer DB-Instance
  - Verwenden von SSL mit einer RDS für Oracle-DB-Instance
  - Verbindungen zu RDS für PostgreSQL mit SSL/TLS sichern
  - Laden Sie Zertifikatspakete für bestimmte AWS-Regionen herunter
    - Laden Sie das CA-2019-Stammzertifikat herunter (im August 2024 abgelaufen)
- Arbeiten mit Optionsgruppen
  - Optionen zu Oracle-DB-Instances hinzufügen
  - Oracle Secure Sockets Layer
- Mit Parametergruppen arbeiten
- PostgreSQL-Verbindungsparameter sslmode
- SSL von JDBC aus verwenden
- Rotation Ihres SSL/TLS-Zertifikats
  - Aktualisierung Ihres CA-Zertifikats durch Änderung Ihrer DB-Instance oder Ihres Clusters
  - Aktualisierung Ihres CA-Zertifikats durch Wartung

AWS SCT

- AWS-Schemakonvertierungstool
- Benutzerhandbuch für das AWS Schema Conversion Tool
- Verwenden der AWS SCT-Benutzeroberfläche
- Verwendung von Oracle Database als Quelle für AWS SCT

AWS DMS

- AWS Database Migration Service
- AWS Database Migration Service — Benutzerhandbuch
  - Verwenden einer Oracle-Datenbank als Quelle für AWS DMS
  - Verwenden einer PostgreSQL-Datenbank als Ziel für AWS DMS
- Verwenden von SSL mit dem AWS Database Migration Service
- Migrieren von Anwendungen, auf denen relationale Datenbanken ausgeführt werden, zu AWS

Zusätzliche Informationen

Die Zertifikate der Amazon RDS Certificate Authority `rds-ca-2019` sind im August 2024 abgelaufen. Wenn Sie SSL oder TLS mit Zertifikatsüberprüfung verwenden oder verwenden möchten, um eine Verbindung zu Ihren RDS-DB-Instances oder Multi-AZ-DB-Clustern herzustellen, sollten Sie die Verwendung eines der neuen CA-Zertifikate in Betracht ziehen:`rds-ca-rsa2048-g1`,`rds-ca-rsa4096-g1`, oder`rds-ca-ecc384-g1`.

Migrieren Sie Oracle SERIALLY_REUSABLE Pragma-Pakete nach PostgreSQL

Erstellt von Vinay Paladi (AWS)

Übersicht

Dieses Muster bietet einen step-by-step Ansatz für die Migration von Oracle-Paketen, die als SERIALLY_REUSABLE Pragma definiert sind, nach PostgreSQL auf Amazon Web Services (AWS). Bei diesem Ansatz wird die Funktionalität des Pragmas SERIALLY_REUSABLE beibehalten.

PostgreSQL unterstützt das Konzept von Paketen und das Pragma SERIALLY_REUSABLE nicht. Um ähnliche Funktionen in PostgreSQL zu erhalten, können Sie Schemas für Pakete erstellen und alle zugehörigen Objekte (wie Funktionen, Prozeduren und Typen) innerhalb der Schemas bereitstellen. Um die Funktionalität des Pragmas SERIALLY_REUSABLE zu erreichen, verwendet das in diesem Muster bereitgestellte Beispiel-Wrapper-Funktionsskript ein AWS Schema Conversion Tool (AWS SCT) -Erweiterungspaket.

Weitere Informationen finden Sie unter SERIALLY_REUSABLE Pragma in der Oracle-Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Die neueste Version von AWS SCT und die erforderlichen Treiber
- Eine Amazon Aurora PostgreSQL-kompatible Edition-Datenbank oder ein Amazon Relational Database Service (Amazon RDS) für PostgreSQL-Datenbank

Produktversionen

- Oracle Database Version 10g und höher

Architektur

Quelltechnologie-Stack

- Oracle-Datenbank vor Ort

Zieltechnologie-Stack

- Aurora PostgreSQL-kompatibel oder Amazon RDS für PostgreSQL
- AWS SCT

Migrationsarchitektur

Tools

AWS-Services

- Das AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist.
- Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt.
- Amazon Relational Database Service (Amazon RDS) für PostgreSQL unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen PostgreSQL-Datenbank in der AWS-Cloud.

Andere Tools

- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL. Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, verwalten und verwenden können.

Epen

Migrieren Sie das Oracle-Paket mithilfe von AWS SCT

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie AWS SCT ein.	Konfigurieren Sie die AWS SCT-Konnektivität zur Quelldatenbank. Weitere Informationen finden Sie unter Verwenden von Oracle	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Database als Quelle für AWS SCT.	
Konvertiere das Skript.	Verwenden Sie AWS SCT, um das Oracle-Paket zu konvertieren, indem Sie die Zieldatenbank als Aurora PostgreSQL-kompatibel auswählen.	DBA, Entwickler
Speichern Sie die .sql-Dateien.	Bevor Sie die SQL-Datei speichern, ändern Sie die Option Projekteinstellungen in AWS SCT auf Einzelne Datei pro Phase. AWS SCT teilt die .sql-Datei je nach Objekttyp in mehrere .sql-Dateien auf.	DBA, Entwickler
Ändern Sie den Code.	Öffnen Sie die von AWS SCT generierte `init` Funktion und ändern Sie sie, wie im Beispiel im Abschnitt Zusätzliche Informationen gezeigt. Es wird eine Variable hinzugefügt, um die Funktionalität `pg_serialize = 0` zu erreichen.	DBA, Entwickler
Testen Sie die Konvertierung.	Stellen Sie die `init` Funktion in der Aurora PostgreSQL-kompatiblen Datenbank bereit und testen Sie die Ergebnisse.	DBA, Entwickler

Zugehörige Ressourcen

- AWS-Schemakonvertierungstool

- Amazon RDS
- Funktionen von Amazon Aurora
- SERIALLY_REUSABLE Pragma

Zusätzliche Informationen

```
Source Oracle Code:

CREATE OR REPLACE PACKAGE test_pkg_var
IS
PRAGMA SERIALLY_REUSABLE;
PROCEDURE function_1
 (test_id number);
PROCEDURE function_2
 (test_id number
 );
END;

CREATE OR REPLACE PACKAGE BODY test_pkg_var
IS
PRAGMA SERIALLY_REUSABLE;
v_char VARCHAR2(20) := 'shared.airline';
v_num number := 123;

PROCEDURE function_1(test_id number)
IS
begin
dbms_output.put_line( 'v_char-'|| v_char);
dbms_output.put_line( 'v_num-'||v_num);
v_char:='test1';
function_2(0);
END;

PROCEDURE function_2(test_id number)
is
begin
dbms_output.put_line( 'v_char-'|| v_char);
dbms_output.put_line( 'v_num-'||v_num);
END;
END test_pkg_var;

Calling the above functions
```

```
set serveroutput on


EXEC test_pkg_var.function_1(1);


EXEC test_pkg_var.function_2(1);


Target Postgresql Code:


CREATE SCHEMA test_pkg_var;

CREATE OR REPLACE FUNCTION test_pkg_var.init(pg_serialize IN INTEGER DEFAULT 0)

RETURNS void
AS
$BODY$

DECLARE

BEGIN

if aws_oracle_ext.is_package_initialized( 'test_pkg_var' ) AND pg_serialize = 0

then

return;

end if;

PERFORM aws_oracle_ext.set_package_initialized( 'test_pkg_var' );

PERFORM aws_oracle_ext.set_package_variable( 'test_pkg_var', 'v_char',
 'shared.airline.basecurrency'::CHARACTER

VARYING(100));

PERFORM aws_oracle_ext.set_package_variable('test_pkg_var', 'v_num', 123::integer);

END;
```

```
$BODY$

LANGUAGE plpgsql;


CREATE OR REPLACE FUNCTION test_pkg_var.function_1(pg_serialize int default 1)

RETURNS void
AS

$BODY$
DECLARE

BEGIN

PERFORM test_pkg_var.init(pg_serialize);

raise notice 'v_char%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_char');

raise notice 'v_num%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_num');

PERFORM aws_oracle_ext.set_package_variable( 'test_pkg_var', 'v_char',
 'test1'::varchar);

PERFORM test_pkg_var.function_2(0);
END;

$BODY$
LANGUAGE plpgsql;


CREATE OR REPLACE FUNCTION test_pkg_var.function_2(IN pg_serialize integer default 1)

RETURNS void

AS

$BODY$

DECLARE

BEGIN

PERFORM test_pkg_var.init(pg_serialize);
```

```
raise notice 'v_char%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_char');

raise notice 'v_num%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_num');

END;
$BODY$
LANGUAGE plpgsql;


Calling the above functions

select test_pkg_var.function_1()

 select test_pkg_var.function_2()
```

Migrieren Sie externe Oracle-Tabellen zu Amazon Aurora PostgreSQL-kompatibel

Erstellt von Anuradha Chintha (AWS) und Rakesh Raghav (AWS)

Übersicht

Externe Tabellen geben Oracle die Möglichkeit, Daten abzufragen, die außerhalb der Datenbank in Flatfiles gespeichert sind. Sie können den ORACLE_LOADER-Treiber verwenden, um auf alle Daten zuzugreifen, die in einem beliebigen Format gespeichert sind und vom SQL*Loader-Hilfsprogramm geladen werden können. Sie können Data Manipulation Language (DML) nicht für externe Tabellen verwenden, aber Sie können externe Tabellen für Abfrage-, Join- und Sortieroperationen verwenden.

Amazon Aurora PostgreSQL-Compatible Edition bietet keine ähnliche Funktionalität wie externe Tabellen in Oracle. Stattdessen müssen Sie die Modernisierung nutzen, um eine skalierbare Lösung zu entwickeln, die funktionale Anforderungen erfüllt und sparsam ist.

Dieses Muster enthält Schritte für die Migration verschiedener Typen von externen Oracle-Tabellen zur Aurora PostgreSQL-kompatiblen Edition in der Amazon Web Services (AWS) Cloud mithilfe der Erweiterung. `aws_s3`

Wir empfehlen, diese Lösung gründlich zu testen, bevor Sie sie in einer Produktionsumgebung implementieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS-Befehlszeilenschnittstelle (AWS Command Line Interface, AWS CLI)
- Eine verfügbare Aurora PostgreSQL-kompatible Datenbankinstanz.
- Eine lokale Oracle-Datenbank mit einer externen Tabelle
- PG.Client-API
- Datendateien

Einschränkungen

- Dieses Muster bietet nicht die Funktionalität, um externe Oracle-Tabellen zu ersetzen. Die Schritte und der Beispielcode können jedoch weiter verbessert werden, um Ihre Ziele bei der Datenbankmodernisierung zu erreichen.

- Dateien sollten nicht das Zeichen enthalten, das in `aws_s3` Export- und Importfunktionen als Trennzeichen übergeben wird.

Produktversionen

- Um aus Amazon S3 in RDS for PostgreSQL zu importieren, muss auf der Datenbank PostgreSQL Version 10.7 oder höher ausgeführt werden.

Architektur

Quelltechnologie-Stack

- Oracle

Quellarchitektur

Zieltechnologie-Stack

- Amazon Aurora PostgreSQL-kompatibel
- Amazon CloudWatch
- AWS Lambda
- AWS Secrets Manager
- Amazon-Simple-Notification-Service (Amazon-SNS)
- Amazon Simple Storage Service (Amazon-S3)

Zielarchitektur

Das folgende Diagramm zeigt eine allgemeine Darstellung der Lösung.

1. Dateien werden in den S3-Bucket hochgeladen.
2. Die Lambda-Funktion wird initiiert.
3. Die Lambda-Funktion initiiert den DB-Funktionsaufruf.
4. Secrets Manager stellt die Anmeldeinformationen für den Datenbankzugriff bereit.
5. Abhängig von der DB-Funktion wird ein SNS-Alarm ausgelöst.

Automatisierung und Skalierung

Alle Ergänzungen oder Änderungen an den externen Tabellen können mit der Metadatenpflege behandelt werden.

Tools

- Amazon Aurora PostgreSQL-kompatibel — Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, PostgreSQL-kompatible und ACID-konforme relationale Datenbank-Engine, die die Geschwindigkeit und Zuverlässigkeit kommerzieller High-End-Datenbanken mit der Kosteneffizienz von Open-Source-Datenbanken kombiniert.
- AWS CLI — AWS Command Line Interface (AWS CLI) ist ein einheitliches Tool zur Verwaltung Ihrer AWS-Services. Mit nur einem Tool zum Herunterladen und Konfigurieren können Sie mehrere AWS-Services von der Befehlszeile aus steuern und über Skripts automatisieren.
- Amazon CloudWatch — Amazon CloudWatch überwacht die Ressourcen und die Nutzung von Amazon S3.
- AWS Lambda — AWS Lambda ist ein serverloser Rechenservice, der die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern, die Erstellung einer auslastungsorientierten Cluster-Skalierungslogik, die Verwaltung von Eventintegrationen oder die Verwaltung von Laufzeiten unterstützt. In diesem Muster führt Lambda die Datenbankfunktion immer dann aus, wenn eine Datei auf Amazon S3 hochgeladen wird.
- AWS Secrets Manager — AWS Secrets Manager ist ein Service zum Speichern und Abrufen von Anmeldeinformationen. Mit Secrets Manager können Sie hartcodierte Anmeldeinformationen in Ihrem Code, einschließlich Kennwörtern, durch einen API-Aufruf an Secrets Manager ersetzen, um das Geheimnis programmgesteuert abzurufen.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) bietet eine Speicherebene zum Empfangen und Speichern von Dateien zur Nutzung und Übertragung zum und vom Aurora PostgreSQL-kompatiblen Cluster.
- aws_s3 — Die `aws_s3` Erweiterung integriert Amazon S3 und Aurora PostgreSQL-kompatibel.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Herausgebern und Kunden. In diesem Muster wird Amazon SNS zum Senden von Benachrichtigungen verwendet.

Code

Immer wenn eine Datei im S3-Bucket platziert wird, muss eine DB-Funktion erstellt und von der verarbeitenden Anwendung oder der Lambda-Funktion aus aufgerufen werden. Einzelheiten finden Sie im Code (beigefügt).

Epen

Erstellen Sie eine externe Datei

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie der Quelldatenbank eine externe Datei hinzu.	Erstellen Sie eine externe Datei und verschieben Sie sie in das `oracle` Verzeichnis.	DBA

Das Ziel konfigurieren (Aurora PostgreSQL-kompatibel)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Aurora PostgreSQL-Datenbank.	Erstellen Sie eine DB-Instanz in Ihrem Amazon Aurora PostgreSQL-kompatiblen Cluster.	DBA
Erstellen Sie ein Schema, die Erweiterung aws_s3 und Tabellen.	Verwenden Sie den Code unter `ext_tbl_scripts` dem Abschnitt Zusätzliche Informationen. Die Tabellen enthalten tatsächliche Tabellen, Staging-Tabellen, Fehler- und Protokolltabellen sowie eine Metatabelle.	DBA, Entwickler
Erstellen Sie die DB-Funktion.	Um die DB-Funktion zu erstellen, verwenden Sie den Code unter `load_external_table_latest`	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Funktion im Abschnitt Zusätzliche Informationen.	

Lambda-Funktion erstellen und konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Rolle.	Erstellen Sie eine Rolle mit Zugriffsberechtigungen für Amazon S3 und Amazon Relational Database Service (Amazon RDS). Diese Rolle wird Lambda für die Ausführung des Musters zugewiesen.	DBA
So erstellen Sie die Lambda-Funktion:	Erstellen Sie eine Lambda-Funktion, die den Dateinamen aus Amazon S3 liest (z. B.`file_key = info.get('object', {}).get('key') )` und die DB-Funktion (z. B.`curs.callproc("load_external_tables", [file_key]) )` mit dem Dateinamen als Eingabeparameter aufruft. Abhängig vom Ergebnis des Funktionsaufrufs wird eine SNS-Benachrichtigung ausgelöst (z. B.`client.publish(TopicArn='arn:',Message='fileloadsuccess',Subjec`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`t='fileloadsuccess ') )`. Basierend auf Ihren Geschäfts anforderungen können Sie bei Bedarf eine Lambda-Funktion mit zusätzlichem Code erstellen. Weitere Informationen finden Sie in der Lambda-Dokumentation.	
Konfigurieren Sie einen S3-Bucket-Ereignisauslöser.	Konfigurieren Sie einen Mechanismus zum Aufrufen der Lambda-Funktion für alle Objekterstellungsereignisse im S3-Bucket.	DBA
Erstelle ein Geheimnis.	Erstellen Sie mit Secrets Manager einen geheimen Namen für die Datenbank anmeldedaten. Übergeben Sie das Geheimnis in der Lambda-Funktion.	DBA
Laden Sie die Lambda-Un terstützungsdateien hoch.	Laden Sie eine ZIP-Datei hoch, die die Lambda-Support-Pakete und das angehängte Python-Skript für die Verbindung mit Aurora PostgreSQL-kompatibel enthält. Der Python-Code ruft die Funktion auf, die Sie in der Datenbank erstellt haben.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein SNS-Thema.	Erstellen Sie ein SNS-Thema , um E-Mails über den Erfolg oder Misserfolg des Datenlade ns zu senden.	DBA

Integration mit Amazon S3 hinzufügen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Erstellen Sie auf der Amazon S3 S3-Konsole einen S3-Bucket mit einem eindeutigen Namen, der keine führenden Schrägstriche enthält. Ein S3-Bucket-Name ist weltweit eindeutig, und der Namespace wird von allen AWS-Konten gemeinsam genutzt.	DBA
Erstellen Sie IAM-Richtlinien.	Verwenden Sie den Code unter `s3bucketp olicy_for_import` dem Abschnitt Zusätzliche Informati onen, um die AWS Identity and Access Management (IAM) -Richtlinien zu erstellen.	DBA
Rollen erstellen.	Erstellen Sie zwei Rollen für Aurora PostgreSQL-kompati bel, eine Rolle für Import und eine Rolle für Export. Weisen Sie den Rollen die entsprech enden Richtlinien zu.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Hängen Sie die Rollen an den Aurora PostgreSQL-kompatiblen Cluster an.	Fügen Sie unter Rollen verwalten die Import- und Exportrollen dem Aurora PostgreSQL-Cluster hinzu.	DBA
Erstellen Sie unterstützende Objekte für Aurora PostgreSQL-kompatibel.	Verwenden Sie für die Tabellenskripten den Code unter dem Abschnitt *ext_tbl_scripts* Zusätzliche Informationen. Verwenden Sie für die benutzerdefinierte Funktion den Code `load_external_Table_latest` unter dem Abschnitt Zusätzliche Informationen.	DBA

Verarbeiten Sie eine Testdatei

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie eine Datei in den S3-Bucket hoch.	Verwenden Sie die Konsole oder den folgenden Befehl in der AWS-CLI, um eine Testdatei in den S3-Bucket hochzuladen. `aws s3 cp /Users/Desktop/ukpost/exttbl/"testing files"/aps s3://s3importtest/inputext/aps`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sobald die Datei hochgeladen wurde, initiiert ein Bucket-Ereignis die Lambda-Funktion, die die Aurora PostgreSQL-kompatible Funktion ausführt.	
Überprüfen Sie die Daten sowie die Protokoll- und Fehlerdateien.	Die Aurora PostgreSQL-kompatible Funktion lädt die Dateien in die Haupttabelle `.log` und erstellt `.bad` Dateien im S3-Bucket.	DBA
Überwachen Sie die Lösung.	Überwachen Sie in der CloudWatch Amazon-Konsole die Lambda-Funktion.	DBA

Zugehörige Ressourcen

- Amazon S3 S3-Integration
- Amazon S3
- Arbeiten mit Amazon Aurora PostgreSQL-Compatible Edition
- AWS Lambda
- Amazon CloudWatch
- AWS Secrets Manager
- Amazon SNS SNS-Benachrichtigungen einrichten

Zusätzliche Informationen

ext_table_scripts

```
CREATE EXTENSION aws_s3 CASCADE;
CREATE TABLE IF NOT EXISTS meta_EXTERNAL_TABLE
(
    table_name_stg character varying(100) ,
    table_name character varying(100)  ,
```

```
    col_list character varying(1000)  ,
    data_type character varying(100)  ,
    col_order numeric,
    start_pos numeric,
    end_pos numeric,
    no_position character varying(100)  ,
    date_mask character varying(100)  ,
    delimeter character(1)  ,
    directory character varying(100)  ,
    file_name character varying(100)  ,
    header_exist character varying(5)
);
CREATE TABLE IF NOT EXISTS ext_tbl_stg
(
    col1 text
);
CREATE TABLE IF NOT EXISTS error_table
(
    error_details text,
    file_name character varying(100),
    processed_time timestamp without time zone
);
CREATE TABLE IF NOT EXISTS log_table
(
    file_name character varying(50) COLLATE pg_catalog."default",
    processed_date timestamp without time zone,
    tot_rec_count numeric,
    proc_rec_count numeric,
    error_rec_count numeric
);
sample insert scripts of meta data:
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'source_filename', 'character varying', 2, 8, 27, NULL, NULL, NULL, 'databasedev',
 'externalinterface/loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'record_type_identifier', 'character varying', 3, 28, 30, NULL, NULL, NULL,
 'databasedev', 'externalinterface/loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
```

```
 'fad_code', 'numeric', 4, 31, 36, NULL, NULL, NULL, 'databasedev', 'externalinterface/
loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'session_sequence_number', 'numeric', 5, 37, 42, NULL, NULL, NULL, 'databasedev',
 'externalinterface/loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'transaction_sequence_number', 'numeric', 6, 43, 48, NULL, NULL, NULL, 'databasedev',
 'externalinterface/loaddir/APS', 'NO');
```

s3bucketpolicy_für den Import

```
---Import role policy
--Create an IAM policy to allow, Get,  and list actions on S3 bucket
 {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "s3import",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::s3importtest",
                "arn:aws:s3:::s3importtest/*"
            ]
        }
    ]
}
--Export Role policy
--Create an IAM policy to allow, put,  and list actions on S3 bucket
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "s3export",
            "Action": [
                "S3:PutObject",
```

```
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::s3importtest/*"
            ]
        }
    ]
}
```

Beispiel für eine DB-Funktion load_external_tables_latest

```
CREATE OR REPLACE FUNCTION public.load_external_tables(pi_filename text)
 RETURNS character varying
 LANGUAGE plpgsql
AS $function$
/* Loading data from S3 bucket into a APG table */
DECLARE
 v_final_sql TEXT;
 pi_ext_table TEXT;
 r refCURSOR;
 v_sqlerrm text;
 v_chunk numeric;
 i integer;
 v_col_list TEXT;
 v_postion_list CHARACTER VARYING(1000);
 v_len  integer;
 v_delim varchar;
 v_file_name CHARACTER VARYING(1000);
 v_directory CHARACTER VARYING(1000);
 v_table_name_stg CHARACTER VARYING(1000);
 v_sql_col TEXT;
 v_sql TEXT;
 v_sql1 TEXT;
 v_sql2 TEXT;
 v_sql3 TEXT;
 v_cnt integer;
 v_sql_dynamic TEXT;
 v_sql_ins TEXT;
 proc_rec_COUNT integer;
 error_rec_COUNT integer;
 tot_rec_COUNT integer;
 v_rec_val integer;
```

```
 rec record;
 v_col_cnt integer;
 kv record;
 v_val text;
 v_header text;
 j integer;
 ERCODE VARCHAR(5);
 v_region text;
 cr CURSOR FOR
 SELECT distinct DELIMETER,
   FILE_NAME,
   DIRECTORY
 FROM  meta_EXTERNAL_TABLE
 WHERE table_name = pi_ext_table
   AND DELIMETER IS NOT NULL;


 cr1 CURSOR FOR
   SELECT   col_list,
   data_type,
   start_pos,
   END_pos,
   concat_ws('',' ',TABLE_NAME_STG) as TABLE_NAME_STG,
   no_position,date_mask
 FROM  meta_EXTERNAL_TABLE
 WHERE table_name = pi_ext_table
 order by col_order asc;
cr2 cursor FOR
SELECT  distinct table_name,table_name_stg
   FROM  meta_EXTERNAL_TABLE
   WHERE upper(file_name) = upper(pi_filename);


BEGIN
 -- PERFORM utl_file_utility.init();
   v_region := 'us-east-1';
   /* find tab details from file name */


   --DELETE FROM  ERROR_TABLE WHERE file_name= pi_filename;
  -- DELETE FROM  log_table WHERE file_name= pi_filename;


 BEGIN
```

```
   SELECT distinct table_name,table_name_stg INTO strict pi_ext_table,v_table_name_stg
   FROM  meta_EXTERNAL_TABLE
   WHERE upper(file_name) = upper(pi_filename);
 EXCEPTION
   WHEN NO_DATA_FOUND THEN
    raise notice 'error 1,%',sqlerrm;
    pi_ext_table := null;
    v_table_name_stg := null;
      RAISE USING errcode = 'NTFIP' ;
    when others then
        raise notice 'error others,%',sqlerrm;
 END;
 j :=1 ;

for rec in  cr2
 LOOP




  pi_ext_table     := rec.table_name;
  v_table_name_stg := rec.table_name_stg;
  v_col_list := null;


 IF pi_ext_table IS NOT NULL
  THEN
    --EXECUTE concat_ws('','truncate table  ' ,pi_ext_table) ;
   EXECUTE concat_ws('','truncate table  ' ,v_table_name_stg) ;




       SELECT distinct DELIMETER INTO STRICT v_delim
       FROM  meta_EXTERNAL_TABLE
       WHERE table_name = pi_ext_table;


       IF v_delim IS NOT NULL THEN
     SELECT distinct DELIMETER,
       FILE_NAME,
       DIRECTORY ,
```

```
      concat_ws('',' ',table_name_stg),
      case  header_exist when 'YES' then 'CSV HEADER' else 'CSV' end as header_exist
    INTO STRICT v_delim,v_file_name,v_directory,v_table_name_stg,v_header
    FROM  meta_EXTERNAL_TABLE
    WHERE table_name = pi_ext_table
      AND DELIMETER IS NOT NULL;


    IF    upper(v_delim) = 'CSV'
    THEN
      v_sql := concat_ws('','SELECT aws_s3.table_import_FROM_s3 ( ''',
      v_table_name_stg,''','''',
      ''DELIMITER '''','''' CSV HEADER QUOTE '''''''''', aws_commons.create_s3_uri
( ''',
      v_directory,''','''',v_file_name,''', ''',v_region,'''))');
      ELSE
      v_sql := concat_ws('','SELECT aws_s3.table_import_FROM_s3(''',
          v_table_name_stg, ''','''', ''DELIMITER AS ''''^''''',''',','
         aws_commons.create_s3_uri
          ( ''',v_directory, ''','''',
          v_file_name, ''',',
           '''',v_region,''')
         )');
         raise notice 'v_sql , %',v_sql;
      begin
       EXECUTE  v_sql;
      EXCEPTION
        WHEN OTHERS THEN
          raise notice 'error 1';
        RAISE USING errcode = 'S3IMP' ;
      END;


      select count(col_list) INTO v_col_cnt
      from  meta_EXTERNAL_TABLE where table_name = pi_ext_table;









       -- raise notice 'v_sql 2, %',concat_ws('','update ',v_table_name_stg, ' set
col1 = col1||''',v_delim,''''');
```

```
      execute concat_ws('','update ',v_table_name_stg, ' set col1 =
col1||''',v_delim,''''); 




      i :=1;
      FOR rec in cr1
      loop
      v_sql1 := concat_ws('',v_sql1,'split_part(col1,''',v_delim,''',', i,')',' as
',rec.col_list,',');
      v_sql2 := concat_ws('',v_sql2,rec.col_list,',');
  --    v_sql3 := concat_ws('',v_sql3,'rec.',rec.col_list,'::',rec.data_type,',');


      case
        WHEN upper(rec.data_type) = 'NUMERIC'
        THEN v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                coalesce((trim(split_part(col1,''',v_delim,''',',
i,')))::NUMERIC,0)::',rec.data_type,' END as ',rec.col_list,',') ;
        WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
'YYYYMMDD'
        THEN v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                to_date(coalesce((trim(split_part(col1,''',v_delim,''',',
i,'))),''99990101''),''YYYYMMDD'')::',rec.data_type,' END as ',rec.col_list,',');
        WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
 'MM/DD/YYYY hh24:mi:ss'
        THEN v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                to_date(coalesce((trim(split_part(col1,''',v_delim,''',',
i,'))),''01/01/9999 0024:00:00''),''MM/DD/YYYY hh24:mi:ss'')::',rec.data_type,' END as
',rec.col_list,',');
         ELSE
       v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
```

```
                THEN null
                 ELSE
                  coalesce((trim(split_part(col1,''',v_delim,''',',
i,'))),''''):',rec.data_type,' END as ',rec.col_list,',') ;
      END case;


      i :=i+1;
      end loop;


        -- raise notice 'v_sql 3, %',v_sql3;


      SELECT trim(trailing ' ' FROM v_sql1) INTO v_sql1;
      SELECT trim(trailing ',' FROM v_sql1) INTO v_sql1;


      SELECT trim(trailing ' ' FROM v_sql2) INTO v_sql2;
      SELECT trim(trailing ',' FROM v_sql2) INTO v_sql2;


      SELECT trim(trailing ' ' FROM v_sql3) INTO v_sql3;
      SELECT trim(trailing ',' FROM v_sql3) INTO v_sql3;


      END IF;
     raise notice 'v_delim , %',v_delim;


    EXECUTE concat_ws('','SELECT COUNT(*) FROM ',v_table_name_stg)  INTO v_cnt;


   raise notice 'stg cnt , %',v_cnt;


   /* if upper(v_delim) = 'CSV' then
      v_sql_ins := concat_ws('', ' SELECT * from ' ,v_table_name_stg );
    else
     -- v_sql_ins := concat_ws('',' SELECT ',v_sql1,'  from (select col1 from
' ,v_table_name_stg , ')sub ');
      v_sql_ins := concat_ws('',' SELECT ',v_sql3,'  from (select col1 from
' ,v_table_name_stg , ')sub ');
      END IF;*/
```

```
v_chunk := v_cnt/100;



for i in 1..101
loop
     BEGIN
    -- raise notice 'v_sql , %',v_sql;
       -- raise notice 'Chunk number , %',i;
       v_sql_ins := concat_ws('',' SELECT ',v_sql3,'  from (select col1 from
 ' ,v_table_name_stg , ' offset ',v_chunk*(i-1), ' limit ',v_chunk,') sub ');


     v_sql := concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins);
     -- raise notice 'select statement , %',v_sql_ins;
          -- v_sql := null;
     -- EXECUTE concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins, 'offset
 ',v_chunk*(i-1), ' limit ',v_chunk );
     --v_sql := concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins );


     -- raise notice 'insert statement , %',v_sql;


    raise NOTICE 'CHUNK START %',v_chunk*(i-1);
   raise NOTICE 'CHUNK END %',v_chunk;


     EXECUTE v_sql;


  EXCEPTION
       WHEN OTHERS THEN
       -- v_sql_ins := concat_ws('',' SELECT ',v_sql1, '  from (select col1 from
 ' ,v_table_name_stg , ' )sub ');
         -- raise notice 'Chunk number for cursor , %',i;


    raise NOTICE 'Cursor - CHUNK START %',v_chunk*(i-1);
   raise NOTICE 'Cursor -  CHUNK END %',v_chunk;
```

```
        v_sql_ins := concat_ws('',' SELECT ',v_sql3, '  from (select col1 from
 ' ,v_table_name_stg , ' )sub ');


        v_final_sql := REPLACE (v_sql_ins, ''''::text, ''''''::text);
       -- raise notice 'v_final_sql %',v_final_sql;
        v_sql :=concat_ws('','do $a$ declare  r refcursor;v_sql text; i
 numeric;v_conname text;  v_typ  ',pi_ext_table,'[]; v_rec  ','record',';
          begin









          open r for execute ''select col1 from ',v_table_name_stg ,'  offset
 ',v_chunk*(i-1), ' limit ',v_chunk,''';
          loop
          begin
          fetch r into v_rec;
          EXIT WHEN NOT FOUND;




          v_sql := concat_ws('''','insert into  ',pi_ext_table,' SELECT ',REPLACE
 (v_sql3, ''''::text, ''''''::text) , '  from ( select ''''''',v_rec.col1,''''''' as
 col1) v'');
           execute v_sql;


          exception
           when others then
         v_sql := ''INSERT INTO  ERROR_TABLE VALUES (concat_ws(''''''''','''''Error
 Name: ''''',$$''||SQLERRM||''$$,'''''Error State: ''''','''''''||
SQLSTATE||''''''','''''record : ''''',$$''||v_rec.col1||''$$),'''''||
pi_filename||''''',now())'';


             execute v_sql;
            continue;
          end ;
          end loop;
          close r;
```

```
          exception
          when others then
        raise;
          end ; $a$');
     -- raise notice ' inside excp v_sql %',v_sql;
         execute v_sql;
     --  raise notice 'v_sql %',v_sql;
      END;
 END LOOP;
    ELSE


    SELECT distinct DELIMETER,FILE_NAME,DIRECTORY ,concat_ws('',' ',table_name_stg),
      case  header_exist when 'YES' then 'CSV HEADER' else 'CSV' end as header_exist
      INTO STRICT v_delim,v_file_name,v_directory,v_table_name_stg,v_header
    FROM  meta_EXTERNAL_TABLE
    WHERE table_name = pi_ext_table                  ;
    v_sql := concat_ws('','SELECT aws_s3.table_import_FROM_s3(''',
      v_table_name_stg, ''','''', ''DELIMITER AS ''''#'''' ',v_header,' '','','
     aws_commons.create_s3_uri
      ( ''',v_directory, ''','''',
      v_file_name, ''',',
       '''',v_region,''')
     )');
        EXECUTE  v_sql;


    FOR rec in cr1
    LOOP


     IF rec.start_pos IS NULL AND rec.END_pos IS NULL AND rec.no_position = 'recnum'
     THEN
       v_rec_val := 1;
     ELSE


      case
        WHEN upper(rec.data_type) = 'NUMERIC'
        THEN v_sql1 := concat_ws('',' case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
               THEN null
                ELSE
```

```
                coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1')))::NUMERIC,0)::',rec.data_type,' END as
',rec.col_list,',') ;
       WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
'YYYYMMDD'
       THEN v_sql1 := concat_ws('','case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
              THEN null
               ELSE
               to_date(coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1'))),''99990101''),''YYYYMMDD''):::',rec.data_type,'
END as ',rec.col_list,',');
       WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
'YYYYMMDDHH24MISS'
       THEN v_sql1 := concat_ws('','case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
              THEN null
               ELSE
               to_date(coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1'))),''9999010100240000''),''YYYYMMDDHH24MISS''):::',rec.data_
END as ',rec.col_list,',');
        ELSE
      v_sql1 := concat_ws('',' case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
              THEN null
               ELSE
                coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1'))),''''):::',rec.data_type,' END as
',rec.col_list,',') ;
     END case;


    END IF;
    v_col_list := concat_ws('',v_col_list ,v_sql1);
   END LOOP;




         SELECT trim(trailing ' ' FROM v_col_list) INTO v_col_list;
         SELECT trim(trailing ',' FROM v_col_list) INTO v_col_list;
```

```
          v_sql_col   :=  concat_ws('',trim(trailing ',' FROM v_col_list) , ' FROM
 ',v_table_name_stg,' WHERE col1 IS NOT NULL AND length(col1)>0 ');




          v_sql_dynamic := v_sql_col;


          EXECUTE  concat_ws('','SELECT COUNT(*) FROM ',v_table_name_stg) INTO v_cnt;




        IF v_rec_val = 1 THEN
            v_sql_ins := concat_ws('',' select row_number() over(order by ctid) as
line_number ,' ,v_sql_dynamic) ;


        ELSE
              v_sql_ins := concat_ws('',' SELECT' ,v_sql_dynamic) ;
          END IF;


    BEGIN
      EXECUTE concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins);
          EXCEPTION
             WHEN OTHERS THEN
         IF v_rec_val = 1 THEN
                v_final_sql := ' select row_number() over(order by ctid) as
line_number ,col1 from ';
               ELSE
                v_final_sql := ' SELECT col1 from';
              END IF;
      v_sql :=concat_ws('','do $a$ declare  r refcursor;v_rec_val numeric :=
',coalesce(v_rec_val,0),';line_number numeric; col1 text; v_typ  ',pi_ext_table,'[];
v_rec  ',pi_ext_table,';
            begin
            open r for execute ''',v_final_sql, ' ',v_table_name_stg,' WHERE col1 IS
NOT NULL AND length(col1)>0 '' ;
            loop
            begin
            if   v_rec_val = 1 then
            fetch r into line_number,col1;
```

```
            else
            fetch r into col1;
            end if;


            EXIT WHEN NOT FOUND;
             if v_rec_val = 1 then
             select line_number,',trim(trailing ',' FROM v_col_list) ,' into v_rec;
             else
               select ',trim(trailing ',' FROM v_col_list) ,' into v_rec;
             end if;


            insert into  ',pi_ext_table,' select v_rec.*;
             exception
             when others then
              INSERT INTO  ERROR_TABLE VALUES (concat_ws('''','Error Name:
'',SQLERRM,''Error State: '',SQLSTATE,''record : '',v_rec),''',pi_filename,''',now());
              continue;
             end ;
              end loop;
            close r;
             exception
             when others then
             raise;
             end ; $a$');
        execute v_sql;


    END;


        END IF;


  EXECUTE concat_ws('','SELECT COUNT(*) FROM  ' ,pi_ext_table)   INTO proc_rec_COUNT;


  EXECUTE concat_ws('','SELECT COUNT(*) FROM  error_table WHERE file_name
='''',pi_filename,''' and processed_time::date = clock_timestamp()::date')  INTO
error_rec_COUNT;


  EXECUTE concat_ws('','SELECT COUNT(*) FROM ',v_table_name_stg)   INTO tot_rec_COUNT;
```

```
   INSERT INTO  log_table values(pi_filename,now(),tot_rec_COUNT,proc_rec_COUNT,
 error_rec_COUNT);


   raise notice 'v_directory, %',v_directory;


   raise notice 'pi_filename, %',pi_filename;


   raise notice 'v_region, %',v_region;


  perform aws_s3.query_export_to_s3('SELECT
 replace(trim(substring(error_details,position(''('' in
 error_details)+1),'')''),'','','';''),file_name,processed_time FROM  error_table WHERE
 file_name = '''||pi_filename||'''',
   aws_commons.create_s3_uri(v_directory, pi_filename||'.bad', v_region),
   options :='FORmat csv, header, delimiter $$,$$'
   );


raise notice 'v_directory, %',v_directory;


   raise notice 'pi_filename, %',pi_filename;


   raise notice 'v_region, %',v_region;


  perform aws_s3.query_export_to_s3('SELECT * FROM  log_table WHERE file_name = '''||
pi_filename||'''',
   aws_commons.create_s3_uri(v_directory, pi_filename||'.log', v_region),
   options :='FORmat csv, header, delimiter $$,$$'
   );




   END IF;
 j := j+1;
```

```
 END LOOP;


       RETURN 'OK';
EXCEPTION
    WHEN  OTHERS THEN
  raise notice 'error %',sqlerrm;
   ERCODE=SQLSTATE;
   IF ERCODE = 'NTFIP' THEN
     v_sqlerrm := concat_Ws('',sqlerrm,'No data for the filename');
   ELSIF ERCODE = 'S3IMP' THEN
    v_sqlerrm := concat_Ws('',sqlerrm,'Error While exporting the file from S3');
   ELSE
      v_sqlerrm := sqlerrm;
   END IF;


 select distinct directory into v_directory from  meta_EXTERNAL_TABLE;




 raise notice 'exc v_directory, %',v_directory;


   raise notice 'exc pi_filename, %',pi_filename;


   raise notice 'exc v_region, %',v_region;


  perform aws_s3.query_export_to_s3('SELECT * FROM  error_table WHERE file_name = '''||
pi_filename||'''',
   aws_commons.create_s3_uri(v_directory, pi_filename||'.bad', v_region),
   options :='FORmat csv, header, delimiter $$,$$'
   );
    RETURN null;
END;
$function$
```

Migrieren Sie funktionsbasierte Indizes von Oracle nach PostgreSQL

Erstellt von Veeranjaneyulu Grandhi (AWS) und Navakanth Talluri (AWS)

Übersicht

Indizes sind eine gängige Methode zur Verbesserung der Datenbankleistung. Ein Index ermöglicht es dem Datenbankserver, bestimmte Zeilen viel schneller zu finden und abzurufen, als dies ohne einen Index möglich wäre. Indizes erhöhen jedoch auch den Mehraufwand für das Datenbanksystem als Ganzes, weshalb sie sinnvoll verwendet werden sollten. Funktionsbasierte Indizes, die auf einer Funktion oder einem Ausdruck basieren, können mehrere Spalten und mathematische Ausdrücke beinhalten. Ein funktionsbasierter Index verbessert die Leistung von Abfragen, die den Indexausdruck verwenden.

PostgreSQL unterstützt nativ nicht die Erstellung funktionsbasierter Indizes mit Funktionen, deren Volatilität als stabil definiert ist. Sie können jedoch ähnliche Funktionen mit Volatilität erstellen `IMMUTABLE` und sie bei der Indexerstellung verwenden.

Eine `IMMUTABLE` Funktion kann die Datenbank nicht ändern, und es ist garantiert, dass sie bei denselben Argumenten für immer dieselben Ergebnisse zurückgibt. Diese Kategorie ermöglicht es dem Optimierer, die Funktion vorab auszuwerten, wenn eine Abfrage sie mit konstanten Argumenten aufruft.

Dieses Muster hilft bei der Migration der funktionsbasierten Oracle-Indizes, wenn sie mit Funktionen wie `to_char`to_date, und `to_number` zum PostgreSQL-Äquivalent verwendet werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS) -Konto
- Eine Oracle-Quelldatenbank-Instance, auf der der Listener-Service eingerichtet ist und läuft
- Vertrautheit mit PostgreSQL-Datenbanken

Einschränkungen

- Die maximale Datenbankgröße beträgt 64 TB.
- Die bei der Indexerstellung verwendeten Funktionen müssen UNVERÄNDERLICH sein.

Produktversionen

- Alle Oracle-Datenbankeditionen für die Versionen 11g (Versionen 11.2.0.3.v1 und höher) und bis zu 12.2 und 18c
- PostgreSQL-Versionen 9.6 und höher

Architektur

Quelltechnologie-Stack

- Eine Oracle-Datenbank vor Ort oder auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance oder eine Amazon RDS for Oracle DB-Instance

Zieltechnologie-Stack

- Beliebige PostgreSQL-Engine

Tools

- pgAdmin 4 ist ein Open-Source-Verwaltungstool für Postgres. Das Tool pgAdmin 4 bietet eine grafische Oberfläche zum Erstellen, Verwalten und Verwenden von Datenbankobjekten.
- Oracle SQL Developer ist eine integrierte Entwicklungsumgebung (IDE) für die Entwicklung und Verwaltung von Oracle Database sowohl in herkömmlichen als auch in Cloud-Bereitstellungen.

Epen

Erstellen Sie einen funktionsbasierten Index mit einer Standardfunktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie mit der Funktion to_char einen funktions basierten Index für eine Spalte.	Verwenden Sie den folgenden Code, um den funktions basierten Index zu erstellen. `postgres=# create table funcindex( col1 timestamp without time zone);`	DBA, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CREATE TABLE postgres=# insert into funcindex values (now()); INSERT 0 1 postgres=# select * from funcindex; col1 ---------- 2022-08-09 16:00:57. 77414 (1 rows) postgres=# create index funcindex_idx on funcindex(to_char(col1,'DD-MM-YYYY HH24:MI:SS')); ERROR: functions in index expression must be marked IMMUTABLE **Note** PostgreSQL erlaubt es nicht, einen funktionsbasierten Index ohne die Klausel zu erstellen. IMMUTABLE	
Überprüfen Sie die Volatilität der Funktion.	Verwenden Sie den Code im Abschnitt Zusätzliche Informationen, um die Volatilität der Funktion zu überprüfen.	DBA

Erstellen Sie funktionsbasierte Indizes mithilfe einer Wrapper-Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Wrapper-Funktion.	Verwenden Sie den Code im Abschnitt Zusätzliche Informationen, um eine Wrapper-Funktion zu erstellen.	PostgreSQL-Entwickler
Erstellen Sie einen Index mithilfe der Wrapper-Funktion.	Verwenden Sie den Code im Abschnitt Zusätzliche Informationen, um eine benutzerdefinierte Funktion mit dem Schlüsselwort `IMMUTABLE` im selben Schema wie die Anwendung zu erstellen, und verweisen Sie im Skript zur Indexerstellung darauf. Wenn eine benutzerdefinierte Funktion in einem gemeinsamen Schema (aus dem vorherigen Beispiel) erstellt wird, aktualisieren Sie diese wie gezeigt. `search_path` `ALTER ROLE <ROLENAME> set search_path=$user, COMMON;`	DBA, PostgreSQL-Entwickler

Überprüfen Sie die Indexerstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Indexerstellung.	Stellen Sie sicher, dass der Index auf der Grundlage von	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Abfragezugriffsmustern erstellt werden muss.	
Stellen Sie sicher, dass der Index verwendet werden kann.	Um zu überprüfen, ob der funktionsbasierte Index vom PostgreSQL Optimizer übernommen wird, führen Sie eine SQL-Anweisung mit explain oder explain analyze aus. Verwenden Sie den Code im Abschnitt Zusätzlic he Informationen. Sammeln Sie nach Möglichkeit auch die Tabellenstatistiken. **Note** Wenn Sie den Explain-Plan bemerken, hat der PostgreSQL-Optimierer aufgrund der Prädikatbedingung einen funktions basierten Index ausgewählt.	DBA

Zugehörige Ressourcen

- Funktionsbasierte Indizes (Oracle-Dokumentation)
- Indizes für Ausdrücke (PostgreSQL-Dokumentation)
- PostgreSQL-Volatilität (PostgreSQL-Dokumentation)
- PostgreSQL search_path (PostgreSQL-Dokumentation)
- Leitfaden für die Migration von Oracle Database 19c zu Amazon Aurora PostgreSQL

Zusätzliche Informationen

Erstellen Sie eine Wrapper-Funktion

```
CREATE OR REPLACE FUNCTION myschema.to_char(var1 timestamp without time zone, var2
 varchar) RETURNS varchar AS $BODY$ select to_char(var1, 'YYYYMMDD'); $BODY$ LANGUAGE
 sql IMMUTABLE;
```

Erstellen Sie einen Index mithilfe der Wrapper-Funktion

```
postgres=# create function common.to_char(var1 timestamp without time zone, var2
 varchar) RETURNS varchar AS $BODY$ select to_char(var1, 'YYYYMMDD'); $BODY$ LANGUAGE
 sql IMMUTABLE;
CREATE FUNCTION
postgres=# create index funcindex_idx on funcindex(common.to_char(col1,'DD-MM-YYYY
 HH24:MI:SS'));
CREATE INDEX
```

Überprüfen Sie die Volatilität der Funktion

```
SELECT DISTINCT p.proname as "Name",p.provolatile as "volatility" FROM
 pg_catalog.pg_proc p
 LEFT JOIN pg_catalog.pg_namespace n ON n.oid = p.pronamespace
 LEFT JOIN pg_catalog.pg_language l ON l.oid = p.prolang
 WHERE n.nspname OPERATOR(pg_catalog.~) '^(pg_catalog)$' COLLATE pg_catalog.default AND
 p.proname='to_char'GROUP BY p.proname,p.provolatile
ORDER BY 1;
```

Stellen Sie sicher, dass der Index verwendet werden kann

```
explain analyze <SQL>


postgres=# explain select col1 from funcindex where common.to_char(col1,'DD-MM-YYYY
 HH24:MI:SS') = '09-08-2022 16:00:57';
                                                        QUERY PLAN
-------------------------------------------------------------------------------------------
 Index Scan using funcindex_idx on funcindex  (cost=0.42..8.44 rows=1 width=8)
   Index Cond: ((common.to_char(col1, 'DD-MM-YYYY HH24:MI:SS'::character
 varying))::text = '09-08-2022 16:00:57'::text)
(2 rows)
```

Migrieren Sie native Oracle-Funktionen mithilfe von Erweiterungen zu PostgreSQL

Erstellt von Pinesh Singal (AWS)

Übersicht

Dieses Migrationsmuster bietet step-by-step Anleitungen für die Migration einer Amazon Relational Database Service (Amazon RDS) for Oracle-Datenbank-Instance zu einer Amazon RDS for PostgreSQL- oder Amazon Aurora PostgreSQL-Compatible Edition-Datenbank durch Änderung des systemeigenen integrierten Codes `aws_oracle_ext` und der `orafce` Erweiterungen von PostgreSQL (). `psql` Dies spart Verarbeitungszeit.

Das Muster beschreibt eine manuelle Offline-Migrationsstrategie ohne Ausfallzeiten für eine Oracle-Quelldatenbank mit mehreren Terabyte und einer hohen Anzahl von Transaktionen.

Der Migrationsprozess verwendet das AWS Schema Conversion Tool (AWS SCT) mit den `orafce` Erweiterungen `aws_oracle_ext` und, um ein Amazon RDS for Oracle Oracle-Datenbankschema in ein Amazon RDS for PostgreSQL- oder Aurora PostgreSQL-kompatibles Datenbankschema zu konvertieren. Dann wird der Code manuell in den von PostgreSQL unterstützten systemeigenen `psql` integrierten Code geändert. Dies liegt daran, dass die Erweiterungsaufrufen die Codeverarbeitung auf dem PostgreSQL-Datenbankserver beeinflussen und nicht der gesamte Erweiterungscode vollständig kompatibel oder kompatibel mit PostgreSQL-Code ist.

Dieses Muster konzentriert sich hauptsächlich auf die manuelle Migration von SQL-Codes mithilfe von AWS SCT und den Erweiterungen `aws_oracle_ext` und. `orafce` Sie konvertieren die bereits verwendeten Erweiterungen in native PostgreSQL (`psql`) -Built-ins. Dann entfernen Sie alle Verweise auf die Erweiterungen und konvertieren die Codes entsprechend.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Betriebssystem (Windows oder Mac) oder EC2 Amazon-Instance (läuft)
- Orace

Einschränkungen

Nicht alle Oracle-Funktionen, die `aws_oracle_ext` unsere `orafce` Erweiterungen verwenden, können in native PostgreSQL-Funktionen konvertiert werden. Möglicherweise muss es manuell überarbeitet werden, um es mit PostgreSQL-Bibliotheken zu kompilieren.

Ein Nachteil der Verwendung von AWS SCT-Erweiterungen ist die langsame Leistung beim Ausführen und Abrufen der Ergebnisse. Die Kosten können anhand des einfachen PostgreSQL EXPLAIN-Plans (Ausführungsplan einer Anweisung) für die Migration der `SYSDATE` Oracle-Funktion zur `NOW()` PostgreSQL-Funktion zwischen allen drei Codes (`aws_oracle_ext`, und `psql` Standard) nachvollzogen werden`orafce`, wie im Abschnitt Leistungsvergleichsprüfung im angehängten Dokument erläutert.

Produktversionen

- Quelle: Amazon RDS for Oracle Oracle-Datenbank 10.2 und höher (für 10.x), 11g (11.2.0.3.v1 und höher) und bis zu 12.2, 18c und 19c (und höher) für Enterprise Edition, Standard Edition, Standard Edition 1 und Standard Edition 2
- Ziel: Amazon RDS for PostgreSQL oder Aurora PostgreSQL-kompatible Datenbank 9.4 und höher (für 9.x), 10.x, 11.x, 12.x, 13.x und 14.x (und höher)
- AWS SCT: Aktuelle Version (dieses Muster wurde mit 1.0.632 getestet)
- Oracle: Aktuelle Version (dieses Muster wurde mit 3.9.0 getestet)

Architektur

Quelltechnologie-Stack

- Eine Amazon RDS for Oracle Oracle-Datenbank-Instance mit Version 12.1.0.2.v18

Zieltechnologie-Stack

- Eine Amazon RDS for PostgreSQL- oder Aurora PostgreSQL-kompatible Datenbank-Instance mit Version 11.5

Architektur für die Datenbankmigration

Das folgende Diagramm stellt die Datenbankmigrationsarchitektur zwischen den Oracle-Quelldatenbanken und den PostgreSQL-Zieldatenbanken dar. Die Architektur umfasst AWS Cloud, eine Virtual Private Cloud (VPC), Availability Zones, ein privates Subnetz, eine Amazon RDS for

Oracle Oracle-Datenbank, AWS SCT, eine Amazon RDS for PostgreSQL- oder Aurora PostgreSQL-kompatible Datenbank, Erweiterungen für Oracle (`aws_oracle_ext`und`orafce`) und strukturierte Abfragesprache-Dateien (SQL).

1. Starten Sie die Amazon RDS for Oracle DB-Instance (Quell-DB).
2. Verwenden Sie AWS SCT mit den Erweiterungspaketen `aws_oracle_ext` und `orafce` Erweiterungspaketen, um den Quellcode von Oracle nach PostreSQL zu konvertieren.
3. Die Konvertierung erzeugt PostgreSQL-unterstützte migrierte .sql-Dateien.
4. Konvertieren Sie die nicht konvertierten Oracle-Erweiterungscodes manuell in PostgreSQL () `psql` -Codes.
5. Die manuelle Konvertierung erzeugt konvertierte .sql-Dateien, die PostgreSQL unterstützen.
6. Führen Sie diese .sql-Dateien auf Ihrer Amazon RDS for PostgreSQL PostgreSQL-DB-Instance (Ziel-DB) aus.

Tools

Tools

AWS-Services

- AWS SCT — Das AWS Schema Conversion Tool (AWS SCT) konvertiert Ihr vorhandenes Datenbankschema von einer Datenbank-Engine in eine andere. Sie können das relationale OLTP-Schema (Online Transactional Processing) oder das Data Warehouse-Schema konvertieren. Ihr konvertiertes Schema ist für eine Amazon RDS for MySQL MySQL-DB-Instance, einen Amazon Aurora Aurora-DB-Cluster, eine Amazon RDS for PostgreSQL PostgreSQL-DB-Instance oder einen Amazon Redshift Redshift-Cluster geeignet. Das konvertierte Schema kann auch mit einer Datenbank auf einer EC2 Amazon-Instance verwendet oder als Daten in einem Amazon S3-Bucket gespeichert werden.

  AWS SCT bietet eine projektbasierte Benutzeroberfläche, mit der Sie das Datenbankschema Ihrer Quelldatenbank automatisch in ein Format konvertieren können, das mit Ihrer Amazon RDS-Zielinstanz kompatibel ist.

  Sie können AWS SCT verwenden, um eine Migration von einer Oracle-Quelldatenbank zu einem der oben aufgeführten Ziele durchzuführen. Mit AWS SCT können Sie die Objektdefinitionen der Quelldatenbank wie Schema, Ansichten, gespeicherte Prozeduren und Funktionen exportieren.

Sie können AWS SCT verwenden, um Daten von Oracle in Amazon RDS for PostgreSQL oder Amazon Aurora PostgreSQL-Compatible Edition zu konvertieren.

In diesem Muster verwenden Sie AWS SCT, um Oracle-Code mithilfe der Erweiterungen und in PostgreSQL zu konvertieren und zu migrieren `aws_oracle_ext` und `orafce` die Erweiterungscodes manuell in `psql` Standard- oder systemeigenen integrierten Code zu migrieren.

- Das AWS SCT-Erweiterungspaket ist ein Zusatzmodul, das in der Quelldatenbank vorhandene Funktionen emuliert, die für die Konvertierung von Objekten in die Zieldatenbank erforderlich sind. Bevor Sie das AWS SCT-Erweiterungspaket installieren können, müssen Sie Ihr Datenbankschema konvertieren.

  Wenn Sie Ihr Datenbank- oder Data Warehouse-Schema konvertieren, fügt AWS SCT Ihrer Zieldatenbank ein zusätzliches Schema hinzu. Über dieses Schema werden SQL-Systemfunktionen der Quelldatenbank implementiert, die zum Schreiben des konvertierten Schemas in die Zieldatenbank benötigt werden. Dieses Zusätzliche Schema wird als Erweiterungspaketschema bezeichnet.

  Das Erweiterungspaket-Schema für OLTP-Datenbanken ist entsprechend der Quelldatenbank benannt. Für Oracle-Datenbanken lautet `AWS_ORACLE_EXT` das Erweiterungspaket-Schema.

Andere Tools

- Oracle — Oracle ist ein Modul, das Oracle-kompatible Funktionen, Datentypen und Pakete implementiert. Es ist ein Open-Source-Tool mit einer Berkeley Source Distribution (BSD) -Lizenz, sodass jeder es verwenden kann. Das `orafce` Modul ist nützlich für die Migration von Oracle zu PostgreSQL, da viele Oracle-Funktionen in PostgreSQL implementiert sind.

Code

Eine Liste aller häufig verwendeten und migrierten Codes von Oracle nach PostgreSQL, um die Verwendung von AWS SCT-Erweiterungscodes zu vermeiden, finden Sie im angehängten Dokument.

Epen

Konfiguration der Amazon RDS for Oracle Oracle-Quelldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Oracle-Datenbankinstanz.	Erstellen Sie eine Amazon RDS for Oracle- oder Aurora PostgreSQL-kompatible Datenbank-Instance von der Amazon RDS-Konsole aus.	Allgemein AWS, DBA
Konfigurieren Sie die Sicherheitsgruppen.	Konfigurieren Sie Sicherheitsgruppen für eingehenden und ausgehenden Datenverkehr.	Allgemeines AWS
Erstellen Sie die Datenbank.	Erstellen Sie die Oracle-Datenbank mit den benötigten Benutzern und Schemas.	Allgemein AWS, DBA
Erstellen Sie die Objekte.	Objekte erstellen und Daten in das Schema einfügen.	DBA

Konfiguration der Amazon RDS for PostgreSQL PostgreSQL-Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die PostgreSQL-Datenbankinstanz.	Erstellen Sie eine Amazon RDS for PostgreSQL- oder Amazon Aurora PostgreSQL-Datenbank-Instance von der Amazon RDS-Konsole aus.	Allgemein AWS, DBA
Konfigurieren Sie die Sicherheitsgruppen.	Konfigurieren Sie Sicherheitsgruppen für eingehenden	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und ausgehenden Datenverkehr.	
Erstellen Sie die Datenbank.	Erstellen Sie die PostgreSQL-Datenbank mit den benötigten Benutzern und Schemas.	Allgemein AWS, DBA
Validieren Sie die Erweiterungen.	Stellen Sie sicher, dass `aws_oracle_ext` und korrekt in der PostgreSQL-Datenbank installiert und konfiguriert `orafce` sind.	DBA
Stellen Sie sicher, dass die PostgreSQL-Datenbank verfügbar ist.	Stellen Sie sicher, dass die PostgreSQL-Datenbank betriebsbereit ist.	DBA

Migrieren Sie das Oracle-Schema mithilfe von AWS SCT und den Erweiterungen nach PostgreSQL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie AWS SCT.	Installieren Sie die neueste Version von AWS SCT.	DBA
Konfigurieren Sie AWS SCT.	Konfigurieren Sie AWS SCT mit Java Database Connectivity (JDBC) -Treibern für Oracle () und `ojdbc8.jar` PostgreSQL (). `postgresql-42.2.5.jar`	DBA
Aktivieren Sie das AWS SCT-Erweiterungspaket oder die Vorlage.	Aktivieren Sie unter AWS SCT Project Settings die Implementierung integrierter Funktionen mit den `orafce` Erweiterungen `aws_oracle_ext` und	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	für das Oracle-Datenbanksc hema.	
Konvertiert das Schema.	Wählen Sie in AWS SCT „Schema konvertieren“, um das Schema von Oracle nach PostgreSQL zu konvertie ren und die SQL-Dateien zu generieren.	DBA

AWS SCT-Erweiterungscode in PSQL-Code konvertieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Den Code manuell konvertie ren.	Konvertieren Sie jede Codezeile, die von Erweiteru ngen unterstützt wird, manuell in den integrier ten `psql` Standardcode, wie im angehängten Dokument beschrieben. Zum Beispiel ändern `AWS_ORACL E_EXT.SYSDATE()` oder `ORACLE.SYSDATE()` zu. `NOW()`	DBA
Bestätigen Sie den Code	(Optional) Überprüfen Sie jede Codezeile, indem Sie sie vorübergehend in der PostgreSQL-Datenbank ausführen.	DBA
Erstellen Sie Objekte in der PostgreSQL-Datenbank.	Um Objekte in der PostgreSQ L-Datenbank zu erstellen , führen Sie die .sql-Date	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ien aus, die von AWS SCT generiert und in den beiden vorherigen Schritten geändert wurden.	

Zugehörige Ressourcen

- Datenbank
  - Oracle auf Amazon RDS
  - PostgreSQL auf Amazon RDS
  - Arbeiten mit Amazon Aurora PostgreSQL
  - PostgreSQL EXPLAIN-Plan
- AWS SCT
  - Überblick über das AWS-Schema-Konvertierungstool
  - AWS SCT-Benutzerhandbuch
  - Verwenden der AWS SCT-Benutzeroberfläche
  - Verwendung von Oracle Database als Quelle für AWS SCT
- Erweiterungen für AWS SCT
  - Verwenden des AWS SCT-Erweiterungspakets
  - Oracle-Funktionalität (de)
  - PGNX Oracle
  - GitHub orafce

Zusätzliche Informationen

Weitere Informationen finden Sie in den ausführlichen Befehlen mit Syntax und Beispielen für die manuelle Konvertierung von Code im angehängten Dokument.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Migrieren Sie mithilfe von AWS DMS eine Db2-Datenbank von Amazon EC2 zu Aurora MySQL-kompatibel

Erstellt von Pinesh Singal (AWS)

Übersicht

Nachdem Sie Ihre IBM Db2 for LUW-Datenbank zu Amazon Elastic Compute Cloud (Amazon EC2) migriert haben, sollten Sie erwägen, die Datenbank neu zu strukturieren, indem Sie zu einer Cloud-nativen Amazon Web Services (AWS) -Datenbank wechseln. Dieses Muster behandelt die Migration einer IBM Db2 for LUW-Datenbank, die auf einer EC2 Amazon-Instance ausgeführt wird, zu einer Amazon Aurora MySQL-Compatible Edition-Datenbank auf AWS.

Das Muster beschreibt eine Online-Migrationsstrategie mit minimalen Ausfallzeiten für eine Db2-Quelldatenbank mit mehreren Terabyte und einer hohen Anzahl von Transaktionen.

Dieses Muster verwendet das AWS Schema Conversion Tool (AWS SCT), um das Db2-Datenbankschema in ein Aurora MySQL-kompatibles Schema zu konvertieren. Anschließend verwendet das Muster den AWS Database Migration Service (AWS DMS), um Daten von der Db2-Datenbank in die Aurora MySQL-kompatible Datenbank zu migrieren. Für den Code, der nicht von AWS SCT konvertiert wurde, sind manuelle Konvertierungen erforderlich.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit einer Virtual Private Cloud (VPC)
- AWS SCT
- AWS DMS

Produktversionen

- Aktuelle Version von AWS SCT
- Db2 für Linux Version 11.1.4.4 und höher

Architektur

Quelltechnologie-Stack

- DB2/Linux x86-64 Bit ist auf einer Instanz gemountet EC2

Zieltechnologie-Stack

- Eine Amazon Aurora MySQL-kompatible Edition-Datenbank-Instance

Quell- und Zielarchitektur

Das folgende Diagramm zeigt die Datenmigrationsarchitektur zwischen der Db2-Quelle und den Aurora MySQL-kompatiblen Zieldatenbanken. Die Architektur in der AWS-Cloud umfasst eine Virtual Private Cloud (VPC) (Virtual Private Cloud), eine Availability Zone, ein öffentliches Subnetz für die Db2-Instance und die AWS DMS-Replikationsinstanz sowie ein privates Subnetz für die Aurora MySQL-kompatible Datenbank.

Tools

AWS-Services

- Amazon Aurora ist eine vollständig verwaltete relationale Datenbank-Engine, die für die Cloud entwickelt wurde und mit MySQL und PostgreSQL kompatibel ist.
- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS-Cloud oder zwischen Kombinationen von Cloud- und lokalen Setups.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Das AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist. AWS SCT unterstützt als Quelle IBM Db2 für LUW-Versionen 9.1, 9.5, 9.7, 10.1, 10.5, 11.1 und 11.5.

Bewährte Methoden

Bewährte Methoden finden Sie unter Bewährte Methoden für AWS Database Migration Service.

Epen

Konfigurieren Sie die IBM Db2-Quelldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IBM Db2-Datenbank auf Amazon EC2.	Sie können eine IBM Db2-Datenbank auf einer EC2 Instance erstellen, indem Sie ein Amazon Machine Image (AMI) von AWS Marketplace verwenden oder indem Sie Db2-Software auf einer EC2 Instance installieren. Starten Sie eine EC2 Instance, indem Sie ein AMI für IBM Db2 auswählen (z. B. IBM Db2 v11.5.7 RHEL 7.9), das einer lokalen Datenbank ähnelt.	DBA, Allgemeines AWS
Konfigurieren Sie Sicherheitsgruppen.	Konfigurieren Sie die eingehenden VPC-Sicherheitsgruppenregeln für SSH (Secure Shell) und TCP mit Port 22 bzw. 50000.	Allgemeines AWS
Erstellen Sie die Datenbankinstanz.	Erstellen Sie eine neue Instanz (Benutzer) und Datenbank (Schema), oder verwenden Sie die `db2inst1` Standardinstanz und Beispieldatenbank. 1. Stellen Sie eine Verbindung mit der EC2 Instanz her, indem Sie das Terminal verwenden, um eine	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Verbindung zur Db2-Datenbank herzustellen. Alternativ können Sie eine beliebige DB-Client-Software installieren, die eine Verbindung zur Db2-Datenbank herstellt. 2. Führen Sie den Befehl aus, um das Passwort des db2inst1-Benutzers festzulegen. `sudo passwd db2inst1` 3. Führen Sie den Befehl aus, um eine Verbindung mit der db2inst1-Instanz herzustellen. `sudo su - db2inst1` 4. Führen Sie den Befehl aus, um eine Verbindung mit der Db2-Datenbank herzustellen. `db2` 5. Verwenden Sie den Befehl`connect to sample`, um eine Verbindung mit der Beispieldatenbank herzustellen. Stellen Sie alternativ eine Verbindung zu der Datenbank her, die Sie erstellt haben. 6. Nachdem Sie eine Verbindung mit der Datenbankinstanz hergestellt haben, erstellen Sie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Objekte und fügen Sie mithilfe von Db2-SQL-A nweisungen Daten in diese Objekte ein.	
Vergewissern Sie sich, dass die Db2-DB-Instance verfügbar ist.	Verwenden Sie den Befehl, um zu bestätigen, dass die Db2-Datenbank-Instance betriebsbereit ist. `Db2pd -`	DBA

Konfigurieren Sie die Aurora MySQL-kompatible Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Aurora MySQL-kompatible Datenbank.	Erstellen Sie eine Amazon Aurora Aurora-Datenbank mit MySQL-Kompatibilität aus dem AWS RDS-Service • Erstellen Sie eine Datenbank auf Amazon Aurora mit MySQL-Kom patibilität und Version Ihrer Wahl, z. B. Aurora (MySQL) —5.6.10a • Installieren Sie die MySQL Workbench-Anwendung oder Ihre bevorzugte DB-Client-Software, mit der Sie eine Verbindung zur MySQL-Datenbank herstelle n können	DBA, Allgemeines AWS
Konfigurieren Sie Sicherhei tsgruppen.	Konfigurieren Sie die eingehenden Regeln der VPC-	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sicherheitsgruppe für SSH- und TCP-Verbindungen.	
Vergewissern Sie sich, dass die Aurora-Datenbank verfügbar ist.	Gehen Sie wie folgt vor, um sicherzustellen, dass die Aurora MySQL-kompatible Datenbank betriebsbereit ist: 1. Stellen Sie über SSH eine Connect mit der EC2 Instance her. 2. Konfigurieren Sie die Aurora MySQL-kompatible Instance von MySQL Workbench aus und stellen Sie eine Verbindung zu ihr her. Verwenden Sie den Endpunkt als Hostnamen, wie im folgenden Beispiel gezeigt. `mysql-cluster-instance-1.cokmvis0v46q.us-east-1.rds.amazonaws.com` 3. Erstellen Sie das neue Schema und stellen Sie eine Verbindung zu diesem her (z. B.`mysql-sample-db2`). 4. Führen Sie die MySQL-Anweisungen aus, um die Schemas und Objekte in der Datenbank zu überprüfen.	DBA

AWS SCT konfigurieren und ausführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie AWS SCT.	Laden Sie die neueste Version von AWS SCT herunter und installieren Sie sie (die aktuelle Version 1.0.628).	Allgemeines AWS
Konfigurieren Sie AWS SCT.	1. Laden Sie die Java Database Connectivity (JDBC) -Treiber für IBM Db2 (Version 4.22.X) und MySQL (8.x) herunter. 2. Um die Treiber in AWS SCT zu konfigurieren, wählen Sie Einstellungen, Globale Einstellungen, Treiber.	Allgemeines AWS
Erstellen Sie ein AWS SCT-Projekt.	Erstellen Sie ein AWS SCT-Projekt und einen Bericht, der Db2 for LUW als Quell-DB-Engine und Aurora MySQL-kompatibel für die Ziel-DB-Engine verwendet. Informationen zu den Rechten, die für die Verbindung mit einer Db2 for LUW-Datenbank erforderlich sind, finden Sie unter Verwenden von Db2 LUW als Quelle für AWS SCT.	Allgemeines AWS
Validieren Sie die Objekte.	Wählen Sie Schema laden und validieren Sie die Objekte. Aktualisieren Sie alle falschen Objekte in der Zieldatenbank:	DBA, Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Stellen Sie eine Verbindung mit dem Amazon Aurora MySQL-kompatiblen Server her, indem Sie die Verbindungsdetails angeben, und wählen Sie Verbindung testen. Sowohl Quell- als auch Zielverbindungen müssen erfolgreich sein, bevor AWS SCT den Migrationsbericht starten kann. 2. Geben Sie nach Abschluss des Berichts das zu konvertierende Schema ein und wählen Sie Fertig stellen. AWS SCT listet alle Quell- und Zielobjekte auf, die konvertiert wurden und Fehler aufweisen. 3. Überprüfen Sie die Fehler und löschen Sie sie manuell. 4. Nachdem alle Fehler behoben wurden, öffnen Sie das Kontextmenü (Rechtsklick) für das Schema und wählen Sie Schema laden aus. 5. Wählen Sie Auf Datenbank anwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Stellen Sie in MySQL Workbench eine Verbindung zur Aurora MySQL-kompatiblen Datenbank her und überprüfen Sie das Schema und die Objekte.	

AWS DMS konfigurieren und ausführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Replikationsinstanz.	Melden Sie sich bei der AWS-Managementkonsole an, navigieren Sie zum AWS DMS-Service und erstellen Sie eine Replikationsinstanz mit gültigen Einstellungen für die VPC-Sicherheitsgruppe, die Sie für die Quell- und Zieldatenbank konfiguriert haben.	Allgemeines AWS
Endpunkte erstellen.	Erstellen Sie den Quellendpunkt für die Db2-Datenbank und den Zielendpunkt für die Aurora MySQL-kompatible Datenbank: 1. Erstellen Sie einen Endpunkt für IBM Db2 als Quelle, indem Sie Select RDS DB-Instance und dann die von Ihnen erstellte Db2-Instance auswählen. Die Details	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zur Endpunktkonfigurat ion werden automatisch ausgefüllt. 2. Fügen Sie in den endpunkts pezifischen Einstellungen die folgenden zusätzlichen Verbindungsattribute hinzu. `CurrentLSN=<scan>; MaxKBytesPerRead=64; SetDataCaptureChanges=true` Wenn Sie diese Attribute nicht angeben, ist die Testverbindung zum Quellendpunkt nicht erfolgreich. Weitere Informationen finden Sie unter IBM Db2 LUW als Quelle für AWS DMS verwenden. 3. Erstellen Sie einen Endpunkt für Aurora MySQL-Compatible als Ziel, indem Sie Select RDS DB-Instance und dann die Aurora MySQL-kom patible Instance auswählen , die Sie erstellt haben. Die Konfigurationsdetails für den Endpunkt werden automatisch ausgefüllt. Weitere Informationen finden Sie unter Verwenden	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	einer MySQL-kompatiblen Datenbank als Ziel für den AWS Database Migration Service. 4. Testen Sie die Quell- und Zielendpunkte. Stellen Sie sicher, dass beide erfolgreich und verfügbar sind 5. Wenn der Test fehlschlägt, stellen Sie sicher, dass die Regeln für eingehende Zugriffe in der Sicherheitsgruppe gültig sind.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Migration saufgaben.	Erstellen Sie eine einzelne Migrationsaufgabe oder mehrere Migrationsaufgaben für Volllast und CDC- oder Datenvalidierung: 1. Um eine Datenbank migrationsaufgabe zu erstellen, wählen Sie die Replikationsinstanz, den Quelldatenbankendp unkt und den Zieldaten bankendpunkt aus. Geben Sie den Migrationstyp als Vorhandene Daten migrieren (Volllast), Nur Datenänderungen replizier en (CDC) oder Vorhanden e Daten migrieren und laufende Änderungen replizieren (Volllast und CDC) an. 2. Unter Tabellenzuordnungen können Sie Auswahlregeln und Transformationsregeln im GUI- oder JSON-Format konfigurieren. 3. Wählen Sie unter Auswahlregeln das Schema aus, geben Sie den Tabellennamen ein und wählen Sie Aktion (Einschli eßen/Ausschließen) aus, die konfiguriert werden soll	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(z. B. Schema: SAMPLE; Tabellenname:%, Aktion: Include). 4. Wählen Sie unter Transformationsregeln das Ziel aus (Schema, Tabelle oder Spalte). Wählen Sie den Schemanamen und dann die Aktion (Groß- und Kleinschreibung, Präfix, Suffix) aus, z. B. Ziel: Schema`mysql-sample-db`; Aktion: Kleinbuchstaben. 5. Aktivieren Sie die Amazon CloudWatch Logs-Überwachung.	
Planen Sie den Produktionslauf.	Bestätigen Sie Ausfallzeiten mit Stakeholdern wie Anwendungseigentümern, um AWS DMS in Produktionssystemen auszuführen.	Leiter der Migration
Führen Sie die Migrationsaufgaben aus.	1. Starten Sie die AWS DMS-Aufgabe mit dem Status Bereit. 2. Überwachen Sie die Protokolle der Migrationsaufgaben in Amazon CloudWatch Logs auf Fehler.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Daten.	Überprüfen Sie die Ergebnisse und Daten der Migrationsaufgaben in den DB2-Quelldatenbanken und den MySQL-Zieldatenbanken: 1. Wenn der Status Load complete running replication lautet, ist der vollständige Ladevorgang mit der CDC-Datenmigration abgeschlossen und die Validierung läuft. 2. Connect zur Aurora MySQL-kompatiblen Datenbank her und überprüfen Sie die Daten. 3. Überprüfen Sie die laufenden Änderungen, indem Sie Daten in die Db2-Datenbank einfügen oder aktualisieren.	DBA
Stoppen Sie die Migrationsaufgaben.	Nachdem die Datenvalidierung erfolgreich abgeschlossen wurde, beenden Sie die Validierungsmigrationsaufgaben.	Allgemeines AWS

Fehlerbehebung

Problem	Lösung
Die Quell- und Zieltestverbindungen von AWS SCT schlagen fehl.	Konfigurieren Sie JDBC-Treiberversionen und eingehende VPC-Sicherheitsgruppenregeln, um den eingehenden Datenverkehr zu akzeptieren.
Der Testlauf für den Db2-Quellendpunkt schlägt fehl.	Konfigurieren Sie die zusätzliche Verbindungseinstellung`CurrentLSN=<scan>;` .

Die AWSDMS Aufgabe kann keine Verbindung zur Db2-Quelle herstellen, und der folgende Fehler wird zurückgegeben.
`database is recoverable if either or both of the database configuration parameters LOGARCHMETH1 and LOGARCHMETH2 are set to ON`
	Führen Sie die folgenden Befehle aus, um den Fehler zu vermeiden:
	1. `$ db2 update db cfg for sample using LOGARCHMETH1 DISK:/home/db2inst1/logs`
	2. `$ db2stop`
	3. `$ db2start`
	4. `$ db2 connect to sample`
	`SQL1116N A connection to or activation of database "SAMPLE" cannot be made because of BACKUP PENDING. SQLSTATE=57019`
	5. `$ db2 backup database sample to ../logs`
	`SQL2036N The path for the file or device "../logs" is not valid`
	6. `$ cd`
	7. `$ pwd`
	`/home/db2inst1`
	8. `$ mkdir /tmp/backup`

Problem	Lösung

	9. `$ db2 backup database sample to /tmp/backup`
	`Backup successful. The timestamp for this backup image is : 20190530084921`
	10. `$ db2 connect to sample`
	`Database Connection Information`
	`Database server = DB2/LINUX 9.7.1`
	`SQL authorization ID = DB2INST1`
	`Local database alias = SAMPLE`

Zugehörige Ressourcen

Amazon EC2

- Amazon EC2
- EC2 Amazon-Benutzerhandbücher

Datenbanken

- IBM Db2-Datenbank
- Amazon Aurora
- Arbeiten mit Amazon Aurora MySQL

AWS SCT

- AWS-DMS-Schemakonvertierung
- Benutzerhandbuch für das AWS Schema Conversion Tool
- Verwenden der AWS SCT-Benutzeroberfläche
- IBM Db2 LUW als Quelle für AWS SCT verwenden

AWS DMS

- AWS Database Migration Service
- AWS Database Migration Service — Benutzerhandbuch
- Quellen für die Datenmigration
- Ziele für die Datenmigration
- AWS Database Migration Service und AWS Schema Conversion Tool unterstützen jetzt IBM Db2 LUW als Quelle (Blogbeitrag)
- Migrieren von Anwendungen, auf denen relationale Datenbanken ausgeführt werden, zu AWS

Migrieren Sie mithilfe von AWS DMS eine Microsoft SQL Server-Datenbank von Amazon EC2 zu Amazon DocumentDB

Erstellt von Umamaheswara Nooka (AWS)

Übersicht

Dieses Muster beschreibt, wie AWS Database Migration Service (AWS DMS) verwendet wird, um eine Microsoft SQL Server-Datenbank, die auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance gehostet wird, zu einer Amazon DocumentDB DocumentDB-Datenbank (mit MongoDB-Kompatibilität) zu migrieren.

Die AWS DMS-Replikationsaufgabe liest die Tabellenstruktur der SQL Server-Datenbank, erstellt die entsprechende Sammlung in Amazon DocumentDB und führt eine Volllastmigration durch.

Sie können dieses Muster auch verwenden, um eine lokale SQL Server- oder Amazon Relational Database Service (Amazon RDS) für SQL Server-DB-Instance zu Amazon DocumentDB zu migrieren. Weitere Informationen finden Sie im Leitfaden Migration von Microsoft SQL Server-Datenbanken zur AWS-Cloud auf der AWS Prescriptive Guidance-Website.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine bestehende SQL Server-Datenbank auf einer Instance. EC2
- Feste Datenbankrolle (db_owner), die AWS DMS in der SQL Server-Datenbank zugewiesen wurde. Weitere Informationen finden Sie unter Rollen auf Datenbankebene in der SQL Server-Dokumentation.
- Vertrautheit mit der Verwendung der `mongoimport` Dienstprogramme `mongodump` `mongorestore``mongoexport`,, und zum Verschieben von Daten in und aus einem Amazon DocumentDB-Cluster.
- Microsoft SQL Server Management Studio, installiert und konfiguriert.

Einschränkungen

- Die Clustergrößenbeschränkung in Amazon DocumentDB beträgt 64 TB. Weitere Informationen finden Sie unter Cluster-Grenzwerte in der Amazon DocumentDB DocumentDB-Dokumentation.

- AWS DMS unterstützt nicht die Zusammenführung mehrerer Quelltabellen zu einer einzigen Amazon DocumentDB-Sammlung.
- Wenn AWS DMS Änderungen aus einer Quelltabelle ohne Primärschlüssel verarbeitet, ignoriert es große Objektspalten (LOB) in der Quelltabelle.

Architektur

Quelltechnologie-Stack

- Amazon EC2

Zielarchitektur

Zieltechnologie-Stack

- Amazon DocumentDB

Tools

- AWS DMS — Mit dem AWS Database Migration Service (AWS DMS) können Sie Datenbanken einfach und sicher migrieren.
- Amazon DocumentDB — Amazon DocumentDB (mit MongoDB-Kompatibilität) ist ein schneller, zuverlässiger und vollständig verwalteter Datenbankservice.
- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud.
- Microsoft SQL Server — SQL Server ist ein relationales Datenbankverwaltungssystem.
- SQL Server Management Studio (SSMS) — SSMS ist ein Tool zur Verwaltung von SQL Server, einschließlich des Zugriffs auf, der Konfiguration und Verwaltung von SQL Server-Komponenten.

Epen

Eine VPC erstellen und konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC.	Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon VPC-Konsole. Erstellen Sie eine Virtual Private Cloud (VPC) mit einem IPv4 CIDR-Bloc kbereich.	Systemadministrator
Erstellen Sie Sicherhei tsgruppen und ein Netzwerk. ACLs	Erstellen Sie auf der Amazon VPC-Konsole gemäß Ihren Anforderungen Sicherhei tsgruppen und Netzwerkz ugriffskontrolllisten (Netzwerk ACLs) für Ihre VPC. Sie können auch die Standarde instellungen für diese Konfigurationen verwenden . Weitere Informationen zu dieser und anderen Geschicht en finden Sie im Abschnitt „Verwandte Ressourcen“.	Systemadministrator

Erstellen und konfigurieren Sie den Amazon DocumentDB-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon DocumentDB-Cluster.	Öffnen Sie die Amazon DocumentDB DocumentD B-Konsole und wählen Sie „Clusters“. Wählen Sie „Erstellen“ und erstellen Sie	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	einen Amazon DocumentDB-Cluster mit einer Instance. Wichtig: Stellen Sie sicher, dass Sie diesen Cluster mit den Sicherheitsgruppen Ihrer VPC konfigurieren.	
Installieren Sie die Mongo-Shell.	Die mongo-Shell ist ein Befehlszeilenprogramm, mit dem Sie eine Verbindung zu Ihrem Amazon DocumentDB-Cluster herstellen und ihn abfragen können. Um sie zu installieren, führen Sie den Befehl „/etc/yum.repos.d/mongodb-org-3.6.repo“ aus, um die Repository-Datei zu erstellen. Führen Sie den Befehl „sudo yum install -y“ aus, um die mongodb-org-shell Mongo-Shell zu installieren. Um Daten während der Übertragung zu verschlüsseln, laden Sie den öffentlichen Schlüssel für Amazon DocumentDB herunter und stellen Sie dann eine Verbindung zu Ihrer Amazon DocumentDB DocumentDB-Instance her. Weitere Informationen zu diesen Schritten finden Sie im Abschnitt „Verwandte Ressourcen“.	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Datenbank im Amazon DocumentDB-Cluster.	Führen Sie den Befehl „use“ mit dem Namen Ihrer Datenbank aus, um eine Datenbank in Ihrem Amazon DocumentDB-Cluster zu erstellen.	Systemadministrator

Erstellen und konfigurieren Sie die AWS DMS-Replikationsinstanz

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die AWS DMS-Replikationsinstanz.	Öffnen Sie die AWS DMS-Konsole und wählen Sie „Replikationsinstanz erstellen “. Geben Sie einen Namen und eine Beschreibung für Ihre Replikationsaufgabe ein. Wählen Sie die Instanzklasse, die Engine-Version, den Speicher, die VPC und die Multi-AZ aus und machen Sie sie öffentlich zugänglich. Wählen Sie den Tab „Erweitert“, um die Netzwerk- und Verschlüsselungseinstellungen festzulegen. Geben Sie die Wartungseinstellungen an und wählen Sie dann „Replikationsinstanz erstellen“.	Systemadministrator
Konfigurieren Sie die SQL Server-Datenbank.	Melden Sie sich bei Microsoft SQL Server an und fügen Sie eine eingehende Regel für die Kommunikation zwischen	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dem Quellendpunkt und der AWS DMS-Replikationsinstanz hinzu. Verwenden Sie die private IP-Adresse der Replikationsinstanz als Quelle. Wichtig: Die Replikationsinstanz und der Zielendpunkt sollten sich auf derselben VPC befinden. Verwenden Sie eine alternative Quelle in der Sicherheitsgruppe, wenn die Quell- und Replikationsinstanzen unterschiedlich VPCs sind.	

Quell- und Zielendpunkte in AWS DMS erstellen und testen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Quell- und Zieldatenbank-Endpunkte.	Öffnen Sie die AWS DMS-Konsole und wählen Sie „Quell- und Zieldatenbank-Endpunkte Connect“. Geben Sie die Verbindungsinformationen für die Quell- und Zieldatenbanken an. Wählen Sie bei Bedarf die Registerkarte „Erweitert“, um Werte für „Zusätzliche Verbindungsattribute“ festzulegen. Laden Sie das Zertifikatspaket herunter und verwenden Sie es in Ihrer Endpunktkonfiguration.	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Endpunktv erbindung.	Wählen Sie „Test ausführen“, um die Verbindung zu testen. Beheben Sie alle Fehlermel dungen, indem Sie die Sicherheitsgruppeneinstellu ngen und die Verbindungen zur AWS DMS-Replikationsin stanz sowohl von der Quell- als auch von der Zieldaten bank-Instance aus überprüfen.	Systemadministrator

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die AWS DMS-Migrationsaufgabe.	Wählen Sie in der AWS DMS-Konsole „Aufgaben“, „Aufgabe erstellen“. Geben Sie die Aufgabenoptionen an, einschließlich der Namen der Quell- und Zielendpu nkte sowie der Namen der Replikationsinstanzen. Wählen Sie unter „Migrationstyp“ die Optionen „Bestehende Daten migrieren“ und „Nur Datenänderungen replizier en“ aus. Wählen Sie „Aufgabe starten“.	Systemadministrator
Führen Sie die AWS DMS-Migrationsaufgabe aus.	Geben Sie unter „Aufgaben einstellungen“ die Einstellu ngen für den Tabellenv orbereitungsmodus an, z. B.	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	„Nichts tun“, „Tabellen auf Ziel löschen“, „Kürzen“ und „LOB-Spalten in die Replikation einbeziehen“. Legen Sie eine maximale LOB-Größe fest, die AWS DMS akzeptiert, und wählen Sie „Protokollierung aktivieren“. Behalten Sie für die „Erweiterten Einstellungen“ die Standardwerte bei und wählen Sie „Aufgabe erstellen “.	
Überwachen Sie die Migration.	Wählen Sie in der AWS DMS-Konsole „Aufgaben“ und wählen Sie Ihre Migration saufgabe aus. Wählen Sie „Aufgabenüberwachung“, um Ihre Aufgabe zu überwache n. Die Aufgabe wird beendet, wenn die Volllastmigration abgeschlossen ist und die zwischengespeicherten Änderungen übernommen wurden.	Systemadministrator

Testen und verifizieren Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie mithilfe der Mongo-Shell eine Connect zum Amazon DocumentDB-Cluster her.	Öffnen Sie die Amazon DocumentDB DocumentD B-Konsole und wählen Sie Ihren Cluster unter „Clusters “ aus. Wählen Sie auf der	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Registerkarte „Konnektivität und Sicherheit“ die Option „Mit der Mongo-Shell mit diesem Cluster Connect“.	
Überprüfen Sie die Ergebnisse Ihrer Migration.	Führen Sie den Befehl „use“ mit dem Namen Ihrer Datenbank und anschließend den Befehl „show collectio ns“ aus. Führen Sie den Befehl „db. .count ();“ mit dem Namen Ihrer Datenbank aus. Wenn die Ergebnisse mit Ihrer Quelldatenbank übereinst immen, war Ihre Migration erfolgreich.	Systemadministrator

Zugehörige Ressourcen

Eine VPC erstellen und konfigurieren

- Erstellen Sie eine Sicherheitsgruppe für Ihre VPC
- Erstellen Sie eine Netzwerk-ACL

Erstellen und konfigurieren Sie den Amazon DocumentDB-Cluster

- Erstellen Sie einen Amazon DocumentDB-Cluster
- Installieren Sie die Mongo-Shell für Amazon DocumentDB
- Connect zu Ihrem Amazon DocumentDB-Cluster her

Erstellen und konfigurieren Sie die AWS DMS-Replikationsinstanz

- Verwenden Sie öffentliche und private Replikationsinstanzen

Quell- und Zielendpunkte in AWS DMS erstellen und testen

- Verwenden Sie Amazon DocumentDB als Ziel für AWS DMS
- Verwenden Sie eine SQL Server-Datenbank als Quelle für AWS DMS
- Verwenden Sie AWS DMS-Endpunkte

Daten migrieren

- Zu Amazon DocumentDB migrieren

Sonstige Ressourcen

- Einschränkungen bei der Verwendung von SQL Server als Quelle für AWS DMS
- So verwenden Sie Amazon DocumentDB, um skalierbare Anwendungen zu erstellen und zu verwalten

Migrieren Sie eine lokale ThoughtSpot Falcon-Datenbank zu Amazon Redshift

Erstellt von Battulga Purevragchaa (AWS) und Antony Prasad Thevaraj (AWS)

Übersicht

Lokale Data Warehouses erfordern viel Verwaltungszeit und Ressourcen, insbesondere bei großen Datensätzen. Die finanziellen Kosten für den Bau, die Wartung und den Ausbau dieser Lagerhäuser sind ebenfalls sehr hoch. Um die Kosten im Griff zu behalten, die Komplexität von Extrahieren, Transformieren und Laden (ETL) gering zu halten und die Leistung auch bei wachsenden Datenmengen zu gewährleisten, müssen Sie ständig entscheiden, welche Daten geladen und welche archiviert werden sollen.

Durch die Migration Ihrer lokalen ThoughtSpot Falcon-Datenbanken in die Amazon Web Services (AWS) Cloud können Sie auf Cloud-basierte Data Lakes und Data Warehouses zugreifen, die Ihre geschäftliche Flexibilität, Sicherheit und Anwendungszuverlässigkeit erhöhen und gleichzeitig Ihre gesamten Infrastrukturkosten senken. Amazon Redshift trägt dazu bei, die Kosten und den Betriebskosten eines Data Warehouse erheblich zu senken. Sie können Amazon Redshift Spectrum auch verwenden, um große Datenmengen im nativen Format zu analysieren, ohne dass Daten geladen werden müssen.

Dieses Muster beschreibt die Schritte und den Prozess für die Migration einer ThoughtSpot Falcon-Datenbank von einem lokalen Rechenzentrum zu einer Amazon Redshift Redshift-Datenbank in der AWS-Cloud.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine ThoughtSpot Falcon-Datenbank, die in einem lokalen Rechenzentrum gehostet wird

Produktversionen

- ThoughtSpot Version 7.0.1

Architektur

Das Diagramm zeigt den folgenden Workflow:

1. Die Daten werden in einer lokalen relationalen Datenbank gehostet.
2. Das AWS Schema Conversion Tool (AWS SCT) konvertiert die Datendefinitionssprache (DDL), die mit Amazon Redshift kompatibel ist.
3. Nachdem die Tabellen erstellt wurden, können Sie die Daten mithilfe des AWS Database Migration Service (AWS DMS) migrieren.
4. Die Daten werden in Amazon Redshift geladen.
5. Die Daten werden in Amazon Simple Storage Service (Amazon S3) gespeichert, wenn Sie Redshift Spectrum verwenden oder die Daten bereits in Amazon S3 hosten.

Tools

- AWS DMS — AWS Data Migration Service (AWS DMS) hilft Ihnen, Datenbanken schnell und sicher zu AWS zu migrieren.
- Amazon Redshift — Amazon Redshift ist ein schneller, vollständig verwalteter Data Warehouse-Service im Petabyte-Bereich, mit dem Sie all Ihre Daten mithilfe Ihrer vorhandenen Business Intelligence-Tools einfach und kostengünstig effizient analysieren können.
- AWS SCT — Das AWS Schema Conversion Tool (AWS SCT) konvertiert Ihr vorhandenes Datenbankschema von einer Datenbank-Engine in eine andere.

Epen

Bereite dich auf die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die entsprechende Amazon Redshift Redshift-Konfiguration.	Identifizieren Sie die passende Amazon Redshift Redshift-Cluster-Konfiguration auf der Grundlage Ihrer Anforderungen und Ihres Datenvolumens. Weitere Informationen finden Sie unter Amazon Redshift	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Redshift-Cluster in der Amazon Redshift Redshift-Dokumentation.	
Informieren Sie sich über Amazon Redshift, um herauszufinden, ob es Ihren Anforderungen entspricht.	Verwenden Sie Amazon Redshift FAQs, um zu verstehen und zu bewerten, ob Amazon Redshift Ihre Anforderungen erfüllt.	DBA

Bereiten Sie den Amazon Redshift Redshift-Zielcluster vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon Redshift Redshift-Cluster.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon Redshift Redshift-Konsole und erstellen Sie dann einen Amazon Redshift Redshift-Cluster in einer Virtual Private Cloud (VPC). Weitere Informationen finden Sie unter Erstellen eines Clusters in einer VPC in der Amazon Redshift Redshift-Dokumentation.	DBA
Führen Sie einen PoC für Ihr Amazon Redshift Redshift-Datenbankdesign durch.	Folgen Sie den Best Practices von Amazon Redshift, indem Sie einen Machbarkeitsnachweis (PoC) für Ihr Datenbankdesign durchführen.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter Durchführung eines Machbarkeitsnachweises für Amazon Redshift in der Amazon Redshift Redshift-Dokumentation.	
Datenbankbenutzer erstellen.	Erstellen Sie die Benutzer in Ihrer Amazon Redshift Redshift-Datenbank und gewähren Sie die entsprech enden Rollen für den Zugriff auf das Schema und die Tabellen. Weitere Informationen finden Sie unter Gewähren von Zugriffsberechtigungen für einen Benutzer oder eine Benutzergruppe in der Amazon Redshift Redshift-Dokumentation.	DBA
Wenden Sie die Konfigura tionseinstellungen auf die Zieldatenbank an.	Wenden Sie die Konfigura tionseinstellungen entsprech end Ihren Anforderungen auf die Amazon Redshift Redshift-Datenbank an. Weitere Informationen zur Aktivierung von Parametern auf Datenbank-, Sitzungs- und Serverebene finden Sie in der Konfigurationsreferenz in der Amazon Redshift Redshift-Dokumentation.	DBA

Objekte im Amazon Redshift Redshift-Cluster erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie manuell Tabellen mit DDL in Amazon Redshift.	(Optional) Wenn Sie AWS SCT verwenden, werden die Tabellen automatisch erstellt. Wenn bei der Replikation jedoch Fehler auftreten DDLs, müssen Sie die Tabellen manuell erstellen	DBA
Erstellen Sie externe Tabellen für Redshift Spectrum.	Erstellen Sie eine externe Tabelle mit einem externen Schema für Amazon Redshift Spectrum. Um externe Tabellen zu erstellen, müssen Sie der Eigentümer des externen Schemas oder ein Datenbank-Superuser sein. Weitere Informationen finden Sie unter Erstellen externer Tabellen für Amazon Redshift Spectrum in der Amazon Redshift-Dokumentation.	DBA

Migrieren Sie Daten mit AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie AWS DMS, um die Daten zu migrieren.	Nachdem Sie die DDL der Tabellen in der Amazon Redshift-Datenbank erstellt haben, migrieren Sie Ihre Daten mithilfe von AWS DMS zu Amazon Redshift.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ausführliche Schritte und Anweisungen finden Sie unter Verwenden einer Amazon Redshift Redshift-Datenbank als Ziel für AWS DMS in der AWS DMS-Dokumentation.	
Verwenden Sie den Befehl COPY, um die Daten zu laden.	Verwenden Sie den Amazon `COPY` Redshift-Befehl, um die Daten von Amazon S3 nach Amazon Redshift zu laden. Weitere Informationen finden Sie unter Verwenden des COPY-Befehls zum Laden aus Amazon S3 in der Amazon Redshift Redshift-Dokumentation.	DBA

Den Amazon Redshift Redshift-Cluster validieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatensätze.	Überprüfen Sie die Tabellenanzahl für die Quell- und Zieldatensätze, die aus Ihrem Quellsystem geladen wurden.	DBA
Implementieren Sie die Best Practices von Amazon Redshift zur Leistungsoptimierung.	Implementieren Sie die Best Practices von Amazon Redshift für das Tabellen- und Datenbankdesign. Weitere Informationen finden Sie im Blogbeitrag Die 10 wichtigsten Techniken zur	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Leistungsoptimierung für Amazon Redshift.	
Optimieren Sie die Abfragele istung.	Amazon Redshift verwendet SQL-basierte Abfragen, um mit Daten und Objekten im System zu interagieren. Die Datenmanipulationssprache (DML) ist die Teilmenge von SQL, mit der Sie Daten anzeigen, hinzufügen, ändern und löschen können. DDL ist die Teilmenge von SQL, die Sie zum Hinzufügen, Ändern und Löschen von Datenbank objekten wie Tabellen und Ansichten verwenden. Weitere Informationen finden Sie unter Optimieren der Abfrageleistung in der Amazon Redshift Redshift-Dokumenta tion.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Implementieren Sie WLM.	Sie können Workload Management (WLM) verwenden, um mehrere Abfragewarteschlangen zu definieren und Abfragen zur Laufzeit an die entsprech enden Warteschlangen weiterzuleiten. Weitere Informationen finden Sie unter Implementieren des Workload-Managements in der Amazon Redshift Redshift-Dokumentation.	DBA
Arbeiten Sie mit Paralleli tätsskalierung.	Mithilfe der Concurrency Scaling-Funktion können Sie praktisch unbegrenzt viele gleichzeitige Benutzer und Abfragen bei gleichbleibend schneller Abfrageleistung unterstützen. Weitere Informationen finden Sie unter Arbeiten mit Paralleli tätsskalierung in der Amazon Redshift Redshift-Dokumenta tion.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie die Best Practices von Amazon Redshift für das Tabellend esign.	Bei der Planung Ihrer Datenbank können bestimmte wichtige Entscheidungen beim Tabellenentwurf die allgemeine Abfrageleistung stark beeinflussen. Weitere Informationen zur Auswahl der am besten geeigneten Tabellene ntwurfsoption finden Sie unter Bewährte Methoden für das Entwerfen von Tabellen für Amazon Redshift in der Amazon Redshift-Dokumenta tion.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie materialisierte Ansichten in Amazon Redshift.	Eine materialisierte Ansicht enthält einen vorberech neten Ergebnissatz, der auf einer SQL-Abfrage über eine oder mehrere Basistabellen basiert. Sie können `SELECT` Anweisungen zur Abfrage einer materialisierten Ansicht genauso ausgeben, wie Sie andere Tabellen oder Ansichten in der Datenbank abfragen. Weitere Informationen finden Sie unter Erstellen materiali sierter Ansichten in Amazon Redshift in der Amazon Redshift Redshift-Dokumenta tion.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie Verknüpfungen zwischen den Tabellen.	Um in mehr als einer Tabelle gleichzeitig zu suchen ThoughtSpot, müssen Sie Verknüpfungen zwischen den Tabellen definieren, indem Sie Spalten angeben, die übereinstimmende Daten aus zwei Tabellen enthalten. Diese Spalten stellen das `primary key` Ende `foreign key` der Verknüpfung dar. Sie können sie definieren, indem Sie den `ALTER TABLE` Befehl in Amazon Redshift oder ThoughtSpot verwenden . Weitere Informationen finden Sie unter ALTER TABLE in der Amazon Redshift Redshift-Dokumentation.	DBA

ThoughtSpot Verbindung zu Amazon Redshift einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie eine Amazon Redshift Redshift-Verbindung hinzu.	Fügen Sie Ihrer lokalen ThoughtSpot Falcon-Da tenbank eine Amazon Redshift Redshift-Verbindung hinzu. Weitere Informationen finden Sie in der ThoughtSp ot Dokumentation unter	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinzufügen einer Amazon Redshift Redshift-Verbindung.	
Bearbeiten Sie die Amazon Redshift Redshift-Verbindung.	Sie können die Amazon Redshift Redshift-Verbindung bearbeiten, um Tabellen und Spalten hinzuzufügen. Weitere Informationen finden Sie in der ThoughtSpot Dokumentation unter Bearbeiten einer Amazon Redshift Redshift-Verbindung.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ordnen Sie die Amazon Redshift Redshift-Verbindung neu zu.	Ändern Sie die Verbindungsparameter, indem Sie die Quell-Mapping-.yaml-Datei bearbeiten, die beim Hinzufügen der Amazon Redshift Redshift-Verbindung erstellt wurde. Sie können beispielsweise die bestehende Tabelle oder Spalte einer anderen Tabelle oder Spalte in einer bestehenden Datenbankverbindung neu zuordnen. ThoughtSpot empfiehlt, die Abhängigkeiten vor und nach der Neuzuweisung einer Tabelle oder Spalte in einer Verbindung zu überprüfen, um sicherzustellen, dass sie wie gewünscht angezeigt werden. Weitere Informationen finden Sie in der Dokumentation unter Eine Amazon Redshift Redshift-Verbindung neu zuordnen. ThoughtSpot	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie eine Tabelle aus der Amazon Redshift Redshift-Verbindung.	(Optional) Wenn Sie versuchen, eine Tabelle in einer Amazon Redshift Redshift-Verbindung zu entfernen, ThoughtSpot sucht es nach Abhängigk eiten und zeigt eine Liste der abhängigen Objekte an. Sie können die aufgelisteten Objekte auswählen, um sie zu löschen oder die Abhängigk eit zu entfernen. Anschließ end können Sie die Tabelle entfernen. Weitere Informationen finden Sie in der ThoughtSpot Dokumentation unter Löschen einer Tabelle aus einer Amazon Redshift Redshift-Verbindung.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie eine Tabelle mit abhängigen Objekten aus einer Amazon Redshift Redshift-Verbindung.	(Optional) Wenn Sie versuchen, eine Tabelle mit abhängigen Objekten zu löschen, wird der Vorgang blockiert. Es wird ein `Cannot delete` Fenster mit einer Liste von Links zu abhängige n Objekten angezeigt. Wenn alle Abhängigkeiten entfernt wurden, können Sie die Tabelle löschen Weitere Informationen finden Sie in der ThoughtSpot Dokumentation unter Löschen einer Tabelle mit abhängige n Objekten aus einer Amazon Redshift Redshift-Verbindung.	DBA
Löschen Sie eine Amazon Redshift Redshift-Verbindung.	(Optional) Da eine Verbindun g in mehreren Datenquel len oder Visualisierungen verwendet werden kann, müssen Sie alle Quellen und Aufgaben löschen, die diese Verbindung verwenden, bevor Sie die Amazon Redshift Redshift-Verbindung löschen können. Weitere Informationen finden Sie in der ThoughtSpot Dokumentation unter Löschen einer Amazon Redshift Redshift-Verbindung.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Verbindungsreferenz für Amazon Redshift.	Stellen Sie sicher, dass Sie die erforderlichen Informationen für Ihre Amazon Redshift Redshift-Verbindung angeben, indem Sie die Verbindungsreferenz in der ThoughtSpot Dokumentation verwenden.	DBA

Zusätzliche Informationen

- KI-gestützte Analysen in jeder Größenordnung mit Amazon ThoughtSpot Redshift
- Amazon-Redshift-Preise
- Erste Schritte mit AWS SCT
- Erste Schritte mit Amazon Redshift
- Verwenden von Datenextraktionsagenten
- Chick-fil-A verbessert die Schnelligkeit, Erkenntnisse mit ThoughtSpot und AWS zu gewinnen

Migrieren Sie eine Oracle-Datenbank mit AWS DMS zu Amazon DynamoDB

Erstellt von Rambabu Karnena (AWS)

Übersicht

Dieses Muster führt Sie durch die Schritte zur Migration einer Oracle-Datenbank zu Amazon DynamoDB mithilfe des AWS Database Migration Service (AWS DMS). Es deckt drei Arten von Quelldatenbanken ab:

- Lokale Oracle-Datenbanken
- Oracle-Datenbanken auf Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Relational Database Service (Amazon RDS) für Oracle-DB-Instances

In diesem Machbarkeitsnachweis konzentriert sich dieses Muster auf die Migration von einer Amazon RDS for Oracle DB-Instance.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Anwendung, die eine Verbindung zu einer Amazon RDS for Oracle Oracle-Datenbank herstellt
- Eine in der Amazon RDS for Oracle Oracle-Quelldatenbank erstellte Tabelle mit einem Primärschlüssel und Beispieldaten

Einschränkungen

- Oracle-Datenbankobjekte wie Prozeduren, Funktionen, Pakete und Trigger werden für die Migration nicht berücksichtigt, da Amazon DynamoDB diese Datenbankobjekte nicht unterstützt.

Produktversionen

- Dieses Muster gilt für alle Editionen und Versionen von Oracle-Datenbanken, die von AWS DMS unterstützt werden. Weitere Informationen finden Sie unter Verwenden einer Oracle-Datenbank als Quelle für AWS DMS und Verwenden einer Amazon DynamoDB DynamoDB-Datenbank als Ziel für AWS DMS. Wir empfehlen Ihnen, die neuesten Versionen von AWS DMS zu verwenden, um die umfassendste Versions- und Funktionsunterstützung zu erhalten.

Architektur

Quelltechnologie-Stack

- Amazon RDS for Oracle Oracle-DB-Instances, Oracle auf Amazon EC2 oder lokale Oracle-Datenbanken

Zieltechnologie-Stack

- Amazon-DynamoDB

AWS-Datenmigrationsarchitektur

Tools

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS-Cloud oder zwischen Kombinationen von Cloud- und lokalen Setups.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der AWS-Cloud. Dieses Muster verwendet Amazon RDS for Oracle.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC.	Erstellen Sie in Ihrem AWS-Konto eine Virtual Private Cloud (VPC) und ein privates Subnetz.	Systemadministrator
Erstellen Sie Sicherheitsgruppen und Listen zur Netzwerkzugriffskontrolle.	Weitere Informationen finden Sie in der AWS-Dokumentation.	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren und starten Sie die Amazon RDS for Oracle DB-Instance.	Weitere Informationen finden Sie in der AWS-Dokumentation.	DBA, Systemadministrator

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle für den Zugriff auf DynamoDB.	Erstellen Sie in der AWS Identity and Access Management (IAM) -Konsole die Rolle, fügen Sie die Richtlinie `AmazonDynamoDBFullAccess to it` hinzu und wählen Sie AWS DMS als Service aus.	Systemadministrator
Erstellen Sie eine AWS DMS-Replikationsinstanz für die Migration.	Die Replikationsinstanz sollte sich in derselben Availability Zone und VPC wie die Quelldatenbank befinden.	Systemadministrator
Erstellen Sie Quell- und Zielendpunkte in AWS DMS.	Um den Quelldatenbank-Endpunkt zu erstellen, haben Sie zwei Möglichkeiten: • Wählen Sie auf der Amazon RDS-Konsole Datenbanken, DB-ID, Konnektivität und Sicherheit und wählen Sie den Endpunkt aus. • Wählen Sie in der AWS DMS-Konsole Select RDS DB Instance aus.	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Um den Zieldatenbank-Endpunkt zu erstellen, wählen Sie die Rolle Amazon Resource Name (ARN) aus der vorherigen Aufgabe für den Zugriff auf DynamoDB aus.	
Erstellen Sie eine AWS-DMS-Aufgabe, um die Oracle-Quelldatenbanktabellen in DynamoDB zu laden.	Wählen Sie die Namen der Quell- und Zielendpunkte sowie die Replikationsinstanz aus den vorherigen Schritten aus. Der Typ kann Volllast sein. Wählen Sie das Oracle-Schema und geben Sie% an, um alle Tabellen auszuwähl en.	Systemadministrator
Überprüfen Sie die Tabellen in DynamoDB.	Um die Migrationsergebnis se anzuzeigen, wählen Sie im linken Navigationsbereich der DynamoDB-Konsole Tabellen aus.	DBA

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie den Anwendung scode.	Um eine Verbindung zu DynamoDB herzustellen und Daten von DynamoDB abzurufen, aktualisieren Sie den Anwendungscode.	App-Besitzer, DBA, Systemadministrator

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung sclients so ein, dass sie DynamoDB verwenden.		DBA, App-Besitzer, Systemadministrator

Schließen Sie das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie AWS-Ressourcen herunter.	Zum Beispiel das Herunterf ahren der Amazon RDS for Oracle-Instance, DynamoDB und der AWS DMS-Repli kationsinstanz.	DBA, Systemadministrator
Sammeln Sie Kennzahlen.	Zu den Kennzahlen gehören die Zeit für die Migration, der prozentuale Anteil manueller Arbeit und der vom Tool ausgeführten Arbeit sowie Kosteneinsparungen.	DBA, App-Besitzer, Systemadministrator

Zugehörige Ressourcen

- AWS Database Migration Service und Amazon DynamoDB: Was Sie wissen müssen (Blogbeitrag)
- Verwenden einer Oracle-Datenbank als Quelle für AWS DMS
- Verwenden einer Amazon DynamoDB DynamoDB-Datenbank als Ziel für den AWS Database Migration Service
- Bewährte Methoden für die Migration von RDBMS zu Amazon DynamoDB (Whitepaper)

Migrieren Sie eine partitionierte Oracle-Tabelle mithilfe von AWS DMS zu PostgreSQL

Erstellt von Saurav Mishra (AWS) und Eduardo Valentim (AWS)

Übersicht

Dieses Muster beschreibt, wie das Laden einer partitionierten Tabelle von Oracle nach PostgreSQL mithilfe von AWS Database Migration Service (AWS DMS) beschleunigt werden kann, der keine native Partitionierung unterstützt. Die PostgreSQL-Zieldatenbank kann auf Amazon Elastic Compute Cloud (Amazon EC2) installiert werden, oder es kann sich um eine Amazon Relational Database Service (Amazon RDS) für PostgreSQL oder eine Amazon Aurora PostgreSQL-kompatible Edition-DB-Instance handeln.

Das Hochladen einer partitionierten Tabelle umfasst die folgenden Schritte:

1. Erstellen Sie eine übergeordnete Tabelle, die der Oracle-Partitionstabelle ähnelt, aber keine Partition enthält.
2. Erstellen Sie untergeordnete Tabellen, die von der übergeordneten Tabelle erben, die Sie in Schritt 1 erstellt haben.
3. Erstellen Sie eine Prozedurfunktion und einen Trigger, um die Einfügungen in der übergeordneten Tabelle zu verarbeiten.

Da der Trigger jedoch bei jeder Einfügung ausgelöst wird, kann das anfängliche Laden mit AWS DMS sehr langsam sein.

Um die anfänglichen Ladevorgänge von Oracle nach PostgreSQL 9.0 zu beschleunigen, erstellt dieses Muster eine separate AWS-DMS-Aufgabe für jede Partition und lädt die entsprechenden untergeordneten Tabellen. Anschließend erstellen Sie während der Umstellung einen Trigger.

PostgreSQL Version 10 unterstützt native Partitionierung. In einigen Fällen können Sie sich jedoch für die Verwendung der vererbten Partitionierung entscheiden. Weitere Informationen finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle-Quelldatenbank mit einer partitionierten Tabelle
- Eine PostgreSQL-Datenbank auf AWS

Produktversionen

- PostgreSQL 9.0

Architektur

Quelltechnologie-Stack

- Eine partitionierte Tabelle in Oracle

Zieltechnologie-Stack

- Eine partitionierte Tabelle in PostgreSQL (auf Amazon EC2, Amazon RDS for PostgreSQL oder Aurora PostgreSQL)

Zielarchitektur

Tools

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS-Cloud oder zwischen Kombinationen von Cloud- und lokalen Setups.

Epen

AWS DMS einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Tabellen in PostgreSQL.	Erstellen Sie die übergeord neten und die entsprechenden untergeordneten Tabellen in PostgreSQL mit den erforderl ichen Prüfbedingungen für Partitionen.	DBA
Erstellen Sie die AWS DMS-Aufgabe für jede Partition.	Nehmen Sie die Filterbed ingung der Partition in die	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	AWS DMS-Aufgabe auf. Ordnen Sie die Partitionen den entsprechenden PostgreSQL-Untertabellen zu.	
Führen Sie die AWS-DMS-Aufgaben mithilfe von Full Load and Change Data Capture (CDC) aus.	Stellen Sie sicher, dass der `StopTaskCachedChanges Applied` Parameter auf eingestellt ist `true` und der `StopTaskCachedChanges NotApplied` Parameter auf eingestellt ist. `false`	DBA

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beenden Sie die Replikationsaufgaben.	Bevor Sie die Aufgaben beenden, stellen Sie sicher, dass Quelle und Ziel synchron sind.	DBA
Erstellen Sie einen Trigger für die übergeordnete Tabelle.	Da die übergeordnete Tabelle alle Befehle zum Einfügen und Aktualisieren empfängt, sollten Sie einen Trigger erstellen , der diese Befehle auf der Grundlage der Partitionierungsbedingung an die jeweiligen untergeordneten Tabellen weiterleitet.	DBA

Zugehörige Ressourcen

- AWS DMS
- Tabellenpartitionierung (PostgreSQL-Dokumentation)

Zusätzliche Informationen

Obwohl PostgreSQL Version 10 die native Partitionierung unterstützt, können Sie sich für die folgenden Anwendungsfälle entscheiden, die vererbte Partitionierung zu verwenden:

- Die Partitionierung erzwingt die Regel, dass alle Partitionen denselben Satz von Spalten wie die übergeordnete Partition haben müssen, aber die Tabellenvererbung unterstützt untergeordnete Partitionen mit zusätzlichen Spalten.
- Die Tabellenvererbung unterstützt mehrere Vererbungen.
- Die deklarative Partitionierung unterstützt nur die Listen- und Bereichspartitionierung. Mit der Tabellenvererbung können Sie die Daten beliebig aufteilen. Wenn der Einschränkungsausschluss Partitionen jedoch nicht effektiv bereinigen kann, wird die Abfrageleistung beeinträchtigt.
- Einige Operationen benötigen eine stärkere Sperre, wenn deklarative Partitionierung verwendet wird als bei Verwendung der Tabellenvererbung. Zum Beispiel erfordert das Hinzufügen oder Entfernen einer Partition zu oder aus einer partitionierten Tabelle eine `ACCESS EXCLUSIVE` Sperre für die übergeordnete Tabelle, wohingegen eine `SHARE UPDATE EXCLUSIVE` Sperre für die reguläre Vererbung ausreicht.

Wenn Sie separate Jobpartitionen verwenden, können Sie Partitionen auch neu laden, falls es Probleme mit der AWS DMS-Validierung gibt. Führen Sie zur besseren Leistungs- und Replikationskontrolle Aufgaben auf separaten Replikationsinstanzen aus.

Migrieren Sie von Amazon RDS for Oracle zu Amazon RDS for MySQL

Erstellt von Jitender Kumar (AWS), Neha Sharma (AWS) und Srini Ramaswamy (AWS)

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer Amazon Relational Database Service (Amazon RDS) für Oracle-DB-Instance zu einer Amazon RDS for MySQL MySQL-DB-Instance auf Amazon Web Services (AWS). Das Muster verwendet den AWS Database Migration Service (AWS DMS) und das AWS Schema Conversion Tool (AWS SCT).

Das Muster bietet bewährte Methoden für den Umgang mit der Migration von gespeicherten Prozeduren. Es behandelt auch Codeänderungen zur Unterstützung der Anwendungsebene.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine Amazon RDS for Oracle Oracle-Quelldatenbank.
- Eine Zieldatenbank von Amazon RDS for MySQL. Quell- und Zieldatenbanken sollten sich in derselben Virtual Private Cloud (VPC) befinden. Wenn Sie mehrere VPCs verwenden oder über die erforderlichen Zugriffsberechtigungen verfügen müssen.
- Sicherheitsgruppen, die Konnektivität zwischen den Quell- und Zieldatenbanken, AWS SCT, dem Anwendungsserver und AWS DMS ermöglichen.
- Ein Benutzerkonto mit den erforderlichen Rechten, um AWS SCT in der Quelldatenbank auszuführen.
- Zusätzliche Protokollierung für die Ausführung von AWS DMS in der Quelldatenbank aktiviert.

Einschränkungen

- Die maximale Größe der Amazon RDS-Quell- und Zieldatenbank beträgt 64 TB. Informationen zur Größe von Amazon RDS finden Sie in der AWS-Dokumentation.
- Oracle unterscheidet bei Datenbankobjekten nicht zwischen Groß- und Kleinschreibung, MySQL jedoch nicht. AWS SCT kann dieses Problem bei der Erstellung eines Objekts lösen. Es ist jedoch ein gewisses Maß an manueller Arbeit erforderlich, um die vollständige Berücksichtigung der Groß- und Kleinschreibung zu gewährleisten.

- Diese Migration verwendet keine MySQL-Erweiterungen, um Oracle-native Funktionen zu aktivieren. AWS SCT übernimmt den größten Teil der Konvertierung, es sind jedoch einige Arbeiten erforderlich, um den Code manuell zu ändern.
- Änderungen des JDBC-Treibers (Java Database Connectivity) sind in der Anwendung erforderlich.

Produktversionen

- Amazon RDS for Oracle 12.2.0.1 und höher. Die derzeit unterstützten Versionen von RDS für Oracle finden Sie in der AWS-Dokumentation.
- Amazon RDS for MySQL 8.0.15 und höher. Die derzeit unterstützten Versionen von RDS für MySQL finden Sie in der AWS-Dokumentation.
- AWS DMS Version 3.3.0 und höher. Weitere Informationen zu den von AWS DMS unterstützten Quell- und Zielendpunkten finden Sie in der AWS-Dokumentation.
- AWS SCT Version 1.0.628 und höher. In der AWS-Dokumentation finden Sie die AWS-SCT-Support-Matrix für Quell- und Zielendpunkte.

Architektur

Quelltechnologie-Stack

- Amazon RDS for Oracle. Weitere Informationen finden Sie unter Verwenden einer Oracle-Datenbank als Quelle für AWS DMS.

Zieltechnologie-Stack

- Amazon RDS for MySQL. Weitere Informationen finden Sie unter Verwenden einer MySQL-kompatiblen Datenbank als Ziel für AWS DMS.

Architektur der Migration

In der folgenden Abbildung kopiert und konvertiert AWS SCT Schemaobjekte aus der Amazon RDS for Oracle Oracle-Quelldatenbank und sendet die Objekte an die Amazon RDS for MySQL MySQL-Zieldatenbank. AWS DMS repliziert Daten aus der Quelldatenbank und sendet sie an die Amazon RDS for MySQL MySQL-Instance.

Tools

- AWS Data Migration Service unterstützt Sie bei der Migration von Datenspeichern in die AWS-Cloud oder zwischen Kombinationen von Cloud- und lokalen Setups.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der AWS-Cloud. Dieses Muster verwendet Amazon RDS for Oracle und Amazon RDS for MySQL.
- Das AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist.

Epen

Bereiten Sie sich auf die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Versionen und Engines der Quell- und Zieldatenbank.		DBA
Identifizieren Sie die Hardwareanforderungen für die Zielserverinstanz.		DBA, SysAdmin
Identifizieren Sie die Speicheranforderungen (Speichertyp und Kapazität).		DBA, SysAdmin
Wählen Sie den richtigen Instanztyp (Kapazität, Speicherfunktionen, Netzwerkfunktionen).		DBA, SysAdmin
Identifizieren Sie die Sicherheitsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie eine Strategie für die Anwendungsmigration.	Überlegen Sie, ob Sie eine vollständige oder eine teilweise Ausfallzeit für Umstellungsaktivitäten wünschen.	DBA, Besitzer der SysAdmin App

Infrastruktur konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC und Subnetze.		SysAdmin
Erstellen Sie Sicherhei tsgruppen und Netzwerkz ugriffskontrolllisten ()ACLs.		SysAdmin
Konfigurieren und starten Sie die Amazon RDS for Oracle Oracle-Instance.		DBA, SysAdmin
Konfigurieren und starten Sie die Amazon RDS for MySQL MySQL-Instance.		DBA, SysAdmin
Bereiten Sie einen Testfall für die Validierung der Codekonve rtierung vor.	Dies hilft beim Testen von Einheiten für den konvertierten Code.	DBA, Entwickler
Konfigurieren Sie die AWS DMS-Instanz.		
Konfigurieren Sie Quell- und Zielendpunkte in AWS DMS.		

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie das Zieldaten bankskript mit AWS SCT.	Überprüfen Sie die Richtigke it des Codes, der von AWS SCT konvertiert wurde. Einige manuelle Arbeiten sind erforderlich.	DBA, Entwickler
Wählen Sie in AWS SCT die Einstellung „Groß- und Kleinschreibung nicht beachten“.	Wählen Sie in AWS SCT Project Settings, Target Case Sensitivity, Case Insensitive aus.	DBA, Entwickler
Entscheiden Sie sich in AWS SCT dafür, die native Oracle-Funktion nicht zu verwenden.	Überprüfen Sie in den Projekteinstellungen die Funktionen TO_ _DATECHAR/ TO_NUMBER/TO.	DBA, Entwickler
Nehmen Sie Änderungen für den Code „sql%notfound“ vor.	Möglicherweise müssen Sie den Code manuell konvertie ren.	
Abfragen von Tabellen und Objekten in gespeicherten Prozeduren (verwenden Sie Abfragen in Kleinbuchstaben).		DBA, Entwickler
Erstellen Sie das primäre Skript, nachdem alle Änderungen vorgenomm en wurden, und stellen Sie dann das primäre Skript in der Zieldatenbank bereit.		DBA, Entwickler
Testen Sie gespeicherte Prozeduren und Anwendung		

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
saufrufen anhand von Beispieldaten auf Unit-Tests.		
Bereinigen Sie Daten, die während des Komponent entests erstellt wurden.		DBA, Entwickler
Löschen Sie Fremdschl üsseleinschränkungen für die Zieldatenbank.	Dieser Schritt ist erforderl ich, um die Anfangsdaten zu laden. Wenn Sie die Fremdschlüsseleinschränkung en nicht aufheben möchten, müssen Sie eine Migration saufgabe für Daten erstellen , die für die Primär- und Sekundärtabellen spezifisch sind.	DBA, Entwickler
Löschen Sie Primärschlüssel und eindeutige Schlüssel in der Zieldatenbank.	Dieser Schritt führt zu einer besseren Leistung beim ersten Laden.	DBA, Entwickler
Aktivieren Sie die zusätzlic he Protokollierung in der Quelldatenbank.		DBA
Erstellen Sie eine Migration saufgabe für das erste Laden in AWS DMS und führen Sie sie dann aus.	Wählen Sie die Option zur Migration vorhandener Daten.	DBA
Fügen Sie die Primärsch lüssel und Fremdschlüssel zur Zieldatenbank hinzu.	Einschränkungen müssen nach dem ersten Laden hinzugefügt werden.	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Migration saufgabe für die laufende Replikation.	Durch die laufende Replikati on wird die Zieldatenbank mit der Quelldatenbank synchroni siert.	DBA

Anwendungen migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ersetzen Sie native Oracle-Fu nktionen durch native MySQL-Funktionen.		Besitzer der App
Stellen Sie sicher, dass in SQL-Abfragen nur Namen in Kleinbuchstaben für Datenbankobjekte verwendet werden.		DBA SysAdmin, App-Besitzer

Wechseln Sie zur Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie den Anwendung sserver herunter.		Besitzer der App
Stellen Sie sicher, dass die Quell- und Zieldatenbanken synchron sind.		DBA, Besitzer der App
Stoppen Sie die Amazon RDS for Oracle DB-Instance.		DBA
Beenden Sie die Migration saufgabe.	Dies wird automatisch beendet, nachdem Sie den	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	vorherigen Schritt abgeschlo ssen haben.	
Ändern Sie die JDBC-Verb indung von Oracle zu MySQL.		Besitzer der App, DBA
Starten Sie die Anwendung.		DBA SysAdmin, App-Besitzer

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen und validieren Sie die Projektdokumente.		DBA, SysAdmin
Erfassen Sie Kennzahlen zur Zeit bis zur Migration, zum Prozentsatz manueller Aufgaben im Vergleich zu Toolaufgaben, zu Kostenein sparungen usw.		DBA, SysAdmin
Stoppen und löschen Sie AWS DMS-Instanzen.		DBA
Entfernen Sie die Quell- und Zielendpunkte.		DBA
Entfernen Sie Migration saufgaben.		DBA
Erstellen Sie einen Snapshot der Amazon RDS for Oracle DB-Instance.		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die Amazon RDS for Oracle DB-Instance.		DBA
Fahren Sie alle anderen temporären AWS-Ressourcen herunter und löschen Sie sie.		DBA, SysAdmin
Schließen Sie das Projekt und geben Sie Feedback.		DBA

Zugehörige Ressourcen

- AWS DMS
- AWS SCT
- Amazon RDS-Preise
- Erste Schritte mit AWS DMS
- Erste Schritte mit Amazon RDS

Migrieren Sie mithilfe von AWS DMS und AWS SCT von IBM Db2 auf Amazon EC2 zu Aurora PostgreSQL-kompatibel

Erstellt von Sirsendu Halder (AWS) und Abhimanyu Chhabra (AWS)

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer IBM Db2-Datenbank auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance zu einer Amazon Aurora PostgreSQL-kompatiblen Edition-DB-Instance. Dieses Muster verwendet AWS Database Migration Service (AWS DMS) und AWS Schema Conversion Tool (AWS SCT) für die Datenmigration und Schemakonvertierung.

Das Muster zielt auf eine Online-Migrationsstrategie mit geringen oder keinen Ausfallzeiten für eine IBM Db2-Datenbank mit mehreren Terabyte und einer hohen Anzahl von Transaktionen ab. Wir empfehlen, die Spalten in Primärschlüsseln (PKs) und Fremdschlüsseln (FKs) mit dem Datentyp `BIGINT` in `INT` oder in PostgreSQL `NUMERIC` zu konvertieren, um die Leistung zu verbessern.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine IBM Db2-Quelldatenbank auf einer Instance EC2

Produktversionen

- DB2/LINUXX8664 Version 11.1.4.4 und höher

Architektur

Quelltechnologie-Stack

- Eine Db2-Datenbank auf einer Instanz EC2

Zieltechnologie-Stack

- Eine Aurora PostgreSQL-kompatible DB-Instance der Version 10.18 oder höher

Architektur der Datenbankmigration

Tools

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenbanken in die AWS-Cloud oder zwischen Kombinationen von Cloud- und lokalen Setups. Die Quelldatenbank bleibt während der Migration voll funktionsfähig, wodurch Ausfallzeiten für Anwendungen, die auf die Datenbank angewiesen sind, minimiert werden. Sie können AWS DMS verwenden, um Ihre Daten zu und von den am häufigsten verwendeten kommerziellen und Open-Source-Datenbanken zu migrieren. AWS DMS unterstützt heterogene Migrationen zwischen verschiedenen Datenbankplattformen wie IBM Db2 zur Aurora PostgreSQL-kompatiblen Version 10.18 oder höher. Einzelheiten finden Sie unter Quellen für die Datenmigration und Ziele für die Datenmigration in der AWS DMS-Dokumentation.
- Das AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil der Datenbankcodeobjekte, einschließlich Ansichten, gespeicherten Prozeduren und Funktionen, automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist. Alle Objekte, die nicht automatisch konvertiert werden, sind deutlich gekennzeichnet, sodass sie manuell konvertiert werden können, um die Migration abzuschließen. AWS SCT kann auch den Quellcode der Anwendung nach eingebetteten SQL-Anweisungen scannen und diese konvertieren.

Epen

Richte die Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Aurora PostgreSQL-kompatible DB-Instance.	Folgen Sie den Anweisungen in der AWS-Dokumentation, um die DB-Instance zu erstellen. Wählen Sie als Motortyp Amazon Aurora. Wählen Sie als Edition die Amazon Aurora PostgreSQL-kompatible Edition. Die Aurora PostgreSQL-kompatible DB-Instance der	Amazon RDS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Version 10.18 oder höher sollte sich in derselben Virtual Private Cloud (VPC) wie die IBM Db2-Quelldatenbank befinden.	

Konvertieren Sie Ihr Datenbankschema

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren und verifizieren Sie AWS SCT.	1. Installieren Sie AWS SCT, indem Sie die Schritte in der AWS SCT-Dokumentation befolgen. 2. Überprüfen Sie die Installation, indem Sie die Verfahren in der AWS SCT-Dokumentation befolgen.	AWS-Administrator, DBA, Migrationsingenieur
Starten Sie AWS SCT und erstellen Sie ein Projekt.	Um das AWS SCT-Tool zu starten und ein neues Projekt zur Ausführung eines Bewertungsberichts zur Datenbankmigration zu erstellen, folgen Sie den Anweisungen in der AWS SCT-Dokumentation.	Migrationsingenieur
Fügen Sie Datenbankserver hinzu und erstellen Sie eine Zuordnungsregel.	1. Fügen Sie Quell- und Zieldatenbankserver hinzu, indem Sie den Anweisungen in der AWS SCT-Dokumentation folgen.	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Erstellen Sie eine Zuordnungsregel, um die Zieldatenbankplattform für Ihre Quelldatenbank zu definieren. Anweisungen finden Sie in der AWS SCT-Dokumentation.	
Erstellen Sie einen Bewertungsbericht zur Datenbankmigration.	Erstellen Sie den Bewertungsbericht zur Datenbankmigration, indem Sie die Schritte in der AWS SCT-Dokumentation befolgen.	Migrationsingenieur
Sehen Sie sich den Bewertungsbericht an.	Verwenden Sie die Registerkarte Zusammenfassung des Bewertungsberichts zur Datenbankmigration, um den Bericht anzuzeigen und die Daten zu analysieren. Anhand dieser Analyse können Sie die Komplexität der Migration ermitteln. Weitere Informationen finden Sie in der AWS SCT-Dokumentation.	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konvertiert das Schema.	Um Ihre Quelldatenbanksche mas zu konvertieren: 1. Wählen Sie in der AWS SCT-Konsole Ansicht und dann Hauptansicht aus. 2. Wählen Sie das Objekt oder den übergeordneten Knoten aus Ihrem Quellsche ma aus, öffnen Sie das Kontextmenü (Rechtskl ick) und wählen Sie dann Schema konvertieren. Weitere Informationen finden Sie in der AWS SCT-Dokum entation.	Ingenieur für Migration
Wenden Sie das konvertie rte Datenbankschema auf die Ziel-DB-Instance an.	1. Wählen Sie das Schema-El ement im rechten Bereich Ihres Projekt aus, der das geplante Schema für Ihre Ziel-DB-Instance anzeigt. 2. Öffnen Sie das Kontextme nü (rechte Maustaste) für das Schema-Element und wählen Sie Apply to database aus. Weitere Informationen finden Sie in der AWS SCT-Dokum entation.	Ingenieur für Migration

Migrieren Sie Ihre Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine VPC und DB-Parametergruppen ein.	Richten Sie eine VPC und DB-Parametergruppen ein und konfigurieren Sie die für die Migration erforderlichen Regeln und Parameter für eingehenden Datenverkehr. Anweisungen finden Sie in der AWS DMS-Dokumentation. Wählen Sie für die VPC-Sicherheitsgruppe sowohl die EC2 Instance für Db2 als auch die Aurora PostgreSQL-kompatible DB-Instance aus. Diese Replikationsinstanz muss sich in derselben VPC wie die Quell- und Ziel-DB-Instances befinden.	Migrationsingenieur
Bereiten Sie Quell- und Ziel-DB-Instances vor.	Bereiten Sie die Quell- und Ziel-DB-Instances für die Migration vor. In einer Produktionsumgebung ist die Quelldatenbank bereits vorhanden. Für die Quelldatenbank muss der Servername das öffentliche Domain Name System (DNS) der EC2 Instanz sein, auf der Db2 läuft. Als Benutzernamen können Sie `db2inst1` gefolgt vom Port	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	verwenden, der für IBM Db2 5000 lautet.	
Erstellen Sie einen EC2 Amazon-Client und Endgeräte.	1. Erstellen Sie einen EC2 Amazon-Client. Sie verwenden diesen Client, um Ihre Quelldatenbank mit zu replizierenden Daten zu füllen. Sie verwenden diesen Client auch, um die Replikation zu überprüfen, indem Sie Abfragen in der Zieldatenbank ausführen. 2. Erstellen Sie Endpunkte für die Quelldatenbank und die Ziel-DB-Instance, die für die nächsten Schritte verwendet werden sollen. Anweisungen finden Sie in der AWS DMS-Dokumentation. Sie müssen separate Endpunkte für die Quell- und Zieldatenbanken erstellen. Für Aurora PostgreSQL-kompatible Version 10.18 oder höher ist der Port 5432, und Sie können den Servernamen vom Endpunkt der DB-Instance abrufen.	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Replikationsinstanz.	Erstellen Sie mithilfe der AWS DMS-Konsole eine Replikationsinstanz und geben Sie die Quell- und Zielendpunkte an. Die Replikationsinstanz führt die Datenmigration zwischen den Endpunkten durch. Weitere Informationen finden Sie in der AWS DMS-Dokumentation.	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS DMS-Aufgabe, um die Daten zu migrieren.	Erstellen Sie eine Aufgabe, um die IBM Db2-Quelltabellen in die PostgreSQL-DB-Ziel instanz zu laden, indem Sie die Schritte in der AWS DMS-Dokumentation befolgen. • Verwenden Sie für Quelle und Ziel die Namen der Quell- und Zielendpunkte. • Der Migrationstyp kann Volllast sein. • Für die Schemaregel können Sie das `inst1` Schema aus der Db2-Daten bank verwenden. • Geben Sie für den Tabellennamen `%` an, dass alle Tabellen migriert werden sollen. Wenn der Ladevorgang abgeschlo ssen ist, werden die Db2-Tabellen des `inst1` Schemas in der Aurora PostgreSQL-kompatiblen Datenbank angezeigt.	Ingenieur für Migration

Zugehörige Ressourcen

Referenzen

- Amazon Aurora Aurora-Dokumentation
- Dokumentation zum PostgreSQL Foreign Data Wrapper (FDW)
- Dokumentation zu PostgreSQL IMPORT FOREIGN SCHEMA

- AWS DMS-Dokumentation
- AWS SCT-Dokumentation

Tutorials und Videos

- Erste Schritte mit AWS DMS (exemplarische Vorgehensweise)
- Einführung in Amazon EC2 — Elastic Cloud Server und Hosting mit AWS (Video)

Migrieren Sie mithilfe von AWS DMS von Oracle 8i oder 9i zu Amazon RDS for PostgreSQL SharePlex

Erstellt von Kumar Babu P G (AWS)

Übersicht

Dieses Muster beschreibt, wie eine lokale Oracle 8i- oder 9i-Datenbank zu Amazon Relational Database Service (Amazon RDS) für PostgreSQL oder Amazon Aurora PostgreSQL migriert wird. AWS Database Migration Service (AWS DMS) unterstützt Oracle 8i oder 9i nicht als Quelle, sodass Quest Daten aus einer lokalen 8i- oder 9i-Datenbank in eine Oracle-Zwischendatenbank (Oracle 10g oder 11g) SharePlex repliziert, die mit AWS DMS kompatibel ist.

Von der Oracle-Zwischeninstanz werden das Schema und die Daten mithilfe des AWS Schema Conversion Tool (AWS SCT) und AWS DMS in die PostgreSQL-Datenbank auf AWS migriert. Diese Methode hilft dabei, ein kontinuierliches Streaming von Daten von der Oracle-Quelldatenbank zur PostgreSQL-DB-Zielinstanz mit minimaler Replikationsverzögerung zu erreichen. In dieser Implementierung ist die Ausfallzeit auf die Zeit begrenzt, die benötigt wird, um alle Fremdschlüssel, Trigger und Sequenzen in der PostgreSQL-Zieldatenbank zu erstellen oder zu validieren.

Die Migration verwendet eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance, auf der Oracle 10g oder 11g installiert ist, um die Änderungen aus der Oracle-Quelldatenbank zu hosten. AWS DMS verwendet diese Oracle-Zwischeninstanz als Quelle, um die Daten an Amazon RDS for PostgreSQL oder Aurora PostgreSQL zu streamen. Die Datenreplikation kann von der lokalen Oracle-Datenbank zur Oracle-Zwischeninstanz angehalten und wieder aufgenommen werden. Es kann auch angehalten und von der Oracle-Zwischeninstanz zur PostgreSQL-Zieldatenbank fortgesetzt werden, sodass Sie die Daten entweder mit der AWS DMS-Datenvalidierung oder einem benutzerdefinierten Datenvalidierungstool validieren können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle 8i- oder 9i-Quelldatenbank in einem lokalen Rechenzentrum
- AWS Direct Connect, konfiguriert zwischen dem lokalen Rechenzentrum und AWS
- Java Database Connectivity (JDBC) -Treiber für AWS SCT-Connectors, die entweder auf einem lokalen Computer oder auf der EC2 Instance installiert sind, auf der AWS SCT installiert ist

- Vertrautheit mit der Verwendung einer Oracle-Datenbank als AWS-DMS-Quelle
- Vertrautheit mit der Verwendung einer PostgreSQL-Datenbank als AWS-DMS-Ziel
- Vertrautheit mit der Quest-Datenreplikation SharePlex

Einschränkungen

- Die maximale Datenbankgröße beträgt 64 TB
- Bei der lokalen Oracle-Datenbank muss es sich um die Enterprise Edition handeln

Produktversionen

- Oracle 8i oder 9i für die Quelldatenbank
- Oracle 10g oder 11g für die Zwischendatenbank
- PostgreSQL 9.6 oder höher

Architektur

Quelltechnologie-Stack

- Oracle 8i- oder 9i-Datenbank
- Suche SharePlex

Zieltechnologie-Stack

- Amazon RDS for PostgreSQL oder Aurora PostgreSQL

Quell- und Zielarchitektur

Tools

- AWS DMS — Mit dem AWS Database Migration Service (AWS DMS) können Sie Datenbanken schnell und sicher migrieren. Die Quelldatenbank bleibt während der Migration voll funktionsfähig,

wodurch Ausfallzeiten für Anwendungen, die auf die Datenbank angewiesen sind, minimiert werden. AWS DMS kann Ihre Daten zu und von den am häufigsten verwendeten kommerziellen und Open-Source-Datenbanken migrieren.

- AWS SCT — Das AWS Schema Conversion Tool (AWS SCT) macht heterogene Datenbankmigrationen vorhersehbar, indem das Quelldatenbankschema und ein Großteil der Datenbankcodeobjekte, einschließlich Ansichten, gespeicherten Prozeduren und Funktionen, automatisch in ein mit der Zieldatenbank kompatibles Format konvertiert werden. Objekte, die nicht automatisch konvertiert werden können, sind deutlich gekennzeichnet, sodass sie manuell konvertiert werden können, um die Migration abzuschließen. AWS SCT kann Ihren Anwendungsquellcode auch nach eingebetteten SQL-Anweisungen scannen und diese im Rahmen eines Datenbankschema-Konvertierungsprojekts konvertieren. Während dieses Prozesses führt AWS SCT eine cloudnative Codeoptimierung durch, indem es ältere Oracle- und SQL Server-Funktionen in ihre AWS-Entsprechungen konvertiert, um Sie bei der Modernisierung Ihrer Anwendungen und der Migration Ihrer Datenbanken zu unterstützen. Wenn die Schemakonvertierung abgeschlossen ist, kann AWS SCT mithilfe integrierter Datenmigrationsagenten bei der Migration von Daten aus einer Reihe von Data Warehouses nach Amazon Redshift helfen.
- Quest SharePlex — Quest SharePlex ist ein Oracle-to-Oracle Datenreplikationstool zum Verschieben von Daten mit minimalen Ausfallzeiten und ohne Datenverlust.

Epen

Erstellen Sie die EC2 Instanz und installieren Sie Oracle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie das Netzwerk für Amazon ein EC2.	Erstellen Sie die Virtual Private Cloud (VPC), die Subnetze, das Internet-Gateway, die Routing-T abellen und die Sicherhei tsgruppen.	AWS SysAdmin
Erstellen Sie die neue EC2 Instanz.	Wählen Sie das Amazon Machine Image (AMI) für die EC2 Instance aus. Wählen Sie die Instanzgröße und konfiguri	AWS SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eren Sie die Instanzdetails: die Anzahl der Instanzen (1), die VPC und das Subnetz aus dem vorherigen Schritt, automatische Zuweisung öffentlicher IP-Adressen und andere Optionen. Fügen Sie Speicher hinzu, konfigurieren Sie Sicherheitsgruppen und starten Sie die Instance. Wenn Sie dazu aufgefordert werden, erstellen und speichern Sie ein key pair für den nächsten Schritt.	
Installieren Sie Oracle auf der EC2 Instanz.	Erwerben Sie die Lizenzen und die erforderlichen Oracle-Binärdateien und installieren Sie Oracle 10g oder 11g auf der Instance. EC2	DBA

SharePlex Auf einer EC2 Instanz einrichten und Datenreplikation konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Einrichten SharePlex.	Erstellen Sie eine EC2 Amazon-Instance und installieren Sie die SharePlex Binärdateien, die mit Oracle 8i oder 9i kompatibel sind.	AWS SysAdmin, DBA
Konfigurieren Sie die Datenreplikation.	Folgen Sie den SharePlex bewährten Methoden, um die Datenreplikation von einer lokalen Oracle 8i/9i-Datenbank	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	auf eine Oracle 10g/11g-I nstanz zu konfigurieren.	

Das Oracle-Datenbankschema nach PostgreSQL konvertieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie AWS SCT ein.	Erstellen Sie einen neuen Bericht und stellen Sie dann eine Verbindung zu Oracle als Quelle und PostgreSQ L als Ziel her. Öffnen Sie in den Projekteinstellungen die Registerkarte SQL Scripting und ändern Sie das Ziel-SQL-Skript in Mehrere Dateien.	DBA
Konvertiert das Oracle-Da tenbankschema.	Wählen Sie auf der Registerk arte Aktion die Optionen Bericht generieren, Schema konvertieren und dann Als SQL speichern aus.	DBA
Ändern Sie die von AWS SCT generierten SQL-Skripts.		DBA

Erstellen und konfigurieren Sie die Amazon RDS-DB-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Amazon RDS-DB-Instance.	Erstellen Sie in der Amazon RDS-Konsole eine neue PostgreSQL-DB-Instance.	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die DB-Instance.	Geben Sie die DB-Engine -Version, die DB-Instance-Klasse, die Multi-AZ-Bereitstellung, den Speichertyp und den zugewiesenen Speicher an. Geben Sie die DB-Instance-ID, einen Master-Benutzernamen und ein Master-Passwort ein.	AWS SysAdmin, DBA
Konfigurieren Sie Netzwerk und Sicherheit.	Geben Sie die VPC, die Subnetzgruppe, den öffentlichen Zugriff, die Availability Zone-Präferenz und die Sicherheitsgruppen an.	AWS SysAdmin, DBA
Datenbankoptionen konfigurieren.	Geben Sie den Datenbanknamen, den Port, die Parametergruppe, die Verschlüsselung und den Hauptschlüssel an.	AWS SysAdmin, DBA
Konfigurieren Sie die Sicherungen.	Geben Sie den Aufbewahrungszeitraum für Backups, das Backup-Fenster, die Startzeit und die Dauer an und ob Tags in Snapshots kopiert werden sollen.	AWS SysAdmin, DBA
Konfigurieren Sie die Überwachungsoptionen.	Aktivieren oder deaktivieren Sie erweiterte Überwachungs- und Leistungseinblicke.	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Wartungsoptionen.	Geben Sie das auto Upgrade der Nebenversion, das Wartungsfenster sowie den Starttag, die Uhrzeit und die Dauer an.	AWS SysAdmin, DBA
Führen Sie die Skripts vor der Migration von AWS SCT aus.	Führen Sie auf der Amazon RDS-Instance die folgenden Skripts aus: create_database.sql, create_sequence.sql, create_table.sql, create_view.sql und create_function.sql.	AWS SysAdmin, DBA

Migrieren Sie Daten mithilfe von AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Replikationsinstanz in AWS DMS.	Füllen Sie die Felder für den Namen, die Instance-Klasse, die VPC (wie für die EC2 Instance), Multi-AZ und den öffentlichen Zugriff aus. Geben Sie im Abschnitt für die erweiterte Konfiguration den zugewiesenen Speicher, die Subnetzgruppe, die Availability Zone, die VPC-Sicherheitsgruppen und den AWS Key Management Service (AWS KMS) -Root-Schlüssel an.	AWS SysAdmin, DBA
Erstellen Sie den Endpunkt der Quelldatenbank.	Geben Sie den Endpunktnamen, den Typ, die Quell-Engine (Oracle), den Servernam	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en (Amazon EC2 Private DNS-Name), den Port, den SSL-Modus, den Benutzern amen, das Passwort, die SID, die VPC (geben Sie die VPC an, die die Replikationsinstanz hat) und die Replikationsinstanz an. Um die Verbindung zu testen, wählen Sie Test ausführen und erstellen Sie dann den Endpunkt. Sie können auch die folgenden erweiterten Einstellungen konfigurieren: maxFileSize und numberDataType Skalieren.	
Erstellen Sie die AWS DMS-Replikationsaufgabe.	Geben Sie den Namen der Aufgabe, die Replikationsinstanz, die Quell- und Zielendpunkte sowie die Replikationsinstanz an. Wählen Sie als Migrationstyp „Bestehende Daten migrieren und laufende Änderungen replizieren“. Deaktivieren Sie das Kontrollkästchen „Aufgabe beim Erstellen starten“.	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Einstellungen für die AWS DMS-Replikationsaufgabe.	Wählen Sie für den Modus zur Vorbereitung der Zieltabelle „Nichts tun“. Beenden Sie die Aufgabe, nachdem der vollständige Ladevorgang abgeschlossen ist, um Primärschlüssel zu erstellen. Geben Sie den eingeschränkten oder vollständigen LOB-Modus an und aktivieren Sie Steuertabellen. Optional können Sie die CommitRate erweiterte Einstellung konfigurieren.	DBA
Konfigurieren Sie die Tabellenzuordnungen.	Erstellen Sie im Abschnitt Tabellenzuordnungen eine Einschlussregel für alle Tabellen in allen Schemas, die in der Migration enthalten sind, und erstellen Sie dann eine Ausschlussregel. Fügen Sie drei Transformationsregeln hinzu, um die Schema-, Tabellen- und Spaltennamen in Kleinbuchstaben umzuwandeln, und fügen Sie alle anderen Regeln hinzu, die für diese spezielle Migration erforderlich sind.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starte die Aufgabe.	Starten Sie die Replikati onsaufgabe. Stellen Sie sicher, dass die Volllast läuft. Führen Sie ALTER SYSTEM SWITCH LOGFILE in der primären Oracle-Datenbank aus, um die Aufgabe zu starten.	DBA
Führen Sie die Skripts während der Migration von AWS SCT aus.	Führen Sie in Amazon RDS for PostgreSQL die folgenden Skripts aus: create_index.sql und create_constraint.sql.	DBA
Starten Sie die Aufgabe neu, um mit der Erfassung von Änderungsdaten (CDC) fortzufahren.	Führen Sie VACUUM in der Amazon RDS for PostgreSQ L PostgreSQL-DB-Instance aus und starten Sie die AWS DMS-Aufgabe neu, um die zwischengespeicherten CDC-Änderungen anzuwenden.	DBA

Wechseln Sie zur PostgreSQL-Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die AWS-DMS-Protokolle und Metadatentabellen.	Überprüfen Sie alle Fehler und korrigieren Sie sie gegebenen falls.	DBA
Stoppen Sie alle Oracle-Ab hängigkeiten.	Fahren Sie die Listener in der Oracle-Datenbank herunter und führen Sie ALTER SYSTEM SWITCH LOGFILE aus. Beenden Sie die AWS	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	DMS-Aufgabe, wenn keine Aktivität angezeigt wird.	
Führen Sie die Skripts nach der Migration von AWS SCT aus.	Führen Sie in Amazon RDS for PostgreSQL die folgenden Skripts aus: create_foreign_key_constraint.sql und create_triggers.sql.	DBA
Führen Sie alle weiteren Schritte von Amazon RDS for PostgreSQL aus.	Inkrementieren Sie die Sequenzen bei Bedarf so, dass sie mit Oracle übereinstimmen, führen Sie VACUUM und ANALYZE aus und erstellen Sie aus Compliance-Gründen einen Snapshot.	DBA
Öffnen Sie die Verbindungen zu Amazon RDS for PostgreSQL.	Entfernen Sie die AWS DMS-Sicherheitsgruppen aus Amazon RDS for PostgreSQL, fügen Sie Produktionssicherheitsgruppen hinzu und verweisen Sie Ihre Anwendungen auf die neue Datenbank.	DBA
Bereinigen Sie die AWS-DMS-Ressourcen.	Entfernen Sie die Endgeräte, Replikationsaufgaben, Replikationsinstanzen und die EC2 Instanz.	SysAdmin, DBA

Zugehörige Ressourcen

- AWS DMS-Dokumentation
- AWS SCT-Dokumentation

- Preise für Amazon RDS for PostgreSQL
- Verwenden einer Oracle-Datenbank als Quelle für AWS DMS
- Verwenden einer PostgreSQL-Datenbank als Ziel für AWS DMS
- SharePlex Quest-Dokumentation

Migrieren Sie mithilfe von Materialized Views und AWS DMS von Oracle 8i oder 9i zu Amazon RDS for PostgreSQL

Erstellt von Kumar Babu P G (AWS) und Pragnesh Patel (AWS)

Übersicht

Dieses Muster beschreibt, wie eine lokale ältere Oracle 8i- oder 9i-Datenbank zu Amazon Relational Database Service (Amazon RDS) for PostgreSQL oder Amazon Aurora PostgreSQL-Compatible Edition migriert wird.

AWS Database Migration Service (AWS DMS) unterstützt Oracle 8i oder 9i nicht als Quelle. Daher verwendet dieses Muster eine zwischengeschaltete Oracle-Datenbankinstanz, die mit AWS DMS kompatibel ist, wie Oracle 10g oder 11g. Es verwendet auch die Funktion Materialized Views, um Daten von der Oracle 8i/9i-Quellinstanz zur Oracle 10g/11g-Zwischeninstanz zu migrieren.

Das AWS Schema Conversion Tool (AWS SCT) konvertiert das Datenbankschema, und AWS DMS migriert die Daten in die PostgreSQL-Zieldatenbank.

Dieses Muster hilft Benutzern, die von älteren Oracle-Datenbanken mit minimaler Datenbankausfallzeit migrieren möchten. In dieser Implementierung wäre die Ausfallzeit auf den Zeitraum begrenzt, der benötigt wird, um alle Fremdschlüssel, Trigger und Sequenzen in der Zieldatenbank zu erstellen oder zu validieren.

Das Muster verwendet Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit einer installierten Oracle 10g/11g-Datenbank, um AWS DMS beim Streamen der Daten zu unterstützen. Sie können die Streaming-Replikation von der lokalen Oracle-Datenbank zur Oracle-Zwischeninstanz vorübergehend unterbrechen, damit AWS DMS die Datenvalidierung catch oder ein anderes Datenvalidierungstool verwenden kann. Die PostgreSQL-DB-Instance und die Oracle-Zwischendatenbank verfügen über dieselben Daten, wenn AWS DMS die Migration der aktuellen Änderungen abgeschlossen hat.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle 8i- oder 9i-Quelldatenbank in einem lokalen Rechenzentrum
- AWS Direct Connect, konfiguriert zwischen dem lokalen Rechenzentrum und AWS

- Java Database Connectivity (JDBC) -Treiber für AWS SCT-Connectors, die entweder auf einem lokalen Computer oder auf der EC2 Instance installiert sind, auf der AWS SCT installiert ist
- Vertrautheit mit der Verwendung einer Oracle-Datenbank als AWS-DMS-Quelle
- Vertrautheit mit der Verwendung einer PostgreSQL-Datenbank als AWS-DMS-Ziel

Einschränkungen

- Die maximale Datenbankgröße beträgt 64 TB

Produktversionen

- Oracle 8i oder 9i für die Quelldatenbank
- Oracle 10g oder 11g für die Zwischendatenbank
- PostgreSQL 10.17 oder höher

Architektur

Quelltechnologie-Stack

- Oracle 8i- oder 9i-Datenbank

Zieltechnologie-Stack

- Amazon RDS for PostgreSQL oder Aurora PostgreSQL-kompatibel

Zielarchitektur

Tools

- AWS DMS hilft bei der schnellen und sicheren Migration von Datenbanken. Die Quelldatenbank bleibt während der Migration voll funktionsfähig, wodurch Ausfallzeiten für Anwendungen, die auf die Datenbank angewiesen sind, minimiert werden. AWS DMS kann Ihre Daten zu und von den am häufigsten verwendeten kommerziellen und Open-Source-Datenbanken migrieren.
- AWS SCT konvertiert automatisch das Quelldatenbankschema und einen Großteil der Datenbankcodeobjekte, einschließlich Ansichten, gespeicherten Prozeduren und Funktionen, in

ein Format, das mit der Zieldatenbank kompatibel ist. Objekte, die nicht automatisch konvertiert werden können, sind deutlich gekennzeichnet, sodass sie manuell konvertiert werden können, um die Migration abzuschließen. AWS SCT kann Ihren Anwendungsquellcode auch nach eingebetteten SQL-Anweisungen scannen und diese im Rahmen eines Datenbankschema-Konvertierungsprojekts konvertieren. Während dieses Prozesses führt AWS SCT eine Cloud-native Code-Optimierung durch, indem es ältere Oracle- und SQL Server-Funktionen in ihre AWS-Entsprechungen konvertiert, um Sie bei der Modernisierung Ihrer Anwendungen und der Migration Ihrer Datenbanken zu unterstützen. Wenn die Schemakonvertierung abgeschlossen ist, kann AWS SCT mithilfe integrierter Datenmigrationsagenten bei der Migration von Daten aus einer Reihe von Data Warehouses nach Amazon Redshift helfen.

Bewährte Methoden

Bewährte Methoden für die Aktualisierung materialisierter Ansichten finden Sie in der folgenden Oracle-Dokumentation:

- Materialisierte Ansichten aktualisieren
- Schnelle Aktualisierung für materialisierte Ansichten

Epen

Installieren Sie Oracle auf einer EC2 Instanz und erstellen Sie materialisierte Ansichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie das Netzwerk für die EC2 Instanz ein.	Erstellen Sie die Virtual Private Cloud (VPC), die Subnetze, das Internet-Gateway, die Routing-T abellen und die Sicherhei tsgruppen.	AWS SysAdmin
Erstellen Sie die EC2 Instanz.	Wählen Sie das Amazon Machine Image (AMI) für die EC2 Instance aus. Wählen Sie die Instanzgröße und konfiguri eren Sie die Instanzdetails:	AWS SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Anzahl der Instanzen (1), die VPC und das Subnetz aus dem vorherigen Schritt, automatische Zuweisung öffentlicher IP-Adressen und andere Optionen. Fügen Sie Speicher hinzu, konfigurieren Sie Sicherheitsgruppen und starten Sie die Instance. Wenn Sie dazu aufgefordert werden, erstellen und speichern Sie ein key pair für den nächsten Schritt.	
Installieren Sie Oracle auf der EC2 Instanz.	Erwerben Sie die Lizenzen und die erforderlichen Oracle-Binärdateien und installieren Sie Oracle 10g oder 11g auf der Instance. EC2	DBA
Konfigurieren Sie das Oracle-Netzwerk.	Ändern oder fügen Sie Einträge hinzu`listener.ora` , um eine Verbindung zur lokalen Oracle 8i/9i-Quelldatenbank herzustellen, und erstellen Sie dann die Datenbank-Links.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie materialisierte Ansichten.	Identifizieren Sie die Datenbankobjekte, die in der Oracle 8i/9i-Quelldatenbank repliziert werden sollen, und erstellen Sie dann mithilfe des Datenbank-Links materiali sierte Ansichten für alle Objekte.	DBA
Stellen Sie Skripts bereit, um materialisierte Ansichten in den erforderlichen Intervallen zu aktualisieren.	Entwickeln und implement ieren Sie Skripts, um materiali sierte Ansichten in den erforderlichen Intervallen auf der Amazon EC2 Oracle 10g/11g-Instance zu aktualisi eren. Verwenden Sie die Option „Inkrementelle Aktualisi erung“, um Materialized Views zu aktualisieren.	DBA

Das Oracle-Datenbankschema nach PostgreSQL konvertieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie AWS SCT ein.	Erstellen Sie einen neuen Bericht und stellen Sie dann eine Verbindung zu Oracle als Quelle und PostgreSQ L als Ziel her. Öffnen Sie in den Projekteinstellungen die Registerkarte SQL Scripting . Ändern Sie das Ziel-SQL-Skript in Mehrere Dateien. (AWS SCT unterstützt keine	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Oracle 8i/9i-Datenbanken, daher müssen Sie den reinen Schema-Dump auf der Oracle 10g/11g-Zwischeninstanz wiederherstellen und ihn als Quelle für AWS SCT verwenden.)	
Konvertiert das Oracle-Datenbankschema.	Wählen Sie auf der Registerkarte Aktion die Optionen Bericht generieren, Schema konvertieren und dann Als SQL speichern aus.	DBA
Ändern Sie die SQL-Skripten.	Nehmen Sie Änderungen auf der Grundlage bewährter Methoden vor. Wechseln Sie beispielsweise zu geeignete n Datentypen und entwickeln Sie PostgreSQL-Äquivalente für Oracle-spezifische Funktionen.	DBA, DevDBA

Erstellen und konfigurieren Sie die Amazon RDS-DB-Instance zum Hosten der konvertierten Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Amazon RDS-DB-Instance.	Erstellen Sie in der Amazon RDS-Konsole eine neue PostgreSQL-DB-Instance.	AWS SysAdmin, DBA
Konfigurieren Sie die DB-Instance.	Geben Sie die DB-Engine -Version, die DB-Instance-Klasse, die Multi-AZ-Bereitste	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	llung, den Speichertyp und den zugewiesenen Speicher an. Geben Sie die DB-Instan ce-ID, einen Master-Be nutzernamen und ein Master-Passwort ein.	
Konfigurieren Sie Netzwerk und Sicherheit.	Geben Sie die VPC, die Subnetzgruppe, den öffentlic hen Zugriff, die Availabil ity Zone-Präferenz und die Sicherheitsgruppen an.	DBA, SysAdmin
Datenbankoptionen konfiguri eren.	Geben Sie den Datenbank namen, den Port, die Parametergruppe, die Verschlüsselung und den Hauptschlüssel an.	DBA, AWS SysAdmin
Konfigurieren Sie die Sicherungen.	Geben Sie den Aufbewahr ungszeitraum für Backups, das Backup-Fenster, die Startzeit und die Dauer an und ob Tags in Snapshots kopiert werden sollen.	AWS SysAdmin, DBA
Konfigurieren Sie die Überwachungsoptionen.	Aktivieren oder deaktivieren Sie erweiterte Überwachungs- und Leistungseinblicke.	AWS SysAdmin, DBA
Konfigurieren Sie die Wartungsoptionen.	Geben Sie das auto Upgrade der Nebenversion, das Wartungsfenster sowie den Starttag, die Uhrzeit und die Dauer an.	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Skripts vor der Migration von AWS SCT aus.	Erstellen Sie auf der Amazon RDS for PostgreSQL PostgreSQL-Zielinstanz das Datenbankschema mithilfe der SQL-Skripts von AWS SCT mit anderen Änderungen. Dazu können die Ausführung mehrerer Skripts gehören, einschlie ßlich Benutzererstellung , Datenbankerstellung, Schemaerstellung, Tabellen, Ansichten, Funktionen und anderer Codeobjekte.	AWS SysAdmin, DBA

Migrieren Sie Daten mithilfe von AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Replikati onsinstanz in AWS DMS.	Füllen Sie die Felder für den Namen, die Instance-Klasse, die VPC (wie für die EC2 Instance), Multi-AZ und den öffentlichen Zugriff aus. Geben Sie im Abschnitt für die erweiterte Konfiguration den zugewiesenen Speicher, die Subnetzgruppe, die Availability Zone, die VPC-Sicherheitsgru ppen und den AWS Key Management Service (AWS KMS) -Schlüssel an.	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Endpunkt der Quelldatenbank.	Geben Sie den Endpunktn amen, den Typ, die Quell-Eng ine (Oracle), den Servernam en (den privaten DNS-Namen der EC2 Instanz), den Port, den SSL-Modus , den Benutzernamen, das Passwort, die SID, die VPC (geben Sie die VPC an, die die Replikationsinstanz hat) und die Replikationsinstanz an. Um die Verbindung zu testen, wählen Sie Test ausführen und erstellen Sie dann den Endpunkt. Sie können auch die folgenden erweiterten Einstellungen konfigurieren: maxFileSizeund numberDat aTypeSkalieren.	AWS SysAdmin, DBA
Connect AWS DMS mit Amazon RDS for PostgreSQL.	Erstellen Sie eine Migration ssicherheitsgruppe für Verbindungen zwischen VPCs, falls sich Ihre PostgreSQL-Datenbank in einer anderen VPC befindet.	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Zieldaten bank-Endpunkt.	Geben Sie den Endpunktn amen, den Typ, die Quell-Engine (PostgreSQL), den Servernamen (Amazon RDS-Endpunkt), den Port, den SSL-Modus, den Benutzern amen, das Passwort, den Datenbanknamen, die VPC (geben Sie die VPC an, die die Replikationsinstanz hat) und die Replikationsinstanz an. Um die Verbindung zu testen, wählen Sie Test ausführen und erstellen Sie dann den Endpunkt. Sie können auch die folgenden erweiterten Einstellungen konfigurieren: maxFileSizeund numberDat aTypeSkalieren.	AWS SysAdmin, DBA
Erstellen Sie die AWS DMS-Replikationsaufgabe.	Geben Sie den Namen der Aufgabe, die Replikati onsinstanz, die Quell- und Zielendpunkte sowie die Replikationsinstanz an. Wählen Sie als Migration styp die Option Bestehende Daten migrieren und laufende Änderungen replizieren aus. Deaktivieren Sie das Kontrollk ästchen Aufgabe bei Erstellun g starten.	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Einstellungen für die AWS DMS-Replikationsaufgabe.	Wählen Sie für den Modus zur Vorbereitung der Zieltabelle die Option Nichts tun. Beenden Sie die Aufgabe, nachdem der vollständige Ladevorgang abgeschlossen ist (um Primärschlüssel zu erstellen). Geben Sie den eingeschränkten oder vollständigen LOB-Modus an und aktivieren Sie Steuertabellen. Optional können Sie die CommitRateerweiterte Einstellung konfigurieren.	DBA
Konfigurieren Sie die Tabellenzuordnungen.	Erstellen Sie im Abschnitt Tabellenzuordnungen eine Einschlussregel für alle Tabellen in allen Schemas, die in der Migration enthalten sind, und erstellen Sie dann eine Ausschlussregel. Fügen Sie drei Transformationsregeln hinzu, um die Schema-, Tabellen- und Spaltennamen in Kleinbuchstaben umzuwandeln, und fügen Sie alle anderen Regeln hinzu, die Sie für diese spezielle Migration benötigen.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starte die Aufgabe.	Starten Sie die Replikationsaufgabe. Stellen Sie sicher, dass die Volllast läuft. Führen Sie es `ALTER SYSTEM SWITCH LOGFILE` in der primären Oracle-Datenbank aus, um die Aufgabe zu starten.	DBA
Führen Sie die Skripts während der Migration von AWS SCT aus.	Führen Sie in Amazon RDS for PostgreSQL die folgenden Skripts aus: `create_index.sql` und `create_constraint.sql` (falls das vollständige Schema nicht ursprünglich erstellt wurde).	DBA
Setzen Sie die Aufgabe fort, um mit der Erfassung von Änderungsdaten (CDC) fortzufahren.	Führen Sie die Ausführung `VACUUM` auf der Amazon RDS for PostgreSQL PostgreSQL-DB-Instance aus und starten Sie die AWS DMS-Aufgabe neu, um zwischengespeicherte CDC-Änderungen anzuwenden.	DBA

Wechseln Sie zur PostgreSQL-Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die AWS DMS-Protokolle und Validierungstabellen.	Überprüfen und beheben Sie alle Replikations- oder Validierungsfehler.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beenden Sie die Verwendung der lokalen Oracle-Datenbank und ihrer Abhängigkeiten.	Beenden Sie alle Oracle-Abhängigkeiten, fahren Sie die Listener in der Oracle-Datenbank herunter und führen Sie den Vorgang aus. `ALTER SYSTEM SWITCH LOGFILE` Beenden Sie die AWS DMS-Aufgabe, wenn keine Aktivität angezeigt wird.	DBA
Führen Sie die Skripts nach der Migration von AWS SCT aus.	Führen Sie in Amazon RDS for PostgreSQL die folgenden Skripts aus:. `create_foreign_key_constraint.sql and create_triggers.sql` Stellen Sie sicher, dass die Sequenzen auf dem neuesten Stand sind.	DBA
Führen Sie zusätzliche Schritte von Amazon RDS for PostgreSQL aus.	Erhöhen Sie die Sequenzen bei Bedarf, sodass sie mit Oracle übereinstimmen, führen Sie den Vorgang aus `VACUUM` und `ANALYZE` erstellen Sie aus Compliance-Gründen einen Snapshot.	DBA
Öffnen Sie die Verbindungen zu Amazon RDS for PostgreSQL.	Entfernen Sie die AWS DMS-Sicherheitsgruppen aus Amazon RDS for PostgreSQL, fügen Sie Produktionssicherheitsgruppen hinzu und verweisen Sie Ihre Anwendungen auf die neue Datenbank.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen Sie die AWS DMS-Objekte.	Entfernen Sie die Endgeräte , Replikationsaufgaben, Replikationsinstanzen und die EC2 Instanz.	SysAdmin, DBA

Zugehörige Ressourcen

- AWS DMS-Dokumentation
- AWS SCT-Dokumentation
- Preise für Amazon RDS for PostgreSQL
- Verwenden einer Oracle-Datenbank als Quelle für AWS DMS
- Verwenden einer PostgreSQL-Datenbank als Ziel für AWS DMS

Migrieren Sie mithilfe von AWS DMS und AWS SCT von Oracle auf Amazon EC2 zu Amazon RDS for MySQL

Erstellt von Anil Kunapareddy (AWS) und Harshad Gohil

Übersicht

Die Verwaltung von Oracle-Datenbanken auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances erfordert Ressourcen und kann kostspielig sein. Das Verschieben dieser Datenbanken in eine Amazon Relational Database Service (Amazon RDS) für MySQL-DB-Instance erleichtert Ihnen die Arbeit, da das gesamte IT-Budget optimiert wird. Amazon RDS for MySQL bietet auch Funktionen wie Multi-AZ, Skalierbarkeit und automatische Backups.

Dieses Muster führt Sie durch die Migration einer Oracle-Quelldatenbank auf Amazon EC2 zu einer Amazon RDS for MySQL MySQL-DB-Zielinstanz. Es verwendet AWS Database Migration Service (AWS DMS), um die Daten zu migrieren, und das AWS Schema Conversion Tool (AWS SCT), um das Quelldatenbankschema und die Objekte in ein Format zu konvertieren, das mit Amazon RDS for MySQL kompatibel ist.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Quelldatenbank mit laufenden Instance- und Listener-Services im ARCHIVELOG-Modus
- Eine Amazon RDS for MySQL MySQL-Zieldatenbank mit ausreichend Speicherplatz für die Datenmigration

Einschränkungen

- AWS DMS erstellt kein Schema in der Zieldatenbank; das müssen Sie tun. Der Schemaname muss für das Ziel bereits vorhanden sein. Tabellen aus dem Quellschema werden in den Benutzer/das Schema importiert, das AWS DMS verwendet, um eine Verbindung mit der Zielinstanz herzustellen. Zum Migrieren von mehreren Schemata müssen Sie mehrere Replikationsaufgaben erstellen.

Produktversionen

- Alle Oracle-Datenbankeditionen für die Versionen 10.2 und höher, 11g und bis zu 12.2 und 18c. Die aktuelle Liste der unterstützten Versionen finden Sie unter Verwenden einer Oracle-Datenbank als Quelle für AWS DMS und Verwenden einer MySQL-kompatiblen Datenbank als Ziel für AWS DMS. Wir empfehlen Ihnen, die neueste Version von AWS DMS zu verwenden, um die umfassendste Version von Versionen und Funktionen zu erhalten. Informationen zu den von AWS SCT unterstützten Oracle-Datenbankversionen finden Sie in der AWS SCT-Dokumentation.
- AWS DMS unterstützt die Versionen 5.5, 5.6 und 5.7 von MySQL.

Architektur

Quelltechnologie-Stack

- Eine Oracle-Datenbank auf einer EC2 Instanz

Zieltechnologie-Stack

- Amazon RDS for MySQL MySQL-DB-Instance

Architektur der Datenmigration

Quell- und Zielarchitektur

Tools

- AWS DMS — AWS Database Migration Service (AWS DMS) ist ein Webservice, mit dem Sie Daten aus Ihrer lokalen Datenbank, auf einer Amazon RDS-DB-Instance oder in einer Datenbank auf einer Instance in eine Datenbank in einem AWS-Service wie Amazon RDS for MySQL oder einer EC2 Instance migrieren können. EC2 Sie können eine Datenbank auch von einem AWS-Service zu einer lokalen Datenbank migrieren. Sie können Daten zwischen heterogenen oder homogenen Datenbank-Engines migrieren.
- AWS SCT — Das AWS Schema Conversion Tool (AWS SCT) macht heterogene Datenbankmigrationen vorhersehbar, indem das Quelldatenbankschema und ein Großteil der Datenbankcode-Objekte, einschließlich Ansichten, gespeicherten Prozeduren und Funktionen, automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist. Nachdem Sie Ihr Datenbankschema und Ihre Codeobjekte mit AWS SCT konvertiert haben, können Sie AWS

DMS verwenden, um Daten von der Quelldatenbank in die Zieldatenbank zu migrieren, um Ihre Migrationsprojekte abzuschließen.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Versionen und Engines der Quell- und Zieldatenbank.		DBA/Entwickler
Identifizieren Sie die DMS-Replikationsinstanz.		DBA/Entwickler
Identifizieren Sie Speicheranforderungen wie Speichertyp und Kapazität.		DBA/Entwickler
Identifizieren Sie Netzwerkanforderungen wie Latenz und Bandbreite.		DBA/Entwickler
Identifizieren Sie die Hardwareanforderungen für die Quell- und Zielserverinstanzen (basierend auf der Oracle-Kompatibilitätsliste und den Kapazitätsanforderungen).		DBA/Entwickler
Identifizieren Sie die Sicherheitsanforderungen für den Netzwerkzugriff für Quell- und Zieldatenbanken.		DBA/Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die AWS SCT- und Oracle-Treiber.		DBA/Entwickler
Legen Sie eine Backup-St rategie fest.		DBA/Entwickler
Ermitteln Sie die Verfügbar keitsanforderungen.		DBA/Entwickler
Identifizieren Sie die Strategie für Anwendungsmigration und Umstellung.		DBA/Entwickler
Wählen Sie den richtigen DB-Instance-Typ auf der Grundlage von Kapazität , Speicher und Netzwerkf unktionen aus.		DBA/Entwickler

Konfigurieren Sie die Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC). Die Quell-, Ziel- und Replikationsinstan z sollten sich in derselben VPC befinden. Es ist auch gut, diese in derselben Availability Zone zu haben.		Developer
Erstellen Sie die erforderlichen Sicherheitsgruppen für den Datenbankzugriff.		Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren und konfigurieren Sie ein key pair.		Developer
Konfigurieren Sie Subnetze, Availability Zones und CIDR-Blöcke.		Developer

Konfigurieren Sie die Quelle: Oracle-Datenbank auf Instanz EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Oracle Database auf Amazon EC2 mit den erforderlichen Benutzern und Rollen.		DBA
Führen Sie die drei Schritte in der nächsten Spalte aus, um von außerhalb der EC2 Instanz auf Oracle zuzugreif en.	1. Ändern Sie den lokalen Host `tnsnames` in Amazon EC2 Public DNS. 2. Ändern Sie den lokalen Host `listener` in Amazon EC2 Public DNS. 3. Stoppen Sie den Listener und starten Sie ihn neu.	DBA
Wenn Amazon neu gestartet EC2 wird, ändert sich das öffentliche DNS. Stellen Sie sicher, dass Sie Amazon EC2 Public DNS in „tnsnames“ und „listener“ aktualisieren oder eine Elastic IP-Adresse verwenden.		DBA/Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die EC2 Instanz-Sicherheitsgruppe so, dass die Replikationsinstanz und die erforderlichen Clients auf die Quelldatenbank zugreifen können.		DBA/Entwickler

Konfigurieren Sie das Ziel: Amazon RDS for MySQL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren und starten Sie die Amazon RDS for MySQL MySQL-DB-Instance.		Developer
Erstellen Sie den erforderlichen Tablespace in der Amazon RDS for MySQL MySQL-DB-Instance.		DBA
Konfigurieren Sie die Sicherheitsgruppe so, dass die Replikationsinstanz und die erforderlichen Clients auf die Zieldatenbank zugreifen können.		Developer

AWS SCT konfigurieren und ein Schema in der Zieldatenbank erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die AWS SCT- und Oracle-Treiber.		Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie die entsprech enden Parameter ein und stellen Sie eine Verbindung zur Quelle und zum Ziel her.		Developer
Generieren Sie einen Bericht zur Schemakonvertierung.		Developer
Korrigieren Sie den Code und das Schema nach Bedarf, insbesondere Tablespaces und Anführungszeichen, und führen Sie die Ausführung in der Zieldatenbank aus.		Developer
Überprüfen Sie das Schema auf Quelle und Ziel, bevor Sie Daten migrieren.		Developer

Migrieren Sie Daten mit AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Für Full-Load and Change Data Capture (CDC) oder nur CDC müssen Sie ein zusätzlic hes Verbindungsattribut festlegen.		Developer
Dem in den Definitionen der AWS-DMS-Oracle-Que lldatenbank angegebenen Benutzer müssen alle erforderl ichen Rechte gewährt werden. Eine vollständige Liste finden		DBA/Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sie unter https://docs.aws.amazon.com/dms/ latest/userguide/CHAP _source.oracle.html #CHAP_Source .Oracle.Self-Managed.		
Aktivieren Sie die zusätzliche Protokollierung in der Quelldatenbank.		DBA/Entwickler
Für Full-Load and Change Data Capture (CDC) oder nur CDC aktivieren Sie den ARCHIVELOG-Modus in der Quelldatenbank.		DBA
Erstellen Sie Quell- und Zielendpunkte und testen Sie die Verbindungen.		Developer
Wenn die Endpunkte erfolgreich verbunden wurden, erstellen Sie eine Replizierungsaufgabe.		Developer
Wählen Sie in der Aufgabe nur CDC (oder) Volllast plus CDC aus, um Änderungen nur für die kontinuierliche Replikation zu erfassen (oder) Volllast plus laufende Änderungen.		Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Replikati onsaufgabe aus und überwachen Sie die CloudWatch Amazon-Pr otokolle.		Developer
Validieren Sie die Daten in den Quell- und Zieldaten banken.		Developer

Migrieren Sie Ihre Anwendung und wechseln Sie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie den Schritten für Ihre Strategie zur Anwendung smigration.		DBA, Entwickler, App-Besitzer
Folgen Sie den Schritten für Ihre Strategie zur Umstellun g und Umstellung von Anwendungen.		DBA, Entwickler, App-Besitzer

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie das Schema und die Daten in Quell- und Zieldatenbanken.		DBA/Entwickler
Erfassen Sie Kennzahlen zum Zeitpunkt der Migration, zum prozentualen Anteil manueller		DBA/Developer/AppOwner

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Änderungen im Vergleich zu Tools, zu Kosteneinsparungen usw.		
Überprüfen Sie die Projektdokumente und Artefakte.		DBA/Developer/AppOwner
Fahren Sie temporäre AWS-Ressourcen herunter.		DBA/Entwickler
Schließen Sie das Projekt ab und geben Sie Feedback.		DBA/Developer/AppOwner

Zugehörige Ressourcen

- AWS DMS-Dokumentation
- AWS DMS-Webseite
- AWS DMS-Blogbeiträge
- Strategien für die Migration von Oracle Database in AWS
- Amazon RDS für Oracle FAQs
- Häufig gestellte Fragen zu Oracle
- Amazon EC2
- Amazon EC2 FAQs
- Lizenzierung von Oracle-Software in der Cloud-Computing-Umgebung

Migrieren Sie mit AWS DMS von Oracle zu Amazon DocumentDB

Erstellt von Sashikanta Pattanayak (AWS) und Munesh Siddappa (AWS)

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer Oracle-Datenbank zu einer Amazon DocumentDB DocumentDB-Datenbank (mit MongoDB-Kompatibilität) mithilfe von AWS Database Migration Service (AWS DMS). Dieser Ansatz kann sowohl auf eine lokale Oracle-Quelldatenbank als auch auf eine Amazon Relational Database Service (Amazon RDS) für Oracle-DB-Instance angewendet werden. Dieses Muster verwendet eine Amazon RDS Oracle DB-Quell-Instance als Beispiel.

Amazon DocumentDB (mit MongoDB-Kompatibilität) ist ein vollständig verwalteter, MongoDB-kompatibler Dokumentendatenbankservice, der das Speichern, Abfragen und Indizieren von JSON-Daten vereinfacht.

Der Anwendungsfall für dieses Muster ist die one-to-one Replikation einer Oracle-Datenbanktabelle in eine Amazon DocumentDB-Sammlung. Das Muster verwendet AWS DMS-Replikationsaufgaben, um die Tabellenstruktur der Oracle-Datenbank zu lesen, die entsprechende Sammlung in Amazon DocumentDB zu erstellen und eine Volllastmigration durchzuführen. Sie können Ihre Daten in Amazon DocumentDB genau wie in MongoDB anzeigen und abfragen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Vertrautheit mit der Verwendung von Oracle-Datenbanken
- Vertrautheit mit der Verwendung von Amazon DocumentDB
- Für den Oracle-Benutzer: Privileg `SELECT ANY TABLE`
- Für die Verwendung von Amazon DocumentDB ist das Recht erforderlich, Daten zu speichern

Einschränkungen

Bei der Verwendung von Amazon DocumentDB als Ziel für AWS DMS gelten die folgenden Einschränkungen:

- In Amazon DocumentDB dürfen Namen für Sammlungen nicht das Dollarzeichen ($) enthalten. Darüber hinaus dürfen Datenbanknamen keine Unicode-Zeichen enthalten.
- AWS DMS unterstützt nicht die Zusammenführung mehrerer Quelltabellen zu einer einzigen Amazon DocumentDB-Sammlung.
- Wenn AWS DMS Änderungen aus einer Quelltabelle verarbeitet, die keinen Primärschlüssel hat, werden alle LOB-Spalten (Large Binary Object) in dieser Tabelle ignoriert.
- Wenn die Option Tabelle ändern aktiviert ist und AWS DMS auf eine Quellspalte mit dem Namen „_id“ stößt, wird diese Spalte in der Änderungstabelle als „__id“ (zwei Unterstriche) angezeigt.
- Wenn Sie Oracle als Quellendpunkt wählen, muss für die Oracle-Quelle die vollständige zusätzliche Protokollierung aktiviert sein. Andernfalls, wenn die Quelle Spalten enthält, die nicht geändert wurden, werden die Daten als Nullwerte in Amazon DocumentDB geladen.

Produktversionen

- Amazon RDS for Oracle Version 11.2.0.3 oder höher
- AWS DMS Version 3.1.3 oder höher (die neuesten Versionsinformationen finden Sie unter Verwenden von Amazon DocumentDB als Ziel für AWS DMS in der AWS DMS-Dokumentation)

Architektur

Quelltechnologie-Stack

- Amazon RDS for Oracle Oracle-DB-Instance

Zieltechnologie-Stack

- Amazon DocumentDB

Quell- und Zielarchitektur

Tools

- AWS DMS — AWS Database Migration Service (AWS DMS) ist ein Webservice, mit dem Sie Daten von einem Quelldatenspeicher zu einem Zieldatenspeicher migrieren können. Das AWS DMS-Benutzerhandbuch spezifiziert die Versionen und Editionen der Oracle-Quelldatenbank, die

für die Verwendung mit AWS DMS unterstützt werden. Weitere Informationen zu diesem Muster finden Sie unter Amazon DocumentDB als Ziel für AWS DMS verwenden.

- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Ihr Amazon DocumentDB-Cluster sollte in Ihrer standardmäßigen Virtual Private Cloud (VPC) laufen. Um mit Ihrem Amazon DocumentDB-Cluster zu interagieren, müssen Sie eine EC2 Instance in Ihrer Standard-VPC in derselben AWS-Region starten, in der Sie Ihren Amazon DocumentDB-Cluster erstellt haben. Einzelheiten finden Sie unter Starten einer EC2 Amazon-Instance in der Amazon DocumentDB-Dokumentation.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Versionen und Engines der Quell- und Zieldatenbank.		AWS-Administrator
Wählen Sie den richtigen Instance-Typ (Kapazität, Speicherfunktionen, Netzwerkfunktionen).		AWS-Administrator
Identifizieren Sie die Sicherheitsanforderungen für den Netzwerk-/Hostzugriff für die Quell- und Zieldatenbanken.		AWS-Administrator
Erstellen Sie eine Sicherheitsgruppe für ausgehenden Datenverkehr zu den Quell- und Zieldatenbanken.		AWS-Administrator
Erstellen und konfigurieren Sie eine EC2 Instanz für Amazon DocumentDB.		AWS-Administrator

Infrastruktur konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC und Subnetze.		AWS-Administrator
Erstellen Sie Sicherhei tsgruppen und Listen zur Netzwerkzugriffskontrolle (ACLs).		AWS-Administrator
Konfigurieren und starten Sie die Amazon RDS for Oracle Oracle-Quell-Instance.		AWS-Administrator
Konfigurieren und starten Sie die Amazon DocumentDB DocumentDB-Instance.		AWS-Administrator

Bereiten Sie die Quelldatenbank vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie anhand der Verbindungsdetails sicher, dass die Oracle-Datenbank verbunden werden kann.		AWS-Administrator
Stellen Sie sicher, dass der Oracle-Benutzer über das SELECT ANY TABLE-Privileg verfügt.		AWS-Administrator

Bereiten Sie die Zieldatenbank vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Amazon DocumentDB-Cluster, indem Sie die richtige Instance-Klasse und Anzahl der Instances auswählen.		AWS-Administrator

Amazon konfigurieren EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die EC2 Instanz.	Um mit Ihrem Amazon DocumentDB-Cluster zu interagieren, müssen Sie eine EC2 Instance in Ihrer Standard-VPC in derselben AWS-Region starten, in der Sie Ihren Amazon DocumentDB-Cluster erstellt haben. Konfigurieren Sie die AWS-Region VPCs, Availability Zones und Subnetze für die EC2 Instance.	AWS-Administrator
Konfigurieren Sie das key pair.	Mit einem öffentlichen/privaten key pair können Sie nach dem Start eine sichere Verbindung zur EC2 Instance herstellen.	AWS-Administrator
Legen Sie die CIDR-Bereiche für den Bastion-Host fest (optional).	Legen Sie den CIDR-IP-Bereich fest, der für den externen Secure Shell (SSH)	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	-Zugriff auf die Bastion-Host-Instanzen zulässig ist.	

Daten migrieren — Volllast

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS DMS-Replikations-Instance.		AWS-Administrator
Erstellen Sie Quell- und Zielendpunkte.		AWS-Administrator
Erstellen Sie AWS DMS-Replikationsaufgaben für eine Volllast.		AWS-Administrator

Testen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie über die EC2 Instance Connect zum Amazon DocumentDB-Cluster her.		AWS-Administrator
Stellen Sie mithilfe der Mongo-Shell eine Connect zum Cluster her.	Anweisungen finden Sie unter den Amazon DocumentD B DocumentDB-Links im Abschnitt Referenzen und Hilfe.	AWS-Administrator
Überprüfen Sie die Ergebnisse der Migration.		AWS-Administrator

Zugehörige Ressourcen

- So funktioniert AWS DMS
- Migration zu Amazon DocumentDB
- Amazon DocumentDB als Ziel für AWS DMS verwenden
- Überblick über Amazon DocumentDB
- Greifen Sie mit der Mongo-Shell auf Ihren Amazon DocumentDB-Cluster zu und verwenden Sie ihn
- Migrieren Sie mithilfe der Offline-Methode von MongoDB zu Amazon DocumentDB (Blogbeitrag)
- So verwenden Sie Amazon DocumentDB (mit MongoDB-Kompatibilität), um skalierbare Anwendungen zu erstellen und zu verwalten (Blogbeitrag)

Migrieren Sie mithilfe von AWS DMS und AWS SCT eine Oracle-Datenbank von Amazon EC2 zu Amazon RDS for MariaDB

Erstellt von Veeranjaneyulu Grandhi (AWS) und Vinod Kumar (AWS)

Übersicht

Dieses Muster führt Sie durch die Schritte zur Migration einer Oracle-Datenbank auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance zu einer Amazon Relational Database Service (Amazon RDS) für MariaDB-DB-Instance. Das Muster verwendet AWS Data Migration Service (AWS DMS) für die Datenmigration und das AWS Schema Conversion Tool (AWS SCT) für die Schemakonvertierung.

Die Verwaltung von Oracle-Datenbanken auf EC2 Instances erfordert mehr Ressourcen und ist kostspieliger als die Verwendung einer Datenbank auf Amazon RDS. Amazon RDS macht es einfach, eine relationale Datenbank in der Cloud einzurichten, zu betreiben und zu skalieren. Amazon RDS bietet kosteneffiziente und anpassbare Kapazität und automatisiert gleichzeitig zeitaufwändige Verwaltungsaufgaben wie Hardwarebereitstellung, Datenbankeinrichtung, Patching und Backups.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine Oracle-Quelldatenbank mit laufenden Instance- und Listener-Services. Diese Datenbank sollte sich im ARCHIVELOG-Modus befinden.
- Vertrautheit mit der Verwendung einer Oracle-Datenbank als Quelle für AWS DMS.
- Vertrautheit mit der Verwendung von Oracle als Quelle für AWS SCT.

Einschränkungen

- Größenbeschränkung der Datenbank: 64 TB

Produktversionen

- Alle Oracle-Datenbankeditionen für die Versionen 10.2 und höher, 11g und bis zu 12.2 und 18c. Die aktuelle Liste der unterstützten Versionen finden Sie unter Using an Oracle Database as a Source for AWS DMS und in der AWS SCT-Versionstabelle in der AWS-Dokumentation.

- Amazon RDS unterstützt die MariaDB Server Community Server-Versionen 10.3, 10.4, 10.5 und 10.6. Die aktuelle Liste der unterstützten Versionen finden Sie in der Amazon RDS-Dokumentation.

Architektur

Quelltechnologie-Stack

- Eine Oracle-Datenbank auf einer EC2 Instanz

Zieltechnologie-Stack

- Amazon RDS für MariaDB

Architektur der Datenmigration

Zielarchitektur

Tools

- Das AWS Schema Conversion Tool (AWS SCT) macht heterogene Datenbankmigrationen vorhersehbar, indem das Quelldatenbankschema und ein Großteil der Datenbankcodeobjekte — einschließlich Ansichten, gespeicherten Prozeduren und Funktionen — automatisch in ein mit der Zieldatenbank kompatibles Format konvertiert werden. Nachdem Sie Ihr Datenbankschema und Ihre Codeobjekte mit AWS SCT konvertiert haben, können Sie AWS DMS verwenden, um Daten von der Quelldatenbank in die Zieldatenbank zu migrieren, um Ihre Migrationsprojekte abzuschließen. Weitere Informationen finden Sie unter Verwenden von Oracle als Quelle für AWS SCT in der AWS SCT-Dokumentation.
- Mit dem AWS Database Migration Service (AWS DMS) können Sie Datenbanken schnell und sicher zu AWS migrieren. Die Quelldatenbank bleibt während der Migration voll funktionsfähig, wodurch die Ausfallzeiten von Anwendungen, die auf die Datenbank angewiesen sind, minimiert werden. AWS DMS kann Ihre Daten zu und von den am häufigsten verwendeten kommerziellen und Open-Source-Datenbanken migrieren. AWS DMS unterstützt homogene Migrationen wie Oracle zu Oracle sowie heterogene Migrationen zwischen verschiedenen Datenbankplattformen wie Oracle oder Microsoft SQL Server zu Amazon Aurora. Weitere Informationen zur Migration von Oracle-Datenbanken finden Sie unter Verwenden einer Oracle-Datenbank als Quelle für AWS DMS in der AWS DMS-Dokumentation.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Versionen und Datenbank-Engines.	Identifizieren Sie die Versionen und Engines der Quell- und Zieldatenbank.	DBA, Entwickler
Identifizieren Sie die Replikationsinstanz.	Identifizieren Sie die AWS DMS-Replikationsinstanz.	DBA, Entwickler
Identifizieren Sie die Speicheranforderungen.	Identifizieren Sie den Speichertyp und die Kapazität.	DBA, Entwickler
Identifizieren Sie die Netzwerkanforderungen.	Identifizieren Sie die Netzwerklatenz und Bandbreite.	DBA, Entwickler
Identifizieren Sie die Hardwareanforderungen.	Identifizieren Sie die Hardwareanforderungen für die Quell- und Zielserverinstanzen (basierend auf der Oracle-Kompatibilitätsliste und den Kapazitätsanforderungen).	DBA, Entwickler
Identifizieren Sie die Sicherheitsanforderungen.	Identifizieren Sie die Sicherheitsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.	DBA, Entwickler
Installieren Sie die Treiber.	Installieren Sie die neuesten AWS SCT- und Oracle-Treiber.	DBA, Entwickler
Legen Sie eine Backup-Strategie fest.		DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie die Verfügbar keitsanforderungen.		DBA, Entwickler
Wählen Sie eine Strategie für Anwendungsmigration/Switcho ver.		DBA, Entwickler
Wählen Sie den -Instance-Typ aus.	Wählen Sie den richtigen Instanztyp auf der Grundlage von Kapazität, Speicher und Netzwerkfunktionen aus.	DBA, Entwickler

Konfigurieren Sie die Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC).	Die Quell-, Ziel- und Replikati onsinstanzen sollten sich in derselben VPC und in derselben Availability Zone befinden (empfohlen).	Developer
Erstellen Sie Sicherhei tsgruppen.	Erstellen Sie die erforderlichen Sicherheitsgruppen für den Datenbankzugriff.	Developer
Erzeugen Sie ein Schlüssel paar.	Generieren und konfigurieren Sie ein key pair.	Developer
Konfigurieren Sie andere Ressourcen.	Konfigurieren Sie Subnetze, Availability Zones und CIDR-Blöcke.	Developer

Konfigurieren Sie die Quelle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die EC2 Instanz.	Anweisungen finden Sie in der EC2 Amazon-Dokumentation.	Developer
Installieren Sie die Oracle-Datenbank.	Installieren Sie die Oracle-Datenbank auf der EC2 Instanz mit den erforderlichen Benutzern und Rollen.	DBA
Folgen Sie den Schritten in der Aufgabenbeschreibung, um von außerhalb der EC2 Instanz auf Oracle zuzugreifen.	1. Ändern Sie den lokalen Host `tnsnames` in Amazon EC2 Public DNS. 2. Ändern Sie den lokalen Host `listener` in Amazon EC2 Public DNS. 3. Stoppen Sie den Listener und starten Sie ihn neu.	DBA
Aktualisieren Sie das EC2 öffentliche DNS von Amazon.	Nach dem Neustart der EC2 Instance ändert sich das öffentliche DNS. Stellen Sie sicher, dass Sie das EC2 öffentliche DNS von Amazon in `tnsnames` und aktualisieren`listener`, oder verwenden Sie eine Elastic IP-Adresse.	DBA, Entwickler
Konfigurieren Sie die EC2 Instanz-Sicherheitsgruppe.	Konfigurieren Sie die EC2 Instanz-Sicherheitsgruppe so, dass die Replikationsinstanz und die erforderlichen Clients auf die Quelldatenbank zugreifen können.	DBA, Entwickler

Konfiguration der Amazon RDS for MariaDB MariaDB-Zielumgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die RDS-DB-In stance.	Konfigurieren und starten Sie die Amazon RDS for MariaDB-DB-Instance.	Developer
Erstellen Sie Tablespaces.	Erstellen Sie alle erforderl ichen Tablespaces in der Amazon RDS MariaDB-D atenbank.	DBA
Konfigurieren Sie eine Sicherheitsgruppe.	Konfigurieren Sie eine Sicherheitsgruppe, sodass die Replikationsinstanz und die erforderlichen Clients auf die Zieldatenbank zugreifen können.	Developer

AWS SCT konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Treiber installieren.	Installieren Sie die neuesten AWS SCT- und Oracle-Tr eiber.	Developer
Connect (Verbinden).	Geben Sie die entsprech enden Parameter ein und stellen Sie dann eine Verbindung zur Quelle und zum Ziel her.	Developer
Generieren Sie einen Bericht zur Schemakonvertierung.	Generieren Sie einen Bericht zur AWS-SCT-Schemakonv ertierung.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Korrigieren Sie den Code und das Schema nach Bedarf.	Nehmen Sie alle erforderl ichen Korrekturen am Code und am Schema vor (insbeson dere an Tablespaces und Anführungszeichen).	DBA, Entwickler
Validieren Sie das Schema.	Überprüfen Sie das Schema auf der Quelle und auf dem Ziel, bevor Sie Daten laden.	Developer

Migrieren Sie Daten mit AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie ein Verbindun gsattribut fest.	Legen Sie für Volllast und Change Data Capture (CDC) oder nur für CDC ein zusätzlic hes Verbindungsattribut fest. Weitere Informationen finden Sie in der Dokumentation zu Amazon RDS.	Developer
Aktivieren Sie die zusätzliche Protokollierung.	Aktivieren Sie die zusätzlic he Protokollierung in der Quelldatenbank.	DBA, Entwickler
Aktivieren Sie den Archiv-Pr otokollmodus.	Für Volllast und CDC (oder nur für CDC) aktivieren Sie den Archiv-Log-Modus in der Quelldatenbank.	DBA
Endpunkte erstellen und testen.	Erstellen Sie Quell- und Zielendpunkte und testen Sie die Verbindungen. Weitere	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Informationen finden Sie in der Amazon DMS-Dokumentation.	
Erstellen Sie eine Replikationsaufgabe.	Wenn die Endpoints erfolgreich verbunden wurden, erstellen Sie eine Replizierungsaufgabe. Weitere Informationen finden Sie in der Amazon DMS-Dokumentation.	Developer
Wählen Sie den Replikationstyp.	Wählen Sie in der Aufgabe nur CDC oder Volllast plus CDC aus, um Änderungen nur für die kontinuierliche Replikation bzw. für Volllast und laufende Änderungen zu erfassen.	Developer
Starten und überwachen Sie die Aufgabe.	Starten Sie die Replikationsaufgabe und überwachen Sie die CloudWatch Amazon-Protokolle. Weitere Informationen finden Sie in der Amazon DMS-Dokumentation.	Developer
Validieren Sie die Daten.	Validieren Sie die Daten in den Quell- und Zieldatenbanken.	Developer

Migrieren Sie Anwendungen und wechseln Sie zur Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der ausgewählten Strategie zur Anwendungsmigration.		DBA, App-Besitzer, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der gewählten Strategie zur Umstellung und Umstellung von Anwendung en.		DBA, App-Besitzer, Entwickler

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie das Schema und die Daten.	Stellen Sie vor Abschluss des Projekts sicher, dass das Schema und die Daten in der Quelle und im Ziel erfolgreich validiert wurden.	DBA, Entwickler
Sammeln Sie Metriken.	Erfassen Sie Kennzahlen zur Zeit bis zur Migration, zum Prozentsatz manueller Aufgaben im Vergleich zu Toolaufgaben, zu Kostenein sparungen und ähnlichen Kriterien.	DBA, App-Besitzer, Entwickler
Lesen Sie die Dokumentation.	Überprüfen Sie die Projektdo kumente und Artefakte.	DBA, App-Besitzer, Entwickler
Ressourcen herunterfahren.	Fahren Sie temporäre AWS-Ressourcen herunter.	DBA, Entwickler
Schließen Sie das Projekt.	Schließen Sie das Migration sprojekt und geben Sie Feedback.	DBA, App-Besitzer, Entwickler

Zugehörige Ressourcen

- Überblick über MariaDB Amazon RDS
- Amazon RDS for MariaDB — Produktdetails
- Verwenden einer Oracle-Datenbank als Quelle für AWS DMS
- Strategien für die Migration von Oracle-Datenbanken zu AWS
- Lizenzierung von Oracle-Software in der Cloud-Computing-Umgebung
- Amazon RDS für Oracle FAQs
- Überblick über AWS DMS
- AWS DMS-Blogbeiträge
- EC2 Überblick über Amazon
- Amazon EC2 FAQs
- AWS SCT-Dokumentation

Migrieren Sie eine lokale Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon RDS for MySQL

Erstellt von Sergey Dmitriev (AWS) und Naresh Damera (AWS)

Übersicht

Dieses Muster führt Sie durch die Migration einer lokalen Oracle-Datenbank zu einer Amazon Relational Database Service (Amazon RDS) für MySQL-DB-Instance. Es verwendet AWS Database Migration Service (AWS DMS), um die Daten zu migrieren, und das AWS Schema Conversion Tool (AWS SCT), um das Quelldatenbankschema und die Objekte in ein Format zu konvertieren, das mit Amazon RDS for MySQL kompatibel ist.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle-Quelldatenbank in einem lokalen Rechenzentrum

Einschränkungen

- Größenbeschränkung der Datenbank: 64 TB

Produktversionen

- Alle Oracle-Datenbankeditionen für die Versionen 11g (Versionen 11.2.0.3.v1 und höher) und bis zu 12.2 und 18c. Die aktuelle Liste der unterstützten Versionen finden Sie unter Using an Oracle Database as a Source for AWS DMS. Wir empfehlen Ihnen, die neueste Version von AWS DMS zu verwenden, um die umfassendste Version von Versionen und Funktionen zu erhalten. Informationen zu den von AWS SCT unterstützten Oracle-Datenbankversionen finden Sie in der AWS SCT-Dokumentation.
- AWS DMS unterstützt derzeit die MySQL-Versionen 5.5, 5.6 und 5.7. Die aktuelle Liste der unterstützten Versionen finden Sie in der AWS-Dokumentation unter Verwenden einer MySQL-kompatiblen Datenbank als Ziel für AWS DMS.

Architektur

Quelltechnologie-Stack

- Lokale Oracle-Datenbank

Zieltechnologie-Stack

- Amazon RDS for MySQL MySQL-DB-Instance

Architektur der Datenmigration

Tools

- AWS DMS — AWS Database Migration Services (AWS DMS) unterstützt Sie bei der Migration von relationalen Datenbanken, Data Warehouses, NoSQL-Datenbanken und anderen Arten von Datenspeichern. Sie können AWS DMS verwenden, um Ihre Daten in die AWS Cloud, zwischen lokalen Instances (über eine AWS Cloud-Einrichtung) oder zwischen Kombinationen aus Cloud und lokalen Einrichtungen zu migrieren.
- AWS SCT — Das AWS Schema Conversion Tool (AWS SCT) wird verwendet, um Ihr Datenbankschema von einer Datenbank-Engine in eine andere zu konvertieren. Der benutzerdefinierte Code, den das Tool konvertiert, umfasst Ansichten, gespeicherte Prozeduren und Funktionen. Jeder Code, den das Tool nicht automatisch konvertieren kann, ist deutlich gekennzeichnet, sodass Sie ihn selbst konvertieren können.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversion und die Engine.		DBA
Identifizieren Sie die Hardwareanforderungen für die Zielserverinstanz.		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Speicheranforderungen (Speichertyp und Kapazität).		DBA, SysAdmin
Wählen Sie den richtigen Instanztyp auf der Grundlage von Kapazität, Speicherf unktionen und Netzwerkf unktionen aus.		DBA, SysAdmin
Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.		DBA, SysAdmin
Identifizieren Sie die Strategie zur Anwendungsmigration.		DBA SysAdmin, Besitzer der App

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine virtuelle private Cloud (VPC) und Subnetze.		SysAdmin
Erstellen Sie die Sicherhei tsgruppen und Netzwerkz ugriffskontrolllisten ()ACLs.		SysAdmin
Konfigurieren und starten Sie eine Amazon RDS-DB-In stance.		DBA, SysAdmin

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie das Datenbank schema mithilfe von AWS SCT.		DBA
Migrieren Sie Daten mithilfe von AWS DMS.		DBA

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie AWS SCT, um den SQL-Code im Anwendung scode zu analysieren und zu konvertieren.	Weitere Informationen finden Sie unter https://docs.aws.amazon.com/SchemaConversionTool/ latest/userguide/ CHAP _Converting.app.html.	Besitzer der App
Folgen Sie der Strategie zur Anwendungsmigration.		DBA SysAdmin, Besitzer der App

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung sclients auf die neue Infrastruktur um.		DBA SysAdmin, Besitzer der App

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die temporären AWS-Ressourcen herunter.		DBA, SysAdmin
Überprüfen und validieren Sie die Projektdokumente.		DBA, SysAdmin
Erfassen Sie Kennzahlen zum Zeitpunkt der Migration, zum prozentualen Anteil manueller Daten im Vergleich zu Tools, zu Kosteneinsparungen usw.		DBA, SysAdmin
Schließen Sie das Projekt ab und geben Sie Feedback.		

Zugehörige Ressourcen

Referenzen

- AWS DMS-Dokumentation
- AWS SCT-Dokumentation
- Amazon RDS — Preise

Tutorial und Videos

- Erste Schritte mit AWS DMS
- Erste Schritte mit Amazon RDS
- AWS DMS (Video)
- Amazon RDS (Video)

Migrieren Sie eine lokale Oracle-Datenbank mithilfe eines Oracle-Bystanders und AWS DMS zu Amazon RDS for PostgreSQL

Erstellt von Cady Motyka (AWS)

Übersicht

Dieses Muster beschreibt, wie Sie eine lokale Oracle-Datenbank mit minimalen Ausfallzeiten auf einen der folgenden PostgreSQL-kompatiblen AWS-Datenbankservices migrieren können:

- Amazon Relational Database Service (Amazon RDS) für PostgreSQL
- Amazon Aurora PostgreSQL-Compatible Edition

Die Lösung verwendet den AWS Database Migration Service (AWS DMS) für die Migration der Daten, das AWS Schema Conversion Tool (AWS SCT) für die Konvertierung des Datenbankschemas und eine Oracle-Bystander-Datenbank für die Verwaltung der Migration. Bei dieser Implementierung ist die Ausfallzeit darauf beschränkt, wie lange es dauert, alle Fremdschlüssel in der Datenbank zu erstellen oder zu validieren.

Die Lösung verwendet auch Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit einer Oracle-Bystander-Datenbank, um den Datenstrom über AWS DMS zu kontrollieren. Sie können die Streaming-Replikation von der lokalen Oracle-Datenbank zum Oracle-Bystander vorübergehend unterbrechen, um AWS DMS zu aktivieren, um die Datenvalidierung catch, oder um ein anderes Datenvalidierungstool zu verwenden. Die Amazon RDS for PostgreSQL PostgreSQL-DB-Instance oder die Aurora PostgreSQL-kompatible DB-Instance und die Bystander-Datenbank verfügen über dieselben Daten, wenn AWS DMS die Migration der aktuellen Änderungen abgeschlossen hat.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle-Quelldatenbank in einem lokalen Rechenzentrum mit konfigurierter Active Data Guard-Standby-Datenbank
- AWS Direct Connect, konfiguriert zwischen dem lokalen Rechenzentrum und AWS Secrets Manager zum Speichern der Datenbankgeheimnisse
- Java Database Connectivity (JDBC) -Treiber für AWS SCT-Konnektoren, die entweder auf einem lokalen Computer oder auf der EC2 Instance installiert sind, auf der AWS SCT installiert ist

- Vertrautheit mit der Verwendung einer Oracle-Datenbank als Quelle für AWS DMS
- Vertrautheit mit der Verwendung einer PostgreSQL-Datenbank als Ziel für AWS DMS

Einschränkungen

- Größenbeschränkung der Datenbank: 64 TB

Produktversionen

- AWS DMS unterstützt alle Oracle-Datenbankeditionen für die Versionen 10.2 und höher (für Versionen 10.x), 11g und bis zu 12.2, 18c und 19c. Die aktuelle Liste der unterstützten Versionen finden Sie unter Using an Oracle Database as a Source for AWS DMS. Wir empfehlen Ihnen, die neueste Version von AWS DMS zu verwenden, um die umfassendste Version von Versionen und Funktionen zu erhalten. Informationen zu den von AWS SCT unterstützten Oracle-Datenbankversionen finden Sie in der AWS SCT-Dokumentation.
- AWS DMS unterstützt die PostgreSQL-Versionen 9.4 und höher (für die Versionen 9.x), 10.x, 11.x, 12.x und 13.x. Aktuelle Informationen finden Sie in der AWS-Dokumentation unter Verwenden einer PostgreSQL-Datenbank als Ziel für AWS DMS.

Architektur

Quelltechnologie-Stack

- Eine lokale Oracle-Datenbank
- Eine EC2 Instanz, die einen Zuschauer für die Oracle-Datenbank hält

Zieltechnologie-Stack

- Amazon RDS for PostgreSQL- oder Aurora PostgreSQL-Instance, PostgreSQL 9.3 und höher

Zielarchitektur

Das folgende Diagramm zeigt einen Beispiel-Workflow für die Migration einer Oracle-Datenbank zu einer PostgreSQL-kompatiblen AWS-Datenbank mithilfe von AWS DMS und einem Oracle-Bystander:

Tools

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS-Cloud oder zwischen Kombinationen von Cloud- und lokalen Setups.
- Das AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der AWS-Cloud.

Epen

Das Oracle-Datenbankschema nach PostgreSQL konvertieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie AWS SCT ein.	Erstellen Sie einen neuen Bericht und stellen Sie eine Verbindung zu Oracle als Quelle und PostgreSQL als Ziel her. Gehen Sie in den Projekteinstellungen zur Registerkarte SQL Scripting . Ändern Sie das Ziel-SQL-Skript in mehrere Dateien. Diese Dateien werden später verwendet und haben den folgenden Namen: • create_database.sql • create_sequence.sql • create_table.sql • create_view.sql • create_function.sql	DBA
Konvertiert das Oracle-Da tenbankschema.	Wählen Sie auf der Registerk arte Aktion die Option Bericht	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	generieren aus. Wählen Sie dann Schema konvertieren und dann Als SQL speichern aus.	
Ändern Sie die Skripts.	Möglicherweise möchten Sie das Skript ändern, wenn eine Zahl im Quellschema in PostgreSQL in ein numerisch es Format konvertiert wurde, aber Sie möchten stattdess en BIGINT verwenden, um die Leistung zu verbessern.	DBA

Erstellen und konfigurieren Sie die Amazon RDS-DB-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Amazon RDS-DB-Instance.	Erstellen Sie in der richtigen AWS-Region eine neue PostgreSQL-DB-Instance. Weitere Informationen finden Sie unter Erstellen einer PostgreSQL-DB-Instance und Herstellen einer Verbindung zu einer Datenbank auf einer PostgreSQL-DB-Instance in der Amazon RDS-Dokum entation.	AWS SysAdmin, DBA
Konfigurieren Sie die Spezifika tionen der DB-Instance.	Geben Sie die DB-Engine -Version, die DB-Instan ce-Klasse, die Multi-AZ-Bereitstellung, den Speichert yp und den zugewiesenen	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Speicher an. Geben Sie die DB-Instance-ID, einen primären Benutzernamen und ein primäres Passwort ein.	
Konfigurieren Sie Netzwerk und Sicherheit.	Geben Sie die Virtual Private Cloud (VPC), die Subnetzgruppe, den öffentlichen Zugriff, die Availability Zone-Präferenz und die Sicherheitsgruppen an.	DBA, SysAdmin
Datenbankoptionen konfigurieren.	Geben Sie den Datenbanknamen, den Port, die Parametergruppe, die Verschlüsselung und den KMS-Schlüssel an.	AWS SysAdmin, DBA
Konfigurieren Sie die Sicherungen.	Geben Sie den Aufbewahrungszeitraum für Backups, das Backup-Fenster, die Startzeit und die Dauer an und ob Tags in Snapshots kopiert werden sollen.	AWS SysAdmin, DBA
Konfigurieren Sie die Überwachungsoptionen.	Aktivieren oder deaktivieren Sie erweiterte Überwachungs- und Leistungseinblicke.	AWS SysAdmin, DBA
Konfigurieren Sie die Wartungsoptionen.	Geben Sie das auto Upgrade der Nebenversion, das Wartungsfenster sowie den Starttag, die Uhrzeit und die Dauer an.	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Skripts vor der Migration von AWS SCT aus.	Führen Sie auf der Amazon RDS-Instance die folgenden von AWS SCT generierten Skripts aus: • create_database.sql • create_sequence.sql • create_table.sql • create_view.sql • create_function.sql	AWS SysAdmin, DBA

Konfigurieren Sie den Oracle-Bystander in Amazon EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie das Netzwerk für Amazon ein EC2.	Erstellen Sie die neue VPC, Subnetze, Internet-Gateways, Routing-Tabellen und Sicherheitsgruppen.	AWS SysAdmin
Erstellen Sie die EC2 Instanz.	Erstellen Sie in der entsprechenden AWS-Region eine neue EC2 Instance. Wählen Sie das Amazon Machine Image (AMI), wählen Sie die Instance-Größe und konfigurieren Sie die Instance-Details: Anzahl der Instances (1), VPC und Subnetz, die Sie in der vorherigen Aufgabe erstellt haben, automatische Zuweisung öffentlicher IP-Adressen und andere Optionen. Speicher hinzufüge	AWS SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	n, Sicherheitsgruppen konfigurieren und starten. Wenn Sie dazu aufgeford ert werden, erstellen und speichern Sie ein key pair für den nächsten Schritt.	
Connect die Oracle-Qu elldatenbank mit der EC2 Instanz.	Kopieren Sie die IPv4 öffentlic he IP-Adresse und den DNS in eine Textdatei und stellen Sie mithilfe von SSH wie folgt eine Verbindung her: ssh -i „your_fil e.pem“ ec2-user@<your-IP - - DNS>. address-or-public	AWS SysAdmin
Richten Sie den ersten Host für einen Zuschauer in Amazon ein. EC2	Richten Sie SSH-Schlü ssel, Bash-Profil, ORATAB und symbolische Links ein. Erstellen Sie Oracle-Ve rzeichnisse.	AWS SysAdmin, Linux-Adm inistrator
Richten Sie die Datenbank kopie für einen Zuschauer in Amazon ein EC2	Verwenden Sie RMAN, um eine Datenbankkopie zu erstellen, die zusätzliche Protokollierung zu aktivieren und die Standby-Steuerdate i zu erstellen. Nachdem der Kopiervorgang abgeschlo ssen ist, versetzen Sie die Datenbank in den Wiederher stellungsmodus.	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Oracle Data Guard ein.	Ändern Sie Ihre Datei listener.ora und starten Sie den Listener. Richten Sie ein neues Archivzie l ein. Versetzen Sie den Zuschauer in den Wiederher stellungsmodus, ersetzen Sie temporäre Dateien, um future Beschädigungen zu vermeiden, installieren Sie bei Bedarf ein Crontab, um zu verhindern, dass dem Archivverzeichnis der Speicherplatz ausgeht, und bearbeiten Sie die manage-tr clog-files-oracle.cfg-Datei für die Quelle und den Standby-M odus.	AWS SysAdmin, DBA
Bereiten Sie die Oracle-Da tenbank für die Versandsy nchronisierung vor.	Fügen Sie die Standby-P rotokolldateien hinzu und ändern Sie den Wiederher stellungsmodus. Ändern Sie den Protokollversand sowohl auf der primären Quelle als auch auf der Standby-Quelle auf SYNC AFFIRM. Schalten Sie die primären Protokolle ein, bestätigen Sie über das Amazon EC2 Bystander Alert Log, dass Sie die Standby-Protokolldateien verwenden , und stellen Sie sicher, dass der Redo-Stream SYNC läuft.	AWS SysAdmin, DBA

Migrieren Sie Daten mit AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Replikationsinstanz in AWS DMS.	Füllen Sie die Felder für den Namen, die Instance-Klasse, die VPC (wie die EC2 Amazon-Instance), Multi-AZ und den öffentlichen Zugriff aus. Geben Sie unter Advance den zugewiesenen Speicher, die Subnetzgruppe, die Availability Zone, die VPC-Sicherheitsgruppen und den AWS Key Management Service (AWS KMS) -Schlüssel an.	AWS SysAdmin, DBA
Erstellen Sie den Endpunkt der Quelldatenbank.	Geben Sie den Endpunktnamen, den Typ, die Quell-Engine (Oracle), den Servernamen (Amazon EC2 Private DNS-Name), den Port, den SSL-Modus, den Benutzernamen, das Passwort, die SID, die VPC (geben Sie die VPC an, die die Replikationsinstanz hat) und die Replikationsinstanz an. Um die Verbindung zu testen, wählen Sie Test ausführen und erstellen Sie dann den Endpunkt. Sie können auch die folgenden erweiterten Einstellungen konfigurieren: maxFileSizeund numberDataTypeSkalieren.	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Connect AWS DMS mit Amazon RDS for PostgreSQL.	Erstellen Sie eine Migration ssicherheitsgruppe für Verbindungen zwischen. VPCs	AWS SysAdmin, DBA
Erstellen Sie den Zieldaten bank-Endpunkt.	Geben Sie den Endpunktn amen, den Typ, die Quell-Engine (PostgreSQL), den Servernamen (Amazon RDS-Endpunkt), den Port, den SSL-Modus, den Benutzern amen, das Passwort, den Datenbanknamen, die VPC (geben Sie die VPC an, die die Replikationsinstanz hat) und die Replikationsinstanz an. Um die Verbindung zu testen, wählen Sie Test ausführen und erstellen Sie dann den Endpunkt. Sie können auch die folgenden erweiterten Einstellungen konfigurieren: maxFileSize und numberDat aTypeSkalieren.	AWS SysAdmin, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die AWS DMS-Replikationsaufgabe.	Geben Sie den Namen der Aufgabe, die Replikationsinstanz, die Quell- und Zielendpunkte sowie die Replikationsinstanz an. Wählen Sie als Migrationstyp die Option Bestehende Daten migrieren und laufende Änderungen replizieren aus. Deaktivieren Sie das Kontrollkästchen Aufgabe bei Erstellung starten.	AWS SysAdmin, DBA
Konfigurieren Sie die Einstellungen für die AWS DMS-Replikationsaufgabe.	Wählen Sie für den Modus zur Vorbereitung der Zieltabelle die Option Nichts tun. Stoppen Sie die Aufgabe, nachdem der vollständige Ladevorgang abgeschlossen ist (um Primärschlüssel zu erstellen). Geben Sie den eingeschränkten oder vollständigen LOB-Modus an und aktivieren Sie die Steuertabellen. Optional können Sie die CommitRateerweiterte Einstellung konfigurieren.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Tabellenzuordnungen.	Erstellen Sie im Abschnitt Tabellenzuordnungen eine Einschlussregel für alle Tabellen in allen Schemas, die in der Migration enthalten sind, und erstellen Sie dann eine Ausschlussregel. Fügen Sie drei Transformationsregeln hinzu, um die Schema-, Tabellen- und Spaltennamen in Kleinbuchstaben umzuwandeln, und fügen Sie alle anderen Regeln hinzu, die für diese spezielle Migration erforderlich sind.	DBA
Starte die Aufgabe.	Starten Sie die Replikationsaufgabe. Stellen Sie sicher, dass die Volllast läuft. Führen Sie ALTER SYSTEM SWITCH LOGFILE in der primären Oracle-Datenbank aus, um die Aufgabe zu starten.	DBA
Führen Sie die Skripts während der Migration von AWS SCT aus.	Führen Sie in Amazon RDS for PostgreSQL die folgenden von AWS SCT generierten Skripts aus: • create_index.sql • create_constraint.sql	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Aufgabe neu, um mit der Erfassung von Änderungsdaten (CDC) fortzufahren.	Führen Sie VACUUM auf der Amazon RDS for PostgreSQ L PostgreSQL-DB-Instance aus und starten Sie die AWS DMS-Aufgabe neu, um zwischengespeicherte CDC-Änderungen anzuwenden.	DBA

Wechseln Sie zur PostgreSQL-Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die AWS DMS-Protokolle und Validieru ngstabellen auf Fehler.	Überprüfen und beheben Sie alle Replikations- oder Validierungsfehler.	DBA
Stoppen Sie alle Oracle-Ab hängigkeiten.	Stoppen Sie alle Oracle-Ab hängigkeiten, fahren Sie die Listener in der Oracle-Da tenbank herunter und führen Sie ALTER SYSTEM SWITCH LOGFILE aus. Beenden Sie die AWS DMS-Aufgabe, wenn keine Aktivität angezeigt wird.	DBA
Führen Sie die Skripts nach der Migration von AWS SCT aus.	Führen Sie in Amazon RDS for PostgreSQL die folgenden von AWS SCT generierten Skripts aus: • create_foreign_key_constrai nt.sql • create_triggers.sql	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie zusätzliche Schritte von Amazon RDS for PostgreSQL aus.	Inkrementieren Sie die Sequenzen bei Bedarf so, dass sie mit Oracle übereinst immen, führen Sie VACUUM und ANALYZE aus und erstellen Sie aus Compliance-Gründen einen Snapshot.	DBA
Öffnen Sie die Verbindun gen zu Amazon RDS for PostgreSQL.	Entfernen Sie die AWS DMS-Sicherheitsgruppen aus Amazon RDS for PostgreSQ L, fügen Sie Produktio nssicherheitsgruppen hinzu und verweisen Sie Ihre Anwendungen auf die neue Datenbank.	DBA
Bereinigen Sie AWS DMS-Objekte.	Entfernen Sie die Endgeräte , Replikationsaufgaben, Replikationsinstanzen und die EC2 Instanz.	SysAdmin, DBA

Zugehörige Ressourcen

- AWS DMS-Dokumentation
- AWS SCT-Dokumentation
- Preise für Amazon RDS for PostgreSQL

Migrieren Sie mithilfe von Oracle von Oracle Database zu Amazon RDS for PostgreSQL GoldenGate

Erstellt von Dhairya Jindani (AWS), Rajeshkumar Sabankar (AWS) und Sindhusha Paturu (AWS)

Übersicht

Dieses Muster zeigt, wie eine Oracle-Datenbank mithilfe von Oracle Cloud Infrastructure (OCI) zu Amazon Relational Database Service (Amazon RDS) für PostgreSQL migriert wird. GoldenGate

Mithilfe von Oracle GoldenGate können Sie Daten mit minimaler Ausfallzeit zwischen Ihrer Quelldatenbank und einer oder mehreren Zieldatenbanken replizieren.

> **Note**
>
> Die Oracle-Quelldatenbank kann sich entweder vor Ort oder auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance befinden. Sie können ein ähnliches Verfahren verwenden, wenn Sie lokale Replikationstools verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine GoldenGate Oracle-Lizenz
- Java Database Connectivity (JDBC) -Treiber für die Verbindung mit der PostgreSQL-Datenbank
- Schema und Tabellen, die mit dem AWS Schema Conversion Tool (AWS SCT) auf der Amazon RDS for PostgreSQL PostgreSQL-Zieldatenbank erstellt wurden

Einschränkungen

- Oracle GoldenGate kann nur bestehende Tabellendaten (erstes Laden) und laufende Änderungen (Erfassung von Änderungsdaten) replizieren

Produktversionen

- Oracle Database Enterprise Edition 10g oder neuere Versionen
- Oracle GoldenGate 12.2.0.1.1 für Oracle oder neuere Versionen

- Oracle GoldenGate 12.2.0.1.1 für PostgreSQL oder neuere Versionen

Architektur

Das folgende Diagramm zeigt einen Beispiel-Workflow für die Migration einer Oracle-Datenbank zu Amazon RDS for PostgreSQL mithilfe von Oracle: GoldenGate

Das Diagramm zeigt den folgenden Workflow:

1. Der Oracle GoldenGate Extract-Prozess wird in der Quelldatenbank ausgeführt, um Daten zu extrahieren.
2. Der Oracle GoldenGate Replicat-Prozess liefert die extrahierten Daten an die Amazon RDS for PostgreSQL PostgreSQL-Zieldatenbank.

Tools

- Oracle GoldenGate unterstützt Sie bei der Entwicklung, Ausführung, Orchestrierung und Überwachung Ihrer Datenreplikations- und Streaming-Datenverarbeitungslösungen in der Oracle Cloud-Infrastruktur.
- Amazon Relational Database Service (Amazon RDS) für PostgreSQL unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen PostgreSQL-Datenbank in der AWS-Cloud.

Epen

Laden Sie Oracle herunter und installieren Sie es GoldenGate

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie Oracle herunter GoldenGate.	Laden Sie die folgenden Versionen von Oracle herunter GoldenGate: • Oracle GoldenGate 12.2.0.1.1 für Oracle oder eine neuere Version	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Oracle GoldenGate 12.2.0.1.1 für PostgreSQL oder eine neuere Version Informationen zum Herunterladen der Software finden Sie unter GoldenGate Oracle-Downloads auf der Oracle-Website.	
Installieren Sie Oracle GoldenGate für Oracle auf dem Oracle-Datenbankquellserver.	Anweisungen finden Sie in der GoldenGate Oracle-Dokumentation.	DBA
Installieren Sie GoldenGate die Oracle for PostgreSQL-Datenbank auf der EC2 Amazon-Instance.	Anweisungen finden Sie in der GoldenGate Oracle-Dokumentation.	DBA

Konfigurieren Sie Oracle GoldenGate in der Quell- und Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Oracle GoldenGate for Oracle Database in der Quelldatenbank ein.	Anweisungen finden Sie in der GoldenGate Oracle-Dokumentation. Stellen Sie sicher, dass Sie Folgendes konfigurieren: • Zusätzliche Protokollierung • Oracle-Benutzer GoldenGate	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Alle erforderlichen Zuschüsse und Berechtigungen • Parameterdateien • Manager-Prozess • Verzeichnis • GLOBALS-Dateien • Oracle-Wallet	
Richten Sie Oracle GoldenGate für PostgreSQL in der Zieldatenbank ein.	Anweisungen finden Sie in Teil VI Using Oracle GoldenGate for PostgreSQL auf der Oracle-Website. Stellen Sie sicher, dass Sie Folgendes konfigurieren: • Manager-Prozess • GLOBALS-Dateien • Oracle-Wallet	DBA

Konfigurieren Sie die Datenerfassung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie den Extraktionsprozess in der Quelldatenbank ein.	Erstellen Sie in der Oracle-Quelldatenbank eine Extraktdatei, um Daten zu extrahieren. Anweisungen finden Sie unter ADD EXTRACT in der Oracle-Dokumentation.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Die Extraktdatei beinhaltet die Erstellung der Extraktparameterdatei und des Traildateiverzeichnisses.	
Richten Sie eine Datenpumpe ein, um die Trail-Datei von der Quell- zur Zieldatenbank zu übertragen.	Erstellen Sie eine EXTRACT-Parameterdatei und ein Traildateiverzeichnis, indem Sie den Anweisungen in PARFILE in Database Utilities auf der Oracle-Website folgen. Weitere Informationen finden Sie unter Was ist ein Trail? in Fusion Middleware Understanding Oracle GoldenGate auf der Oracle-Website.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Replikation auf der EC2 Amazon-Instance ein.	Erstellen Sie eine Replikationsparameterdatei und ein Traildateiverzeichnis. Weitere Informationen zum Erstellen von Replikationsparameterdateien finden Sie in Abschnitt 3.5 Validierung einer Parameterdatei in der Oracle Database-Dokumentation. Weitere Informationen zum Erstellen eines Traildateiverzeichnisses finden Sie unter Creating a Trail in der Oracle Cloud-Dokumentation. **Important** Stellen Sie sicher, dass Sie der GLOBALS-Datei am Ziel einen Checkpoint-Tabelleneintrag hinzufügen. Weitere Informationen finden Sie unter Was ist ein Replikat? in Fusion Middleware Understanding Oracle GoldenGate auf der Oracle-Website.	DBA

Konfigurieren Sie die Datenreplikation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie in der Quelldatenbank eine Parameterdatei, um Daten für den ersten Ladevorgang zu extrahieren.	Folgen Sie den Anweisungen unter Eine Parameterdatei in GGSCI erstellen in der Oracle Cloud-Dokumentation. **Important** Stellen Sie sicher, dass der Manager auf dem Ziel läuft.	DBA
Erstellen Sie in der Zieldatenbank eine Parameterdatei, um Daten für den ersten Ladevorgang zu replizieren.	Folgen Sie den Anweisungen unter Eine Parameterdatei in GGSCI erstellen in der Oracle Cloud-Dokumentation. **Important** Stellen Sie sicher, dass Sie den Replicat-Prozess hinzufügen und starten.	DBA

Wechseln Sie zur Amazon RDS-Datenbank für PostgreSQL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beenden Sie den Replicat-Prozess und stellen Sie sicher, dass die Quell- und Zieldatenbanken synchronisiert sind.	Vergleichen Sie die Zeilenanzahl zwischen der Quell- und der Zieldatenbank, um sicherzustellen, dass die	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Datenreplikation erfolgreich war.	
Konfigurieren Sie die Unterstützung für Data Definition Language (DDL).	Führen Sie das DDL-Skript zum Erstellen von Triggern, Sequenzen, Synonymen und Referenzschlüsseln in PostgreSQL aus. **Note** Sie können jede Standard-SQL-Clientanwendung verwenden, um eine Verbindung zu einer Datenbank in Ihrem DB-Cluster herzustellen. Sie können beispielsweise pgAdmin verwenden, um eine Verbindung zu Ihrer DB-Instance herzustellen.	DBA

Zugehörige Ressourcen

- Amazon RDS for PostgreSQL (Amazon RDS-Benutzerhandbuch)
- EC2 Amazon-Dokumentation
- Von Oracle GoldenGate unterstützte Verarbeitungsmethoden und Datenbanken (Oracle-Dokumentation)

Migrieren Sie eine Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon Redshift

Erstellt von Piyush Goyal (AWS) und Brian Motzer (AWS)

Übersicht

Dieses Muster bietet Anleitungen für die Migration von Oracle-Datenbanken zu einem Amazon Redshift Cloud Data Warehouse in der Amazon Web Services (AWS) -Cloud mithilfe von AWS Database Migration Service (AWS DMS) und AWS Schema Conversion Tool (AWS SCT). Das Muster deckt Oracle-Quelldatenbanken ab, die lokal installiert oder auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance installiert sind. Es behandelt auch Amazon Relational Database Service (Amazon RDS) für Oracle-Datenbanken.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Oracle-Datenbank, die in einem lokalen Rechenzentrum oder in der AWS-Cloud läuft
- Ein aktives AWS-Konto
- Vertrautheit mit der Verwendung einer Oracle-Datenbank als Quelle für AWS DMS
- Vertrautheit mit der Verwendung einer Amazon Redshift Redshift-Datenbank als Ziel für AWS DMS
- Kenntnisse über Amazon RDS, Amazon Redshift, die anwendbaren Datenbanktechnologien und SQL
- Java Database Connectivity (JDBC) -Treiber für AWS SCT-Konnektoren, auf denen AWS SCT installiert ist

Produktversionen

- Für selbstverwaltete Oracle-Datenbanken unterstützt AWS DMS alle Oracle-Datenbankeditionen für Versionen 10.2 und höher (für Versionen 10. x), 11g und bis zu 12.2, 18c und 19c. Für Amazon RDS for Oracle Oracle-Datenbanken, die AWS verwaltet, unterstützt AWS DMS alle Oracle-Datenbankeditionen für die Versionen 11g (Versionen 11.2.0.4 und höher) und bis zu 12.2, 18c und 19c. Wir empfehlen Ihnen, die neueste Version von AWS DMS zu verwenden, um die umfassendste Version von Versionen und Funktionen zu erhalten.

Architektur

Quelltechnologie-Stack

Eine der beiden folgenden Komponenten:

- Eine lokale Oracle-Datenbank
- Eine Oracle-Datenbank auf einer Instanz EC2
- Eine Amazon RDS for Oracle DB-Instance

Zieltechnologie-Stack

- Amazon Redshift

Zielarchitektur

Von einer Oracle-Datenbank, die in der AWS-Cloud läuft, zu Amazon Redshift:

Von einer Oracle-Datenbank, die in einem lokalen Rechenzentrum läuft, zu Amazon Redshift:

Tools

- AWS DMS — AWS Data Migration Service (AWS DMS) hilft Ihnen, Datenbanken schnell und sicher zu AWS zu migrieren. Die Quelldatenbank bleibt während der Migration voll funktionsfähig, wodurch Ausfallzeiten für Anwendungen, die auf die Datenbank angewiesen sind, minimiert werden. AWS DMS kann Ihre Daten zu und von den am häufigsten verwendeten kommerziellen und Open-Source-Datenbanken migrieren.
- AWS SCT — Das AWS Schema Conversion Tool (AWS SCT) kann verwendet werden, um Ihr vorhandenes Datenbankschema von einer Datenbank-Engine in eine andere zu konvertieren. Es unterstützt verschiedene Datenbank-Engines, darunter Oracle, SQL Server und PostgresSQL, als Quellen.

Epen

Bereite dich auf die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Datenbank versionen.	Überprüfen Sie die Quell- und Zieldatenbankversionen und stellen Sie sicher, dass sie von AWS DMS unterstützt werden. Informationen zu unterstützten Oracle-Datenbankversionen finden Sie unter Eine Oracle-Datenbank als Quelle für AWS DMS verwenden. Informationen zur Verwendung von Amazon Redshift als Ziel finden Sie unter Verwenden einer Amazon Redshift Redshift-Datenbank als Ziel für AWS DMS.	DBA
Erstellen Sie eine VPC und eine Sicherheitsgruppe.	Erstellen Sie in Ihrem AWS-Konto eine Virtual Private Cloud (VPC), falls diese nicht existiert. Erstellen Sie eine Sicherheitsgruppe für ausgehenden Datenverkehr zu Quell- und Zieldatenbanken. Weitere Informationen finden Sie in der Dokumentation zu Amazon Virtual Private Cloud (Amazon VPC).	Systemadministrator
Installieren Sie AWS SCT.	Laden Sie die neueste Version von AWS SCT und die entsprechenden Treiber herunter und installieren Sie	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	sie. Weitere Informationen finden Sie unter Installation, Überprüfung und Aktualisierung des AWS SCT.	
Erstellen Sie einen Benutzer für die AWS DMS-Aufgabe.	Erstellen Sie einen AWS DMS-Benutzer in der Quelldatenbank und gewähren Sie ihm READ-Rechte. Dieser Benutzer wird sowohl von AWS SCT als auch von AWS DMS verwendet.	DBA
Testen Sie die DB-Konnektivität.	Testen Sie die Konnektivität zur Oracle-DB-Instance.	DBA
Erstellen Sie ein neues Projekt in AWS-SCT.	Öffnen Sie das AWS SCT-Tool und erstellen Sie ein neues Projekt.	DBA
Analysieren Sie das zu migrierende Oracle-Schema.	Verwenden Sie AWS SCT, um das zu migrierende Schema zu analysieren und einen Bewertungsbericht zur Datenbankmigration zu erstellen. Weitere Informationen finden Sie unter Erstellen eines Bewertungsberichts zur Datenbankmigration in der AWS SCT-Dokumentation.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Bewertungsbericht.	Überprüfen Sie den Bericht auf die Durchführbarkeit der Migration. Einige DB-Objekte müssen möglicher weise manuell konvertiert werden. Weitere Informationen zum Bericht finden Sie unter Bewertungsbericht anzeigen in der AWS SCT-Dokumentation.	DBA

Bereiten Sie die Zieldatenbank vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon Redshift Redshift-Cluster.	Erstellen Sie einen Amazon Redshift Redshift-Cluster in der VPC, die Sie zuvor erstellt haben. Weitere Informationen finden Sie unter Amazon Redshift Redshift-Cluster in der Amazon Redshift Redshift-Dokumentation.	DBA
Datenbankbenutzer erstellen.	Extrahieren Sie die Liste der Benutzer, Rollen und Berechtigungen aus der Oracle-Quelldatenbank. Erstellen Sie Benutzer in der Amazon Redshift Redshift-Zieldatenbank und wenden Sie die Rollen aus dem vorherigen Schritt an.	DBA
Evaluieren Sie Datenbank parameter.	Überprüfen Sie die Datenbank optionen, Parameter	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	, Netzwerkdateien und Datenbank-Links aus der Oracle-Quelldatenbank und bewerten Sie deren Anwendbarkeit auf das Ziel.	
Wenden Sie alle relevanten Einstellungen auf das Ziel an.	Weitere Informationen zu diesem Schritt finden Sie unter Konfigurationsreferenz in der Amazon Redshift Redshift-Dokumentation.	DBA

Objekte in der Zieldatenbank erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen AWS DMS-Benutzer in der Zieldatenbank.	Erstellen Sie einen AWS DMS-Benutzer in der Zieldatenbank und gewähren Sie ihm Lese- und Schreibbe rechtigungen. Überprüfen Sie die Konnektivität von AWS SCT.	DBA
Konvertieren Sie das Schema, überprüfen Sie den SQL-Bericht und speichern Sie alle Fehler oder Warnungen.	Weitere Informationen finden Sie unter Konvertieren von Datenbankschemas mithilfe von AWS SCT in der AWS SCT-Dokumentation.	DBA
Wenden Sie die Schemaänd erungen auf die Zieldaten bank an oder speichern Sie sie als.sql-Datei.	Anweisungen finden Sie unter Speichern und Anwenden Ihres konvertierten Schemas	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	im AWS SCT in der AWS SCT-Dokumentation.	
Validieren Sie die Objekte in der Zieldatenbank.	Validieren Sie die Objekte, die im vorherigen Schritt in der Zieldatenbank erstellt wurden. Schreiben Sie alle Objekte, die nicht erfolgreich konvertie rt wurden, neu oder entwerfen Sie sie neu.	DBA
Deaktivieren Sie Fremdschl üssel und Trigger.	Deaktivieren Sie alle Fremdschlüssel und Trigger. Diese können zu Problemen beim Laden von Daten während des Vollladevorgangs führen, wenn AWS DMS ausgeführt wird.	DBA

Migrieren Sie Daten mit AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS DMS-Replikations-Instance.	Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS DMS-Konsole. Wählen Sie im Navigationsbereich Replikati onsinstanzen, Replikati onsinstanz erstellen aus. Eine ausführliche Anleitung finden Sie in Schritt 1 unter Erste Schritte mit AWS DMS in der AWS DMS-Dokumentation.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Quell- und Zielendpunkte.	Erstellen Sie Quell- und Zielendpunkte und testen Sie die Verbindung zwischen der Replikationsinstanz und den Quell- und Zielendpunkten. Eine ausführliche Anleitung finden Sie in Schritt 2 unter Erste Schritte mit AWS DMS in der AWS DMS-Dokum entation.	DBA
Erstellen Sie eine Replikati onsaufgabe.	Erstellen Sie eine Replikati onsaufgabe und wählen Sie die entsprechende Migration smethode aus. Eine ausführli che Anleitung finden Sie in Schritt 3 unter Erste Schritte mit AWS DMS in der AWS DMS-Dokumentation.	DBA
Starten Sie die Datenrepl ikation.	Starten Sie die Replikati onsaufgabe und überwachen Sie die Protokolle auf Fehler.	DBA

Migrieren Sie Ihre Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Anwendungsserver erstellen.	Erstellen Sie die neuen Anwendungsserver auf AWS.	Besitzer der Anwendung
Migrieren Sie den Anwendung scode.	Migrieren Sie den Anwendung scode auf die neuen Server.	Besitzer der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Anwendungsserver.	Konfigurieren Sie den Anwendungsserver für die Zieldatenbank und die Treiber.	Besitzer der Anwendung
Optimieren Sie den Anwendungscode.	Optimieren Sie den Anwendungscode für die Ziel-Engine.	Besitzer der Anwendung

Wechseln Sie zur Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Benutzer validieren.	Validieren Sie Benutzer in der Amazon Redshift Redshift-Zieldatenbank und gewähren Sie ihnen Rollen und Rechte.	DBA
Stellen Sie sicher, dass die Anwendung gesperrt ist.	Stellen Sie sicher, dass die Anwendung gesperrt ist, um weitere Änderungen zu verhindern.	Besitzer der Anwendung
Validieren Sie die Daten.	Überprüfen Sie die Daten in der Amazon Redshift Redshift-Zieldatenbank.	DBA
Aktivieren Sie Fremdschlüssel und Trigger.	Aktivieren Sie Fremdschlüssel und Trigger in der Amazon Redshift Redshift-Zieldaten bank.	DBA
Connect der neuen Datenbank her.	Konfigurieren Sie die Anwendung für die Verbindun g mit der neuen Amazon Redshift Redshift-Datenbank.	Besitzer der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die letzten Prüfungen durch.	Führen Sie vor der Inbetrieb nahme eine letzte, umfassend e Systemüberprüfung durch.	DBA, Besitzer der Anwendung
Geh live.	Gehen Sie mit der Amazon Redshift Redshift-Zieldaten bank live.	DBA

Schließen Sie das Migrationsprojekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre AWS-Ressourcen herunter.	Fahren Sie temporäre AWS-Ressourcen wie die AWS DMS-Replikationsinstanz und die für AWS SCT verwendete EC2 Instanz herunter.	DBA, Systemadministrator
Dokumente überprüfen.	Überprüfen und validieren Sie die Dokumente des Migration sprojekts.	DBA, Systemadministrator
Sammeln Sie Kennzahlen.	Sammeln Sie Informationen über das Migrationsprojekt, z. B. die Zeit für die Migration , den Prozentsatz manueller Aufgaben im Vergleich zu den Toolaufgaben und die Gesamtkosteneinsparungen.	DBA, Systemadministrator
Schließt das Projekt ab.	Schließen Sie das Projekt ab und geben Sie Feedback.	DBA, Systemadministrator

Zugehörige Ressourcen

Referenzen

- AWS DMS-Benutzerhandbuch
- AWS SCT-Benutzerhandbuch
- Leitfaden „Erste Schritte“ mit Amazon Redshift

Tutorials und Videos

- Tauchen Sie tief in AWS SCT und AWS DMS ein (Präsentation von AWS re:Invent 2019)
- Erste Schritte mit dem AWS Database Migration Service

Migrieren Sie eine Oracle-Datenbank mit AWS DMS und AWS SCT zu Aurora PostgreSQL

Erstellt von Senthil Ramasamy (AWS)

Übersicht

Dieses Muster beschreibt, wie eine Oracle-Datenbank mithilfe von AWS Data Migration Service (AWS DMS) und AWS Schema Conversion Tool (AWS SCT) zu Amazon Aurora PostgreSQL-Compatible Edition migriert wird.

Das Muster umfasst Oracle-Quelldatenbanken, die sich vor Ort befinden, Oracle-Datenbanken, die auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances installiert sind, und Amazon Relational Database Service (Amazon RDS) für Oracle-Datenbanken. Das Muster konvertiert diese Datenbanken in Aurora PostgreSQL-kompatible Datenbanken.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine Oracle-Datenbank in einem lokalen Rechenzentrum oder in der AWS-Cloud.
- SQL-Clients, die entweder auf einem lokalen Computer oder auf einer EC2 Instanz installiert sind.
- Java Database Connectivity (JDBC) -Treiber für AWS SCT-Konnektoren, die entweder auf einem lokalen Computer oder einer EC2 Instance installiert sind, auf der AWS SCT installiert ist.

Einschränkungen

- Größenbeschränkung der Datenbank: 128 TB
- Wenn die Quelldatenbank eine kommerzielle off-the-shelf (COTS) Anwendung unterstützt oder herstellerspezifisch ist, können Sie sie möglicherweise nicht in eine andere Datenbank-Engine konvertieren. Stellen Sie vor der Verwendung dieses Musters sicher, dass die Anwendung Aurora PostgreSQL-kompatibel unterstützt.

Versionen der Produkte

- Für selbstverwaltete Oracle-Datenbanken unterstützt AWS DMS alle Oracle-Datenbankeditionen für die Versionen 10.2 und höher (für Versionen 10.x), 11g und bis zu 12.2, 18c und 19c. Die

aktuelle Liste der unterstützten Oracle-Datenbankversionen (sowohl selbstverwaltete als auch Amazon RDS for Oracle) finden Sie unter Verwenden einer Oracle-Datenbank als Quelle für AWS DMS und Verwenden einer PostgreSQL-Datenbank als Ziel für AWS DMS.

- Wir empfehlen Ihnen, die neueste Version von AWS DMS zu verwenden, um die umfassendste Version von Versionen und Funktionen zu erhalten. Informationen zu den von AWS SCT unterstützten Oracle-Datenbankversionen finden Sie in der AWS SCT-Dokumentation.
- Aurora unterstützt die in den Amazon Aurora PostgreSQL-Versionen und Engine-Versionen aufgeführten PostgreSQL-Versionen.

Architektur

Quelltechnologie-Stack

Eine der beiden folgenden Komponenten:

- Eine lokale Oracle-Datenbank
- Eine Oracle-Datenbank auf einer Instanz EC2
- Eine Amazon RDS for Oracle Oracle-DB-Instance

Zieltechnologie-Stack

- Aurora PostgreSQL-kompatibel

Zielarchitektur

Architektur der Datenmigration

- Aus einer Oracle-Datenbank, die in der AWS-Cloud läuft

- Aus einer Oracle-Datenbank, die in einem lokalen Rechenzentrum läuft

Tools

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS-Cloud oder zwischen Kombinationen von Cloud- und lokalen Setups.
- Das AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein mit der Zieldatenbank kompatibles Format konvertiert werden.

Epen

Bereite dich auf die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Quelldatenbank vor.	Informationen zur Vorbereitung der Quelldatenbank finden Sie unter Verwenden von Oracle Database als Quelle für AWS SCT in der AWS SCT-Dokumentation.	DBA
Erstellen Sie eine EC2 Instanz für AWS SCT.	Erstellen und konfigurieren Sie bei Bedarf eine EC2 Instanz für AWS SCT.	DBA
Laden Sie AWS SCT herunter.	Laden Sie die neueste Version von AWS SCT und die zugehörigen Treiber herunter. Weitere Informationen finden Sie unter Installation, Überprüfung und Aktualisierung von AWS SCT in der AWS SCT-Dokumentation.	DBA
Fügen Sie Benutzer und Berechtigungen hinzu.	Fügen Sie die erforderlichen Benutzer und Berechtigungen	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in der Quelldatenbank hinzu und überprüfen Sie sie.	
Erstellen Sie ein AWS SCT-Projekt.	Erstellen Sie ein AWS SCT-Projekt für den Workload und stellen Sie eine Verbindun g zur Quelldatenbank her. Anweisungen finden Sie in der AWS SCT-Dokumentation unter Erstellen eines AWS-SCT-Projekts und Hinzufügen von Datenbankservern.	DBA
Beurteilen Sie die Machbarke it.	Generieren Sie einen Bewertungsbericht, der Aktionspunkte für Schemas zusammenfasst, die nicht automatisch konvertie rt werden können, und Schätzungen für den manuellen Konvertie rungsaufwand enthält. Weitere Informationen finden Sie unter Erstellen und Überprüfen des Bewertungsberichts zur Datenbankmigration in der AWS SCT-Dokumentation.	DBA

Bereiten Sie die Zieldatenbank vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon RDS-DB-Zielinstanz.	Erstellen Sie eine Amazon RDS-DB-Zielinstanz mit Amazon Aurora als Datenbank	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	-Engine. Anweisungen finden Sie in der Amazon RDS-Dokumentation unter Erstellen einer Amazon RDS-DB-Instance.	
Extrahieren Sie Benutzer, Rollen und Berechtigungen.	Extrahieren Sie die Liste der Benutzer, Rollen und Berechtigungen aus der Quelldatenbank.	DBA
Benutzer zuordnen.	Ordnen Sie die vorhanden en Datenbankbenutzer den neuen Datenbankbenutzern zu.	Besitzer der App
Benutzer erstellen.	Benutzer in der Zieldatenbank erstellen.	DBA, Besitzer der App
Rollen anwenden.	Wenden Sie Rollen aus dem vorherigen Schritt auf die Zieldatenbank an.	DBA
Überprüfen Sie Optionen, Parameter, Netzwerkdateien und Datenbanklinks.	Überprüfen Sie die Quelldate nbank auf Optionen, Parameter, Netzwerkdateien und Datenbanklinks und bewerten Sie dann deren Anwendbarkeit auf die Zieldatenbank.	DBA
Einstellungen übernehmen.	Wenden Sie alle relevanten Einstellungen auf die Zieldaten bank an.	DBA

Objekte übertragen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die AWS SCT-Konnektivität.	Konfigurieren Sie die AWS SCT-Konnektivität zur Zieldatenbank.	DBA
Konvertieren Sie das Schema mit AWS SCT.	AWS SCT konvertiert das Quelldatenbankschema und den größten Teil des benutzerdefinierten Codes automatisch in ein Format, das mit der Zieldatenbank kompatibel ist. Jeder Code, den das Tool nicht automatis ch konvertieren kann, ist deutlich gekennzeichnet, sodass Sie ihn manuell konvertieren können.	DBA
Überprüfen Sie den Bericht.	Überprüfen Sie den generiert en SQL-Bericht und speichern Sie alle Fehler und Warnungen.	DBA
Wenden Sie automatische Schemaänderungen an.	Wenden Sie automatische Schemaänderungen auf die Zieldatenbank an oder speichern Sie sie als.sql-Datei.	DBA
Objekte validieren.	Überprüfen Sie, ob AWS SCT die Objekte auf dem Ziel erstellt hat.	DBA
Behandelt Elemente, die nicht konvertiert wurden.	Alle Elemente, die nicht automatisch konvertiert werden konnten, können	DBA, Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	manuell neu geschrieben, zurückgewiesen oder neu gestaltet werden.	
Rollen- und Benutzerb erechtigungen anwenden.	Wenden Sie die generiert en Rollen- und Benutzerb erechtigungen an und überprüfen Sie alle Ausnahmen.	DBA

Migrieren Sie die Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie die Methode.	Ermitteln Sie die Methode für die Datenmigration.	DBA
Erstellen Sie eine Replikati onsinstanz.	Erstellen Sie eine Replikati onsinstanz von der AWS DMS-Konsole aus. Weitere Informationen finden Sie unter Arbeiten mit einer AWS DMS-Replikationsinstanz in der AWS DMS-Dokumentation.	DBA
Erstellen Sie die Quell- und Zielendpunkte.	Um Endpoints zu erstellen, folgen Sie den Anweisungen unter Quell- und Zielendpu nkte erstellen in der AWS DMS-Dokumentation.	DBA
Erstellen Sie eine Replikati onsaufgabe.	Informationen zum Erstellen einer Aufgabe finden Sie unter Arbeiten mit AWS DMS-Aufga	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ben in der AWS DMS-Dokum entation.	
Starten Sie die Replikati onsaufgabe und überwachen Sie die Protokolle.	Weitere Informationen zu diesem Schritt finden Sie unter Überwachung von AWS DMS-Aufgaben in der AWS DMS-Dokumentation.	DBA

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren und konvertie ren Sie SQL-Elemente im Anwendungscode.	Verwenden Sie AWS SCT, um die SQL-Elemente im Anwendungscode zu analysier en und zu konvertieren. Wenn Sie Ihr Datenbankschema von einer Engine in eine andere konvertieren, müssen Sie auch den SQL-Code in Ihren Anwendungen aktualisieren, damit diese mit der neuen Datenbank-Engine anstelle der alten interagieren. Sie können den konvertierten SQL-Code anzeigen, analysier en, bearbeiten und speichern.	Besitzer der App
Anwendungsserver erstellen.	Erstellen Sie die neuen Anwendungsserver auf AWS.	Besitzer der App
Migrieren Sie den Anwendung scode.	Migrieren Sie den Anwendung scode auf die neuen Server.	Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Anwendungsserver.	Konfigurieren Sie die Anwendungsserver für die Zieldatenbank und die Treiber.	Besitzer der App
Code korrigieren.	Korrigieren Sie jeglichen Code, der spezifisch für die Quelldatenbank-Engine in Ihrer Anwendung ist.	Besitzer der App
Code optimieren.	Optimieren Sie Ihren Anwendungscode für die Zieldatenbank-Engine.	Besitzer der App

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wechseln Sie zur Zieldaten bank.	Führen Sie die Umstellung auf die neue Datenbank durch.	DBA
Sperren Sie die Anwendung.	Sperren Sie die Anwendung vor weiteren Änderungen.	Besitzer der App
Änderungen validieren.	Stellen Sie sicher, dass alle Änderungen an die Zieldaten bank weitergegeben wurden.	DBA
Zur Zieldatenbank umleiten.	Verweisen Sie die neuen Anwendungsserver auf die Zieldatenbank.	Besitzer der App
Überprüfe alles.	Führen Sie einen abschließ enden, umfassenden Systemcheck durch.	Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geh live.	Erledigen Sie die letzten Umstellungsaufgaben.	Besitzer der App

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Temporäre Ressourcen abschalten.	Fahren Sie die temporäre n AWS-Ressourcen wie die AWS DMS-Replikationsin stanz und die für AWS SCT verwendete EC2 Instanz herunter.	DBA, Besitzer der App
Feedback aktualisieren.	Aktualisieren Sie das Feedback zum AWS DMS-Prozess für interne Teams.	DBA, Besitzer der App
Überarbeiten Sie den Prozess und die Vorlagen.	Überarbeiten Sie den AWS-DMS-Prozess und verbesser n Sie gegebenenfalls die Vorlage.	DBA, Besitzer der App
Dokumente validieren.	Überprüfen und validieren Sie die Projektdokumente.	DBA, Besitzer der App
Sammeln Sie Metriken.	Sammeln Sie Kennzahlen, um den Zeitaufwand für die Migration, den prozentua len Anteil der manuellen Kosten im Vergleich zu den Werkzeugkosten usw. zu bewerten.	DBA, Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schließt das Projekt.	Schließen Sie das Migration sprojekt ab und geben Sie den Beteiligten Feedback.	DBA, Besitzer der App

Zugehörige Ressourcen

Referenzen

- Verwenden einer Oracle-Datenbank als Quelle für AWS DMS
- Verwenden einer PostgreSQL-Datenbank als Ziel für den AWS Database Migration Service
- Leitfaden zur Migration von Oracle Database 11g/12c zu Amazon Aurora mit PostgreSQL-Kompatibilität (9.6.x)
- Playbook zur Migration von Oracle Database 19c zu Amazon Aurora mit PostgreSQL-Kompatibilität (12.4)
- Migration einer Amazon RDS for Oracle Oracle-Datenbank zur Amazon Aurora PostgreSQL-kompatiblen Edition
- AWS-Datenmigrationsservice
- AWS-Schemakonvertierungstool
- Migrieren Sie von Oracle zu Amazon Aurora
- Amazon-RDS-Preise

Tutorials und Videos

- Step-by-StepExemplarische Vorgehensweisen zur Datenbankmigration
- Erste Schritte mit AWS DMS
- Erste Schritte mit Amazon RDS
- AWS-Datenmigrationsservice (Video)
- Migration einer Oracle-Datenbank zu PostgreSQL (Video)

Zusätzliche Informationen

.

Migrieren Sie Daten von einer lokalen Oracle-Datenbank zu Aurora PostgreSQL

Erstellt von Michelle Deng (AWS) und Shunan Xiang (AWS)

Übersicht

Dieses Muster bietet Anleitungen für die Datenmigration von einer lokalen Oracle-Datenbank zur Amazon Aurora PostgreSQL-Compatible Edition. Es zielt auf eine Online-Datenmigrationsstrategie mit minimalen Ausfallzeiten für Oracle-Datenbanken mit mehreren Terabyte ab, die große Tabellen mit umfangreichen Aktivitäten in der Datenmanipulationssprache (DML) enthalten. Eine Oracle Active Data Guard-Standby-Datenbank wird als Quelle verwendet, um die Datenmigration von der Primärdatenbank auszulagern. Die Replikation von der Oracle-Primärdatenbank zur Standby-Datenbank kann während der Volllast unterbrochen werden, um ORA-01555-Fehler zu vermeiden.

Tabellenspalten in Primärschlüsseln (PKs) oder Fremdschlüsseln (FKs) mit dem Datentyp NUMBER werden in Oracle häufig zum Speichern von Ganzzahlen verwendet. Wir empfehlen, dass Sie diese in PostgreSQL in INT oder BIGINT konvertieren, um eine bessere Leistung zu erzielen. Sie können das AWS Schema Conversion Tool (AWS SCT) verwenden, um die standardmäßige Datentypzuordnung für PK- und FK-Spalten zu ändern. (Weitere Informationen finden Sie im AWS-Blogbeitrag Convert the NUMBER-Datentyp von Oracle nach PostgreSQL.) Die Datenmigration in diesem Muster verwendet AWS Database Migration Service (AWS DMS) sowohl für Volllast als auch für Change Data Capture (CDC).

Sie können dieses Muster auch verwenden, um eine lokale Oracle-Datenbank zu Amazon Relational Database Service (Amazon RDS) für PostgreSQL oder eine Oracle-Datenbank, die auf Amazon Elastic Compute Cloud (Amazon EC2) gehostet wird, entweder zu Amazon RDS for PostgreSQL oder Aurora PostgreSQL-kompatibel zu migrieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle-Quelldatenbank in einem lokalen Rechenzentrum mit konfiguriertem Active Data Guard-Standby
- AWS Direct Connect, konfiguriert zwischen dem lokalen Rechenzentrum und der AWS-Cloud
- Vertrautheit mit der Verwendung einer Oracle-Datenbank als Quelle für AWS DMS
- Vertrautheit mit der Verwendung einer PostgreSQL-Datenbank als Ziel für AWS DMS

Einschränkungen

- Amazon Aurora Aurora-Datenbankcluster können mit bis zu 128 TiB Speicher erstellt werden. Amazon RDS for PostgreSQL PostgreSQL-Datenbank-Instances können mit bis zu 64 TiB Speicher erstellt werden. Die neuesten Speicherinformationen finden Sie in der AWS-Dokumentation unter Amazon Aurora Aurora-Speicher und Zuverlässigkeit und Amazon RDS-DB-Instance-Speicher.

Produktversionen

- AWS DMS unterstützt alle Oracle-Datenbankeditionen für die Versionen 10.2 und höher (für Versionen 10.x), 11g und bis zu 12.2, 18c und 19c. Die aktuelle Liste der unterstützten Versionen finden Sie unter Using an Oracle Database as a Source for AWS DMS in der AWS-Dokumentation.

Architektur

Quelltechnologie-Stack

- Lokale Oracle-Datenbanken mit konfiguriertem Oracle Active Data Guard Standby

Zieltechnologie-Stack

- Aurora PostgreSQL-kompatibel

Architektur für die Datenmigration

Tools

- AWS DMS — AWS Database Migration Service (AWS DMS) unterstützt mehrere Quell- und Zieldatenbanken. Eine Liste der unterstützten Versionen und Editionen der Oracle-Quell- und Zieldatenbank finden Sie unter Verwenden einer Oracle-Datenbank als Quelle für AWS DMS in der AWS DMS-Dokumentation. Wenn die Quelldatenbank nicht von AWS DMS unterstützt wird, müssen Sie in Phase 6 (im Abschnitt Epics) eine andere Methode für die Migration der Daten auswählen. Wichtiger Hinweis: Da es sich um eine heterogene Migration handelt, müssen Sie zunächst prüfen, ob die Datenbank eine kommerzielle off-the-shelf (COTS) Anwendung unterstützt. Wenn es sich bei der Anwendung um COTS handelt, wenden Sie sich an den Hersteller, um zu überprüfen, ob Aurora PostgreSQL-kompatibel unterstützt wird, bevor Sie fortfahren. Weitere

Informationen finden Sie unter AWS DMS Step-by-Step Migration Walkthroughs in der AWS-Dokumentation.

- AWS SCT — Das AWS Schema Conversion Tool (AWS SCT) erleichtert heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist. Der benutzerdefinierte Code, den das Tool konvertiert, umfasst Ansichten, gespeicherte Prozeduren und Funktionen. Jeder Code, den das Tool nicht automatisch konvertieren kann, ist deutlich gekennzeichnet, sodass Sie ihn selbst konvertieren können.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversionen.		DBA
Installieren Sie AWS SCT und die Treiber.		DBA
Fügen Sie die erforderlichen Benutzer und die Quelldatenbank für AWS SCT-Zusch üsse hinzu und validieren Sie sie.		DBA
Erstellen Sie ein AWS SCT-Projekt für den Workload und stellen Sie eine Verbindung zur Quelldatenbank her.		DBA
Erstellen Sie einen Bewertungsbericht und bewerten Sie die Machbarkeit.		DBA, Besitzer der App

Bereiten Sie die Zieldatenbank vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Aurora PostgreSQL-kompatible Zieldatenbank.		DBA
Extrahieren Sie die Liste der Benutzer, Rollen und Berechtigungen aus der Quelldatenbank.		DBA
Ordnen Sie die vorhanden en Datenbankbenutzer den neuen Datenbankbenutzern zu.		Besitzer der App
Erstellen Sie Benutzer in der Zieldatenbank.		DBA
Wenden Sie Rollen aus dem vorherigen Schritt auf die Aurora PostgreSQL-kompati ble Zieldatenbank an.		DBA
Überprüfen Sie die Datenbank optionen, Parameter , Netzwerkdateien und Datenbank-Links aus der Quelldatenbank und bewerten Sie deren Anwendbarkeit auf die Zieldatenbank.		DBA, Besitzer der App
Wenden Sie alle relevanten Einstellungen auf die Zieldaten bank an.		DBA

Bereiten Sie sich auf die Konvertierung des Datenbankobjektcodes vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die AWS SCT-Konnektivität zur Zieldatenbank.		DBA
Konvertieren Sie das Schema in AWS SCT und speichern Sie den konvertierten Code als.sql-Datei.		DBA, Besitzer der App
Konvertieren Sie manuell alle Datenbankobjekte, die nicht automatisch konvertiert werden konnten.		DBA, Besitzer der App
Optimieren Sie die Konvertie rung des Datenbankcodes.		DBA, Besitzer der App
Teilen Sie die .sql-Date i je nach Objekttyp in mehrere .sql-Dateien auf.		DBA, Besitzer der App
Validieren Sie die SQL-Skripts in der Zieldatenbank.		DBA, Besitzer der App

Bereiten Sie sich auf die Datenmigration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS DMS-Replikations-Instance.		DBA
Erstellen Sie die Quell- und Zielendpunkte.	Wenn der Datentyp von PKs und von NUMBER in Oracle in BIGINT in PostgreSQL	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	konvertiert FKs wird, sollten Sie das Verbindungsattribu t angeben, `numberDat aTypeScale=-2` wenn Sie den Quellendpunkt erstellen.	

Daten migrieren — Volllast

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Schema und die Tabellen in der Zieldaten bank.		DBA
Erstellen Sie AWS DMS-Volllastaufgaben, indem Sie entweder Tabellen gruppiere n oder eine große Tabelle basierend auf der Tabelleng röße aufteilen.		DBA
Stoppen Sie die Anwendung en in den Oracle-Quelldatenb anken für einen kurzen Zeitraum.		Besitzer der App
Stellen Sie sicher, dass die Oracle-Standby-Datenbank mit der Primärdatenbank synchron ist, und beenden Sie die Replikation von der Primärdatenbank zur Standby-Datenbank.		DBA, Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie Anwendungen in der Oracle-Quelldatenbank.		Besitzer der App
Starten Sie die AWS DMS-Volllastaufgaben parallel von der Oracle-Standby-Datenbank zur Aurora PostgreSQL-kompatiblen Datenbank.		DBA
Erstellen Sie PKs und sekundäre Indizes, nachdem der vollständige Ladevorgang abgeschlossen ist.		DBA
Validieren Sie die Daten.		DBA

Daten migrieren — CDC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie fortlaufende AWS DMS-Replikationsaufgaben, indem Sie eine benutzerdefinierte CDC-Startzeit oder eine Systemänderungsnummer (SCN) angeben, als der Oracle-Standby mit der Primärdatenbank synchronisiert wurde und bevor die Anwendungen in der vorherigen Aufgabe neu gestartet wurden.		DBA
Starten Sie AWS DMS-Aufgaben parallel, um laufende		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Änderungen von der Oracle-Standby-Datenbank in die Aurora PostgreSQL-kompatible Datenbank zu replizieren.		
Stellen Sie die Replikation von der Oracle-Primärdatenbank zur Standby-Datenbank wieder her.		DBA
Überwachen Sie die Protokolle und beenden Sie die Anwendungen in der Oracle-Datenbank, wenn die Aurora PostgreSQL-kompatible Zieldatenbank fast synchron mit der Oracle-Quelldatenbank ist.		DBA, Besitzer der App
Beenden Sie die AWS DMS-Aufgaben, wenn das Ziel vollständig mit der Oracle-Quelldatenbank synchronisiert ist.		DBA
Erstellen FKs und validieren Sie die Daten in der Zieldatenbank.		DBA
Erstellen Sie Funktionen, Ansichten, Trigger, Sequenzen und andere Objekttypen in der Zieldatenbank.		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wenden Sie Rollenzuw eisungen in der Zieldatenbank an.		DBA

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie AWS SCT, um die SQL-Anweisungen im Anwendungscode zu analysier en und zu konvertieren.		Besitzer der App
Erstellen Sie neue Anwendung sserver auf AWS.		Besitzer der App
Migrieren Sie den Anwendung scode auf die neuen Server.		Besitzer der App
Konfigurieren Sie den Anwendungsserver für die Zieldatenbank und die Treiber.		Besitzer der App
Korrigieren Sie jeglichen Code, der für die Quelldate nbank-Engine in der Anwendung spezifisch ist.		Besitzer der App
Optimieren Sie den Anwendungscode für die Zieldatenbank.		Besitzer der App

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verweisen Sie den neuen Anwendungsserver auf die Zieldatenbank.		DBA, Besitzer der App
Führen Sie Plausibilitätsprüf ungen durch.		DBA, Besitzer der App
Geh live.		DBA, Besitzer der App

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre AWS-Ressourcen herunter.		DBA, Systemadministrator
Überprüfen und validieren Sie die Projektdokumente.		DBA, Besitzer der App
Erfassen Sie Kennzahlen zur Zeit bis zur Migration, zum Prozentsatz der manuellen Nutzung im Vergleich zu den Tools, zu Kosteneinsparungen und ähnlichen Daten.		DBA, Besitzer der App
Schließen Sie das Projekt ab und geben Sie Feedback.		DBA, Besitzer der App

Zugehörige Ressourcen

Referenzen

- PostgreSQL-kompatibel mit Oracle Database zu Aurora: Leitfaden zur Migration

- Migration einer Amazon RDS for Oracle Database zu Amazon Aurora MySQL
- AWS DMS-Webseite
- AWS DMS-Dokumentation
- AWS SCT-Webseite
- AWS SCT-Dokumentation
- Migrieren Sie von Oracle zu Amazon Aurora

Tutorials

- Erste Schritte mit AWS DMS
- Erste Schritte mit Amazon RDS
- Step-by-StepExemplarische Vorgehensweisen zum AWS Database Migration Service

Migrieren Sie mithilfe von AWS DMS von SAP ASE zu Amazon RDS for SQL Server

Erstellt von Amit Kumar (AWS)

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer SAP Adaptive Server Enterprise (ASE) -Datenbank auf eine Amazon Relational Database Service (Amazon RDS) -DB-Instance, auf der Microsoft SQL Server ausgeführt wird. Die Quelldatenbank kann sich in einem lokalen Rechenzentrum oder auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance befinden. Das Muster verwendet AWS Database Migration Service (AWS DMS) zur Migration von Daten und (optional) Tools zur Computer-Aided Software Engineering (CASE) zur Konvertierung des Datenbankschemas.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine SAP ASE-Datenbank in einem lokalen Rechenzentrum oder auf einer Instanz EC2
- Eine Amazon RDS for SQL Server Server-Zieldatenbank, die läuft

Einschränkungen

- Größenbeschränkung der Datenbank: 64 TB

Produktversionen

- Nur SAP ASE-Version 15.7 oder 16.x. Aktuelle Informationen finden Sie unter Verwenden einer SAP-Datenbank als Quelle für AWS DMS.
- Für Amazon RDS-Zieldatenbanken unterstützt AWS DMS Microsoft SQL Server-Versionen auf Amazon RDS für die Enterprise-, Standard-, Web- und Express-Editionen. Aktuelle Informationen zu unterstützten Versionen finden Sie in der AWS DMS-Dokumentation. Wir empfehlen Ihnen, die neueste Version von AWS DMS zu verwenden, um die umfassendste Version von Versionen und Funktionen zu erhalten.

Architektur

Quelltechnologie-Stack

- Eine SAP ASE-Datenbank, die sich vor Ort oder auf einer EC2 Amazon-Instance befindet

Zieltechnologie-Stack

- Eine Amazon RDS for SQL Server Server-DB-Instance

Quell- und Zielarchitektur

Von einer SAP ASE-Datenbank auf Amazon EC2 zu einer Amazon RDS for SQL Server-DB-Instance:

Von einer lokalen SAP ASE-Datenbank zu einer Amazon RDS for SQL Server-DB-Instance:

Tools

- AWS Database Migration Service (AWS DMS) ist ein Webservice, mit dem Sie Daten aus Ihrer lokalen Datenbank, auf einer Amazon RDS-DB-Instance oder in einer Datenbank auf einer Instance in eine Datenbank auf einem AWS-Service wie Amazon RDS for SQL Server oder einer EC2 EC2 Instance migrieren können. Sie können eine Datenbank auch von einem AWS-Service zu einer lokalen Datenbank migrieren. Sie können Daten zwischen heterogenen oder homogenen Datenbank-Engines migrieren.
- Für Schemakonvertierungen können Sie optional Erwin Data Modeler oder SAP verwenden. PowerDesigner

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversionen.		DBA
Identifizieren Sie die Speicheranforderungen (Speichertyp und Kapazität).		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie den richtigen Instanztyp auf der Grundlage von Kapazität, Speicherf unktionen und Netzwerkf unktionen aus.		DBA, SysAdmin
Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.		DBA, SysAdmin
Identifizieren Sie die Strategie zur Anwendungsmigration.		DBA SysAdmin, Besitzer der App

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine virtuelle private Cloud (VPC) und Subnetze.		SysAdmin
Erstellen Sie Sicherhei tsgruppen und Netzwerkz ugriffskontrolllisten ()ACLs.		SysAdmin
Konfigurieren und starten Sie eine Amazon RDS-DB-In stance.		SysAdmin

Daten migrieren — Option 1

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie das Datenbank schema manuell oder verwenden Sie ein CASE-Tool wie Erwin Data Modeler oder SAP. PowerDesigner		DBA

Daten migrieren — Option 2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie Daten mit AWS DMS.		DBA

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Anwendungsmigration.		DBA SysAdmin, Besitzer der App

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung sclients auf die neue Infrastru ktur um.		DBA SysAdmin, Besitzer der App

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die temporären AWS-Ressourcen herunter.		DBA, SysAdmin
Überprüfen und validieren Sie die Projektdokumente.		DBA SysAdmin, Besitzer der App
Erfassen Sie Kennzahlen wie die Zeit bis zur Migration , den Prozentsatz manueller Aufgaben im Vergleich zu automatisierten Aufgaben und Kosteneinsparungen.		DBA SysAdmin, Besitzer der App
Schließen Sie das Projekt ab und geben Sie Feedback.		DBA SysAdmin, Besitzer der App

Zugehörige Ressourcen

Referenzen

- AWS DMS-Webseite
- Amazon RDS — Preise
- Verwenden einer SAP ASE-Datenbank als Quelle für AWS DMS
- Einschränkungen für RDS Custom for SQL Server

Tutorials und Videos

- Erste Schritte mit AWS DMS
- Erste Schritte mit Amazon RDS
- AWS DMS (Video)
- Amazon RDS (Video)

Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mit AWS DMS zu Amazon Redshift

Erstellt von Marcelo Fernandes (AWS)

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer lokalen Microsoft SQL Server-Datenbank zu Amazon Redshift mithilfe von AWS Data Migration Service (AWS DMS).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Microsoft SQL Server-Quelldatenbank in einem lokalen Rechenzentrum
- Erledigte Voraussetzungen für die Verwendung einer Amazon Redshift Redshift-Datenbank als Ziel für AWS DMS, wie in der AWS DMS-Dokumentation beschrieben

Produktversionen

- SQL Server 2005-2019, Enterprise, Standard, Workgroup, Developer und Web. Die aktuelle Liste der unterstützten Versionen finden Sie in der AWS-Dokumentation unter Verwenden einer Microsoft SQL Server-Datenbank als Quelle für AWS DMS.

Architektur

Quelltechnologie-Stack

- Eine lokale Microsoft SQL Server-Datenbank

Zieltechnologie-Stack

- Amazon Redshift

Architektur der Datenmigration

Tools

- AWS DMS ist ein Datenmigrationsservice, der verschiedene Arten von Quell- und Zieldatenbanken unterstützt. Informationen zu den Microsoft SQL Server-Datenbankversionen und -Editionen, die für die Verwendung mit AWS DMS unterstützt werden, finden Sie unter Verwenden einer Microsoft SQL Server-Datenbank als Quelle für AWS DMS in der AWS DMS-Dokumentation. Wenn AWS DMS Ihre Quelldatenbank nicht unterstützt, müssen Sie eine alternative Methode für die Datenmigration auswählen.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversion und die Engine.		DBA
Identifizieren Sie die Hardwareanforderungen für die Zielserverinstanz.		DBA, Systemadministrator
Identifizieren Sie die Speicheranforderungen (Speichertyp und Kapazität).		DBA, Systemadministrator
Wählen Sie den richtigen Instanztyp auf der Grundlage von Kapazität, Speicherf unktionen und Netzwerkf unktionen aus.		DBA, Systemadministrator
Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.		DBA, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Strategie zur Anwendungsmigration.		DBA, App-Besitzer, Systemadministrator

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC).	Weitere Informationen finden Sie in der AWS-Dokum entation unter Arbeiten mit einer DB-Instance in einer VPC.	Systemadministrator
Erstellen Sie Sicherhei tsgruppen.		Systemadministrator
Konfigurieren und starten Sie einen Amazon Redshift Redshift-Cluster.	Weitere Informationen finden Sie unter Erstellen eines Amazon Redshift Redshift-Beispiel-Clusters in der Amazon Redshift Redshift-Dokumentation.	DBA, Systemadministrator

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie die Daten mithilfe von AWS DMS aus der Microsoft SQL Server-Da tenbank.		DBA

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Anwendungsmigration.		DBA, App-Besitzer, Systemadministrator

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung sclients auf die neue Infrastru ktur um.		DBA, App-Besitzer, Systemadministrator

Schließen Sie das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die temporären Ressourcen herunter.		DBA, Systemadministrator
Überprüfen und validieren Sie die Projektdokumente.		DBA, App-Besitzer, Systemadministrator
Erfassen Sie Kennzahlen wie die Zeit bis zur Migration , den Prozentsatz manueller Aufgaben im Vergleich zu automatisierten Aufgaben und Kosteneinsparungen.		DBA, App-Besitzer, Systemadministrator
Schließen Sie das Projekt ab und geben Sie Feedback.		DBA, App-Besitzer, Systemadministrator

Zugehörige Ressourcen

Referenzen

- AWS DMS-Dokumentation
- Amazon Redshift Redshift-Dokumentation
- Amazon Redshift — Preise

Tutorials und Videos

- Erste Schritte mit AWS DMS
- Erste Schritte mit Amazon Redshift
- Verwenden einer Amazon Redshift Redshift-Datenbank als Ziel für den AWS Database Migration Service
- AWS DMS (Video)

Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mithilfe von AWS SCT-Datenextraktionsagenten zu Amazon Redshift

Erstellt von Neha Thakur (AWS)

Übersicht

Dieses Muster beschreibt die Schritte für die Migration einer lokalen Microsoft SQL Server-Quelldatenbank zu einer Amazon Redshift Redshift-Zieldatenbank mithilfe der Datenextraktionsagenten des AWS Schema Conversion Tool (AWS SCT). Ein Agent ist ein externes Programm, das in AWS SCT integriert ist, die Datentransformation jedoch an anderer Stelle durchführt und in Ihrem Namen mit anderen AWS-Services interagiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Microsoft SQL Server-Quelldatenbank, die für die Data Warehouse-Arbeitslast in einem lokalen Rechenzentrum verwendet wird
- Ein aktives AWS-Konto

Produktversionen

- Microsoft SQL Server Version 2008 oder höher. Die aktuelle Liste der unterstützten Versionen finden Sie in der AWS SCT-Dokumentation.

Architektur

Technologie-Stack: Quelle

- Eine lokale Microsoft SQL Server-Datenbank

Technologie-Stack Target

- Amazon Redshift

Architektur der Datenmigration

Tools

- Das AWS Schema Conversion Tool (AWS SCT) verarbeitet heterogene Datenbankmigrationen, indem es das Quelldatenbankschema und einen Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert, das mit der Zieldatenbank kompatibel ist. Wenn die Quell- und Zieldatenbanken sehr unterschiedlich sind, können Sie einen AWS SCT-Agenten verwenden, um zusätzliche Datentransformationen durchzuführen. Weitere Informationen finden Sie in der AWS-Dokumentation unter Migrieren von Daten aus einem lokalen Data Warehouse zu Amazon Redshift.

Bewährte Methoden

- Bewährte Methoden für AWS SCT
- Bewährte Methoden für Amazon Redshift

Epen

Bereiten Sie sich auf die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Versionen und Engines der Quell- und Zieldatenbank.		DBA
Identifizieren Sie die Hardwareanforderungen für die Zielserverinstanz.		DBA, SysAdmin
Identifizieren Sie die Speicheranforderungen (Speichertyp und Kapazität).		DBA, SysAdmin
Wählen Sie den richtigen Instanztyp (Kapazität, Speicherfunktionen, Netzwerkfunktionen).		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Sicherheitsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.		DBA, SysAdmin
Wählen Sie eine Strategie für die Anwendungsmigration.		DBA SysAdmin, Besitzer der App

Infrastruktur konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine virtuelle private Cloud (VPC) und Subnetze.		SysAdmin
Erstellen Sie Sicherheitsgruppen.		SysAdmin
Konfigurieren und starten Sie den Amazon Redshift Redshift-Cluster.		SysAdmin

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie die Daten mithilfe der AWS SCT-Daten extraktionsagenten.		DBA

Anwendungen migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der ausgewählten Strategie zur Anwendungsmigration.		DBA SysAdmin, Besitzer der App

Wechseln Sie zur Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendungsclients auf die neue Infrastruktur um.		DBA SysAdmin, Besitzer der App

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre AWS-Ressourcen herunter.		DBA, SysAdmin
Überprüfen und validieren Sie die Projektdokumente.		DBA SysAdmin, Besitzer der App
Erfassen Sie Kennzahlen wie die Zeit bis zur Migration, den Prozentsatz manueller Aufgaben im Vergleich zu automatisierten Aufgaben und Kosteneinsparungen.		DBA SysAdmin, Besitzer der App
Schließen Sie das Projekt und geben Sie Feedback.		DBA SysAdmin, Besitzer der App

Zugehörige Ressourcen

Referenzen

- AWS SCT-Benutzerhandbuch
- Verwendung von Datenextraktionsagenten
- Amazon Redshift — Preise

Tutorials und Videos

- Erste Schritte mit dem AWS Schema Conversion Tool
- Erste Schritte mit Amazon Redshift

Migrieren Sie eine Teradata-Datenbank mithilfe von AWS SCT-Datenextraktionsagenten zu Amazon Redshift

Erstellt von Sergey Dmitriev (AWS)

Übersicht

Dieses Muster führt Sie durch die Schritte zur Migration einer Teradata-Datenbank, die als Data Warehouse in einem lokalen Rechenzentrum verwendet wird, zu einer Amazon Redshift Redshift-Datenbank. Das Muster verwendet Datenextraktionsagenten des AWS Schema Conversion Tool (AWS SCT). Ein Agent ist ein externes Programm, das in AWS SCT integriert ist, die Datentransformation jedoch an anderer Stelle durchführt und in Ihrem Namen mit anderen AWS-Services interagiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Teradata-Quelldatenbank in einem lokalen Rechenzentrum

Produktversionen

- Teradata Version 13 und höher. Die aktuelle Liste der unterstützten Versionen finden Sie in der AWS SCT-Dokumentation.

Architektur

Quelltechnologie-Stack

- Lokale Teradata-Datenbank

Zieltechnologie-Stack

- Amazon-Redshift-Cluster

Architektur der Datenmigration

Tools

- AWS SCT — Das AWS Schema Conversion Tool (AWS SCT) verarbeitet heterogene Datenbankmigrationen, indem es das Quelldatenbankschema und einen Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert, das mit der Zieldatenbank kompatibel ist. Wenn sich die Quell- und Zieldatenbanken stark voneinander unterscheiden, können Sie einen AWS SCT-Agenten verwenden, um zusätzliche Datentransformationen durchzuführen. Weitere Informationen finden Sie in der AWS-Dokumentation unter Migrieren von Daten aus einem lokalen Data Warehouse zu Amazon Redshift.

Epen

Bereiten Sie sich auf die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Versionen und Engines der Quell- und Zieldatenbank.		DBA
Identifizieren Sie die Hardwareanforderungen für die Zielserverinstanz.		DBA, SysAdmin
Identifizieren Sie die Speicheranforderungen (Speichertyp und Kapazität).		DBA, SysAdmin
Wählen Sie den richtigen Instanztyp (Kapazität, Speicherfunktionen, Netzwerkfunktionen).		DBA, SysAdmin
Identifizieren Sie die Sicherheitsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie eine Strategie für die Anwendungsmigration.		DBA SysAdmin, Besitzer der App

Infrastruktur konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine virtuelle private Cloud (VPC) und Subnetze.		SysAdmin
Erstellen Sie Sicherhei tsgruppen.		SysAdmin
Konfigurieren und starten Sie den Amazon Redshift Redshift-Cluster.		SysAdmin

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie Daten mithilfe von AWS SCT-Datenextraktio nsagenten.	Detaillierte Informationen zur Verwendung von AWS SCT-Datenextraktionsagenten finden Sie unter den Links im Abschnitt Referenzen und Hilfe.	DBA

Anwendungen migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der ausgewähl ten Strategie zur Anwendung smigration.		DBA SysAdmin, Besitzer der App

Wechseln Sie zur Amazon Redshift Redshift-Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung sclients auf die neue Infrastru ktur um.		DBA SysAdmin, Besitzer der App

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre AWS-Ressourcen herunter.		DBA, SysAdmin
Überprüfen und validieren Sie die Projektdokumente.		DBA SysAdmin, Besitzer der App
Sammeln Sie Kennzahlen zur Zeit bis zur Migration, zum Prozentsatz manueller Aufgaben im Vergleich zu Toolaufgaben, zu Kostenein sparungen usw.		DBA SysAdmin, Besitzer der App
Schließen Sie das Projekt und geben Sie Feedback.		

Zugehörige Ressourcen

Referenzen

- AWS SCT-Benutzerhandbuch
- Verwendung von Datenextraktionsagenten
- Amazon Redshift — Preise
- Konvertieren Sie die Teradata RESET WHEN-Funktion auf Amazon Redshift SQL (AWS Prescriptive Guidance)
- Konvertieren Sie die temporale Funktion Teradata NORMALIZE in Amazon Redshift SQL (AWS Prescriptive Guidance)

Tutorials

- Erste Schritte mit dem AWS Schema Conversion Tool
- Erste Schritte mit Amazon Redshift

Migrieren Sie eine lokale Vertica-Datenbank mithilfe von AWS SCT-Datenextraktionsagenten zu Amazon Redshift

Erstellt von Sergey Dmitriev (AWS)

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer lokalen Vertica-Datenbank zu einem Amazon Redshift Redshift-Cluster mithilfe der Datenextraktionsagenten des AWS Schema Conversion Tool (AWS SCT). Ein Agent ist ein externes Programm, das in AWS SCT integriert ist, die Datentransformation jedoch an anderer Stelle durchführt und in Ihrem Namen mit anderen AWS-Services interagiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Vertica-Quelldatenbank, die für die Data Warehouse-Arbeitslast in einem lokalen Rechenzentrum verwendet wird
- Ein Amazon Redshift Redshift-Zielcluster

Produktversionen

- Vertica Version 7.2.2 und höher. Die aktuelle Liste der unterstützten Versionen finden Sie in der AWS SCT-Dokumentation.

Architektur

Quelltechnologie-Stack

- Eine lokale Vertica-Datenbank

Zieltechnologie-Stack

- Ein Amazon Redshift Redshift-Cluster

Architektur der Datenmigration

Tools

- Das AWS Schema Conversion Tool (AWS SCT) verarbeitet heterogene Datenbankmigrationen, indem es das Quelldatenbankschema und einen Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert, das mit der Zieldatenbank kompatibel ist. Wenn sich die Quell- und Zieldatenbanken stark voneinander unterscheiden, können Sie einen AWS SCT-Agenten verwenden, um zusätzliche Datentransformationen durchzuführen. Weitere Informationen finden Sie in der AWS-Dokumentation unter Migrieren von Daten aus einem lokalen Data Warehouse zu Amazon Redshift.

Epen

Bereiten Sie sich auf die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Quell- und Zieldatenbankversionen.		DBA
Identifizieren Sie die Speicheranforderungen (Speichertyp und Kapazität).		DBA, SysAdmin
Wählen Sie den richtigen Instanztyp (Kapazität, Speicherfunktionen, Netzwerkfunktionen).		DBA, SysAdmin
Identifizieren Sie die Sicherheitsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.		DBA, SysAdmin
Wählen Sie eine Strategie für die Anwendungsmigration.		DBA SysAdmin, Besitzer der App

Infrastruktur konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine virtuelle private Cloud (VPC) und Subnetze.		SysAdmin
Erstellen Sie Sicherhei tsgruppen.		SysAdmin
Konfigurieren und starten Sie einen Amazon Redshift Redshift-Cluster.		SysAdmin

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie die Daten mithilfe der AWS SCT-Daten extraktionsagenten.	Detaillierte Informationen zur Verwendung von AWS SCT-Datenextraktionsagenten finden Sie unter den Links im Abschnitt Referenzen und Hilfe.	DBA

Anwendungen migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der ausgewähl ten Strategie zur Anwendung smigration.		DBA SysAdmin, Besitzer der App

Wechseln Sie zur Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung sclients auf die neue Infrastru ktur um.		DBA SysAdmin, Besitzer der App

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre AWS-Ressourcen herunter.		DBA, SysAdmin
Überprüfen und validieren Sie die Projektdokumente.		DBA SysAdmin, Besitzer der App
Sammeln Sie Kennzahlen zur Zeit bis zur Migration, zum Prozentsatz manueller Aufgaben im Vergleich zu Toolaufgaben, zu Kostenein sparungen usw.		DBA SysAdmin, Besitzer der App
Schließen Sie das Projekt und geben Sie Feedback.		

Zugehörige Ressourcen

Referenzen

- AWS SCT-Benutzerhandbuch
- Verwendung von Datenextraktionsagenten
- Amazon Redshift — Preise

Tutorials und Videos

- Erste Schritte mit dem AWS Schema Conversion Tool
- Erste Schritte mit Amazon Redshift

Migrieren Sie Legacy-Anwendungen von Oracle Pro*C zu ECPG

Erstellt von Sai Parthasaradhi (AWS) und Mahesh Balumuri (AWS)

Übersicht

Die meisten älteren Anwendungen mit eingebettetem SQL-Code verwenden den Oracle Pro*C-Precompiler für den Zugriff auf die Datenbank. Wenn Sie diese Oracle-Datenbanken zu Amazon Relational Database Service (Amazon RDS) for PostgreSQL oder Amazon Aurora PostgreSQL-Compatible Edition migrieren, müssen Sie Ihren Anwendungscode in ein Format konvertieren, das mit dem Precompiler in PostgreSQL kompatibel ist, das als ECPG bezeichnet wird. Dieses Muster beschreibt, wie Oracle Pro*C-Code in sein Äquivalent in PostgreSQL ECPG konvertiert wird.

Weitere Informationen zu Pro*C finden Sie in der Oracle-Dokumentation. Eine kurze Einführung in ECPG finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Amazon RDS for PostgreSQL- oder Aurora PostgreSQL-kompatible Datenbank
- Eine Oracle-Datenbank, die vor Ort läuft

Tools

- Die im nächsten Abschnitt aufgeführten PostgreSQL-Pakete.
- AWS CLI — Die AWS-Befehlszeilenschnittstelle (AWS CLI) ist ein Open-Source-Tool für die Interaktion mit AWS-Services über Befehle in Ihrer Befehlszeilen-Shell. Mit minimaler Konfiguration können Sie AWS-CLI-Befehle, die Funktionen implementieren, die denen entsprechen, die von der browserbasierten AWS-Managementkonsole bereitgestellt werden, von einer Befehlszeile aus ausführen.

Epen

Stellen Sie die Build-Umgebung auf CentOS oder RHEL ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie PostgreSQL-Pakete.	Installieren Sie die erforderl ichen PostgreSQL-Pakete mithilfe der folgenden Befehle.
	`yum update -y`
	`yum install -y yum-utils`
	`rpm -ivh https://download.postgresql.org/pub/repos/yum/reporpms/EL-8-x86_64/pgdg-redhat-repo-latest.noarch.rpm`
	`dnf -qy module disable postgresql`
		App-Entwickler, Ingenieur DevOps

Installieren Sie die Header-Dateien und Bibliotheken.	Installieren Sie das `postgresql12-devel` Paket, das Header-Dateien und Bibliotheken enthält, mithilfe der folgenden Befehle. Installieren Sie das Paket sowohl in der Entwicklungs- als auch in der Laufzeitumgebung, um Fehler in der Laufzeitumgebung zu vermeiden.
	`dnf -y install postgresql12-devel`
	`yum install ncompress zip ghostscript jq unzip wget git -y`
		App-Entwickler, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Führen Sie nur für die Entwicklungsumgebung auch die folgenden Befehle aus.
	`yum install zlib-devel make -y`
	`ln -s /usr/pgsql-12/bin/ecpg /usr/bin/`	

Konfigurieren Sie die Umgebungspfadvariable.	Legen Sie den Umgebungspfad für PostgreSQL-Clientbibliotheken fest. `export PATH=$PATH:/usr/pgsql-12/bin`	App-Entwickler, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie bei Bedarf zusätzliche Software.	Falls erforderlich, installieren Sie PGLoader als Ersatz für SQL*Loader in Oracle.
	`wget -O /etc/yum.repos.d/pgloader-ccl.repo https://dl.packager.io/srv/opf/pgloader-ccl/master/installer/el/7.repo`
	`yum install pgloader-ccl -y`
	`ln -s /opt/pgloader-ccl/bin/pgloader /usr/bin/`
	Wenn Sie Java-Anwendungen von Pro*C-Modulen aus aufrufen, installieren Sie Java.
	`yum install java -y`
	Installieren Sie Ant, um den Java-Code zu kompilieren.
	`yum install ant -y`
		App-Entwickler, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie den AWS CLI.	Installieren Sie die AWS-CLI, um Befehle zur Interaktion mit AWS-Services wie AWS Secrets Manager und Amazon Simple Storage Service (Amazon S3) von Ihren Anwendungen aus auszuführen.
	`cd /tmp/`
	`curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"`
	`unzip awscliv2.zip`
	`./aws/install -i /usr/local/aws-cli -b /usr/local/bin --update`
		App-Entwickler, DevOps Ingenieur

Identifizieren Sie die Programme, die konvertiert werden sollen.	Identifizieren Sie die Anwendungen, die Sie von Pro*C nach ECPG konvertieren möchten.	App-Entwickler, App-Besitzer

Pro*C-Code nach ECPG konvertieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Unerwünschte Header entfernen.	Entfernen Sie die `include` Header, die in PostgreSQL nicht erforderlich sind, wie`oci.h`, und`oratypes.sqlda`	App-Besitzer, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Variablendeklarationen aktualisieren.	Fügen Sie `EXEC SQL` Anweisungen für alle Variablendeklarationen hinzu, die als Hostvariablen verwendet werden. Entfernen Sie die `EXEC SQL VAR` Deklarationen wie die folgenden aus Ihrer Anwendung. `EXEC SQL VAR query IS STRING(2048);`	App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisieren Sie die ROWNUM-Funktionalität.	Die `ROWNUM` Funktion ist in PostgreSQL nicht verfügbar . Ersetzen Sie dies in SQL-Abfragen durch die `ROW_NUMBER` Fensterfu nktion.
	
	Pro*C-Code:
	
	`SELECT SUBSTR(RT RIM(FILE_NAME,'.tx t'),12) INTO :gcpclFil eseq FROM (SELECT FILE_NAME FROM DEMO_FILES_TABLE WHERE FILE_NAME LIKE '%POC%' ORDER BY FILE_NAME DESC) FL2 WHERE ROWNUM <=1 ORDER BY ROWNUM;`
	
	ECPG-Kode:
	
	`SELECT SUBSTR(RT RIM(FILE_NAME,'.tx t'),12) INTO :gcpclFil eseq FROM (SELECT FILE_NAME , ROW_NUMBE R() OVER (ORDER BY FILE_NAME DESC) AS ROWNUM FROM demo_sche ma.DEMO_FILES_TABLE WHERE FILE_NAME LIKE '%POC%'`
		App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`ORDER BY FILE_NAME DESC) FL2 WHERE ROWNUM <=1 ORDER BY ROWNUM;`	

Aktualisieren Sie die Funktionsparameter, um Aliasvariablen zu verwenden.	In PostgreSQL können Funktionsparameter nicht als Hostvariablen verwendet werden. Überschreiben Sie sie mithilfe einer Aliasvariablen.
	
	Pro*C-Code:
	
	`int processData(int referenceId){ EXEC SQL char col_val[100]; EXEC SQL select column_name INTO :col_val from table_name where col=:referenceId; }`
	
	ECPG-Kode:
	
	`int processData(int referenceIdParam){ EXEC SQL int referenceId = referenceIdParam; EXEC SQL char col_val[100]; EXEC SQL select column_name INTO :col_val from table_name where col=:referenceId; }`
		App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Strukturtypen.	Definieren Sie `struct` Typen in `EXEC SQL BEGIN` und `END` Blöcke mit`typedef`, wenn die `struct` Typvariablen als Hostvariablen verwendet werden. Wenn die `struct` Typen in Header (`.h`) -Dateien definiert sind, schließen Sie die Dateien mit `EXEC SQL` Include-Anweisungen ein. Pro*C-Code: Header-Datei () `demo.h` `struct s_partiti on_ranges { char sc_table_ group[31]; char sc_table_ name[31]; char sc_range_ value[10]; }; struct s_partiti on_ranges_ind { short ss_table_ group; short ss_table_ name; short ss_range_ value; };` ECPG-Code: Header-Datei () `demo.h`	App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
EXEC SQL BEGIN DECLARE
 SECTION;
typedef struct
{
  char   sc_table_
group[31];
  char   sc_table_
name[31];
  char   sc_range_
value[10];
} s_partition_ranges;
typedef struct
{
  short    ss_table_
group;
  short    ss_table_
name;
  short    ss_range_
value;
} s_partition_ranges
_ind;
EXEC SQL END DECLARE
 SECTION;
```

Pro*C-Datei () `demo.pc`

```
#include "demo.h"
struct s_partiti
on_ranges gc_partit
ion_data[MAX_PART_
TABLE] ;
struct s_partiti
on_ranges_ind
 gc_partition_data_
ind[MAX_PART_TABLE] ;
```

ECPG-Datei () `demo.pc`

```
exec sql include
 "demo.h"
```

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`EXEC SQL BEGIN DECLARE SECTION; s_partition_ranges gc_partition_data[ MAX_PART_TABLE] ; s_partition_ranges_ind gc_partition_data_ ind[MAX_PART_TABLE] ; EXEC SQL END DECLARE SECTION;`	

Ändern Sie die Logik, um von Cursorn abzurufen.	Um mithilfe von Array-Var iablen mehrere Zeilen aus Cursorn abzurufen, ändern Sie den zu verwendenden Code. `FETCH FORWARD`
	
	Pro*C-Code:
	
	`EXEC SQL char aPoeFiles [MAX_FILES][FILENA ME_LENGTH]; EXEC SQL FETCH filename_ cursor into :aPoeFile s;`
	
	ECPG-Kode:
	
	`EXEC SQL char aPoeFiles [MAX_FILES][FILENA ME_LENGTH]; EXEC SQL int fetchSize = MAX_FILES; EXEC SQL FETCH FORWARD :fetchSiz e filename_cursor into :aPoeFiles;`
		App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Ändern Sie Paketaufrufe, die keine Rückgabewerte haben.	Oracle-Paketfunktionen, die keine Rückgabewerte haben, sollten mit einer Indikator variablen aufgerufen werden. Wenn Ihre Anwendung mehrere Funktionen mit demselben Namen enthält oder wenn die Funktionen unbekannter Typen Laufzeitf ehler erzeugen, typisieren Sie die Werte in die Datentypen.
	
	Pro*C-Code:
	
	`void ProcessData (char *data , int id) { EXEC SQL EXECUTE BEGIN pkg_demo. process_data (:data, :id); END; END-EXEC; }`
	
	ECPG-Kode:
	
	`void ProcessData (char *dataParam, int idParam ) { EXEC SQL char *data = dataParam;`
		App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>EXEC SQL int id
	= idParam;
	EXEC SQL short
	rowInd;
	EXEC SQL short
	rowInd = 0;
	EXEC SQL SELECT
	pkg_demo.process_data
	(
	
	inp_data => :data::te
	xt,
	
	inp_id => :id
	)
	INTO :rowInd;
	}</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Schreiben Sie SQL_CURSOR-Variablen neu.	Schreiben Sie die `SQL_CURSOR` Variable und ihre Implementierung neu.
	
	Pro*C-Code:
	
	`/* SQL Cursor */`
	`SQL_CU`
	`RSOR demo_cursor;`
	`EXEC SQL`
	`ALLOCATE :demo_cursor;`
	`EXEC SQL EXECUTE`
	`BEGIN`
	`pkg_demo.`
	`get_cursor(`
	`demo_cur=`
	`>:demo_cursor`
	`);`
	`END;`
	`END-EXEC;`
	
	ECPG-Kode:
	
	`EXEC SQL DECLARE`
	`demo_cursor CURSOR FOR`
	`SELECT`
	`* from`
	`pkg_demo.open_file`
	`name_rc(`
	`demo_cur=`
	`>refcursor`
	`) ;`
	`EXEC SQL char open_file`
	`name_rcInd[100];`
	`# As the below function`
	`returns cursor_name`
	`as`
	`# return we need to`
	`use char[] type as`
	`indicator.`
		App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`EXEC SQL SELECT pkg_demo.get_cursor ( demo_cur=>'demo_cursor' ) INTO :open_filename_rcInd;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wenden Sie gängige Migration smuster an.	• Ändern Sie SQL-Abfragen so, dass sie mit PostgreSQL kompatibel sind. • Verschieben Sie anonyme Blöcke, wenn sie in ECPG nicht unterstützt werden, in die Datenbank. • Entfernen Sie die `dbms_application_info` Logik, die von PostgreSQL nicht unterstützt wird. • Verschiebt die `EXEC SQL COMMIT` Anweisungen, nachdem der Cursor geschlossen wurde. Wenn Sie Abfragen ausführen , während Sie sich in der Schleife befinden, um die Datensätze vom Cursor abzurufen, wird der Cursor geschlossen und die Fehlermeldung Cursor existiert nicht angezeigt. • Informationen zur Behandlung von Ausnahmen in ECPG und Fehlercodes finden Sie unter Fehlerbehandlung in der PostgreSQL-Dokumentation.	App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie das Debugging, falls erforderlich.	Um das ECPG-Programm im Debug-Modus auszuführ en, fügen Sie dem Hauptfunk tionsblock den folgenden Befehl hinzu. `ECPGdebug(1, stderr);`	App-Entwickler, App-Besitzer

Kompilieren Sie ECPG-Programme

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine ausführbare Datei für ECPG.	Wenn Sie eine eingebettete SQL C-Quelldatei mit dem Namen haben`prog1.pgc` , können Sie mithilfe der folgenden Befehlsfolge ein ausführbares Programm erstellen.
	`ecpg prog1.pgc`
	`cc -I/usr/local/pgsql/ include -c prog1.c`
	`cc -o prog1 prog1.o -L/ usr/local/pgsql/lib - lecpg`
		App-Entwickler, App-Besitzer

Erstellen Sie eine Make-Datei für die Kompilierung.	Erstellen Sie eine Make-Datei, um das ECPG-Prog ramm zu kompilieren, wie in der folgenden Beispieldatei gezeigt.	App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`CFLAGS ::= $(CFLAGS) -I/usr/pgsql-12/include -g -Wall`
	`LDFLAGS ::= $(LDFLAGS) -L/usr/pgsql-12/lib -Wl,-rpath,/usr/pgsql-12/lib`
	`LDLIBS ::= $(LDLIBS) -lecpg`
	`PROGRAMS = test`
	`.PHONY: all clean`
	`%.c: %.pgc`
	`  ecpg $<`
	`all: $(PROGRAMS)`
	`clean:`
	`  rm -f $(PROGRAMS) $(PROGRAMS:%=%.c) $(PROGRAMS:%=%.o)`	

Testen der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie den Code.	Testen Sie den konvertierten Anwendungscode, um sicherzustellen, dass er ordnungsgemäß funktioniert.	App-Entwickler, App-Besitzer, Testingenieur

Zugehörige Ressourcen

- ECPG - Eingebettetes SQL in C (PostgreSQL-Dokumentation)
- Fehlerbehandlung (PostgreSQL-Dokumentation)
- Warum sollte man den Oracle Pro*C/C++ Precompiler verwenden (Oracle-Dokumentation)

Zusätzliche Informationen

PostgreSQL hat einen eingebetteten SQL-Precompiler, ECPG, der dem Oracle Pro*C-Precompiler entspricht. ECPG konvertiert C-Programme mit eingebetteten SQL-Anweisungen in Standard-C-Code, indem es die SQL-Aufrufe durch spezielle Funktionsaufrufe ersetzt. Die Ausgabedateien können dann mit jeder C-Compiler-Toolchain verarbeitet werden.

Eingabe- und Ausgabedateien

ECPG konvertiert jede Eingabedatei, die Sie in der Befehlszeile angeben, in die entsprechende C-Ausgabedatei. Wenn ein Eingabedateiname keine Dateierweiterung hat, wird .pgc angenommen. Die Erweiterung der Datei wird durch ersetzt, `.c` um den Namen der Ausgabedatei zu erstellen. Sie können jedoch den Standardnamen der Ausgabedatei überschreiben, indem Sie die `-o` Option verwenden.

Wenn Sie einen Bindestrich (`-`) als Namen der Eingabedatei verwenden, liest ECPG das Programm aus der Standardeingabe und schreibt in die Standardausgabe, sofern Sie dies nicht mit der `-o` Option überschreiben.

Header-Dateien

Wenn der PostgreSQL-Compiler die vorverarbeiteten C-Codedateien kompiliert, sucht er im PostgreSQL-Verzeichnis nach den ECPG-Header-Dateien. `include` Daher müssen Sie möglicherweise die `-I` Option verwenden, um den Compiler auf das richtige Verzeichnis zu verweisen (z. B.). `-I/usr/local/pgsql/include`

Bibliotheken

Programme, die C-Code mit Embedded SQL verwenden, müssen mit der `libecpg` Bibliothek verknüpft werden. Sie können beispielsweise die Linker-Optionen `-L/usr/local/pgsql/lib -lecpg` verwenden.

Konvertierte ECPG-Anwendungen rufen Funktionen in der `libpq` Bibliothek über die Embedded SQL-Bibliothek (`ecpglib`) auf und kommunizieren mit dem PostgreSQL-Server unter Verwendung des Standard-Frontend-/Backend-Protokolls.

Migrieren Sie virtuell generierte Spalten von Oracle nach PostgreSQL

Erstellt von Veeranjaneyulu Grandhi (AWS), Rajesh Madiwale (AWS) und Ramesh Pathuri (AWS)

Übersicht

In Version 11 und früher bietet PostgreSQL keine Funktion, die direkt einer virtuellen Oracle-Spalte entspricht. Der Umgang mit virtuell generierten Spalten bei der Migration von Oracle Database zu PostgreSQL Version 11 oder früher ist aus zwei Gründen schwierig:

- Virtuelle Spalten sind während der Migration nicht sichtbar.
- PostgreSQL unterstützt den `generate` Ausdruck vor Version 12 nicht.

Es gibt jedoch Problemumgehungen, um ähnliche Funktionen zu emulieren. Wenn Sie AWS Database Migration Service (AWS DMS) verwenden, um Daten von Oracle Database zu PostgreSQL Version 11 und früher zu migrieren, können Sie Triggerfunktionen verwenden, um die Werte in virtuell generierten Spalten aufzufüllen. Dieses Muster enthält Beispiele für Oracle-Datenbank- und PostgreSQL-Code, den Sie für diesen Zweck verwenden können. Auf AWS können Sie Amazon Relational Database Service (Amazon RDS) für PostgreSQL oder Amazon Aurora PostgreSQL-Compatible Edition für Ihre PostgreSQL-Datenbank verwenden.

Ab PostgreSQL Version 12 werden generierte Spalten unterstützt. Generierte Spalten können entweder spontan aus anderen Spaltenwerten berechnet oder berechnet und gespeichert werden. Von PostgreSQL generierte Spalten ähneln virtuellen Oracle-Spalten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle-Quelldatenbank
- PostgreSQL-Zieldatenbanken (auf Amazon RDS für PostgreSQL oder Aurora PostgreSQL-kompatibel)
- Erfahrung in der PL/PgSQL-Codierung

Einschränkungen

- Gilt nur für PostgreSQL-Versionen vor Version 12.

- Gilt für Oracle Database Version 11g oder höher.
- Virtuelle Spalten werden in Datenmigrationstools nicht unterstützt.
- Gilt nur für Spalten, die in derselben Tabelle definiert sind.
- Wenn sich eine virtuell generierte Spalte auf eine deterministische benutzerdefinierte Funktion bezieht, kann sie nicht als Partitionierungsschlüsselspalte verwendet werden.
- Die Ausgabe des Ausdrucks muss ein Skalarwert sein. Es kann keinen von Oracle angegebenen Datentyp, einen benutzerdefinierten Typ, oder zurückgeben. `LOB LONG RAW`
- Indizes, die für virtuelle Spalten definiert sind, entsprechen funktionsbasierten Indizes in PostgreSQL.
- Tabellenstatistiken müssen gesammelt werden.

Tools

- pgAdmin 4 ist ein Open-Source-Verwaltungstool für PostgreSQL. Dieses Tool bietet eine grafische Oberfläche, die die Erstellung, Wartung und Verwendung von Datenbankobjekten vereinfacht.
- Oracle SQL Developer ist eine kostenlose, integrierte Entwicklungsumgebung für die Arbeit mit SQL in Oracle-Datenbanken sowohl in herkömmlichen als auch in Cloud-Umgebungen.

Epen

Erstellen Sie Quell- und Zieldatenbanktabellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Oracle-Datenbankquelltabelle.	Erstellen Sie in Oracle Database eine Tabelle mit virtuell generierten Spalten, indem Sie die folgende Anweisung verwenden. `CREATE TABLE test.generated_column ( CODE NUMBER, STATUS VARCHAR2(12) DEFAULT 'PreOpen', FLAG CHAR(1) GENERATED ALWAYS AS (CASE`	DBA, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>UPPER(STATUS) WHEN 'OPEN' THEN 'N' ELSE 'Y' END) VIRTUAL VISIBLE);</pre> In dieser Quelltabelle werden die Daten in der `STATUS` Spalte über AWS DMS in die Zieldatenbank migriert. Die `FLAG` Spalte wird jedoch mithilfe von `generate by` Funktionen gefüllt, sodass diese Spalte für AWS DMS während der Migration nicht sichtbar ist. Um die Funktionalität von zu implementierengenerated by, müssen Sie Trigger und Funktionen in der Zieldatenbank verwenden, um die Werte in der `FLAG` Spalte aufzufüllen, wie im nächsten Epic gezeigt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine PostgreSQL-Zieltabelle auf AWS.	Erstellen Sie mithilfe der folgenden Anweisung eine PostgreSQL-Tabelle auf AWS. `CREATE TABLE test.generated_column ( code integer not null, status character varying(12) not null , flag character(1) );` In dieser Tabelle ist die `status` Spalte eine Standardspalte. Bei der `flag` Spalte handelt es sich um eine generierte Spalte, die auf den Daten in der `status` Spalte basiert.	DBA, App-Entwickler

Erstellen Sie eine Triggerfunktion zur Behandlung der virtuellen Spalte in PostgreSQL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen PostgreSQL-Trigger.	Erstellen Sie in PostgreSQL einen Trigger. `CREATE TRIGGER tgr_gen_column AFTER INSERT OR UPDATE OF status ON test.generated_column FOR EACH ROW`	DBA, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`EXECUTE FUNCTION test.tgf_gen_column();`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine PostgreSQL-Triggerfunktion.	Erstellen Sie in PostgreSQL eine Funktion für den Trigger. Diese Funktion füllt eine virtuelle Spalte, die von der Anwendung oder AWS DMS eingefügt oder aktualisiert wird, und validiert die Daten. `CREATE OR REPLACE FUNCTION test.tgf_gen_column() RETURNS trigger AS $VIRTUAL_COL$ BEGIN IF (TG_OP = 'INSERT') THEN IF (NEW.flag IS NOT NULL) THEN RAISE EXCEPTION 'ERROR: cannot insert into column "flag"' USING DETAIL = 'Column "flag" is a generated column.'; END IF; END IF; IF (TG_OP = 'UPDATE') THEN IF (NEW.flag::VARCHAR != OLD.flag::varchar) THEN RAISE EXCEPTION 'ERROR: cannot update column "flag"' USING DETAIL = 'Column "flag" is a generated column.'; END IF; END IF; IF TG_OP IN ('INSERT','UPDATE') THEN`	DBA, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`IF (old.flag is NULL) OR (coalesce(old.status,'') != coalesce(new.status,'')) THEN UPDATE test.generated_column SET flag = (CASE UPPER(status) WHEN 'OPEN' THEN 'N' ELSE 'Y' END) WHERE code = new.code; END IF; END IF; RETURN NEW; END $VIRTUAL_COL$ LANGUAGE plpgsql;`	

Testen Sie die Datenmigration mithilfe von AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Replikationsinstanz.	Folgen Sie den Anweisungen in der AWS DMS-Dokumentation, um eine Replikationsinstanz zu erstellen. Die Replikationsinstanz sollte sich in derselben Virtual Private Cloud (VPC) wie Ihre Quell- und Zieldatenbanken befinden.	DBA, App-Entwickler
Erstellen Sie Quell- und Zielendpunkte.	Folgen Sie den Anweisungen in der AWS DMS-Dokumentation, um die Endpoints zu erstellen.	DBA, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Endpunktv erbindungen.	Sie können die Endpunktv erbindungen testen, indem Sie die VPC und die Replikati onsinstanz angeben und Test ausführen wählen.	DBA, App-Entwickler
Erstellen und starten Sie eine Vollladeaufgabe.	Anweisungen finden Sie in der AWS DMS-Dokumentation unter Aufgaben erstellen und Aufgabeneinstellungen unter Vollladen.	DBA, App-Entwickler
Überprüfen Sie die Daten für die virtuelle Spalte.	Vergleichen Sie die Daten in der virtuellen Spalte in der Quell- und Zieldatenbank. Sie können die Daten manuell validieren oder ein Skript für diesen Schritt schreiben.	DBA, App-Entwickler

Zugehörige Ressourcen

- Erste Schritte mit AWS Database Migration Service (AWS DMS-Dokumentation)
- Verwenden einer Oracle-Datenbank als Quelle für AWS DMS (AWS DMS-Dokumentation)
- Verwenden einer PostgreSQL-Datenbank als Ziel für AWS DMS (AWS DMS-Dokumentation)
- Generierte Spalten in PostgreSQL (PostgreSQL-Dokumentation)
- Triggerfunktionen (PostgreSQL-Dokumentation)
- Virtuelle Spalten in der Oracle-Datenbank (Oracle-Dokumentation)

Richten Sie die Oracle UTL_FILE-Funktionalität auf Aurora PostgreSQL-Compatible ein

Erstellt von Rakesh Raghav (AWS) und Anuradha Chintha (AWS)

Übersicht

Im Rahmen Ihrer Migration von Oracle zu Amazon Aurora PostgreSQL-Compatible Edition in der Amazon Web Services (AWS) Cloud können Sie auf mehrere Herausforderungen stoßen. Beispielsweise ist die Migration von Code, der auf dem `UTL_FILE` Oracle-Hilfsprogramm basiert, immer eine Herausforderung. In Oracle PL/SQL wird das `UTL_FILE` Paket in Verbindung mit dem zugrunde liegenden Betriebssystem für Dateioperationen wie Lesen und Schreiben verwendet. Das `UTL_FILE` Hilfsprogramm funktioniert sowohl für Server- als auch für Client-Computersysteme.

Amazon Aurora PostgreSQL-Compatible ist ein Angebot für verwaltete Datenbanken. Aus diesem Grund ist es nicht möglich, auf Dateien auf dem Datenbankserver zuzugreifen. Dieses Muster führt Sie durch die Integration von Amazon Simple Storage Service (Amazon S3) und Amazon Aurora PostgreSQL-kompatibel, um einen Teil der Funktionalität zu erreichen. `UTL_FILE` Mit dieser Integration können wir Dateien erstellen und verwenden, ohne Tools oder Dienste von Drittanbietern zum Extrahieren, Transformieren und Laden (ETL) zu verwenden.

Optional können Sie CloudWatch Amazon-Überwachung und Amazon SNS-Benachrichtigungen einrichten.

Wir empfehlen, diese Lösung gründlich zu testen, bevor Sie sie in einer Produktionsumgebung implementieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Fachwissen zum AWS Database Migration Service (AWS DMS)
- Fachwissen in der PL/pgSQL-Codierung
- Ein Amazon Aurora PostgreSQL-kompatibler Cluster
- Ein S3-Bucket

Einschränkungen

Dieses Muster bietet nicht die Funktionalität, um das Oracle-Hilfsprogramm zu ersetzen. `UTL_FILE` Die Schritte und der Beispielcode können jedoch weiter verbessert werden, um Ihre Ziele bei der Datenbankmodernisierung zu erreichen.

Produktversionen

- Amazon Aurora PostgreSQL-kompatible Ausgabe 11.9

Architektur

Zieltechnologie-Stack

- Amazon Aurora PostgreSQL-kompatibel
- Amazon CloudWatch
- Amazon-Simple-Notification-Service (Amazon-SNS)
- Amazon S3

Zielarchitektur

Das folgende Diagramm zeigt eine allgemeine Darstellung der Lösung.

1. Dateien werden aus der Anwendung in den S3-Bucket hochgeladen.
2. Die `aws_s3` Erweiterung greift mithilfe von PL/pgSQL auf die Daten zu und lädt die Daten in Aurora PostgreSQL-kompatibel hoch.

Tools

- Amazon Aurora PostgreSQL-kompatibel — Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, PostgreSQL-kompatible und ACID-konforme relationale Datenbank-Engine. Sie kombiniert die Geschwindigkeit und Zuverlässigkeit kommerzieller High-End-Datenbanken mit der Wirtschaftlichkeit von Open-Source-Datenbanken.
- AWS CLI — Die AWS-Befehlszeilenschnittstelle (AWS CLI) ist ein einheitliches Tool zur Verwaltung Ihrer AWS-Services. Mit nur einem Tool zum Herunterladen und Konfigurieren können Sie mehrere AWS-Services von der Befehlszeile aus steuern und mithilfe von Skripts automatisieren.

- Amazon CloudWatch — Amazon CloudWatch überwacht die Ressourcen und die Nutzung von Amazon S3.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Speicher für das Internet. In diesem Muster bietet Amazon S3 eine Speicherebene zum Empfangen und Speichern von Dateien für den Verbrauch und die Übertragung zum und vom Aurora PostgreSQL-kompatiblen Cluster.
- aws_s3 — Die `aws_s3` Erweiterung integriert Amazon S3 und Aurora PostgreSQL-kompatibel.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Herausgebern und Kunden. In diesem Muster wird Amazon SNS zum Senden von Benachrichtigungen verwendet.
- pgAdmin — pgAdmin ist ein Open-Source-Verwaltungstool für Postgres. pgAdmin 4 bietet eine grafische Oberfläche zum Erstellen, Verwalten und Verwenden von Datenbankobjekten.

Code

Um die erforderliche Funktionalität zu erreichen, erstellt das Muster mehrere Funktionen mit einer ähnlichen Benennung wie. `UTL_FILE` Der Abschnitt Zusätzliche Informationen enthält die Codebasis für diese Funktionen.

Ersetzen Sie den Code `testaurorabucket` durch den Namen Ihres Test-S3-Buckets. `us-east-1`Ersetzen Sie durch die AWS-Region, in der sich Ihr Test-S3-Bucket befindet.

Epen

Integrieren Sie Amazon S3 und Aurora PostgreSQL-kompatibel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie IAM-Richtlinien ein.	Erstellen Sie AWS Identity and Access Management (IAM) -Richtlinien, die Zugriff auf den S3-Bucket und die darin enthaltenen Objekte gewähren. Den Code finden Sie im Abschnitt Zusätzliche Informationen.	AWS-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Amazon S3 S3-Zugriffsrollen zu Aurora PostgreSQL hinzu.	Erstellen Sie zwei IAM-Rollen: eine Rolle für den Lese- und eine Rolle für den Schreibzugriff auf Amazon S3. Hängen Sie die beiden Rollen an den Aurora PostgreSQL-kompatiblen Cluster an: • Eine Rolle für die S3Export-Funktion • Eine Rolle für die S3Import-Funktion Weitere Informationen finden Sie in der Aurora PostgreSQL-kompatiblen Dokumentation zum Import und Export von Daten nach Amazon S3.	AWS-Administrator, DBA

Richten Sie die Erweiterungen in Aurora PostgreSQL-kompatibel ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Erweiterung aws_commons.	Die `aws_commons` Erweiterung ist eine Abhängigkeit von der `aws_s3` Erweiterung.	DBA, Entwickler
Erstellen Sie die Erweiterung aws_s3.	Die `aws_s3` Erweiterung interagiert mit Amazon S3.	DBA, Entwickler

Validieren Sie die Amazon S3- und Aurora PostgreSQL-kompatible Integration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie den Import von Dateien aus Amazon S3 nach Aurora PostgreSQL.	Um den Import von Dateien in Aurora PostgreSQL-Compatible zu testen, erstellen Sie eine CSV-Beispieldatei und laden Sie sie in den S3-Bucket hoch. Erstellen Sie eine Tabellendefinition auf der Grundlage der CSV-Datei und laden Sie die Datei mithilfe der Funktion in die Tabelle. `aws_s3.table_import_from_s3`	DBA, Entwickler
Testen Sie den Export von Dateien von Aurora PostgreSQL nach Amazon S3.	Um den Export von Dateien aus Aurora PostgreSQL-Compatible zu testen, erstellen Sie eine Testtabelle, füllen Sie sie mit Daten und exportieren Sie die Daten dann mithilfe der Funktion. `aws_s3.query_export_to_s3`	DBA, Entwickler

Um das UTL_FILE-Hilfsprogramm nachzuahmen, erstellen Sie Wrapper-Funktionen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Schema utl_file_utility.	Das Schema hält die Wrapper-Funktionen zusammen. Führen Sie den folgenden Befehl aus, um das Schema zu erstellen.	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`CREATE SCHEMA utl_file_utility;`	
Erstellen Sie den Typ file_type .	Verwenden Sie den folgenden Code, um den `file_type` Typ zu erstellen. `CREATE TYPE utl_file_utility.file_type AS ( p_path character varying(30), p_file_name character varying );`	DBA/Entwickler
Erstellen Sie die Init-Funktion.	Die `init` Funktion initialisiert eine gemeinsame Variable wie oder. `bucket` `region` Den Code finden Sie im Abschnitt Zusätzliche Informationen.	DBA/Entwickler
Erstellen Sie die Wrapper-F unktionen.	Erstellen Sie die Wrapper-F unktionen `fopen` `put_line`, und. `fclose` Code finden Sie im Abschnitt Zusätzliche Informationen.	DBA, Entwickler

Testen Sie die Wrapper-Funktionen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Wrapper-F unktionen im Schreibmodus.	Um die Wrapper-Funktionen im Schreibmodus zu testen, verwenden Sie den Code im	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Abschnitt Zusätzliche Informationen.	
Testen Sie die Wrapper-Funktionen im Append-Modus.	Um die Wrapper-Funktionen im Append-Modus zu testen, verwenden Sie den Code im Abschnitt Zusätzliche Informationen.	DBA, Entwickler

Zugehörige Ressourcen

- Amazon S3 S3-Integration
- Amazon S3
- Aurora
- Amazon CloudWatch
- Amazon SNS

Zusätzliche Informationen

Richten Sie IAM-Richtlinien ein

Erstellen Sie die folgenden Richtlinien.

Name der Richtlinie

S3 IntRead

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3integrationtest
",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
```

```
            "Resource": [
          "arn:aws:s3:::testaurorabuc
ket/*",
          "arn:aws:s3:::testaurorabuc
ket"
            ]
        }
    ]
}
```

S 3 IntWrite

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3integrationtest
",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",

                "s3:ListBucket"
            ],
            "Resource": [
    "arn:aws:s3:::testaurorabucket/
*",                "arn:aws:s3:::test
aurorabucket"
            ]
        }
    ]
}
```

Erstellen Sie die Init-Funktion

Um allgemeine Variablen wie `bucket` oder zu initialisieren`region`, erstellen Sie die `init` Funktion mit dem folgenden Code.

```
CREATE OR REPLACE FUNCTION utl_file_utility.init(
    )
    RETURNS void
    LANGUAGE 'plpgsql'
```

```
    COST 100
    VOLATILE
AS $BODY$
BEGIN
      perform set_config
      ( format( '%s.%s','UTL_FILE_UTILITY', 'region' )
      , 'us-east-1'::text
      , false );

      perform set_config
      ( format( '%s.%s','UTL_FILE_UTILITY', 's3bucket' )
      , 'testaurorabucket'::text
      , false );
END;
$BODY$;
```

Erstellen Sie die Wrapper-Funktionen

Erstellen Sie die `fclose` Wrapper-Funktionen `fopenput_line`, und.

öffnen

```
CREATE OR REPLACE FUNCTION utl_file_utility.fopen(
    p_file_name character varying,
    p_path character varying,
    p_mode character DEFAULT 'W'::bpchar,
    OUT p_file_type utl_file_utility.file_type)
    RETURNS utl_file_utility.file_type
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
declare
    v_sql character varying;
    v_cnt_stat integer;
    v_cnt integer;
    v_tabname character varying;
    v_filewithpath character varying;
    v_region character varying;
    v_bucket character varying;

BEGIN
    /*initialize common variable */
```

```
   PERFORM utl_file_utility.init();
   v_region := current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 'region' ) );
   v_bucket :=  current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 's3bucket' ) );

   /* set tabname*/
   v_tabname := substring(p_file_name,1,case when strpos(p_file_name,'.') = 0 then
length(p_file_name) else strpos(p_file_name,'.') - 1 end );
   v_filewithpath := case when NULLif(p_path,'') is null then p_file_name else
concat_ws('/',p_path,p_file_name) end ;
   raise notice 'v_bucket %, v_filewithpath % , v_region %', v_bucket,v_filewithpath,
v_region;

   /* APPEND MODE HANDLING; RETURN EXISTING FILE DETAILS IF PRESENT ELSE CREATE AN
EMPTY FILE */
   IF p_mode = 'A' THEN
       v_sql := concat_ws('','create temp table if not exists ', v_tabname,' (col1
text)');
       execute v_sql;

       begin
       PERFORM aws_s3.table_import_from_s3
           ( v_tabname,
           '',
           'DELIMITER AS ''#''',
           aws_commons.create_s3_uri
           (     v_bucket,
               v_filewithpath ,
               v_region)
           );
       exception
           when others then
            raise notice 'File load issue ,%',sqlerrm;
            raise;
       end;
       execute concat_ws('','select count(*) from ',v_tabname) into v_cnt;

       IF v_cnt > 0
       then
           p_file_type.p_path := p_path;
           p_file_type.p_file_name := p_file_name;
       else
           PERFORM aws_s3.query_export_to_s3('select ''''',
                           aws_commons.create_s3_uri(v_bucket, v_filewithpath,
v_region)
```

```
                              );

            p_file_type.p_path := p_path;
            p_file_type.p_file_name := p_file_name;
        end if;
        v_sql := concat_ws('','drop table ', v_tabname);
        execute v_sql;
    ELSEIF p_mode = 'W' THEN
            PERFORM aws_s3.query_export_to_s3('select ''''',
                           aws_commons.create_s3_uri(v_bucket, v_filewithpath,
 v_region)
                              );
            p_file_type.p_path := p_path;
            p_file_type.p_file_name := p_file_name;
    END IF;

EXCEPTION
        when others then
            p_file_type.p_path := p_path;
            p_file_type.p_file_name := p_file_name;
            raise notice 'fopenerror,%',sqlerrm;
            raise;
END;
$BODY$;
```

put_line

```
CREATE OR REPLACE FUNCTION utl_file_utility.put_line(
    p_file_name character varying,
    p_path character varying,
    p_line text,
    p_flag character DEFAULT 'W'::bpchar)
    RETURNS boolean
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
/*****************************************************************
* Write line, p_line in windows format to file, p_fp - with carriage return
* added before new line.
*****************************************************************/
declare
```

```
    v_sql varchar;
    v_ins_sql varchar;
    v_cnt INTEGER;
    v_filewithpath character varying;
    v_tabname  character varying;
    v_bucket character varying;
    v_region character varying;

BEGIN
 PERFORM utl_file_utility.init();

/* check if temp table already exist */

 v_tabname := substring(p_file_name,1,case when strpos(p_file_name,'.') = 0 then
 length(p_file_name) else strpos(p_file_name,'.') - 1 end );

 v_sql := concat_ws('','select count(1) FROM pg_catalog.pg_class c LEFT JOIN
 pg_catalog.pg_namespace n ON n.oid = c.relnamespace where n.nspname like ''pg_temp_
%'''
                        ,' AND pg_catalog.pg_table_is_visible(c.oid) AND
 Upper(relname) = Upper( '''
                        ,  v_tabname ,''' ) ');

 execute v_sql into v_cnt;

  IF v_cnt = 0 THEN
         v_sql := concat_ws('','create temp table ',v_tabname,' (col text)');
        execute v_sql;
        /* CHECK IF APPEND MODE */
        IF upper(p_flag) = 'A' THEN
            PERFORM utl_file_utility.init();
            v_region := current_setting( format( '%s.%s', 'UTL_FILE_UTILITY',
 'region' ) );
            v_bucket :=  current_setting( format( '%s.%s', 'UTL_FILE_UTILITY',
 's3bucket' ) );

            /* set tabname*/
            v_filewithpath := case when NULLif(p_path,'') is null then p_file_name else
 concat_ws('/',p_path,p_file_name) end ;

            begin
               PERFORM aws_s3.table_import_from_s3
                     ( v_tabname,
                          '',
```

```
                        'DELIMITER AS ''#''',
                         aws_commons.create_s3_uri
                            ( v_bucket,
                                v_filewithpath,
                                v_region    )
                    );
            exception
                when others then
                    raise notice  'Error Message : %',sqlerrm;
                    raise;
            end;
        END IF;
    END IF;
    /* INSERT INTO TEMP TABLE */
    v_ins_sql := concat_ws('','insert into ',v_tabname,' values(''',p_line,''')');
    execute v_ins_sql;
    RETURN TRUE;
    exception
            when others then
                raise notice  'Error Message : %',sqlerrm;
                raise;
END;
$BODY$;
```

schließen

```
CREATE OR REPLACE FUNCTION utl_file_utility.fclose(
    p_file_name character varying,
    p_path character varying)
    RETURNS boolean
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
DECLARE
    v_filewithpath character varying;
    v_bucket character varying;
    v_region character varying;
    v_tabname character varying;
    v_sql character varying;
BEGIN
      PERFORM utl_file_utility.init();
```

```
    v_region := current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 'region' ) );
    v_bucket :=  current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 's3bucket' ) );

    v_tabname := substring(p_file_name,1,case when strpos(p_file_name,'.') = 0 then
 length(p_file_name) else strpos(p_file_name,'.') - 1 end );
    v_filewithpath := case when NULLif(p_path,'') is null then p_file_name else
 concat_ws('/',p_path,p_file_name) end ;

    raise notice 'v_bucket %, v_filewithpath % , v_region %', v_bucket,v_filewithpath,
 v_region ;

    /* exporting to s3 */
    perform aws_s3.query_export_to_s3
        (concat_ws('','select * from ',v_tabname,'  order by ctid asc'),
            aws_commons.create_s3_uri(v_bucket, v_filewithpath, v_region)
        );
    v_sql := concat_ws('','drop table ', v_tabname);
    execute v_sql;
    RETURN TRUE;
EXCEPTION
       when others then
     raise notice 'error fclose %',sqlerrm;
     RAISE;
END;
$BODY$;
```

Testen Sie Ihr Setup und Ihre Wrapper-Funktionen

Verwenden Sie die folgenden anonymen Codeblöcke, um Ihr Setup zu testen.

Testen Sie den Schreibmodus

Der folgende Code schreibt eine Datei mit dem Namen `s3inttest` im S3-Bucket.

```
do $$
declare
l_file_name varchar := 's3inttest' ;
l_path varchar := 'integration_test' ;
l_mode char(1) := 'W';
l_fs utl_file_utility.file_type ;
l_status boolean;

begin
```

```
select * from
utl_file_utility.fopen( l_file_name, l_path , l_mode ) into l_fs ;
raise notice 'fopen : l_fs : %', l_fs;

select * from
utl_file_utility.put_line( l_file_name, l_path ,'this is test file:in s3bucket: for
 test purpose', l_mode ) into l_status ;
raise notice 'put_line : l_status %', l_status;

select * from utl_file_utility.fclose( l_file_name , l_path ) into l_status ;
raise notice 'fclose : l_status %', l_status;

end;
$$
```

Testen Sie den Append-Modus

Der folgende Code fügt Zeilen an die `s3inttest` Datei an, die im vorherigen Test erstellt wurde.

```
do $$
declare
l_file_name varchar := 's3inttest' ;
l_path varchar := 'integration_test' ;
l_mode char(1) := 'A';
l_fs utl_file_utility.file_type ;
l_status boolean;

begin
select * from
utl_file_utility.fopen( l_file_name, l_path , l_mode ) into l_fs ;
raise notice 'fopen : l_fs : %', l_fs;


select * from
utl_file_utility.put_line( l_file_name, l_path ,'this is test file:in s3bucket: for
 test purpose : append 1', l_mode ) into l_status ;
raise notice 'put_line : l_status %', l_status;

select * from
utl_file_utility.put_line( l_file_name, l_path ,'this is test file:in s3bucket : for
 test purpose : append 2', l_mode ) into l_status ;
raise notice 'put_line : l_status %', l_status;

select * from utl_file_utility.fclose( l_file_name , l_path ) into l_status ;
```

```
raise notice 'fclose : l_status %', l_status;

end;
$$
```

Amazon SNS SNS-Benachrichtigungen

Optional können Sie CloudWatch Amazon-Überwachung und Amazon SNS-Benachrichtigungen im S3-Bucket einrichten. Weitere Informationen finden Sie unter Amazon S3 überwachen und Amazon SNS SNS-Benachrichtigungen einrichten.

Datenbankobjekte nach der Migration von Oracle zu Amazon Aurora PostgreSQL validieren

Erstellt von Venkatramana Chintha (AWS) und Eduardo Valentim (AWS)

Übersicht

Dieses Muster beschreibt einen step-by-step Ansatz zur Validierung von Objekten nach der Migration einer Oracle-Datenbank zur Amazon Aurora PostgreSQL-Compatible Edition.

In diesem Muster werden Nutzungsszenarien und Schritte für die Validierung von Datenbankobjekten beschrieben. Weitere Informationen finden Sie im AWS-Datenbank-Blog unter Validieren von Datenbankobjekten nach der Migration mit AWS SCT und AWS DMS.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine lokale Oracle-Datenbank, die auf eine Aurora PostgreSQL-kompatible Datenbank migriert wurde.
- Anmeldeinformationen für die Aurora PostgreSQL-kompatible Datenbank, auf die die RDSDataFullAccessAmazon-Richtlinie angewendet wurde.
- Dieses Muster verwendet den Abfrage-Editor für Aurora Serverless DB-Cluster, der in der Amazon Relational Database Service (Amazon RDS) -Konsole verfügbar ist. Sie können dieses Muster jedoch mit jedem anderen Abfrage-Editor verwenden.

Einschränkungen

- Oracle SYNONYM-Objekte sind in PostgreSQL nicht verfügbar, können aber teilweise durch Views oder SET search_path-Abfragen validiert werden.
- Der Amazon RDS-Abfrage-Editor ist nur in bestimmten AWS-Regionen und für bestimmte MySQL- und PostgreSQL-Versionen verfügbar.

Architektur

Tools

Tools

- Amazon Aurora PostgreSQL-Compatible Edition — Aurora PostgreSQL-Compatible ist eine vollständig verwaltete, PostgreSQL-kompatible und ACID-konforme relationale Datenbank-Engine, die die Geschwindigkeit und Zuverlässigkeit kommerzieller High-End-Datenbanken mit der Einfachheit und Wirtschaftlichkeit von Open-Source-Datenbanken kombiniert.
- Amazon RDS — Amazon Relational Database Service (Amazon RDS) erleichtert die Einrichtung, den Betrieb und die Skalierung einer relationalen Datenbank in der AWS-Cloud. Dieser Service bietet kostengünstige und anpassbare Kapazität für eine Branchenstandards entsprechende relationale Datenbank sowie die Verwaltung gängiger Datenbankaufgaben.
- Abfrage-Editor für Aurora Severless — Der Abfrage-Editor unterstützt Sie bei der Ausführung von SQL-Abfragen in der Amazon RDS-Konsole. Sie können jede gültige SQL-Anweisung auf dem Aurora Serverless DB-Cluster ausführen, einschließlich Datenmanipulations- und Datendefinitionsanweisungen.

Um die Objekte zu validieren, verwenden Sie die vollständigen Skripten in der Datei „Objektvalidierungsskripten“ im Abschnitt „Anlagen“. Verwenden Sie die folgende Tabelle als Referenz.

Oracle-Objekt	Zu verwendendes Skript
Pakete	Abfrage 1
Tabellen	Abfrage 3
Ansichten	Abfrage 5
Sequenzen	Abfrage 7
Auslöser	Abfrage 9
Primärschlüssel	Abfrage 11
Indizes	Abfrage 13
Einschränkungen prüfen	Abfrage 15

Fremdschlüssel	Abfrage 17

PostgreSQL-Objekt	Zu verwendendes Skript
Pakete	Abfrage 2
Tabellen	Abfrage 4
Ansichten	Abfrage 6
Sequenzen	Abfrage 8
Auslöser	Abfrage 10
Primärschlüssel	Abfrage 12
Indizes	Abfrage 14
Einschränkungen prüfen	Abfrage 16
Fremdschlüssel	Abfrage 18

Epen

Validieren Sie Objekte in der Oracle-Quelldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Validierungsabfrage „Pakete“ in der Oracle-Quelldatenbank aus.	Laden Sie die Datei „Objektvalidierungsskripten“ aus dem Abschnitt „Anlagen“ herunter und öffnen Sie sie. Stellen Sie über Ihr Client-Programm eine Connect zur Oracle-Quelldatenbank her. Führen Sie das Validierungsskript „Query 1“ aus der Datei „Objektvalidierungsskripten	Entwickler, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	“ aus. Wichtig: Geben Sie in den Abfragen Ihren Oracle-Benutzernamen statt „your_schema“ ein. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	
Führen Sie die Validierungsabfrage „Tabellen“ aus.	Führen Sie das Skript „Query 3“ aus der Datei „Objektvalidierungsskripten“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA
Führen Sie die Validierungsabfrage „Views“ aus.	Führen Sie das Skript „Query 5“ aus der Datei „Objektvalidierungsskripten“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA
Führen Sie die Überprüfung der Anzahl der „Sequenzen“ durch.	Führen Sie das Skript „Query 7“ aus der Datei „Objektvalidierungsskripten“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA
Führen Sie die Validierungsabfrage „Trigger“ aus.	Führen Sie das Skript „Query 9“ aus der Datei „Objektvalidierungsskripten“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Validierungsabfrage für „Primärschlüssel“ aus.	Führen Sie das Skript „Query 11“ aus der Datei „Objektvalidierungsskripten“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA
Führen Sie die Validierungsabfrage „Indizes“ aus.	Führen Sie das Validierungsskript „Query 13“ aus der Datei „Objektvalidierungsskripten“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA
Führen Sie die Validierungsabfrage „Check Constraints“ aus.	Führen Sie das Skript „Query 15“ aus der Datei „Objektvalidierungsskripten“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA
Führen Sie die Validierungsabfrage für „Fremdschlüssel“ aus.	Führen Sie das Validierungsskript „Query 17“ aus der Datei „Objektvalidierungsskripten“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA

Objekte in der Aurora PostgreSQL-kompatiblen Zieldatenbank validieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie mithilfe des Abfrage-Editors eine Connect zur Aurora PostgreSQL-kompatiblen Zieldatenbank her.	Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon RDS-Konsole. Wählen Sie in der oberen rechten Ecke die AWS-Region aus, in der Sie die Aurora PostgreSQL-kompatible Datenbank erstellt haben. Wählen Sie im Navigationsbereich „Datenbanken“ und wählen Sie die Aurora PostgreSQL-kompatible Zieldatenbank aus. Wählen Sie unter „Aktionen“ die Option „Abfrage“ aus. Wichtig: Wenn Sie noch keine Verbindung mit der Datenbank hergestellt haben, wird die Seite „Mit Datenbank verbinden“ geöffnet. Anschließend müssen Sie Ihre Datenbankinformationen wie Benutzername und Passwort eingeben.	Entwickler, DBA
Führen Sie die Validierungsabfrage für „Pakete“ aus.	Führen Sie das Skript „Query 2“ aus der Datei „Objektvalidierungsskripten“ im Abschnitt „Anlagen“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Validieru ngsabfrage „Tabellen“ aus.	Kehren Sie zum Abfrage-E ditor für die Aurora PostgreSQ L-kompatible Datenbank zurück und führen Sie das Skript „Query 4“ aus der Datei „Objektvalidierungsskripten“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA
Führen Sie die Validieru ngsabfrage „Views“ aus.	Kehren Sie zum Abfrage-E ditor für die Aurora PostgreSQ L-kompatible Datenbank zurück und führen Sie das Skript „Query 6“ aus der Datei „Objektvalidierungsskripten“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA
Führen Sie die Überprüfung der Anzahl der „Sequenzen“ durch.	Kehren Sie zum Abfrage-E ditor für die Aurora PostgreSQ L-kompatible Datenbank zurück und führen Sie das Skript „Query 8“ aus der Datei „Objektvalidierungsskripten“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Validierungsabfrage „Trigger“ aus.	Kehren Sie zum Abfrage-Editor für die Aurora PostgreSQL-kompatible Datenbank zurück und führen Sie das Skript „Query 10“ aus der Datei „Objektvalidierungsskripten“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA
Führen Sie die Validierungsabfrage für „Primärschlüssel“ aus.	Kehren Sie zum Abfrage-Editor für die Aurora PostgreSQL-kompatible Datenbank zurück und führen Sie das Skript „Query 12“ aus der Datei „Objektvalidierungsskripten“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA
Führen Sie die Validierungsabfrage „Indizes“ aus.	Kehren Sie zum Abfrage-Editor für die Aurora PostgreSQL-kompatible Datenbank zurück und führen Sie das Skript „Query 14“ aus der Datei „Object Validation scripts“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Validierungsabfrage „Check Constraints“ aus.	Führen Sie das Skript „Query 16“ aus der Datei „Objektvalidierungsskripten“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA
Führen Sie die Validierungsabfrage für „Fremdschlüssel“ aus.	Führen Sie das Validierungsskript „Query 18“ aus der Datei „Objektvalidierungsskripten“ aus. Stellen Sie sicher, dass Sie Ihre Abfrageergebnisse aufzeichnen.	Entwickler, DBA

Vergleichen Sie die Validierungsdatensätze der Quell- und Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vergleichen und validieren Sie beide Abfrageergebnisse.	Vergleichen Sie die Abfrageergebnisse der Oracle- und Aurora PostgreSQL-kompatiblen Datenbanken, um alle Objekte zu validieren. Wenn sie alle übereinstimmen, wurden alle Objekte erfolgreich validiert.	Entwickler, DBA

Zugehörige Ressourcen

- Validierung von Datenbankobjekten nach einer Migration mit AWS SCT und AWS DMS
- Amazon Aurora Aurora-Funktionen: PostgreSQL-kompatible Edition

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Erneut hosten

Themen

- Beschleunigen Sie die Erkennung und Migration von Microsoft-Workloads zu AWS
- Automatisieren Sie Aktivitäten zur Erfassung vor dem Workload für AWS Managed Services unter Windows
- Erstellen Sie einen Genehmigungsprozess für Firewallanfragen während einer Rehost-Migration zu AWS
- EC2 Windows-Instances in ein AWS Managed Services Services-Konto aufnehmen und migrieren
- Migrieren Sie eine Couchbase Server-Datenbank zu Amazon EC2
- Migrieren Sie Db2 for LUW zu Amazon mithilfe EC2 von Protokollversand, um Ausfallzeiten zu reduzieren
- Migrieren Sie Db2 for LUW zu Amazon EC2 mit Disaster Recovery mit hoher Verfügbarkeit
- Migrieren Sie EC2 mithilfe des Application Migration Service eine lokale Microsoft SQL Server-Datenbank zu Amazon
- Migrieren Sie VMware VMs mit HCX Automation mithilfe von PowerCLI
- Migrieren Sie einen F5 BIG-IP-Workload zu F5 BIG-IP VE in der AWS-Cloud
- Migrieren Sie eine lokale Go-Webanwendung mithilfe der binären Methode zu AWS Elastic Beanstalk
- Migrieren Sie einen lokalen SFTP-Server zur Verwendung von AWSAWS Transfer for SFTP
- Migrieren Sie eine lokale VM EC2 mithilfe des AWS Application Migration Service zu Amazon
- Migrieren Sie kleine Datensätze mithilfe von AWS SFTP von der lokalen Infrastruktur zu Amazon S3
- Migrieren Sie von Oracle GlassFish zu AWS Elastic Beanstalk
- Migrieren Sie eine lokale Oracle-Datenbank zu Oracle auf Amazon EC2
- Migrieren Sie eine lokale Oracle-Datenbank mithilfe EC2 von Oracle Data Pump zu Amazon
- Migrieren Sie RHEL-BYOL-Systeme mithilfe von AWS MGN zu Instances mit AWS-Lizenz
- Migrieren Sie eine lokale SAP ASE-Datenbank zu Amazon EC2
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Amazon EC2
- Migrieren Sie eine lokale MySQL-Datenbank zu Amazon EC2
- Reduzieren Sie die Umstellungszeit für homogene SAP-Migrationen mithilfe des Application Migration Service

- Rehosten Sie lokale Workloads in der AWS-Cloud: Migrationscheckliste
- Richten Sie mithilfe von Amazon eine Multi-AZ-Infrastruktur für einen SQL Server Always On FCI ein FSx
- Verwenden Sie BMC Discovery-Abfragen, um Migrationsdaten für die Migrationsplanung zu extrahieren

Beschleunigen Sie die Erkennung und Migration von Microsoft-Workloads zu AWS

Erstellt von Ali Alzand

Übersicht

Dieses Muster zeigt Ihnen, wie Sie das PowerShell Modul Migration Validator Toolkit verwenden, um Ihre Microsoft-Workloads zu erkennen und zu AWS zu migrieren. Das Modul führt mehrere Prüfungen und Validierungen für häufige Aufgaben im Zusammenhang mit beliebigen Microsoft-Workloads durch. Das Modul sucht beispielsweise nach Instances, an die möglicherweise mehrere Festplatten angeschlossen sind, oder nach Instances, die viele IP-Adressen verwenden. Eine vollständige Liste der Prüfungen, die das Modul durchführen kann, finden Sie im Abschnitt Prüfungen auf der GitHub Seite des Moduls.

Das PowerShell Modul Migration Validator Toolkit kann Ihrem Unternehmen dabei helfen, den Zeit- und Arbeitsaufwand für die Ermittlung der Anwendungen und Dienste zu reduzieren, die auf Ihren Microsoft-Workloads ausgeführt werden. Das Modul unterstützt Sie außerdem dabei, die Konfigurationen Ihrer Workloads zu identifizieren, sodass Sie herausfinden können, ob Ihre Konfigurationen auf AWS unterstützt werden. Das Modul bietet auch Empfehlungen für die nächsten Schritte und Abhilfemaßnahmen, sodass Sie Fehlkonfigurationen vor, während oder nach der Migration vermeiden können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Lokales Administratorkonto
- PowerShell 4.0

Einschränkungen

- Funktioniert nur auf Microsoft Windows Server 2012 R2 oder höher

Tools

Tools

- PowerShell 4.0

Code-Repository

Das Migration Validator PowerShell Toolkit-Modul für dieses Muster ist im Repository -microsoft-workloads verfügbar. GitHub migration-validator-toolkit-for

Epen

Führen Sie das PowerShell Modul Migration Validator Toolkit auf einem einzigen Ziel aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Laden Sie das Modul herunter, extrahieren Sie es, importieren Sie es und rufen Sie es auf.	Wählen Sie eine der folgenden Methoden, um das Modul herunterzuladen und bereitzustellen:
	• Führen Sie das PowerShell Skript aus
	• Laden Sie die ZIP-Datei herunter und entpacken Sie sie
	• Klonen Sie das Repository GitHub
	
	Führen Sie das PowerShell Skript aus
	
	Führen Sie in PowerShell den folgenden Beispielcode aus:
	
	`#MigrationValidatorToolkit`
	`$uri = 'https://github.com/aws-samples/migration-validator-toolkit-for-microsoft-workloads/archive/refs/heads/main.zip'`
		Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`$destination = (Get-Location).Path`
	`if ((Test-Path -Path "$destination\MigrationValidatorToolkit.zip" -PathType Leaf) -or (Test-Path -Path "$destination\MigrationValidatorToolkit")) {`
	`write-host "File $destination\MigrationValidatorToolkit.zip or folder $destination\MigrationValidatorToolkit found, exiting"`
	`}else {`
	`Write-host "Enable TLS 1.2 for this PowerShell session only."`
	`[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12`
	`$webClient = New-Object System.Net.WebClient`
	`Write-host "Downloading MigrationValidatorToolkit.zip"`
	`$webClient.DownloadFile($uri, "$destination\MigrationValidatorToolkit.zip")`
	`Write-host "MigrationValidatorToolkit.zip download successfully"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> Add-Type -Assembly
	 "system.io.compres
	sion.filesystem"
	    [System.IO.Compres
	sion.ZipFile]::Ext
	ractToDirectory("$
	destination\Migrat
	ionValidatorToolki
	t.zip","$destinati
	on\MigrationValida
	torToolkit")
	    Write-host
	 "Extracting Migration
	ValidatorToolkit.zip
	 complete successfully"
	    Import-Module
	 "$destination\Migr
	ationValidatorToolkit
	\migration-validator-
	toolkit-for-microsoft
	-workloads-main\Mi
	grationValidatorTo
	olkit.psm1"; Invoke-
	MigrationValidatorTo
	olkit
	}</pre>
	Der Code lädt das Modul aus einer ZIP-Datei herunter. Anschließend extrahiert, importiert und ruft der Code das Modul auf.
	
	Laden Sie die ZIP-Datei herunter und extrahieren Sie sie
	
	1. Laden Sie die ZIP-Datei herunter (Download).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Entpacken Sie die ZIP-Datei. 3. Folgen Sie den Schritten im Abschnitt Manuelles Aufrufen des Moduls in diesem Handbuch. Klonen Sie das Repository GitHub 1. Um das Repository GitHub migration-validator-toolkit-for-microsoft-workloads zu klonen, führen Sie den folgenden Git-Befehl in einem Terminalfenster aus: `git clone https://github.com/aws-samples/migration-validator-toolkit-for-microsoft-workloads.git` 2. Folgen Sie den Schritten im Abschnitt Manuelles Aufrufen des Moduls in diesem Handbuch.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Rufen Sie das Modul manuell auf.	1. Gehen Sie in das Verzeichnis, in dem das heruntergeladene Modul gespeichert ist.
	2. Um die Ausgabe Ihrer Wahl zu generieren, führen Sie als Administrator einen der folgenden Befehle aus PowerShell:
	
	Format und Tabellenformat:
	`Import-Module .\MigrationValidatorToolkit.psm1;Invoke-MigrationValidatorToolkit`
	
	Format der Liste:
	`Import-Module .\MigrationValidatorToolkit.psm1;Invoke-MigrationValidatorToolkit -List`
	
	Ausgabeformat: GridView
	`Import-Module .\MigrationValidatorToolkit.psm1;Invoke-MigrationValidatorToolkit -GridView`
	
	ConvertTo-CSv-Format:
		Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`Import-Module .\MigrationValidatorToolkit.psm1;Invoke-MigrationValidatorToolkit -csv`	

Führen Sie das Modul Migration Validator Toolkit PowerShell auf mehreren Zielen aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die ZIP-Datei herunter oder klonen Sie das GitHub Repository.	Wählen Sie eine der folgenden Optionen: • Laden Sie die Zip-Datei herunter. (herunterladen). • Um das Repository GitHub migration-validator-toolkit-for-microsoft-workloads zu klonen, führen Sie den folgenden Git-Befehl in einem Terminalfenster aus: `git clone https://github.com/aws-samples/migration-validator-toolkit-for-microsoft-workloads.git`	Systemadministrator
Aktualisieren Sie die Liste server.csv.	Wenn Sie die ZIP-Datei heruntergeladen haben, gehen Sie wie folgt vor: 1. Entpacken Sie die ZIP-Datei.	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wechseln Sie zum Verzeichnis `Migration ValidatorToolkit\I nputs\ .` 3. Aktualisieren Sie `serverlist.csv` mit dem Hostnamen Ihrer Zielcomputer.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie das Modul auf.	Sie können jeden Computer innerhalb der Domäne verwenden, der einen Domänenbenutzer verwendet , der Administratorzugriff auf Zielcomputer hat. 1. Laden Sie den Quellcode als ZIP-Datei herunter und entpacken Sie die Datei. 2. Führen Sie als Administrator in PowerShell den folgenden Befehl aus: `Import-Module .\MigrationValidatorToolkit.psm1;Invoke-DomainComputers` Die CSV-Ausgabedatei wird `MigrationValidatorToolkit\Outputs\folder` mit dem Präfixnamen `DomainComputers_MigrationAutomations_YYYY-MM-DDTHH-MM-SS` gespeichert.	Systemadministrator

Fehlerbehebung

Problem	Lösung
`MigrationValidatorToolkit` schreibt Informationen über Ausführungen, Befehle und	Sie können Protokolldateien manuell am folgenden Speicherort anzeigen:

Problem	Lösung
Fehler in Protokolldateien auf dem laufenden Host.	1. Wechseln Sie zum Verzeichnis `Migration ValidatorToolkit\logs\ .` 2. Suchen Sie die Protokolldatei. Das Format des Namens der Protokolldatei ist: `ComputerName_MigrationValid atorToolkit_YYYY-MM-SSTHH-MM-SS.log`

Zugehörige Ressourcen

- Optionen, Tools und bewährte Methoden für die Migration von Microsoft-Workloads zu AWS (AWS Prescriptive Guidance)
- Microsoft-Migrationsmuster (AWS Prescriptive Guidance)
- Kostenlose Cloud-Migrationsservices auf AWS (AWS-Dokumentation)
- Vordefinierte Aktionen nach der Markteinführung (Dokumentation für das Anwendungsmarketing)

Zusätzliche Informationen

Häufig gestellte Fragen

Wo kann ich das Modul Migration Validator Toolkit ausführen? PowerShell

Sie können das Modul auf Microsoft Windows Server 2012 R2 oder höher ausführen.

Wann führe ich dieses Modul aus?

Wir empfehlen, dass Sie das Modul während der Bewertungsphase der Migration ausführen.

Ändert das Modul meine vorhandenen Server?

Nein. Alle Aktionen in diesem Modul sind schreibgeschützt.

Wie lange dauert es, das Modul auszuführen?

Die Ausführung des Moduls dauert in der Regel 1—5 Minuten, hängt jedoch von der Ressourcenzuweisung Ihres Servers ab.

Welche Berechtigungen benötigt das Modul, um ausgeführt zu werden?

Sie müssen das Modul von einem lokalen Administratorkonto aus ausführen.

Kann ich das Modul auf physischen Servern ausführen?

Ja, sofern das Betriebssystem Microsoft Windows Server 2012 R2 oder höher ist.

Wie führe ich das Modul skalierbar für mehrere Server aus?

Um das Modul auf mehreren domänengebundenen Computern in großem Umfang auszuführen, folgen Sie den Schritten im Abschnitt Ausführen des Migration Validator PowerShell Toolkit-Moduls auf mehreren Zielen in diesem Handbuch. Verwenden Sie für Computer, die nicht in eine Domäne eingebunden sind, einen Remote-Aufruf oder führen Sie das Modul lokal aus, indem Sie den Schritten im Modul Migration Validator Toolkit PowerShell auf einem einzelnen Ziel ausführen in diesem Handbuch folgen.

Automatisieren Sie Aktivitäten zur Erfassung vor dem Workload für AWS Managed Services unter Windows

Erstellt von Jacob Zhang (AWS), Calvin Yeh (AWS) und Dwayne Bordelon (AWS)

Übersicht

In der Amazon Web Services (AWS) -Cloud verwendet AWS Managed Services (AMS) AMS Workload Ingest (WIGS), um bestehende Workloads in eine von AMS verwaltete VPC zu verschieben. Dieses Muster beschreibt eine Lösung zur Automatisierung gängiger Aktivitäten vor der Workload, wie z. B. das Upgrade von .NET und Windows PowerShell und die Ausführung der von AMS verwalteten Windows WIGS-Validierung vor der Datenaufnahme. Das Muster bietet auch eine einheitliche Benutzeroberfläche für die Ausführungsergebnisse. Es verpackt ein AWS Systems Manager Command-Dokument, das die Aktivitäten vor der Aufnahme durchführt, in eine AWS-Vorlage. CloudFormation Die Vorlage kann wiederholt bereitgestellt werden, ohne dass Zugriff auf Systems Manager selbst erforderlich ist oder dass sie mit Automatisierungen von AMS in Konflikt gerät.

Geschäftlicher Hintergrund

Migrationen zu AMS erfordern die Bereitstellung neuer Amazon Elastic Compute Cloud (Amazon EC2) -Instances mithilfe von AMS verwalteten Amazon Machine Images (AMIs), die AMS-Komponenten enthalten. Alle Workloads oder Anwendungen, die in bestehenden Rechenzentren ausgeführt werden, müssen auf neue EC2 Instances umverteilt werden, die von diesen AMS aus gestartet werden. AMIs Um die potenziell enorme Menge an manueller Arbeit während des Prozesses zu vermeiden, hat das AMS-Team den AMS Workload Ingest (WIGS) -Workflow entwickelt, um Ihre benutzerdefinierten Images in AMS zu integrieren.

Windows-Instances müssen einige Voraussetzungen erfüllen, bevor der WIGS-Prozess stattfindet. PowerShell Windows-Skripts werden normalerweise verwendet, um die notwendigen Vorbereitungen zu treffen (WIGS-Vorbereitung) und um zu überprüfen, ob die Instanzen bereit dafür sind WIGs (WIGS-Validierung vor der Aufnahme). Für die Vorbereitungs- und Validierungsprozesse muss ein Techniker 15 bis 30 Minuten auf jedem Server verbringen, sich manuell anmelden und die Skripts nacheinander ausführen.

Geschäftlicher Faktor

Traditionell können Sie mit Systems Manager betriebliche Aufgaben wie das Ausführen von PowerShell Windows-Skripts automatisieren. Aufgrund der erhöhten Risiken und der häufigen

Konflikte zwischen Automatisierungen von AMS und denen der Benutzer gewährt AMS seinen Benutzern jedoch normalerweise keinen Zugriff auf Systems Manager.

Bei Massenmigrationen mit dem AWS Application Migration Service (AWS MGN) werden PowerShell Windows-Skripts in der `C:\Program Files (x86)\AWS Replication Agent\post_launch folder` Regel automatisch ausgeführt, wenn eine Test- oder Übernahmeinstanz gestartet wird. Diese Skripts stehen jedoch häufig in Konflikt mit Automatisierungen von AMS, wenn sie unmittelbar während des Starts einer Instance ausgeführt werden. Infolgedessen schlägt der Start möglicherweise fehl, ohne dass die Ausführungsergebnisse bereitgestellt werden, die Sie zur Behebung des Fehlers benötigen.

Dieses Muster behebt diese Probleme und bietet eine funktionierende automatisierte Lösung.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit AMS-Onboarding wurde abgeschlossen.
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket im AWS-Konto. Wenn es in dem Konto keinen S3-Bucket gibt, über den Sie die Kontrolle haben, verwenden Sie einen Request for Change (RFC), um einen zu erstellen.
- Die Vorlage Pre WIGs _CFN.json wurde aus dem Repository heruntergeladen. ams-auto-prewigs-windows
- Ein Server, auf den Sie dieses Muster anwenden, muss die folgenden Anforderungen erfüllen:
  - Führen Sie Windows Server 2012 oder höher aus.
  - Im Sandbox-VPC-Migrationssubnetz gestartet oder startbereit sein.
  - Haben Sie einen AWS Systems Manager Agent (SSM Agent) installiert.
  - Haben Sie ein AWS Identity and Access Management (IAM) -Instance-Profil angehängt. Das Instance-Profil muss über Berechtigungen zum Herunterladen von Dateien aus S3-Buckets im selben AWS-Konto verfügen. Ein Instanzprofil, das die oben genannten Anforderungen erfüllt, wurde in der Regel bereits bei früheren Setups einer Migration erstellt.
  - Von AWS Systems Manager Fleet Manager aus sichtbar sein.

Einschränkungen

- Die Aktivitäten vor der WIGS-Einführung variieren je nach Ihrer Umgebung und Ihren Geschäftsanforderungen. Möglicherweise müssen Sie kleinere Änderungen an diesem Muster vornehmen, um es an Ihre spezifischen Bedürfnisse anzupassen.

Produktversionen

- Das Muster wurde mit Windows Server 2012, 2012 R2, 2016 und 2019 getestet. Es funktioniert theoretisch mit späteren Windows-Versionen. Es funktioniert nicht mit früheren Windows-Versionen.

Architektur

Das Architekturdiagramm zeigt Folgendes:

1. Eine Sandbox-VPC mit einem Migrationssubnetz, das Server enthält, die nicht vorbereitet wurden.
2. Der S3-Bucket, in dem Skripts gespeichert werden, die von der Vorlage verwendet werden. CloudFormation
3. Die CloudFormation Vorlage stellt das Systems Manager Command-Dokument bereit. Der Prozess wiederholt sich, bis die Schritte abgeschlossen sind.
4. Die Instanzen sind vorbereitet und RFCs für WIGS erstellt.
5. In der von AMS verwalteten VPC enthält das von AMS verwaltete Subnetz die Server nach der Workload-Aufnahme.

Funktionsweise

- Dieses Muster ist in einer CloudFormation AWS-Vorlage zusammengefasst, die wiederholbare Bereitstellungen von Infrastructure as Code (IaC) ermöglicht. Sie müssen diese Vorlage nur einmal für jedes AWS-Konto bereitstellen, für das diese Automatisierung erforderlich ist.
- Die Automatisierung wird auf alle EC2 Instances mit einem Tag-Schlüssel AutoPreWIGsim AWS-Konto angewendet, in dem dieses Muster bereitgestellt wird. Wenn eine Amazon EC2 Windows-Instance mit dem Tag-Schlüssel zum ersten Mal AutoPreWIGsgestartet wird, führt die Automatisierung die folgenden Aufgaben aus.
  1. Führt ein Upgrade von Windows PowerShell auf Version 5.1 und .NET auf Version 4.5.2 durch. Die Instanz wird je nach den vorhandenen Windows- PowerShell und .NET-Versionen

möglicherweise mehrmals neu gestartet. Nach jedem Neustart werden die Upgrades fortgesetzt, bis sie abgeschlossen sind. In diesem Schritt wird eingebetteter Code in der CloudFormation Vorlage verwendet, der anhand eines PowerShell Windows-Skripts geändert wurde, sowie spezielle Systems Manager Manager-Anleitungen für Serverneustarts.

2. Lädt von Amazon S3 herunter und führt ein PowerShell Windows-Skript aus, das Sie angepasst haben, um die Amazon EC2 Windows-Instance für WIGS vorzubereiten. Weitere Informationen finden Sie im Abschnitt Epics.
3. Installiert das Windows WIGS PowerShell Pre-Ingestion-Validierungsmodul von AWS.
4. Führt die Windows WIGS-Validierung vor der Aufnahme aus und macht die Ergebnisse im Systems Manager State Manager sichtbar.

Tools

- AWS CloudFormation — AWS CloudFormation ist ein Service, der Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen unterstützt. Sie können eine verwenden, die alle gewünschten AWS-Ressourcen und deren Abhängigkeiten beschreibt, sodass Sie diese Ressourcen als Stack starten und konfigurieren können., Dieses Muster verwendet eine CloudFormation Vorlage, um die Bereitstellung der Ressourcen in diesem Muster zu automatisieren.
- AWS Managed Services — AWS Managed Services (AMS) ist ein Unternehmensservice, der die kontinuierliche Verwaltung Ihrer AWS-Infrastruktur ermöglicht. Änderungen an der Infrastruktur in einer AMS-Umgebung müssen über einen RFC vorgenommen werden.
- AWS Systems Manager — AWS Systems Manager (früher bekannt als SSM) ist ein AWS-Service, mit dem Sie Ihre Infrastruktur auf AWS anzeigen und steuern können. Mithilfe der Systems Manager Manager-Konsole können Sie Betriebsdaten von mehreren AWS-Services anzeigen und betriebliche Aufgaben in Ihren AWS-Ressourcen automatisieren. Dieses Muster verwendet Systems Manager, um die Ausführungsergebnisse der Pre-WIGS-Aktivitäten auszuführen und anzuzeigen.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice, der branchenführende Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet. Dieses Muster verwendet Amazon S3 zum Speichern der CloudFormation Vorlage und eines heruntergeladenen PowerShell Windows-Skripts.

Epen

Erstellen Sie ein benutzerdefiniertes PowerShell Windows-Skript, um zusätzliche Aufgaben zu automatisieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Nehmen Sie die erforderlichen Änderungen an den Servern auf der Grundlage der Geschäftsanforderungen vor.	Wenn Sie möchten, dass Änderungen automatisch auf Ihre Server angewendet werden, bevor sie aufgenommen werden, erstellen Sie ein PowerShell Windows-Skript mit dem Namen. `ingestion-prep.ps1` **Important** Das Skript darf keine Anweisungen zum Neustart des Servers enthalten und es darf keine Administratorrechte erfordern.	PowerShell Scripting
Entfernen Sie Software, die von AMS nicht unterstützt wird.	AMS erfordert, dass bestimmte Software, wie z. B. Antiviren-Anwendungen und VMware Tools, entfernt wird, bevor WIGS ausgeführt werden kann. Nehmen Sie die Deinstallation in das `ingestion-prep.ps1` Skript auf. Weitere Informationen zu Software, die nicht unterstützt wird, finden Sie in der AWS-Dokumentation.	PowerShell Scripting

Laden Sie die CloudFormation Vorlage und das optionale PowerShell Windows-Skript auf Amazon S3 hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Ordner in S3.	Erstellen Sie in einem S3-Bucket in demselben AWS-Konto, in dem Sie dieses Muster bereitstellen, einen Ordner.	Allgemeines AWS
Laden Sie die Skripte hoch.	Laden Sie die `PreWIGs_CFN.json` CloudFormation Vorlage und das `ingestion-prep.ps1` PowerShell Windows-Skript, die Sie im vorherigen Epic erstellt haben, in den Amazon S3 S3-Ordner hoch.	Allgemeines AWS

Stellen Sie den CloudFormation Stack bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie den Änderungstyp aus.	Navigieren Sie zur AMS-Konsole, um einen RFC zu erstellen. Verwenden Sie den Änderungstyp Create Stack from CloudFormation (CFN) Template.	Allgemeines AMS
Legen Sie die Ausführungsparameter für den Pfad zur CloudFormation Vorlage fest.	Erweitern Sie im Abschnitt Ausführungskonfiguration den Eintrag Zusätzliche Konfiguration. Fügen Sie im Feld CloudFormation für den S3-Endpunkt der Vorlage	Allgemeines AMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die URL zur CloudFormation Vorlage ein.	
Geben Sie den Pfad zum Amazon S3 S3-Ordner an.	Verwenden Sie unter Parameter ScriptSourceden Namen. Geben Sie unter Value den Pfad zum S3-Ordner ein, der die PowerShel l Windows-Skripts enthält. Stellen Sie sicher, dass Sie die `https://xxx` URL anstelle der `s3://xxx` URI verwenden, und fügen Sie `/` am Ende die hinzu.	Allgemeines AMS
Stellen Sie den Stack bereit.	Um den Stack bereitzustellen, wählen Sie Create.	Allgemeines AMS
Eskalieren Sie den RFC an AMS Ops.	Der RFC muss manuell vom AMS Ops-Team implement iert werden, da es Systems Manager für die Bereitstellung von Ressourcen verwendet und eine Sicherheitsüberprü fung erfordert. Sobald Sie den RFC erstellen, wird er automatisch vom System abgelehnt. Wählen Sie den RFC aus und fügen Sie dem RFC eine Entsprechung mit der Aufschrift Bitte manuell ausführen hinzu. Notieren Sie sich die RFC-ID und eskaliere n Sie sie mit einer Servicean frage.	Allgemeines AMS

Wenden Sie die Automatisierung auf die Instanzen an

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie das AutoPre WIGs Tag zu Instanzen hinzu.	Notieren IDs Sie sich alle Instances, auf die Sie diese Automatisierung anwenden möchten, und warten Sie mindestens 30 Minuten, bis die Instance die von AMS implementierten Automatis ierungen abgeschlossen hat. Reichen Sie einen automatis ierten RFC ein, um das Tag mit AutoPreWIGsdem Schlüssel und einer beliebigen Zeichenfolge, z. B. 1, als Wert hinzuzufügen. Die Automatisierung wird einige Minuten nach dem Hinzufügen des Tags angewendet.	Allgemeines AMS
Überprüfen Sie die Automatis ierungsergebnisse.	Öffnen Sie die Systems Manager Manager-Konsole und wählen Sie State Manager. Wählen Sie die Zuordnungs-ID mit dem Namen AMS-Prewig-Prep-an d-Validation-Association. Auf der Registerkarte Ausführun gsverlauf können Sie die Ergebnisse der Automatis ierung sehen.	Allgemeines AMS
Beheben Sie vorhandene Fehler.	Wenn die Automatisierung fehlschlägt, wählen Sie die	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zugehörige Ausführungs-ID. Sie können die Ausführun gsergebnisse für jede EC2 Instanz sehen. Um die Details für jeden Schritt der Automatis ierung zu sehen, wählen Sie Ausgabe. Wenn ein bestimmter Schritt fehlschlägt, verwenden Sie die Informati onen in den Abschnitten Ausgabe und Fehler, um das Problem zu diagnostizieren.	
Entfernen Sie das AutoPre WIGs Tag.	**Important** Nachdem Sie die Fehler, falls vorhanden , behoben haben, reichen Sie einen automatisierten RFC ein, um das AutoPreWIGsTag zu entfernen. WIGS schlägt fehl, wenn Sie das Tag nicht entfernen.	Allgemeines AMS

Investieren Sie die vorbereiteten Instanzen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
RFCs Für WIGS einreichen.	Jetzt, da die Instances für die Workload-Aufnahme bereit	Allgemeines AMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	sind, reichen Sie das RFCs für WIGS ein.	

Zugehörige Ressourcen

- AMS Workload Ingest (WIGS)
- Migration von Workloads: Windows-Validierung vor der Datenaufnahme
- Kurzanleitung für den AWS Application Migration Service
- Erste Schritte mit AWS CloudFormation
- Einrichtung von AWS Systems Manager

Erstellen Sie einen Genehmigungsprozess für Firewallanfragen während einer Rehost-Migration zu AWS

Erstellt von Srikanth Rangavajhala (AWS)

Übersicht

Wenn Sie Cloud Migration Factory on AWS für eine Rehost-Migration auf die verwenden AWS Application Migration Servicemöchten, ist eine der Voraussetzungen AWS Cloud, dass Sie die TCP-Ports 443 und 1500 offen halten müssen. In der Regel erfordert das Öffnen dieser Firewall-Ports die Zustimmung Ihres Informationssicherheitsteams (InfoSec).

In diesem Muster wird beschrieben, wie Sie bei einer Rehost-Migration auf die Genehmigung einer Firewall-Anfrage von einem InfoSec Team einholen. AWS Cloud Sie können dieses Verfahren verwenden, um zu verhindern, dass Ihre Firewall-Anfrage vom InfoSec Team abgelehnt wird, was teuer und zeitaufwändig werden kann. Der Firewall-Anforderungsprozess umfasst zwei Überprüfungs- und Genehmigungsschritte zwischen AWS Migrationsberatern und Führungskräften, die mit Ihren InfoSec und den Anwendungsteams zusammenarbeiten, um die Firewall-Ports zu öffnen.

Bei diesem Muster wird davon ausgegangen, dass Sie eine Rehost-Migration mit AWS Beratern oder Migrationsspezialisten aus Ihrem Unternehmen planen. Sie können dieses Muster verwenden, wenn in Ihrer Organisation kein Firewall-Genehmigungsverfahren oder kein Formular zur pauschalen Genehmigung für Firewallanfragen eingerichtet wurde. Weitere Informationen dazu finden Sie im Abschnitt Einschränkungen dieses Musters. Weitere Informationen zu den Netzwerkanforderungen für den Application Migration Service finden Sie unter Netzwerkanforderungen in der Dokumentation zum Application Migration Service.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine geplante Rehost-Migration mit AWS Beratern oder Migrationsspezialisten aus Ihrem Unternehmen
- Die für die Migration des Stacks erforderlichen Port- und IP-Informationen
- Bestehende und future Zustandsarchitekturdiagramme
- Firewall-Informationen über die lokale Infrastruktur und die Zielinfrastruktur, die Ports und zone-to-zone den Verkehrsfluss
- Eine Checkliste zur Überprüfung der Firewall-Anfrage (im Anhang)

- Ein Dokument zur Firewall-Anforderung, das gemäß den Anforderungen Ihres Unternehmens konfiguriert wurde
- Eine Kontaktliste für die Prüfer und Genehmiger der Firewall, einschließlich der folgenden Rollen:
  - Einreicher der Firewall-Anfrage — Spezialist oder Berater für AWS Migration. Der Einsender der Firewall-Anfrage kann auch ein Migrationsspezialist aus Ihrem Unternehmen sein.
  - Überprüfer von Firewall-Anfragen — In der Regel handelt es sich dabei um den zentralen Ansprechpartner (SPOC) von. AWS
  - Genehmiger für Firewall-Anfragen — Ein InfoSec Teammitglied.

Einschränkungen

- Dieses Muster beschreibt einen generischen Genehmigungsprozess für Firewallanfragen. Die Anforderungen können für einzelne Organisationen unterschiedlich sein.
- Stellen Sie sicher, dass Sie die Änderungen an Ihrem Firewall-Anforderungsdokument nachverfolgen.

Die folgende Tabelle zeigt die Anwendungsfälle für dieses Muster.

Verfügt Ihr Unternehmen bereits über ein Firewall-Genehmigungsverfahren?	Verfügt Ihr Unternehmen bereits über ein Firewall-Antragsformular?	Vorgeschlagene Maßnahme
Ja	Ja	Arbeiten Sie mit AWS Beratern oder Ihren Migrationsspezialisten zusammen, um den Prozess Ihres Unternehmens zu implementieren.
Nein	Ja	Verwenden Sie den Firewall-Genehmigungsprozess dieses Musters. Verwenden Sie entweder einen AWS Berater oder einen Migrationsspezialisten aus Ihrem Unternehmen, um das Formular zur pauschalen Genehmigung für

		die Firewall-Anfrage einzureic hen.
Nein	Nein	Verwenden Sie den Firewall-Genehmigungsprozess dieses Musters. Verwenden Sie entweder einen AWS Berater oder einen Migrationsspeziali sten aus Ihrem Unternehm en, um das Formular zur pauschalen Genehmigung für die Firewall-Anfrage einzureic hen.

Architektur

Das folgende Diagramm zeigt die Schritte für den Genehmigungsprozess für Firewallanfragen.

Tools

Sie können Scanner-Tools wie Palo Alto Networks oder SolarWindszur Analyse und Validierung von Firewalls und IP-Adressen verwenden.

Epen

Analysieren Sie die Firewall-Anfrage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie die Ports und IP-Adressen.	Der Absender der Firewall-Anfrage führt eine erste Analyse durch, um die erforderlichen Firewall-Ports und IP-Adressen zu ermitteln . Sobald dieser Vorgang abgeschlossen ist, wird Ihr InfoSec Team aufgefordert,	AWS-Cloud-Ingenieur, Migrationsspezialist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die erforderlichen Ports zu öffnen und die IP-Adressen zuzuordnen.	

Validieren Sie die Firewall-Anfrage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Firewall-Informationen.	Der AWS Cloud Techniker vereinbart ein Treffen mit Ihrem InfoSec Team. Während dieses Treffens untersucht und validiert der Techniker die Informationen zur Firewall-Anforderung. In der Regel handelt es sich bei dem Absender der Firewall-Anfrage um dieselbe Person wie der Firewall-Anforderer. Diese Überprüfu ngsphase kann auf der Grundlage des Feedbacks des Genehmiger iterativ werden, falls etwas beachtet oder empfohlen wird.	AWS-Cloud-Ingenieur, Migrationsspezialist
Aktualisieren Sie das Dokument mit der Firewall-Anforderung.	Nachdem das InfoSec Team sein Feedback geteilt hat, wird das Dokument mit der Firewall-Anforderung bearbeitet, gespeichert und erneut hochgeladen. Dieses Dokument wird nach jeder Iteration aktualisiert.	AWS-Cloud-Ingenieur, Migrationsspezialist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wir empfehlen, dieses Dokument in einem versionskontrollierten Speicherordner zu speichern. Das bedeutet, dass alle Änderungen nachverfolgt und korrekt angewendet werden.	

Reichen Sie die Firewall-Anfrage ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Reichen Sie die Firewall-Anfrage ein.	Nachdem der Genehmigungsberechtigte für die Firewall-Anfrage die pauschale Genehmigungsanfrage genehmigt hat, reicht der AWS Cloud Techniker die Firewall-Anfrage ein. In der Anfrage werden die Ports angegeben, die geöffnet sein müssen, und die IP-Adressen, die für die Zuordnung und Aktualisierung der erforderlich sind. AWS-Konto Sie können Vorschläge machen oder Feedback geben, nachdem die Firewall-Anfrage eingereicht wurde. Wir empfehlen Ihnen, diesen Feedback-Prozess zu automatisieren und alle Änderungen über	AWS-Cloud-Ingenieur, Migrationsspezialist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	einen definierten Workflow-Mechanismus zu versenden.	

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

EC2 Windows-Instances in ein AWS Managed Services Services-Konto aufnehmen und migrieren

Erstellt von Anil Kunapareddy (AWS) und Venkatramana Chintha (AWS)

Übersicht

Dieses Muster erklärt den step-by-step Prozess der Migration und Aufnahme von Amazon Elastic Compute Cloud (Amazon EC2) Windows-Instances in ein Amazon Web Services (AWS) Managed Services (AMS) -Konto. AMS kann Ihnen helfen, die Instance effizienter und sicherer zu verwalten. AMS bietet betriebliche Flexibilität, verbessert Sicherheit und Compliance und hilft Ihnen, Kapazitäten zu optimieren und Kosten zu senken.

Dieses Muster beginnt mit einer EC2 Windows-Instance, die Sie in ein Staging-Subnetz in Ihrem AMS-Konto migriert haben. Für diese Aufgabe stehen eine Vielzahl von Migrationsservices und Tools zur Verfügung, z. B. der AWS Application Migration Service.

Um eine Änderung an Ihrer von AMS verwalteten Umgebung vorzunehmen, erstellen Sie eine Änderungsanforderung (Request for Change, RFC) für einen bestimmten Vorgang oder eine bestimmte Aktion und reichen diese ein. Mithilfe eines AMS Workload Ingest (WIGS) -RFC nehmen Sie die Instance in das AMS-Konto auf und erstellen ein benutzerdefiniertes Amazon Machine Image (AMI). Anschließend erstellen Sie die AMS-verwaltete EC2 Instance, indem Sie einen weiteren RFC zur Erstellung eines Stacks einreichen. EC2 Weitere Informationen finden Sie unter AMS Workload Ingest in der AMS-Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives, von AMS verwaltetes AWS-Konto
- Eine bestehende landing zone
- Berechtigungen zum Vornehmen von Änderungen in der von AMS verwalteten VPC
- Eine Amazon EC2 Windows-Instance in einem Staging-Subnetz in Ihrem AMS-Konto
- Erfüllung der allgemeinen Voraussetzungen für die Migration von Workloads mithilfe von AMS WIGS
- Erfüllung der Windows-Voraussetzungen für die Migration von Workloads mit AMS WIGS

Einschränkungen

- Dieses Muster gilt für EC2 Instanzen, auf denen Windows Server ausgeführt wird. Dieses Muster gilt nicht für Instanzen, auf denen andere Betriebssysteme wie Linux ausgeführt werden.

Architektur

Quelltechnologie-Stack

Amazon EC2 Windows-Instance in einem Staging-Subnetz in Ihrem AMS-Konto

Zieltechnologie-Stack

Von AWS Managed Services (AMS) verwaltete Amazon EC2 Windows-Instance

Zielarchitektur

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können Amazon verwenden EC2 , um so viele oder so wenige virtuelle Server zu starten, wie Sie benötigen, und Sie können nach oben oder unten skalieren.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Mit AWS Managed Services (AMS) können Sie effizienter und sicherer arbeiten, indem Sie Ihre AWS-Infrastruktur kontinuierlich verwalten, einschließlich Überwachung, Vorfallmanagement, Sicherheitsberatung, Patch-Support und Backup für AWS-Workloads.

Andere Dienste

- PowerShellist ein Automatisierungs- und Konfigurationsverwaltungsprogramm von Microsoft, das unter Windows, Linux und macOS läuft.

Epen

Konfigurieren Sie die Einstellungen auf der Instanz

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die DNS-Client-Einstellungen.	1. Öffnen Sie auf der EC2 Quellinstanz die Eingabeaufforderung als Administrator, geben Sie ein`pedit.msc` , und drücken Sie dann die Eingabetaste. 2. Navigieren Sie im Editor für lokale Gruppenrichtlinien zu Computerkonfiguration, Administrative Vorlagen, Netzwerk, DNS-Client. 3. Wählen Sie für Primäres DNS-Suffix die Option Nicht konfiguriert aus. 4. Wählen Sie für Dezentral isierung des primären DNS-Suffixes die Option Nicht konfiguriert aus.	Ingenieur für Migration
Ändern Sie die Windows Update-Einstellungen.	1. Navigieren Sie im Editor für lokale Gruppenrichtlinien zu Computerkonfiguration, Administrative Vorlagen, Windows-Komponenten, Windows Update. 2. Wählen Sie für Intranet-Standort für Microsoft Update Service angeben die Option Nicht konfiguriert aus.	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie für Automatische Updates konfigurieren die Option Nicht konfiguriert aus. 4. Wählen Sie für die Erkennungshäufigkeit von automatischen Updates die Option Nicht konfiguriert aus. 5. Schließen Sie den Editor für lokale Gruppenrichtlinien.	
Aktivieren Sie die Firewall.	1. Öffnen Sie auf der EC2 Quellinstanz die Eingabeaufforderung als Administrator, geben Sie ein`services.msc` , und drücken Sie dann die Eingabetaste. 2. Aktivieren Sie in den Windows-Diensten die Firewall. 3. Schließen Sie die Windows-Dienste.	Ingenieur für Migration

Bereiten Sie die Instanz für AMS WIGS vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen Sie die Instanz und bereiten Sie sie vor.	1. Stellen Sie mithilfe eines Bastion-Hosts und lokaler Anmeldeinformationen eine RDP-Verbindung (Remote Desktop Protocol) zur EC2	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Instanz im Staging-Subnetz her. 2. Entfernen Sie alle älteren Software-, Antiviren- und Backup-Lösungen, die in AMS nicht erforderlich sind.	

Reparieren Sie die Datei sppnp.dll.	1. Wechseln Sie zu `C:\Windows\System32\sppnp.dll` .
	2. Umbenennen `sppnp.dll` in `sppnp_old.dll` .
	3. Geben Sie mit PowerShell Administratoranmeldedaten die folgenden Befehle ein:
	`dism /online /cleanup-image /restorehealth`
	`sfc /scannnow`
	4. Starten Sie die EC2 Windows-Instanz neu.
		Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das Pre-WIG-Validierungsskript aus.	1. Laden Sie die ZIP-Datei mit der Windows-WIGS-Validierung vor der Datenaufnahme (`windows-prewings-valication.zip`) unter Migrating workloads: Windows pre-ingestion validation in der AMS-Dokumentation herunter. 2. Führen Sie das Windows Pre-WIG-Validierungsskript aus und überprüfen Sie die Ergebnisse. 3. Wenn die Überprüfung fehlschlägt, beheben Sie das Problem und führen Sie das Überprüfungsskript erneut aus, bis die Überprüfung erfolgreich ist.	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Failsafe-AMI.	Nachdem die Pre-WIG-V alidierung bestanden wurde, erstellen Sie wie folgt ein Pre-Ingestion-AMI: 1. Wählen Sie Deploymen t, Advanced Stack Components, AMI, Create. 2. Fügen Sie während der Erstellung ein Tag hinzu`Key=Name, Value=APPLICATION-ID_IngestReady` . 3. Warten Sie, bis AMI erstellt wurde, bevor Sie fortfahren. Weitere Informationen finden Sie unter AMI | Create in der AMS-Dokumentation.	Ingenieur für Migration

Investieren und validieren Sie die Instanz

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Reichen Sie den RFC ein, um den Workload-Ingest-Stack zu erstellen.	Reichen Sie eine Änderungs anforderung (RFC) ein, um das AMS WIGS zu starten. Anweisungen finden Sie unter Workload Ingest Stack: Creating in der AMS-Dokum entation. Dadurch wird die Workload-Aufnahme gestartet und die gesamte von AMS	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	benötigte Software installie rt, einschließlich Backup-To ols, EC2 Amazon-Verwaltungs software und Antiviren software.	
Bestätigen Sie die erfolgreiche Migration.	Nachdem die Workload-Erfassung abgeschlossen ist, können Sie die AMS-verwa ltete Instance und das AMS-aufgenommene AMI sehen. 1. Melden Sie sich mit Domänenanmeldedaten bei der AMS-verwalteten Instance an. 2. Überprüfen Sie den Domänenbeitritt wie folgt: a. Klicken Sie im Windows Explorer mit der rechten Maustaste auf Dieser PC und wählen Sie dann Eigenschaften. b. Vergewissern Sie sich im Abschnitt Gerätespe zifikation, dass die Domäne im vollständigen Gerätenamen aufgeführt ist. 3. Überprüfen Sie die Quell- und Zielfestplatten.	Ingenieur für Migration

Starten Sie die Instanz im AMS-Zielkonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Reichen Sie den RFC ein, um einen EC2 Stack zu erstellen.	1. Bereiten Sie mithilfe des AMS-aufgenommenen AMI der Windows-I nstance einen RFC für einen EC2 Stack gemäß den Anweisungen unter Stack-Instanz erstellen EC2 in der AMS-Dokum entation vor. Geben Sie im EC2 Stack-RFC alle Parameter an, einschlie ßlich Servername, Tags, Ziel-VPC, Zielsubnetz, Instanztyp, Zielsiche rheitsgruppen, Aufnahme-AMI und Rolle. 2. Reichen Sie den RFC für den EC2 Stack ein und warten Sie dann, bis die Instance erfolgreich erstellt wurde.	Ingenieur für Migration

Zugehörige Ressourcen

AWS Prescriptive Guidance

- Automatisieren Sie Aktivitäten zur Erfassung vor dem Workload für AWS Managed Services unter Windows
- Automatisches Erstellen eines RFC in AMS mit Python

AMS-Dokumentation

- Erfassung von AMS-Workloads
- Wie die Migration Ihre Ressourcen verändert
- Migration von Workloads: Standardprozess

Ressourcen für Marketing

- AWS Managed Services
- AWS Managed Services FAQs
- Ressourcen für AWS Managed Services
- Funktionen von AWS Managed Services

Migrieren Sie eine Couchbase Server-Datenbank zu Amazon EC2

Erstellt von Subhani Shaik (AWS)

Übersicht

Dieses Muster beschreibt, wie Sie Couchbase Server von einer lokalen Umgebung auf Amazon Elastic Compute Cloud (Amazon EC2) migrieren können. AWS

Couchbase Server ist eine verteilte NoSQL-Datenbank (JSON-Dokument), die relationale Datenbankfunktionen bietet. Die Migration einer Couchbase Server-Datenbank AWS kann zu erhöhter Skalierbarkeit, verbesserter Leistung, Kosteneffizienz, verbesserter Sicherheit, vereinfachter Verwaltung und globaler Reichweite führen, was Anwendungen zugute kommen kann, die Datenzugriff mit hoher Verfügbarkeit und geringer Latenz erfordern. Darüber hinaus erhalten Sie über AWS Managed Services Zugriff auf erweiterte Funktionen.

Couchbase Server on AWS bietet die folgenden Hauptfunktionen:

- Architektur, bei der der Arbeitsspeicher im Vordergrund steht
- Hohe Verfügbarkeit, Notfallwiederherstellung und Lastenausgleich
- Bereitstellung auf mehreren Mastern und in mehreren Regionen für optimale Leistung

Weitere Informationen zu den wichtigsten Vorteilen finden Sie im Abschnitt Zusätzliche Informationen und auf der Couchbase-Website.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine aktive AWS-Konto mit einer Virtual Private Cloud (VPC), zwei Availability Zones, privaten Subnetzen und einer Sicherheitsgruppe. Anweisungen finden Sie unter Erstellen einer VPC in der Dokumentation zu Amazon Virtual Private Cloud (Amazon VPC).
- Konnektivität zwischen Quell- und Zielumgebungen aktiviert. Informationen zu den von Couchbase Server verwendeten TCX-Ports finden Sie in der Couchbase-Dokumentation.

Architektur

Das folgende Diagramm zeigt die High-Level-Architektur für die Migration von Couchbase Server zu. AWS

Aus dem lokalen Couchbase-Cluster werden Daten über ein Kunden-Gateway übertragen, indem AWS Direct Connect Die Daten passieren einen Router und eine AWS Direct Connect Route und erreichen die VPC über ein AWS Virtual Private Network (AWS VPN) -Gateway. Die VPC enthält eine EC2 Instanz, auf der Couchbase Server ausgeführt wird. Die AWS Infrastruktur umfasst auch AWS Identity and Access Management (IAM) für die Zugriffskontrolle, AWS Key Management Service (AWS KMS) für die Datenverschlüsselung, Amazon Elastic Block Store (Amazon EBS) für Blockspeicher und Amazon Simple Storage Service (Amazon S3) für die Datenspeicherung.

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- AWS Direct Connectverbindet Ihr internes Netzwerk über ein Standard-Ethernet-Glasfaserkabel mit einem AWS Direct Connect Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt zur Öffentlichkeit einrichten AWS-Services und dabei Internetdienstanbieter in Ihrem Netzwerkpfad umgehen.

Bewährte Methoden

- Installation und Konfiguration von Couchbase auf verschiedenen Betriebsplattformen
- Bewährte Methoden für die Bereitstellung von Couchbase Server auf AWS
- Einen Couchbase-Cluster erstellen
- Bewährte Methoden zur Leistung von Couchbase-Anwendungen
- Bewährte Sicherheitsmethoden für Couchbase Server
- Bewährte Speichermethoden für Couchbase Server-Datenbanken

Epen

Stellen Sie eine EC2 Amazon-Instance für Couchbase Server bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Öffnen Sie die EC2 Amazon-Konsole.	Melden Sie sich bei der an AWS Management Consoleund öffnen Sie die EC2 Amazon-Konsole.	DevOps Ingenieur, Couchbase -Administrator
Stellen Sie eine EC2 Amazon-Instance bereit.	Starten Sie eine EC2 Instance, die den lokalen Couchbase Server-Konfigurationen entspricht. Weitere Informati onen zur Bereitstellung einer EC2 Instance finden Sie unter Starten einer EC2 Amazon-In stance in der EC2 Amazon-Do kumentation.	DevOps Ingenieur, Couchbase -Administrator

Installieren und konfigurieren Sie Couchbase Server auf Amazon EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie einen Couchbase-Cluster.	Lesen Sie die Bereitste llungsrichtlinien für Couchbase Server, bevor Sie Couchbase Server auf Amazon installie ren. EC2 Informationen zur Installation von Couchbase Server finden Sie in der Couchbase Server-Dokumentation	Couchbase-Administrator
Konfigurieren Sie den Cluster.	Informationen zur Konfigura tion des Clusters finden Sie	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	unter Cluster-Konfigurationsoptionen in der Couchbase-Dokumentation.	

Fügen Sie einen neuen Knoten hinzu und gleichen Sie den Couchbase-Cluster neu aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie einen Knoten für die EC2 Instanz hinzu.	Fügen Sie die neu bereitgestellte EC2 Instanz, auf der Couchbase installiert ist, dem vorhandenen lokalen Cluster hinzu. Anweisungen finden Sie in der Couchbase Server-Dokumentation unter Knoten hinzufügen und Rebalancing durchführen.	Couchbase-Administrator
Richten Sie den Cluster neu aus.	Durch den Rebalancing-Prozess wird der neu hinzugefügte Knoten mit der EC2 Instanz zu einem aktiven Mitglied des Couchbase-Clusters. Anweisungen finden Sie in der Couchbase Server-Dokumentation unter Knoten hinzufügen und Rebalance neu ausrichten	Couchbase-Administrator

Verbindungen neu konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die lokalen Knoten und führen Sie eine Neuverteilung durch.	Sie können jetzt die lokalen Knoten aus dem Cluster entfernen. Nachdem Sie die Knoten entfernt haben, folgen Sie dem Rebalance-Prozess, um Daten, Indizes, Ereignis- und Abfrageverarbeitung auf die verfügbaren Knoten im Cluster neu zu verteilen . Anweisungen finden Sie in der Couchbase Server-Dokumentation unter Knoten entfernen und neu verteilen.	Couchbase-Administrator
Aktualisieren Sie die Verbindungsparameter.	Aktualisieren Sie die Verbindungsparameter Ihrer Anwendung, sodass sie die neue EC2 Amazon-IP-Adresse verwenden, damit Ihre Anwendung eine Verbindung zum neuen Knoten herstellen kann.	Entwickler der Couchbase-Anwendung

Zugehörige Ressourcen

- Couchbase-Server-Dienste
- Stellen Sie Couchbase Server bereit mit AWS Marketplace
- Connect zum Couchbase Server her
- Buckets verwalten
- Rechenzentrumsübergreifende Replikation (XDCR)
- Lizenzvereinbarung von Couchbase Inc.

Zusätzliche Informationen

Die wichtigsten Vorteile

Die Migration Ihrer Couchbase-Datenbank zu AWS bietet die folgenden Vorteile:

Skalierbarkeit. Sie können Ihren Couchbase-Cluster je nach Bedarf nach oben oder unten skalieren, ohne physische Hardware verwalten zu müssen, sodass Sie schwankende Datenmengen und Anwendungsnutzung problemlos bewältigen können. AWS bietet:

- Optionen für die vertikale und horizontale Skalierung
- Funktionen für den weltweiten Einsatz
- Lastenausgleich zwischen AWS-Regionen
- Lösungen zur Datenbankskalierung
- Optimierung der Inhaltsbereitstellung

Optimierung der Leistung. AWS bietet eine leistungsstarke Netzwerkinfrastruktur und optimierte Instanztypen, um einen schnellen Datenzugriff und eine geringe Latenz für Ihre Couchbase-Datenbank zu gewährleisten.

- Optionen für Hochleistungsdatenverarbeitung (HPC)
- Weltweite Bereitstellung von Inhalten über Amazon CloudFront
- Mehrere Speicheroptionen
- Erweiterte Datenbankservices, einschließlich Amazon Relational Database Service (Amazon RDS) und Amazon DynamoDB
- Verbindungen mit niedriger Latenz mit AWS Direct Connect

Kostenoptimierung. Wählen Sie den geeigneten Instanztyp und die entsprechende Konfiguration aus, um Leistung und Kosten auf der Grundlage Ihrer Arbeitslast in Einklang zu bringen. Zahlen Sie nur für die Ressourcen, die Sie tatsächlich nutzen. Dadurch können Sie potenziell Ihre Betriebskosten senken, da Sie keine Hardware vor Ort verwalten müssen und AWS Cloud Skaleneffekte nutzen.

- Reserved Instances können Ihnen helfen, vorausschauend zu planen und Ihre Kosten erheblich zu senken, wenn Sie Couchbase on verwenden. AWS
- Die automatische Skalierung verhindert eine übermäßige Bereitstellung und hilft Ihnen, Ihre Auslastung und Kosteneffizienz zu optimieren.

Verbesserte Sicherheit. Profitieren Sie von den robusten Sicherheitsfunktionen wie Datenverschlüsselung AWS, Zugriffskontrollen und Sicherheitsgruppen, um die vertraulichen Daten, die Sie in Couchbase speichern, zu schützen. Zusätzliche Vorteile:

- Das Modell der AWS gemeinsamen Verantwortung unterscheidet klar zwischen der Sicherheit der Cloud (AWS Verantwortung) und der Sicherheit in der Cloud (Kundenverantwortung).
- AWS Die Einhaltung der Vorschriften unterstützt wichtige Sicherheitsstandards.
- AWS bietet erweiterte Verschlüsselungsoptionen.
- AWS Identity and Access Management (IAM) unterstützt Sie bei der Verwaltung des sicheren Zugriffs auf Ihre Ressourcen.

Vereinfachtes Management. AWS bietet verwaltete Dienste für Couchbase, sodass Sie sich auf die Anwendungsentwicklung konzentrieren können, anstatt die zugrunde liegende Infrastruktur zu verwalten.

Globale Reichweite. Sie können Ihren Couchbase-Cluster auf mehreren Servern einsetzen, AWS-Regionen um eine geringe Latenz für Benutzer auf der ganzen Welt zu erreichen. Sie können Ihre Datenbanken vollständig in der Cloud oder in einer Hybridumgebung bereitstellen. Sie können Ihre Daten mit integrierter Sicherheit auf Unternehmensniveau und schneller, effizienter bidirektionaler Synchronisation von Daten vom Edge bis zur Cloud schützen. Gleichzeitig können Sie die Entwicklung mit einem konsistenten Programmiermodell für die Erstellung von Web- und mobilen Apps vereinfachen.

Geschäftskontinuität:

- Datensicherung und Wiederherstellung. Im Falle eines Problems können Sie damit AWS Backupdie Datenstabilität und die einfache Wiederherstellung sicherstellen. Optionen für die Notfallwiederherstellung finden Sie in der AWS Well-Architected Framework-Dokumentation.
- Bereitstellung von Couchbase in mehreren Regionen: Um eine Couchbase-Datenbank in einer AWS Umgebung mit mehreren Regionen bereitzustellen, können Sie Couchbase Server in abonnieren, AWS CloudFormationVorlagen verwenden, um separate Couchbase-Cluster in jeder Region zu erstellen AWS Marketplace, und dann die regionsübergreifende Replikation konfigurieren, um Daten zwischen Regionen zu synchronisieren. Diese Konfiguration gewährleistet eine hohe Verfügbarkeit und geografische Redundanz in mehreren Regionen. Weitere Informationen finden Sie unter Deploy Couchbase Server Using AWS Marketplace in der Couchbase-Dokumentation.

Agilität der Infrastruktur:

- Schnelle Bereitstellung und Deprovisionierung von Ressourcen
- Globale Reichweite der Infrastruktur
- Automatische Skalierung je nach Bedarf
- Infrastructure as Code (IaC) für konsistente Bereitstellungen
- Mehrere Instance-Typen, die für unterschiedliche Workloads optimiert sind

Förderung von Innovationen:

- Zugang zu den neuesten Technologien, einschließlich KI/ML, IoT und Analytik
- Verwaltete Services, die den betrieblichen Aufwand reduzieren
- Moderne Verfahren zur Anwendungsentwicklung
- Serverlose Computeroptionen

Operative Exzellenz:

- Zentralisierte Überwachung und Protokollierung
- Automatisiertes Ressourcenmanagement
- Funktionen für vorausschauende Wartung
- Verbesserter Einblick in die Ressourcennutzung
- Optimierte Bereitstellungsprozesse

Möglichkeiten zur Modernisierung:

- Microservices-Architektur
- DevOpspraktiziert die Implementierung
- Cloud-native Anwendungsentwicklung
- Modernisierung älterer Anwendungen

Wettbewerbsvorteile:

- Schnellere Markteinführungszeit
- Verbessertes Kundenerlebnis

- Datengestützte Entscheidungsfindung
- Verbesserte Geschäftsintelligenz

Migrieren Sie Db2 for LUW zu Amazon mithilfe EC2 von Protokollversand, um Ausfallzeiten zu reduzieren

Erstellt von Feng Cai (AWS), Ambarish Satarkar (AWS) und Saurabh Sharma (AWS)

Übersicht

Wenn Kunden ihre IBM Db2 for LUW-Workloads (Linux, UNIX und Windows) zu Amazon Web Services (AWS) migrieren, ist die Verwendung von Amazon Elastic Compute Cloud (Amazon EC2) mit dem Bring Your Own License (BYOL) -Modell der schnellste Weg. Die Migration großer Datenmengen von lokalem Db2 nach AWS kann jedoch eine Herausforderung sein, insbesondere wenn das Ausfallfenster kurz ist. Viele Kunden versuchen, das Ausfallfenster auf weniger als 30 Minuten festzulegen, sodass wenig Zeit für die Datenbank selbst bleibt.

Dieses Muster beschreibt, wie eine Db2-Migration mit einem kurzen Ausfallfenster mithilfe des Transaktionsprotokollversands durchgeführt werden kann. Dieser Ansatz gilt für Db2 auf einer Little-Endian-Linux-Plattform.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Db2-Instance, die auf einer EC2 Instance ausgeführt wird, die den lokalen Dateisystem-Layouts entspricht
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket, auf den die EC2 Instance zugreifen kann
- Eine Richtlinie und Rolle für AWS Identity and Access Management (IAM) für programmatische Aufrufe an Amazon S3
- Synchronisierte Zeitzone und Systemuhren auf Amazon EC2 und dem lokalen Server
- Das lokale Netzwerk, das über AWS Site-to-SiteVPN oder AWS AWS Direct Connect verbunden ist

Einschränkungen

- Die lokale Db2-Instance und Amazon EC2 müssen sich auf derselben Plattformfamilie befinden.
- Der lokale Db2-Workload muss protokolliert werden. Um alle nicht protokollierten Transaktionen zu blockieren, legen Sie dies `blocknonlogged=yes` in der Datenbankkonfiguration fest.

Versionen der Produkte

- Db2 für LUW Version 11.5.9 und höher

Architektur

Quelltechnologie-Stack

- Db2 auf Linux x86_64

Zieltechnologie-Stack

- Amazon EBS
- Amazon EC2
- AWS Identity and Access Management (IAM)
- Amazon S3
- AWS Site-to-Site VPN oder Direct Connect

Zielarchitektur

Das folgende Diagramm zeigt eine lokal ausgeführte Db2-Instance mit einer VPN-Verbindung (Virtual Private Network) zu Db2 auf Amazon. EC2 Die gepunkteten Linien stellen den VPN-Tunnel zwischen Ihrem Rechenzentrum und der AWS-Cloud dar.

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS Direct Connect verbindet Ihr internes Netzwerk über ein Standard-Ethernet-Glasfaserkabel mit einem Direct Connect-Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt zu öffentlichen AWS-Services erstellen und dabei Internetdienstanbieter in Ihrem Netzwerkpfad umgehen.
- Amazon Elastic Block Store (Amazon EBS) bietet Speichervolumes auf Blockebene zur Verwendung mit Amazon Elastic Compute Cloud (Amazon EC2) -Instances.

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Mit AWS Site-to-Site VPN können Sie den Datenverkehr zwischen Instances, die Sie auf AWS starten, und Ihrem eigenen Remote-Netzwerk weiterleiten.

Andere Tools

- db2cli ist der interaktive Db2-CLI-Befehl.

Bewährte Methoden

- Verwenden Sie in der Zieldatenbank Gateway-Endpunkte für Amazon S3, um auf das Datenbank-Backup-Image und die Protokolldateien in Amazon S3 zuzugreifen.
- Verwenden Sie in der Quelldatenbank AWS PrivateLink für Amazon S3, um das Datenbank-Backup-Image und die Protokolldateien an Amazon S3 zu senden.

Epen

Festlegen von Umgebungsvariablen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie Umgebungs variablen fest.	Dieses Muster verwendet die folgenden Namen: • Instance-Name: `db2inst1` • Datenbankname: `SAMPLE`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie können sie an Ihre Umgebung anpassen.	

Konfigurieren Sie den lokalen Db2-Server

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Einrichten des AWS CLI.	Führen Sie die folgenden Befehle aus, um die neueste Version der AWS-CLI herunterzuladen und zu installieren:
	`$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"`
	`unzip awscliv2.zip`
	`sudo ./aws/install`
		Linux-Administrator

Richten Sie ein lokales Ziel für Db2-Archivprotokolle ein.	Um die Zieldatenbank auf Amazon EC2 mit der lokalen Quelldatenbank synchron zu halten, müssen die neuesten Transaktionsprotokolle von der Quelle abgerufen werden. In diesem Setup `/db2logs` wird von `LOGARCHMETH2` auf der Quelle als Staging-Bereich festgelegt. Die archivierten Protokolle in diesem Verzeichnis werden mit Amazon S3 synchronisiert und von Db2 auf Amazon	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	abgerufen. EC2 Das Muster wird verwendetLOGARCHMETH2 , weil LOGARCHMETH1 es möglicherweise für die Verwendung eines Drittanbietertools konfiguriert wurde, auf das der AWS-CLI-Befehl nicht zugreifen kann. Führen Sie den folgenden Befehl aus, um die Protokolle abzurufen:
	`db2 connect to sample`
	`db2 update db cfg for SAMPLE using LOGARCHMETH2 disk:/db2logs`	

Führen Sie eine Online-Datenbanksicherung durch.	Führen Sie eine Online-Datenbanksicherung aus und speichern Sie sie im lokalen Backup-Dateisystem: `db2 backup db sample online to /backup`	DBA

Richten Sie den S3-Bucket und die IAM-Richtlinie ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Erstellen Sie einen S3-Bucket für den lokalen Server, an den die Backup-DB2-Images und Protokolldateien auf AWS gesendet werden sollen. Auf den Bucket wird auch Amazon zugreifen EC2:	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws s3api create-bucket --bucket logshipmig-db2 --region us-east-1`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Richtlinie.	Die `db2bucket.json` Datei enthält die IAM-Richtlinie für den Zugriff auf den Amazon S3 S3-Bucket: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "kms:GenerateDataKey", "kms:Decrypt", "s3:PutObject", "s3:GetObject", "s3:AbortMultipartUpload", "s3:ListBucket", "s3:DeleteObject", "s3:GetObjectVersion", "s3:ListMultipartUploadParts" ], "Resource": [`	AWS-Administrator, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"arn:aws:s3:::logshipmig-db2/*",
	
	"arn:aws:s3:::logshipmig-db2"
	]
	}
	]
	}</pre>
	Verwenden Sie den folgenden AWS-CLI-Befehl, um die Richtlinie zu erstellen:
	<pre>aws iam create-policy \
	--policy-name db2s3policy \
	--policy-document file://db2bucket.json</pre>
	Die JSON-Ausgabe zeigt den Amazon-Ressourcennamen (ARN) für die Richtlinie, wobei `aws_account_id` es sich um Ihre Konto-ID handelt:
	<pre>"Arn": "arn:aws:iam::aws_account_id:policy/db2s3policy"</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Hängen Sie die IAM-Richtlinie an die von der Instance verwendete IAM-Rolle an EC2 .	In den meisten AWS-Umgebungen hat eine laufende EC2 Instance eine IAM-Rolle, die von Ihrem Systemadministrator festgelegt wurde. Wenn die IAM-Rolle nicht festgelegt ist, erstellen Sie die Rolle und wählen Sie in der EC2 Konsole IAM-Rolle modifizieren aus, um die Rolle der EC2 Instance zuzuordnen, die die Db2-Datenbank hostet. Hängen Sie die IAM-Richtlinie mit dem Richtlinien-ARN an die IAM-Rolle an: `aws iam attach-role-policy \ --policy-arn "arn:aws:iam::aws_account_id:policy/db2s3policy" \ --role-name db2s3role` Nachdem die Richtlinie angehängt wurde, kann jede EC2 Instance, die der IAM-Rolle zugeordnet ist, auf den S3-Bucket zugreifen.	AWS-Administrator, AWS-Systemadministrator

Senden Sie das Backup-Image und die Protokolldateien der Quelldatenbank an Amazon S3

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie die AWS-CLI auf dem lokalen Db2-Server.	Konfigurieren Sie die AWS-CLI mit dem `Access Key ID` und, das im vorherigen Schritt `Secret Access Key` generiert wurde:
	`$ aws configure`
	`AWS Access Key ID [None]: **********`
	`AWS Secret Access Key [None]: ********** **********`
	`Default region name [None]: us-east-1`
	`Default output format [None]: json`
		AWS-Administrator, AWS-Systemadministrator

Senden Sie das Backup-Image an Amazon S3.	Zuvor wurde ein Online-Datenbank-Backup im `/backup` lokalen Verzeichnis gespeichert. Führen Sie den folgenden Befehl aus, um dieses Backup-Image an den S3-Bucket zu senden: `aws s3 sync /backup s3://logshipmig-db2/SAMPLE_backup`	AWS-Administrator, Migrationsingenieur
Senden Sie die Db2-Archivprotokolle an Amazon S3.	Synchronisieren Sie die lokalen Db2-Archivprotokolle mit dem S3-Bucket, auf den die Db2-Zielinstanz bei Amazon zugreifen kann: EC2	AWS-Administrator, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws s3 sync /db2logs s3://logshipmig-db2/SAMPLE_LOG` Führen Sie diesen Befehl regelmäßig mithilfe von Cron oder anderen Planungstools aus. Die Häufigkeit hängt davon ab, wie oft die Quelldatenbank Transaktionsprotokolldateien archiviert.	

Connect Db2 on Amazon mit Amazon EC2 S3 und starten Sie die Datenbanksynchronisierung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie einen PKCS12 Keystore.	Db2 verwendet einen PKCS-Verschlüsselungs-Keystore (Public-Key Cryptography Standards), um den AWS-Zugriffsschlüssel zu schützen. Erstellen Sie einen Keystore und konfigurieren Sie die Db2-Quellinstanz so, dass sie ihn verwendet:
	
	`gsk8capicmd_64 -keydb -create -db "/home/db2inst1/.keystore/db2s3.p12" -pw "<password>" -type pkcs12 -stash`
	
	`db2 "update dbm cfg using keystore_location /home/db2`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`inst1/.keystore/db2s3.p12 keystore_type pkcs12"`	

Erstellen Sie den Alias für den Db2-Speicherzugriff.	Verwenden Sie die folgende Skriptsyntax, um den Alias für den Speicherzugriff zu erstellen:
	
	`db2 "catalog storage access alias <alias_name> vendor S3 server <S3 endpoint> container '<bucket_name>'"`
	
	Ihr Skript könnte beispielsweise wie folgt aussehen:
	
	`db2 "catalog storage access alias DB2AWSS3 vendor S3 server s3.us-east-1.amazonaws.com container 'logshipmig-db2'"`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Bereitstellungsbereich ein.	Standardmäßig verwendet Db2 `DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH` als Staging-Bereich zum Hoch- und Herunterladen von Dateien zu und von Amazon S3. Der Standardpfad befindet sich `sqllib/tmp/RemoteStorage.xxxx` im Home-Verzeichnis der Instance und `xxxx` bezieht sich auf die Db2-Partitionsnummer. Beachten Sie, dass der Staging-Bereich über genügend Kapazität für die Backup-Images und Protokolldateien verfügen muss. Sie können die Registrierung verwenden, um den Staging-Bereich auf ein anderes Verzeichnis zu verweisen. Wir empfehlen außerdem `DB2_ENABLE_COS_SDK=ON`, und den Link zur `awssdk` Bibliothek zu verwenden `DB2_OBJECT_STORAGE_SETTINGS=EnableStreamingRestore`, um den Amazon S3 S3-Staging-Bereich für Datenbanksicherungen und -wiederherstellungen zu umgehen:	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`#By root:`
	`cp -rp /home/db2inst1/sqllib/lib64/awssdk/RHEL/7.6/* /home/db2inst1/sqllib/lib64/`
	
	`#By db2 instance owner:`
	`db2set DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH=/db2stage`
	`db2set DB2_ENABLE_COS_SDK=ON`
	`Db2set DB2_OBJECT_STORAGE_SETTINGS=EnableStreamingRestore`
	`db2stop`
	`db2start`	

Stellen Sie die Datenbank aus dem Backup-Image wieder her.	Stellen Sie die Zieldatenbank auf Amazon EC2 aus dem Backup-Image im S3-Bucket wieder her: `db2 restore db sample from DB2REMOTE://DB2AWSS3/logshipmig-db2/SAMPLE_backup replace existing`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Die Datenbank weiterleiten.	Nach Abschluss der Wiederherstellung wird die Zieldatenbank in den Status „Rollforward ausstehend“ versetzt. Konfigurieren Sie `LOGARCHMETH1` `LOGARCHMETH2` so, dass Db2 weiß, wo die Transaktionsprotokolldateien abgerufen werden sollen:
	`db2 update db cfg for SAMPLE using LOGARCHMETH1 'DB2REMOTE://DB2AWSS3//SAMPLE_LOGS/'`
	`db2 update db cfg for SAMPLE using LOGARCHMETH2 OFF`
	Starten Sie den Datenbank-Rollforward:
	`db2 ROLLFORWARD DATABASE sample to END OF LOGS`
	Dieser Befehl verarbeitet alle Protokolldateien, die in den S3-Bucket übertragen wurden. Führen Sie ihn regelmäßig auf der Grundlage der Häufigkeit des `s3 sync` Befehls auf den lokalen Db2-Servern aus. Wenn der Befehl beispielsweise zu jeder Stunde `s3 sync` ausgeführt wird und
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Synchronisierung aller Protokolldateien 10 Minuten dauert, legen Sie fest, dass der Befehl jeweils 10 Minuten nach jeder Stunde ausgeführt wird.	

Bringen Sie Db2 auf Amazon während des EC2 Umstellungsfensters online

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bringen Sie die Zieldatenbank online.	Führen Sie während des Übernahmefensters einen der folgenden Schritte aus:
	• Platzieren Sie die lokale Datenbank und führen Sie den `s3 sync` Befehl aus`ADMIN MODE`, um die Archivierung des letzten Transaktionsprotokolls zu erzwingen.
	• Fahren Sie die Datenbank herunter.
	
	Nachdem das letzte Transakti onsprotokoll mit Amazon S3 synchronisiert wurde, führen Sie den `ROLLFORWARD` Befehl zum letzten Mal aus:
	`db2 rollforward DB sample to END OF LOGS`
	`db2 rollforward DB sample complete`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`Rollforward Status .... Rollforward status = not pending .... DB20000I The ROLLFORWARD command completed successfully.`
	
	`db2 activate db sample DB20000I The ACTIVATE DATABASE command completed successfully.`
	
	Bringen Sie die Zieldatenbank online und verweisen Sie die Anwendungsverbindungen auf Db2 on Amazon EC2.	

Fehlerbehebung

Problem	Lösung
Wenn mehrere Datenbanken denselben Instanznamen und Datenbanknamen auf unterschiedlichen Hosts (DEV, QA, PROD) haben, werden Backups und Logs möglicher weise in dasselbe Unterverzeichnis verschobe n.	Verwenden Sie unterschiedliche S3-Bucket s für DEV, QA und PROD und fügen Sie den Hostnamen als Unterverzeichnispräfix hinzu, um Verwirrung zu vermeiden.

Problem	Lösung
Wenn sich mehrere Backup-Images am selben Speicherort befinden, wird bei der Wiederherstellung die folgende Fehlermeldung angezeigt: `SQL2522N More than one backup file matches the time stamp value provided for the backed up database image.`	Fügen Sie im `restore` Befehl den Zeitstempel der Sicherung hinzu: `db2 restore db sample from DB2REMOTE://DB2AWSS3/logshipmig-db2/SAMPLE_backup taken at 20230628164042 replace existing`

Zugehörige Ressourcen

- DB2-Backup- und Wiederherstellungsvorgänge zwischen verschiedenen Betriebssystemen und Hardwareplattformen
- Richten Sie Db2 STORAGE ACCESS ALIAS und REMOTE ein DB2
- Db2-Befehl ROLLFORWARD
- Methode für die sekundäre Protokollarchivierung von Db2

Migrieren Sie Db2 for LUW zu Amazon EC2 mit Disaster Recovery mit hoher Verfügbarkeit

Erstellt von Feng Cai (AWS), Aruna Gangireddy (AWS) und Venkatesan Govindan (AWS)

Übersicht

Wenn Kunden ihren IBM Db2 LUW-Workload (Linux, UNIX und Windows) zu Amazon Web Services (AWS) migrieren, ist die Verwendung von Amazon Elastic Compute Cloud (Amazon EC2) mit dem Bring Your Own License (BYOL) -Modell der schnellste Weg. Die Migration großer Datenmengen von lokalem Db2 nach AWS kann jedoch eine Herausforderung sein, insbesondere wenn das Ausfallfenster kurz ist. Viele Kunden versuchen, das Ausfallfenster auf weniger als 30 Minuten festzulegen, sodass wenig Zeit für die Datenbank selbst bleibt.

Dieses Muster beschreibt, wie eine Db2-Migration mit einem kurzen Ausfallfenster mithilfe von Db2 High Availability Disaster Recovery (HADR) durchgeführt werden kann. Dieser Ansatz gilt für Db2-Datenbanken, die sich auf der Little-Endian-Linux-Plattform befinden und die Datenpartitionsfunktion (DPF) nicht verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Db2-Instance, die auf einer EC2 Amazon-Instance ausgeführt wird und den lokalen Dateisystem-Layouts entspricht
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket, auf den die EC2 Instance zugreifen kann
- Eine Richtlinie und Rolle für AWS Identity and Access Management (IAM) für programmatische Aufrufe an Amazon S3
- Synchronisierte Zeitzone und Systemuhren auf Amazon EC2 und dem lokalen Server
- Das lokale Netzwerk, das über AWS Site-to-SiteVPN oder AWS AWS Direct Connect verbunden ist
- Kommunikation zwischen dem lokalen Server und Amazon EC2 über HADR-Ports

Einschränkungen

- Die lokale Db2-Instance und Amazon EC2 müssen sich auf derselben Plattformfamilie befinden.

- HADR wird in einer partitionierten Datenbankumgebung nicht unterstützt.
- HADR unterstützt die Verwendung von Raw-I/O (direkter Festplattenzugriff) für Datenbank-Logdateien nicht.
- HADR unterstützt keine unendliche Protokollierung.
- `LOGINDEXBUILD`muss auf gesetzt sein`YES`, wodurch die Protokollnutzung für die Neuerstellung des Index erhöht wird.
- Die lokale Db2-Arbeitslast muss protokolliert werden. `blocknonlogged=yes`In der Datenbankkonfiguration so eingestellt, dass alle nicht protokollierten Transaktionen blockiert werden.

Versionen der Produkte

- Db2 für LUW Version 11.5.9 und höher

Architektur

Quelltechnologie-Stack

- Db2 auf Linux x86_64

Zieltechnologie-Stack

- Amazon EC2
- AWS Identity and Access Management (IAM)
- Amazon S3
- Site-to-SiteAWS-VPN

Zielarchitektur

In der folgenden Abbildung wird Db2 on Premises `db2-server1` als primäres System ausgeführt. Es hat zwei HADR-Standby-Ziele. Ein Standby-Ziel befindet sich vor Ort und ist optional. Das andere Standby-Ziel,`db2-ec2`, befindet sich bei Amazon EC2. Nachdem die Datenbank auf AWS umgestellt wurde, `db2-ec2` wird sie zur primären Datenbank.

1. Protokolle werden von der lokalen Primärdatenbank zur lokalen Standby-Datenbank gestreamt.

2. Mithilfe von Db2 HADR werden Protokolle von der primären lokalen Datenbank über Site-to-Site VPN zu Db2 bei Amazon gestreamt. EC2
3. DB2-Backup- und Archivierungsprotokolle werden von der primären lokalen Datenbank an den S3-Bucket auf AWS gesendet.

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS Direct Connect verbindet Ihr internes Netzwerk über ein Standard-Ethernet-Glasfaserkabel mit einem Direct Connect-Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt zu öffentlichen AWS-Services erstellen und dabei Internetdienstanbieter in Ihrem Netzwerkpfad umgehen.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Mit AWS Site-to-Site VPN können Sie den Datenverkehr zwischen Instances, die Sie auf AWS starten, und Ihrem eigenen Remote-Netzwerk weiterleiten.

Andere Tools

- db2cli ist der interaktive Db2-CLI-Befehl.

Bewährte Methoden

- Verwenden Sie in der Zieldatenbank Gateway-Endpunkte für Amazon S3, um auf das Datenbank-Backup-Image und die Protokolldateien in Amazon S3 zuzugreifen.
- Verwenden Sie in der Quelldatenbank AWS PrivateLink für Amazon S3, um das Datenbank-Backup-Image und die Protokolldateien an Amazon S3 zu senden.

Epen

Festlegen von Umgebungsvariablen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie Umgebungs variablen fest.	Dieses Muster verwendet die folgenden Namen und Ports: 1. Lokaler DB2-Hostname: `db2-server1` 2. HADR-Standby-Hostn ame: `db2-server2` (wenn HADR derzeit lokal ausgeführt wird) 3. EC2 Amazon-Hostname: `db2-ec2` 4. Instance-Name: `db2inst1` 5. Datenbankname: `SAMPLE` 6. Festplattenanschlüsse: • `db2-server1: 50010` • `db2-server2: 50011` • `db2-ec2: 50012` Sie können sie an Ihre Umgebung anpassen.	DBA

Konfigurieren Sie den lokalen Db2-Server

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die AWS-CLI ein.	Führen Sie die folgenden Befehle aus, um die neueste Version von AWS CLI	Linux-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	herunterzuladen und zu installieren:
	
	`$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"`
	`unzip awscliv2.zip`
	`sudo ./aws/install`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie ein lokales Ziel für Db2-Archivprotokolle ein.	Bedingungen wie umfangreiche Batch-Aktualisierungsaufträge und Netzwerkverlangsamungen können dazu führen, dass der HADR-Standby-Server verzögert wird. Um catch, benötigt der Standby-Server die Transaktionsprotokolle des Primärservers. Die Reihenfolge der Stellen, an denen Logs angefordert werden, ist wie folgt: • Das aktive Protokollverzeichnis auf dem Primärserver • Der `LOGARCHMETH1` oder `LOGARCHMETH2` -Standort auf dem Standby-Server • Der `LOGARCHMETH2` Standort `LOGARCHMETH1` oder auf dem Primärserver In diesem Setup `/db2logs` wird von `LOGARCHMETH2` auf der Quelle als Staging-Bereich festgelegt. Die archivierten Protokolle in diesem Verzeichnis werden mit Amazon S3 synchronisiert und von Db2 auf Amazon abgerufen. EC2 Das Muster verwendet`LOGARCHMETH2` , weil `LOGARCHMETH1`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	es möglicherweise für die Verwendung eines Drittanbietertools konfiguriert wurde, auf das der AWS-CLI-Befehl nicht zugreifen kann:
	`db2 connect to sample`
	`db2 update db cfg for SAMPLE using LOGARCHMETH2 disk:/db2logs`	

Führen Sie eine Online-Datenbanksicherung durch.	Führen Sie eine Online-Datenbanksicherung aus und speichern Sie sie im lokalen Backup-Dateisystem: `db2 backup db sample online to /backup`	DBA

Richten Sie den S3-Bucket und die IAM-Richtlinie ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Erstellen Sie einen S3-Bucket für den lokalen Server, an den die Backup-DB2-Images und Protokolldateien auf AWS gesendet werden sollen. Auf den Bucket wird von Amazon zugegriffen EC2: `aws s3api create-bucket --bucket hadrmig-db2 --region us-east-1`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Richtlinie.	Die `db2bucket.json` Datei enthält die IAM-Richtlinie für den Zugriff auf den S3-Bucket: `{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["kms:GenerateDataKey", "kms:Decrypt", "s3:PutObject", "s3:GetObject", "s3:AbortMultipartUpload", "s3:ListBucket", "s3:DeleteObject", "s3:GetObjectVersion", "s3:ListMultipartUploadParts"], "Resource": ["arn:aws:s3:::hadrmig-db2/*",`	AWS-Administrator, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"arn:aws:s3:::hadrmig-db2"
	            ]
	        }
	    ]
	}</pre>
	Verwenden Sie den folgenden AWS-CLI-Befehl, um die Richtlinie zu erstellen:
	<pre>aws iam create-policy \
	      --policy-name db2s3hapolicy \
	      --policy-document file://db2bucket.json</pre>
	Die JSON-Ausgabe zeigt den Amazon-Ressourcennamen (ARN) für die Richtlinie, wobei `aws_account_id` es sich um Ihre Konto-ID handelt:
	<pre>"Arn": "arn:aws:iam::aws_account_id:policy/db2s3hapolicy"</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die IAM-Richtlinie an die IAM-Rolle an.	Normalerweise würde der EC2 Instance, auf der Db2 läuft, vom Systemadministrator eine IAM-Rolle zugewiesen. Wenn keine IAM-Rolle zugewiese n ist, können Sie in der EC2 Amazon-Konsole die Option IAM-Rolle ändern auswählen. Hängen Sie die IAM-Richt linie an die IAM-Rolle an, die der Instance zugeordnet ist. EC2 Nachdem die Richtlinie angehängt wurde, kann die EC2 Instance auf den S3-Bucket zugreifen: `aws iam attach-role-policy --policy-arn "arn:aws:iam::aws_account_id:policy/db2s3hapolicy" --role-name db2s3harole`	

Senden Sie das Backup-Image und die Protokolldateien der Quelldatenbank an Amazon S3

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie AWS CLI auf dem lokalen Db2-Server.	Konfigurieren Sie die AWS-CLI mit dem `Access Key ID` und`Secret Access Key`, das Sie zuvor generiert haben: `$ aws configure`	AWS-Administrator, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`AWS Access Key ID [None]: ************ AWS Secret Access Key [None]: ********* ********** Default region name [None]: us-east-1 Default output format [None]: json`	
Senden Sie das Backup-Image an Amazon S3.	Zuvor wurde ein Online-Datenbank-Backup im `/backup` lokalen Verzeichnis gespeichert. Führen Sie den folgenden Befehl aus, um dieses Backup-Image an den S3-Bucket zu senden: `aws s3 sync /backup s3://hadrmig-db2/SAMPLE_backup`	AWS-Administrator, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie die Db2-Archivprotokolle an Amazon S3.	Synchronisieren Sie die lokalen Db2-Archivprotokolle mit dem Amazon S3 S3-Bucket, auf den die Ziel-Db2-Instance auf Amazon zugreifen kann: EC2 `aws s3 sync /db2logs s3://hadrmig-db2/SAMPLE_LOGS` Führen Sie diesen Befehl regelmäßig mithilfe von Cron oder anderen Planungstools aus. Die Häufigkeit hängt davon ab, wie oft die Quelldatenbank Transaktionsprotokolldateien archiviert.	

Connect Db2 on Amazon mit Amazon EC2 S3 und starten Sie die erste Datenbanksynchronisierung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen PKCS12 Keystore.	Db2 verwendet einen PKCS-Verschlüsselungs-Keystore (Public-Key Cryptography Standards), um den AWS-Zugriffsschlüssel zu schützen. Erstellen Sie einen Keystore und konfigurieren Sie den Quell-Db2 so, dass er ihn verwendet: `gsk8capicmd_64 -keydb -create -db "/home/db`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2inst1/.keystore/db2s3.p12" -pw "<password>" -type pkcs12 -stash db2 "update dbm cfg using keystore_location /home/db2inst1/.keystore/db2s3.p12 keystore_type pkcs12"	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den Alias für den Db2-Speicherzugriff.	Db2 verwendet einen Speicherzugriffsalias, um mit den `RESTORE DATABASE` Befehlen`INGEST`, `LOADBACKUP DATABASE`, oder direkt auf Amazon S3 zuzugreifen.
	
	Weil Sie der EC2 Instance eine IAM-Rolle zugewiese n haben `USER` und nicht erforderlich `PASSWORD` sind:
	
	`db2 "catalog storage access alias <alias_na me> vendor S3 server <S3 endpoint> container '<bucket_ name>'"`
	
	Ihr Skript könnte beispiels weise wie folgt aussehen:
	
	`db2 "catalog storage access alias DB2AWSS3 vendor S3 server s3.us-east-1.amazo naws.com container 'hadrmig-db2'"`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie den Bereitstellungsbereich ein.	Wir empfehlen `DB2_ENABLE_COS_SDK=ON` ,`DB2_OBJECT_STORAGE_SETTINGS=EnableStreamingRestore` , und den Link zur `awssdk` Bibliothek zu verwenden, um den Amazon S3 S3-Staging-Bereich für Datenbank-Backups und -Wiederherstellungen zu umgehen:
	`#By root:`
	`cp -rp /home/db2inst1/sqllib/lib64/awssdk/RHEL/7.6/* /home/db2inst1/sqllib/lib64/`
	
	`#By db2 instance owner:`
	`db2set DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH=/db2stage`
	`db2set DB2_ENABLE_COS_SDK=ON`
	`db2set DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH=/db2stage`
	`db2stop`
	`db2start`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die Datenbank aus dem Backup-Image wieder her.	Stellen Sie die Zieldatenbank auf Amazon EC2 aus dem Backup-Image im S3-Bucket wieder her:
	`db2 create db sample on /data1`
	`db2 restore db sample from DB2REMOTE://DB2AWSS3/hadrmig-db2/SAMPLE_backup replace existing`
		DBA

Richten Sie HADR ohne HADR vor Ort ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den lokalen Db2-Server als primären Server.	Aktualisieren Sie die Datenbankkonfigurationseinstellungen für HADR on `db2-server1` (die lokale Quelle) als Primärserver. Stellen Sie `HADR_SYNCMODE` den `SUPERASYNC` Modus ein, der die kürzeste Transaktionsantwortzeit hat: `db2 update db cfg for sample using HADR_LOCAL_HOST db2-server1 HADR_LOCAL_SVC 50010 HADR_REMOTE_HOST db2-ec2 HADR_REMOTE_SVC 50012 HADR_REMOTE_INST db2inst1`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`HADR_SYNCMODE SUPERASYNC DB20000 I The UPDATE DATABASE CONFIGURATION command completed successfu lly` Es wird mit einigen Netzwerkv erzögerungen zwischen dem lokalen Rechenzentrum und AWS gerechnet. (Sie können je nach Netzwerkz uverlässigkeit einen anderen `HADR_SYNCMODE` Wert festlegen. Weitere Informati onen finden Sie im Abschnitt Verwandte Ressourcen.)	
Ändern Sie das Ziel des Zieldatenbank-Logarchivs.	Ändern Sie das Zielziel des Datenbank-Logarchivs so, dass es der EC2 Amazon-Um gebung entspricht: `db2 update db cfg for SAMPLE using LOGARCHME TH1 'DB2REMOTE://DB2AW SS3//SAMPLE_LOGS/' LOGARCHMETH2 OFF DB20000I The UPDATE DATABASE CONFIGURA TION command completed successfully`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie HADR für Db2 auf dem EC2 Amazon-Server.	Aktualisieren Sie die Datenbankkonfiguration für HADR im `db2-ec2` Standby-Modus: `db2 update db cfg for sample using HADR_LOCAL_HOST db2-ec2 HADR_LOCAL_SVC 50012 HADR_REMOTE_HOST db2-server1 HADR_REMOTE_SVC 50010 HADR_REMOTE_INST db2inst1 HADR_SYNCMODE SUPERASYNC DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie das HADR-Setup.	Überprüfen Sie die HADR-Parameter auf den Quell- und Ziel-DB2-Servern. Führen Sie den folgenden Befehl aus, um zu überprüfe `ndb2-server1` , ob das Setup aktiviert ist: `db2 get db cfg for sample|grep HADR HADR database role = PRIMARY HADR local host name (HADR_LOCAL_HOST) = db2-server1 HADR local service name (HADR_LOCAL_SVC) = 50010 HADR remote host name (HADR_REMOTE_HOST) = db2-ec2 HADR remote service name (HADR_REMOTE_SVC) = 50012 HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1 HADR timeout value (HADR_TIMEOUT) = 120 HADR target list (HADR_TARGET_LIST) = HADR log write synchronization mode`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	(HADR_SYNCMODE) = NEARSYNC
	HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000)
	HADR log replay delay (seconds) (HADR_REPLAY_DELAY) = 0
	HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0
	HADR SSL certificate label (HADR_SSL_LABEL) =
	HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF
	
	Führen Sie den folgenden Befehl aus, um zu überprüfe `ndb2-ec2`, ob das Setup aktiviert ist:
	
	`db2 get db cfg for sample|grep HADR`
	`HADR database role = STANDBY`
	`HADR local host name (HADR_LOCAL_HOST) = db2-ec2`
	`HADR local service name (HADR_LOCAL_SVC) = 50012`
	`HADR remote host name (HADR_REM`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	OTE_HOST) = db2-serve r1 HADR remote service name (HADR_REMOTE_SVC) = 50010 HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1 HADR timeout value (HADR_TIMEOUT) = 120 HADR target list (HADR_TAR GET_LIST) = HADR log write synchronization mode (HADR_SYNCMODE) = SUPERASYNC HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000) HADR log replay delay (seconds) (HADR_REP LAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certifica te label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF Die HADR_REMOTE_SVC ParameterHADR_LOCA L_HOST , HADR_LOCA	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`L_SVC HADR_REMO TE_HOST` , und geben das eine primäre und ein Standby-HARD-Setup an.	

Starten Sie die Db2 HADR-Instanz.	Starten Sie zuerst die Db2 HADR-Instanz auf dem Standby-Server: `db2-ec2`
	`db2 start hadr on db sample as standby`
	`DB20000I The START HADR ON DATABASE command completed successfully.`
	Starten Sie Db2 HADR auf dem primären (Quell-) Server: `db2-server1`
	`db2 start hadr on db sample as primary`
	`DB20000I The START HADR ON DATABASE command completed successfully.`
	Die HADR-Verbindung zwischen Db2 vor Ort und Amazon EC2 wurde nun erfolgreich hergestellt. Der Db2-Primärserver `db2-server1` beginnt, Transakti onsprotokolleinträge `db2-ec2` in Echtzeit zu streamen.
		DBA

Richten Sie HADR ein, wenn HADR lokal vorhanden ist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Db2 bei Amazon EC2 als zusätzliches Standby hinzu.	Wenn HADR auf der lokalen Db2-Instance ausgeführt wird, können Sie Db2 auf Amazon EC2 als Auxiliary Standby hinzufügen, `HADR_TARGET_LIST` indem Sie die folgenden Befehle auf ausführen: `db2-ec2` `db2 update db cfg for sample using HADR_LOCAL_HOST db2-ec2 HADR_LOCAL_SVC 50012 HADR_REMOTE_HOST db2-server1 HADR_REMOTE_SVC 50010 HADR_REMOTE_INST db2inst1 HADR_SYNCMODE SUPERASYNC DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. db2 update db cfg for sample using HADR_TARGET_LIST "db2-server1:50010 |db2-server2:50011 " DB20000I The UPDATE DATABASE CONFIGURATION command`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`completed successfully.`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die zusätzlichen Standby-Informationen zu den lokalen Servern hinzu.	Update `HADR_TARGET_LIST` auf den beiden lokalen Servern (Primär- und Standby-Server). Führen Sie auf `db2-server1` den folgenden Code aus: `db2 update db cfg for sample using HADR_TARGET_LIST "db2-server2:50011|db2-ec2:50012" DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. SQL1363W One or more of the parameters submitted for immediate modification were not changed dynamically. For these configuration parameters, the database must be shutdown and reactivated before the configuration parameter changes become effective.`  Führen Sie `db2-server2` unter den folgenden Code aus:	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`db2 update db cfg for sample using HADR_TARGET_LIST "db2-server1:50010|db2-ec2:50012" DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. SQL1363W One or more of the parameters submitted for immediate modification were not changed dynamically. For these configuration parameters, the database must be shutdown and reactivated before the configuration parameter changes become effective.`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie das HADR-Setup.	Überprüfen Sie die HADR-Parameter auf den Quell- und Ziel-DB2-Servern.
	
	Führen Sie auf `db2-server1` den folgenden Code aus:
	
	`db2 get db cfg for sample|grep HADR`
	`HADR database role = PRIMARY`
	`HADR local host name (HADR_LOCAL_HOST) = db2-server1`
	`HADR local service name (HADR_LOCAL_SVC) = 50010`
	`HADR remote host name (HADR_REMOTE_HOST) = db2-server2`
	`HADR remote service name (HADR_REMOTE_SVC) = 50011`
	`HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1`
	`HADR timeout value (HADR_TIMEOUT) = 120`
	`HADR target list (HADR_TARGET_LIST) = db2-server2:50011|db2-ec2:50012`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	HADR log write synchronization mode (HADR_SYNCMODE) = NEARSYNC HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000) HADR log replay delay (seconds) (HADR_REPLAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certificate label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF Führen Sie `db2-server2` unter den folgenden Code aus: `db2 get db cfg for sample|grep HADR` HADR database role = STANDBY HADR local host name (HADR_LOCAL_HOST) = db2-server2 HADR local service name (HADR_LOCAL_SVC) = 50011 HADR remote host name (HADR_REM	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	OTE_HOST) = db2-serve r1 HADR remote service name (HADR_REMOTE_SVC) = 50010 HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1 HADR timeout value (HADR_TIMEOUT) = 120 HADR target list (HADR_TAR GET_LIST) = db2-serve r1:50010|db2-ec2:5 0012 HADR log write synchronization mode (HADR_SYNCMODE) = NEARSYNC HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000) HADR log replay delay (seconds) (HADR_REP LAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certifica te label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Führen Sie `db2-ec2` unter den folgenden Code aus:
	
	`db2 get db cfg for sample|grep HADR`
	`HADR database role = STANDBY`
	`HADR local host name (HADR_LOCAL_HOST) = db2-ec2`
	`HADR local service name (HADR_LOCAL_SVC) = 50012`
	`HADR remote host name (HADR_REMOTE_HOST) = db2-server1`
	`HADR remote service name (HADR_REMOTE_SVC) = 50010`
	`HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1`
	`HADR timeout value (HADR_TIMEOUT) = 120`
	`HADR target list (HADR_TARGET_LIST) = db2-server1:50010|db2-server2:50011`
	`HADR log write synchronization mode (HADR_SYNCMODE) = SUPERASYNC`
	`HADR spool log data limit (4KB)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(HADR_SPOOL_LIMIT) = AUTOMATIC(52000) HADR log replay delay (seconds) (HADR_REPLAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certificate label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF Die HADR_TARGET_LIST ParameterHADR_LOCAL_HOST , HADR_LOCAL_SVC HADR_REMOTE_HOST , und geben anHADR_REMOTE_SVC , dass ein primäres und zwei Standby-HADR-Setup vorhanden sind.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stoppen und starten Sie Db2 HADR.	`HADR_TARGET_LIST` ist jetzt auf allen drei Servern eingerichtet. Jeder Db2-Server kennt die anderen beiden. Beenden Sie HADR (kurzer Ausfall) und starten Sie es erneut, um die Vorteile der neuen Konfiguration zu nutzen.
	
	Führen Sie bei `db2-server1` eingeschaltetem Gerät die folgenden Befehle aus:
	
	`db2 stop hadr on db sample`
	`db2 deactivate db sample`
	`db2 activate db sample`
	
	Führen Sie bei `db2-server2` aktivierter Option die folgenden Befehle aus:
	
	`db2 deactivate db sample`
	`db2 start hadr on db sample as standby`
	`SQL1766W The command completed successfully`
	
	Führen Sie bei `db2-ec2` aktivierter Option die folgenden Befehle aus:
	
	`db2 start hadr on db sample as standby`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`SQL1766W The command completed successfully`
	
	Führen Sie bei `db2-server1` aktivierter Option die folgenden Befehle aus:
	
	`db2 start hadr on db sample as primary`
	`SQL1766W The command completed successfully`
	
	Die HADR-Verbindung zwischen Db2 vor Ort und Amazon wurde EC2 jetzt erfolgreich hergestellt. Der Db2-Primärserver `db2-server1` beginnt mit dem Streaming von Transaktionsprotokolldatensätzen in beide Länder `db2-server2` und `db2-ec2` in Echtzeit.	

Machen Sie Db2 auf Amazon EC2 während des Umstellungsfensters zur primären Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass es auf dem Standby-Server keine HADR-Verzögerung gibt.	Überprüfen Sie den HADR-Status vom Primärserver aus. `db2-server1` Seien Sie nicht beunruhigt, wenn der `REMOTE_CATCHUP` Status `HADR_STATE` aktiviert ist, was normal ist, wenn er auf eingestellt `HADR_SYNC`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	MODE ist. SUPERASYNC Die PRIMARY_LOG_TIME und STANDBY_REPLAY_LOG _TIME zeigen, dass sie synchron sind:
	
	`db2pd -hadr -db sample`
	
	`HADR_ROLE = PRIMARY`
	
	`REPLAY_TYPE = PHYSICAL`
	
	`HADR_SYNCMODE = SUPERASYNC`
	
	`STANDBY_ID = 2`
	
	`LOG_STREAM_ID = 0`
	
	`HADR_STATE = REMOTE_CATCHUP`
	`.....`
	
	`PRIMARY_LOG_TIME = 10/26/2022 02:11:32.000000 (1666750292)`
	
	`STANDBY_LOG_TIME = 10/26/2022 02:11:32.000000 (1666750292)`
	`STANDBY_REPLAY_LOG_TIME = 10/26/2022 02:11:32.000000 (1666750292)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Führen Sie HADR Takeover aus.	Um die Migration abzuschli eßen, erstellen Sie `db2-ec2` die Primärdatenbank, indem Sie den Befehl HADR Takeover ausführen . Verwenden Sie den Befehl`db2pd`, um den `HADR_ROLE` Wert zu überprüfen:
	
	`db2 TAKEOVER HADR ON DATABASE sample`
	`DB20000I The TAKEOVER HADR ON DATABASE command completed successfully.`
	
	`db2pd -hadr -db sample`
	`Database Member 0 -- Database SAMPLE -- Active -- Up 0 days 00:03:25 -- Date 2022-10-26-02.46.45.048988`
	
	`HADR_ROLE = PRIMARY`
	
	`REPLAY_TYPE = PHYSICAL`
	
	Um die Migration zu AWS abzuschließen, verweisen Sie die Anwendungsverbindungen auf Db2 auf Amazon EC2.	

Fehlerbehebung

Problem	Lösung
Wenn Sie NAT aus Firewall- und Sicherheitsgründen verwenden, kann der Host zwei IP-Adressen haben (eine interne und eine externe), was dazu führen kann, dass die HADR-IP-Adressüberprüfung fehlschlägt. Der `START HADR ON DATABASE` Befehl gibt die folgende Meldung zurück: `HADR_LOCAL_HOST:HADR_LOCAL_SVC (-xx-xx-xx-xx.:50011 (xx.xx.xx.xx:50011)) on remote database is different from HADR_REMOTE_HOST:HADR_REMOTE_SVC (xx-xx-xx-xx.:50011 (x.x.x.x:50011)) on local database.`	Um HADR in einer NAT-Umgebung zu unterstützen, können Sie die sowohl `HADR_LOCAL_HOST` mit der internen als auch mit der externen Adresse konfigurieren. Wenn der Db2-Server beispielsweise den internen Namen `host1` und den externen Namen hat`host1E`, `HADR_LOCAL_HOST` kann das sein. `HADR_LOCAL_HOST: "host1 | host1E"`

Zugehörige Ressourcen

- Sicherungs- und Wiederherstellungsvorgänge von DB2 zwischen verschiedenen Betriebssystemen und Hardwareplattformen
- Richten Sie Db2 STORAGE ACCESS ALIAS und REMOTE ein DB2
- Db2-Disaster Recovery mit hoher Verfügbarkeit
- hadr_syncmode — HADR-Synchronisationsmodus für Protokollschreibvorgänge im Peer-State-Konfigurationsparameter

Migrieren Sie EC2 mithilfe des Application Migration Service eine lokale Microsoft SQL Server-Datenbank zu Amazon

Erstellt von Senthil Ramasamy (AWS)

Übersicht

Dieses Muster beschreibt die Schritte zur Migration einer Microsoft SQL Server-Datenbank von einem lokalen Rechenzentrum zu einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance. Es verwendet das AWS Application Migration Service (AWS MGN), um Ihre Datenbank mithilfe einer automatisierten Migration neu zu hosten. lift-and-shift AWS MGN führt die Replikation Ihres Quelldatenbankservers auf Blockebene durch.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Eine Microsoft SQL Server-Quelldatenbank in einem lokalen Rechenzentrum

Einschränkungen

- Ihre Netzwerkbandbreite zwischen dem lokalen Rechenzentrum und ist möglicherweise begrenzt. AWS
- AWS MGN ist auf Datenbanken beschränkt, die auf eigenständigen Servern mit dediziertem Speicher gehostet werden. Es unterstützt nicht die Migration von geclusterten Datenbanksystemen und Datenbanksystemen, bei denen die Änderungsrate den Durchsatz eines Netzwerks übersteigt.
- Einige AWS-Services sind nicht in allen verfügbar. AWS-Regionen Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie auf der Seite Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Produktversionen

- Alle Versionen der Microsoft SQL Server-Datenbank
- Windows- und Linux-Betriebssysteme, die AWS MGN unterstützen

Architektur

Quelltechnologie-Stack

Eine lokale Microsoft SQL Server-Datenbank

Zieltechnologie-Stack

Eine Microsoft SQL Server-Datenbank auf einer EC2 Amazon-Instance

Zielarchitektur

Diese Architektur verwendet AWS MGN, um Daten aus einem lokalen Unternehmensrechenzentrum zu replizieren. AWS Das Diagramm zeigt den Datenreplikationsprozess, die API-Kommunikation sowie die Test- und Umstellungsphasen.

1. Datenreplikation:
   - AWS MGN repliziert Daten aus dem lokalen Unternehmensrechenzentrum in das Rechenzentrum des Unternehmens AWS und initiiert die fortlaufende Replikation von Änderungen.
   - Replikationsserver im Staging-Subnetz empfangen und verarbeiten die Daten.
2. API-Kommunikation:
   - Replikationsserver stellen über TCP-Port 443 eine Verbindung zu den API-Endpunkten von AWS MGN EC2, Amazon und Amazon Simple Storage Service (Amazon S3) her.
   - AWS MGN verwaltet die Migration.
   - Amazon EC2 verwaltet den Instanzbetrieb.
3. Test und Umstellung:
   - Test-Instances werden im betriebsbereiten Subnetz mit replizierten Daten gestartet.
   - Nach erfolgreichen Tests erstellt AWS MGN Cutover-Instanzen für die endgültige Migration.

Tools

- AWS Application Migration Service (AWS MGN) unterstützt Sie beim Rehosten (Lift and Shift) von Anwendungen AWS Cloud ohne Änderungen und mit minimalen Ausfallzeiten.
- AWS Direct Connectverbindet Ihr internes Netzwerk über ein Standard-Ethernet-Glasfaserkabel mit einem Direct Connect-Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt

zu öffentlichen AWS Diensten einrichten und dabei Internetdienstanbieter in Ihrem Netzwerkpfad umgehen.

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Bewährte Methoden

- Richten Sie regionale API-Endpunkte für AWS MGN EC2, Amazon und Amazon S3 in der Virtual Private Cloud (VPC) ein, um den öffentlichen Zugriff über das Internet zu verbieten.
- Richten Sie die AWS MGN-Starteinstellungen ein, um Zieldatenbankserver in einem privaten Subnetz zu starten.
- Erlauben Sie nur die erforderlichen Ports in Datenbanksicherheitsgruppen.
- Folgen Sie dem Prinzip der geringsten Rechte und gewähren Sie die für die Ausführung einer Aufgabe erforderlichen Mindestberechtigungen. Weitere Informationen finden Sie in der IAM-Dokumentation unter Gewährung der geringsten Rechte und bewährte Methoden zur Sicherheit.

Epen

AWS MGN einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
AWS MGN konfigurieren.	Suchen Sie nach dem AWS Application Migration Service AWS Management Console in und starten Sie den Einrichtu ngsvorgang. Dadurch wird eine Replikationsvorlag e erstellt und Sie werden zur Seite Quellserver der MGN-Konsole weitergeleitet. Wählen Sie bei der Konfigura	DBA, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	tion des MGN-Dienstes eine Servicerolle aus der generiert en Liste aus.	
Quellserver hinzufügen.	Fügen Sie Details zu Ihrem lokalen Quelldatenbankserver hinzu und fügen Sie dann den Server hinzu.	DBA, Migrationsingenieur
Installieren Sie den AWS MGN-Agenten auf dem Quellserver.	Laden Sie das Installat ionsprogramm für den AWS MGN Agent auf Ihr lokales System herunter und übertragen Sie das Installationsprogramm auf Ihren Quelldatenbankserver. Informationen zur Überprüfu ng des Installer-Hash finden Sie unter Überprüfen des heruntergeladenen AWS Replication Agent-Installation sprogramms für Windows 2012.	DBA, Migrationsingenieur

Installieren Sie den AWS MGN Agent auf Quellcomputern

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie Client-IAM-Anmeldeinformationen.	Generieren Sie vor der Installation des AWS MGN-Agenten AWS Anmeldein formationen, indem Sie einen neuen IAM-Benutzer mit den entsprechenden Berechtig ungen erstellen.	DBA, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien für AWS Application Migration Service und Generierung der erforderlichen AWS Anmeldeinformationen.	
Installieren Sie den Agenten auf dem Quellserver.	Installieren Sie den Agenten auf dem Quellcomputer, der die Microsoft SQL Server-Datenbank hostet. Weitere Informationen finden Sie unter Installation des AWS Replication Agents auf Windows-Servern. Geben Sie die folgenden AWS-Anmeldeinformationen ein: • AWS-Region • AWS Zugriffsschlüssel-ID • AWS geheimer Zugriffsschlüssel Ihre eindeutigen AWS Anmeldeinformationen ermöglichen es dem AWS MGN-Agenten, sich zu authentifizieren und Migrationsaufgaben auszuführen.	App-Besitzer, DBA, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie die zu replizier enden Festplatten aus.	Nach Eingabe Ihrer AWS Anmeldeinformationen überprüft das Installat ionsprogramm, ob Ihr Server die Mindestanforderungen für die Agenteninstallation erfüllt (z. B. ob der Server über ausreichend Festplatt enspeicher für die Installat ion des AWS MGN-Agent en verfügt). Das Installat ionsprogramm zeigt die Datenträgerbezeichnungen und Speicherdetails an. Um Ihre Datenbank mithilfe des AWS MGN-Dienstes zu replizieren, wählen Sie die entsprechenden Festplatt en auf Ihrem Quellserver aus. Geben Sie den Pfad der einzelnen Festplatten durch Kommas getrennt ein. Wenn Sie alle Festplatten replizieren möchten, lassen Sie den Pfad leer. Nachdem Sie die ausgewählten Festplatt en bestätigt haben, wird die Installation fortgesetzt.	DBA, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überwachen Sie den Synchronisierungsfortschritt.	AWS Der Replication Agent initiiert den Synchroni sierungsvorgang, indem er zuerst einen Snapshot der ausgewählten Festplatten erstellt und dann die Daten repliziert. Sie können den Synchroni sierungsfortschritt auf der Seite Quellserver in der AWS MGN-Konsole überwachen. Weitere Informationen finden Sie unter Überwachen des Servers im Migrationslebenszy klus.	DBA, Migrationsingenieur

Replikation mit AWS MGN

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwalten Sie den Replikati onsfortschritt.	Nachdem Sie die erste Synchronisation gestartet haben, wird Ihr Quellserv er in der AWS MGN-Konso le angezeigt, wo Sie die Migration verwalten und überwachen können. In der Konsole wird eine geschätzt e Zeit für die vollständige Replikation angezeigt, die auf der Gesamtgröße der ausgewählten Festplatten und	DBA, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der verfügbaren Netzwerkb andbreite basiert.	
Überprüfen Sie die Synchroni sation.	Nachdem die Festplatten auf dem Quellserver vollständ ig synchronisiert wurden, stellen Sie sicher, dass alle ausgewählten Festplatten als vollständig synchronisiert aufgeführt sind und dass in der Konsole keine Fehler gemeldet werden. Die AWS MGN-Konsole wechselt dann automatisch den Status des Migration slebenszyklus auf Bereit zum Testen, was darauf hinweist, dass die replizierte Umgebung für Leistungs- und Funktions tests vorbereitet AWS ist.	App-Besitzer, DBA, Migration singenieur

Testen und überarbeiten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Starteins tellungen.	Wählen Sie den Quellserv er in der AWS MGN-Konso le aus und aktualisieren Sie die Starteinstellungen für die Ziel-Testinstanz. Navigiere n Sie auf der Detailseite des Quellservers zur Registerk arte Starteinstellungen, um die Testinstanz zu konfigurieren.	DBA, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wählen Sie einen kostengün stigen Instance-Typ und einen Amazon Elastic Block Store (Amazon EBS) -Volumetyp und konfigurieren Sie dann die Sicherheitsgruppen und Netzwerkanforderungen. Weitere Informationen finden Sie unter Starteinstellungen.	
Starten Sie die Ziel-Test instanz.	Navigieren Sie zur AWS MGN-Konsole Ihres synchroni sierten Quellcomputers und starten Sie eine Ziel-Test instanz, indem Sie Testen und Überschneiden und dann Testinstanzen starten auswählen. Dadurch wird ein Startjob erstellt, der die Testinsta nz mithilfe Ihrer konfiguri erten Einstellungen bereitste llt. Die Instance wird in der Umgebung Ihres Quelldate nbankservers gestartet AWS Cloud und replizier t diese. Überwachen Sie den Startfortschritt auf der Seite mit dem Startverlauf, auf der Sie die Erstellung der Instance verfolgen und etwaige Probleme beheben können.	DBA, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Ziel-Test instanz.	Überprüfen Sie den EC2 Amazon-Datenbankserver: 1. Stellen Sie sicher, dass die AWS MGN-Konsole anzeigt, dass die Test-Inst ance erfolgreich ausgeführt wird. 2. Verwenden Sie einen RDP-Client, um sich anzumelde n. 3. Öffnen Sie im Startmenü den SQL Server-Konfigurati ons-Manager. 4. Überprüfen Sie den Status der SQL Server-Dienste, einschließlich SQL Server (`MSSQLSERVER`) und SQL Server-Agent, und stellen Sie sicher, dass sie intakt sind und auf den richtigen Starttyp eingestellt sind. 5. Vergleichen Sie die Festplatteneinstellungen und Konfigurationen zwischen der Testinsta nz und dem Quelldate nbankserver und stellen Sie sicher, dass Laufwerks buchstaben, Volumes, Festplattenzuweisungen und die erforderlichen Verzeichnisse korrekt zugeordnet sind.	DBA, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Connect zum SQL Server auf der EC2 Test-Amazon-Instance her und überprüfen Sie, ob alle Quelldatenbanken migriert wurden und in der Datenbankliste erscheinen. Führen Sie Validierungstests durch, um sicherzustellen, dass die Datenbank wie erwartet funktioniert.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Benennen Sie den Server um.	AWS Die MGN-Migration beinhaltet eine Kopie Ihres lokalen Quellservers auf Speicherebene. Ihre SQL EC2 Server-Instanz enthält nur die Details des ursprüngl ichen Quellservers in ihren Binärdateien. Aktualisieren Sie daher die Binärinformationen , sodass sie den Namen des neuen Servers widerspiegeln.
	1. Verwenden Sie SQL Server Management Studio (SSMS), um eine Verbindun g zu Ihrer SQL EC2 Server-Instanz herzustellen.
	2. Überprüfen Sie den Namen des Servers:
	`SELECT @@SERVERNAME AS 'Current Server Name';`
	3. Benennen Sie die SQL Server-Instanz um, indem Sie sie `NEW_SERVE R_NAME` durch den Namen Ihres Servers ersetzen:
	`EXEC sp_dropserver 'OLD_SERVER_NAME'`
	`EXEC sp_addserver 'NEW_SERVER_NAME', 'local';`
		DBA, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Stellen Sie sicher, dass der Servername korrekt ist: `SELECT @@SERVERNAME AS 'Updated Server Name';` 5. Starten Sie die SQL Server-Instanz neu.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Cutover-Instanz.	Vergewissern Sie sich in der AWS MGN-Konsole auf der Seite Quellserver, dass der Status des Migrationslebenszyklus des Servers „Bereit für die Übernahme“ lautet. Konfigurieren Sie die Starteinstellungen für die Cutover-Instance und stellen Sie sicher, dass die Einstellungen Ihrer lokalen Umgebung entsprechen. Bevor Sie die Übernahme einleiten, fahren Sie Ihre lokale Datenbank herunter. Dadurch wird Folgendes gewährleistet: • Alle laufenden Transaktionen sind abgeschlossen. • Während des Umstellungsprozesses werden keine neuen Transaktionen stattfinden. • Die Datensynchronisierung zwischen den Quell- und Zielfestplatten ist abgeschlossen. Initiieren Sie die Cutover-Instanz in der AWS MGN-Konsole. Wenn die Cutover-Instanz betriebsbereit ist, melden Sie sich bei der	App-Besitzer, DBA, Migrationsingenieur, Migrationsleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Instanz an und führen Sie die folgenden Tests durch: 1. Stellen Sie sicher, dass SQL Server korrekt gestartet wird und dass auf die Datenbanken zugegriff en werden kann. 2. Stellen Sie sicher, dass Ihre Daten intakt sind und mit dem Quellserver konsistent sind. 3. Führen Sie alle Anwendung stests durch, um sicherzus tellen, dass sie wie erwartet funktionieren. 4. Setzen Sie in der AWS MGN-Konsole den Migrationsstatus auf Übernahme abgeschlossen. 5. Beginnen Sie mit der Weiterleitung des Datenverkehrs an die Instanz EC2 .	

Fehlerbehebung

Problem	Lösung
Die erste Synchronisation schlägt beim Authentifizierungsschritt fehl.	Dies ist ein Problem mit der Netzwerkk onnektivität. Der Replikationsserver kann keine Verbindung zu AWS MGN herstellen.

Zugehörige Ressourcen

AWS-Dokumentation

- Erste Schritte mit AWS Application Migration Service
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Amazon EC2
- Was ist Microsoft SQL Server auf Amazon EC2?

Videos

- Durchführung einer Lift-and-Shift-Migration mit AWS Application Migration Service (Video)

Migrieren Sie VMware VMs mit HCX Automation mithilfe von PowerCLI

Erstellt von Giri Nadiminty (AWS), Hassan Adekoya (AWS) und Naveen Deshwal

Übersicht

> Hinweis: Seit dem 30. April 2024 wird VMware Cloud on AWS nicht mehr von oder seinen Channel-Partnern weiterverkauft. AWS Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

Dieses Muster beschreibt, wie VMware lokale virtuelle Maschinen (VMs) mithilfe von VMware Hybrid VMware Cloud Extension (HCX) Automation, die auf VMware PowerCLI-Skripts basiert, zu Cloud on AWS migriert werden. PowerCLI ist ein Befehlszeilentool, das auf Windows basiert. PowerShell Es hilft Ihnen bei der Verwaltung von VMware Software und automatisiert Infrastruktur- und Migrationsaufgaben.

Sie können dieses Muster für die Migration zwischen einer beliebigen Kombination von vCentern, softwaredefinierten Rechenzentren (SDDCs) und Cloud-Umgebungen anpassen. Die in diesem Muster enthaltenen PowerCLI-Skripts verwenden Automatisierung anstelle von Mausklicks für alle VM-Konfiguration und Scheduling-Aufgaben, sodass sie Zeit bei Migrationsaktivitäten sparen und das Risiko menschlicher Fehler verringern.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein VMware Cloud on AWS-Konto bei SDDC
- Ein vorhandenes lokales oder cloudbasiertes vCenter oder SDDC
- Ein Benutzerkonto mit den erforderlichen Berechtigungen für Quell- und Ziel-vCenter oder SDDCs
- HCX Site Pairing mit HCX Network Extension (HCX-NE), konfiguriert zwischen Quell- und Ziel-vCenter oder SDDCs
- VMware PowerCLI ist auf dem Server Ihrer Wahl installiert

Einschränkungen

- Wenn das Quell-vCenter Cross-vCenter NSX verwendet, funktioniert das PowerCLI-Modul nicht. Verwenden Sie eine Skriptmethode (wie Python) mit der HCX-API anstelle von PowerCLI.

- Wenn die migrierten VMs Benutzer neue Namen oder IP-Adressen benötigen, verwenden Sie eine Skriptmethode (wie Python) mit der HCX-API.
- Dieses Muster füllt die CSV-Datei nicht auf, was erforderlich ist. Sie können die Datei mithilfe von VMware vRealize Network Insight (vRNI) oder einer anderen Methode auffüllen.

Produktversionen

- VMware vSphere Version 5 oder höher
- VMware HCX Version 4.4 oder höher
- VMware PowerCLI Version 12.7 oder höher

Architektur

Quelltechnologie-Stack

- Lokal oder cloudbasiert VMware

Zieltechnologie-Stack

- VMware Cloud auf AWS

Zielarchitektur

Tools

AWS-Services

- VMware Cloud on AWS ist ein Service, der gemeinsam von AWS entwickelt wurde und VMware Sie bei der Migration und Erweiterung Ihrer lokalen VMware vSphere-basierten Umgebungen in die AWS-Cloud unterstützt.

Andere Tools

- VMware Hybrid Cloud Extension (HCX) ist ein Hilfsprogramm für die Migration von Workloads aus Ihrer lokalen VMware Umgebung zu VMware Cloud on AWS, ohne die zugrunde liegende

Plattform zu ändern. Hinweis: Dieses Produkt war früher als Hybrid Cloud Extension und NSX Hybrid Connect bekannt. Dieses Muster verwendet HCX für die VM-Migration.

- VMware PowerCLI ist ein Befehlszeilentool zur Automatisierung des vSphere- und VMware vCloud-Managements. Sie führen PowerCLI-Befehle in Windows mithilfe von Cmdlets aus. PowerShell PowerShell Dieses Muster verwendet PowerCLI, um Migrationsbefehle auszuführen.

Code

Einfaches, eigenständiges Skript

Es wird empfohlen, dieses Skript für einen einzelnen Computer für erste Tests zu verwenden, um sicherzustellen, dass die Konfigurationsoptionen akzeptiert werden und sich erwartungsgemäß verhalten. Anweisungen finden Sie im Abschnitt Epics.

```
<# Manual Variables #>
$HcxServer = "[enterValue]"
$SrcNetworkName = "[enterValue]"
$DstNetworkName = "[enterValue]"
$DstComputeName = "[enterValue]"
$DstDSName = "[enterValue]"
$DstFolderName = "[enterValue]"
$vmName = "[enterValue]"

<# Environment Setup #>
Connect-HCXServer -Server $HcxServer
$HcxDstSite = Get-HCXSite -Destination
$HcxSrcSite = Get-HCXSite -Source
$SrcNetwork = Get-HCXNetwork -Name $SrcNetworkName -Type VirtualWire -Site $HcxSrcSite
$DstNetwork = Get-HCXNetwork -Name $DstNetworkName -Type NsxtSegment -Site $HcxDstSite
$DstCompute = Get-HCXContainer -Name $DstComputeName -Site $HcxDstSite
$DstDS = Get-HCXDatastore -Name $DstDSName -Site $HcxDstSite
$DstFolder = Get-HCXContainer -name $DstFolderName -Site $HcxDstSite
$vm = Get-HCXVM -Name $vmName

<# Migration #>
$NetworkMapping = New-HCXNetworkMapping -SourceNetwork $SrcNetwork -DestinationNetwork
 $DstNetwork
$NewMigration = New-HCXMigration -VM $vm -MigrationType vMotion -SourceSite $HcxSrcSite
 -DestinationSite $HcxDstSite -Folder $DstFolder -TargetComputeContainer $DstCompute
 -TargetDatastore $DstDS -NetworkMapping $NetworkMapping -DiskProvisionType Thin
```

```
 -UpgradeVMTools $True -RemoveISOs $True -ForcePowerOffVm $True -RetainMac $True -
UpgradeHardware $True -RemoveSnapshots $True
```

.csv-basiertes Skript mit vollem Funktionsumfang

Nach Abschluss der Tests können Sie das folgende Skript in Ihren Produktionsumgebungen verwenden. Anweisungen finden Sie im Abschnitt Epics.

```
<# Schedule #>
write-host("Getting Time for Scheduling")
$startTime = [DateTime]::Now.AddDays(12)
$endTime = [DateTime]::Now.AddDays(15)

<# Migration #>
Connect-HCXServer -Server [enterValue]
write-host("Getting Source Site")
$HcxSrcSite = Get-HCXSite
write-host("Getting Target Site")
$HcxDstSite = Get-HCXSite -Destination
$HCXVMS = Import-CSV .\Import_VM_list.csv
ForEach ($HCXVM in $HCXVMS) {
    $DstFolder = Get-HCXContainer $HCXVM.DESTINATION_VM_FOLDER -Site $HcxDstSite
    $DstCompute = Get-HCXContainer $HCXVM.DESTINATION_COMPUTE  -Site $HcxDstSite
    $DstDatastore = Get-HCXDatastore $HCXVM.DESTINATION_DATASTORE -Site $HcxDstSite
    $SrcNetwork = Get-HCXNetwork $HCXVM.SOURCE_NETWORK -Type VirtualWire -Site
 $HcxSrcSite
    $DstNetwork = Get-HCXNetwork $HCXVM.DESTINATION_NETWORK -Type NsxtSegment -Site
 $HcxDstSite
    $NetworkMapping = New-HCXNetworkMapping -SourceNetwork $SrcNetwork -
DestinationNetwork $DstNetwork
    $NewMigration = New-HCXMigration -VM (Get-HCXVM $HCXVM.VM_NAME) -MigrationType
 Bulk -SourceSite $HcxSrcSite -DestinationSite $HcxDstSite -Folder $DstFolder -
TargetComputeContainer $DstCompute -TargetDatastore $DstDatastore -NetworkMapping
 $NetworkMapping -DiskProvisionType Thin -UpgradeVMTools $True -RemoveISOs $True -
ForcePowerOffVm $True -RetainMac $True -UpgradeHardware $True -RemoveSnapshots $True -
ScheduleStartTime $startTime -ScheduleEndTime $endTime
    Start-HCXMigration -Migration $NewMigration -Confirm:$false
}
```

Epen

Sammeln Sie Informationen für manuelle Variablen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Suchen Sie die Quell- und Ziel-vCenter- und SDDC-Servernamen.	PowerCLI-Skripts benötigen die in diesem Epos beschriebenen Variablen. Sie können diese Informationen im Voraus sammeln, um die Verwendung des Skripts zu vereinfachen. Wählen Sie im Abschnitt HCX der vSphere-Konsole Infrastructure, Site Pairing aus. Notieren Sie sich die angezeigten Quell- und Zielservernamen.	Cloud-Architekt
Suchen Sie die HCX-Quell- und Zielnamen.	Wählen Sie im HCX-Bereich der vSphere-Konsole System, Administration aus. Notieren Sie sich die angezeigten Quell- und Ziel-HCX-Namen.	Cloud-Architekt
Finden Sie die Namen des Quell- und Zielnetzwerks.	Wählen Sie im HCX-Bereich der vSphere-Konsole System, Network Extension aus. Notieren Sie sich die Namen des Quell- und Zielnetzwerks. **Note** Alternativ können Sie die Quell- und Zielnetzwerknamen mithilfe der PowerCLI-	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Befehle Get-HCXNetwork und Get-HCXNetwork -Destination abrufen, nachdem Sie eine Verbindung zum HCX-Server hergestellt haben.	
Sammeln Sie zusätzliche Informationen in der vSphere-Konsole.	Sammeln Sie auf der vSphere-Konsole die folgenden Informationen: • Namen der Dateien VMs , die Sie migrieren möchten • Ziel-Computerumgebung (Cluster/Host) • Zieldatenspeicher • Name des Ordners der Ziel-VM	Cloud-Architekt

Treffen Sie Migrationsentscheidungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie die Migrationsoptionen.	Ermitteln Sie Folgendes: • `MigrationType` — Die HCX-unterstützten Migrationstypen sind vMotion, Bulk, Cold und RAV. Ihre Wahl hängt von Ihren Ausfallanforderungen, der Netzwerkbandbreite, dem Migrationszeitraum und der Art der	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Arbeitslast ab. Weitere Informationen finden Sie im AWS-Blogbeitrag Migrieren von Workloads zur VMware Cloud auf AWS mit Hybrid Cloud Extension (HCX). • `DiskProvisionType (Thin, Thick)` • `UpgradeVMTools ($True, $False)` • `RemoveISOs ($True, $False)` • `ForcePowerOffVm ($True, $False)` • `RetainMac ($True, $False)` • `UpgradeHardware ($True, $False)` • `RemoveSnapshots ($True, $False)` Weitere Informationen zu den einzelnen Optionen finden Sie in der VMware Entwickle rdokumentation.	

Führen Sie das einfache Skript für erste Tests aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopieren Sie das Skript.	Die einfache Version des Skripts ist eigenständig in	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	einer einzigen Datei enthalten. Sie können es verwenden, um die Migration einer einzelnen Maschine zu testen. Kopieren Sie das erste Skript aus dem Codeabschnitt dieses Musters und speichern Sie es auf dem Computer, auf dem das VMware PowerCLI-Modul installiert ist. (Folgen Sie den Anweisungen in der VMware Dokumentation, um PowerCLI zu installieren.)	
Legen Sie Skriptvariablen fest.	Legen Sie alle Variablen im `Manual Variables` Abschnitt des Skripts fest.	Cloud-Architekt
Legen Sie Migrationsvariablen fest.	Stellen Sie alle `New-HCXMigration` Einstellungen im `Migration` Abschnitt des Skripts ein.	Cloud-Architekt
Geben Sie Websites an.	(Optional) Wenn die Quelle oder das Ziel mehrere Sites hat, geben Sie die Sites manuell im `Environment Setup` Abschnitt des Skripts an. Wenn die Quelle und das Ziel einzelne Websites haben, sucht das Skript automatisch nach den Informationen.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das Skript aus.	Führen Sie auf dem Server, auf dem PowerCLI installiert ist, in einem PowerShell Fenster mit erhöhten Rechten das Skript aus und geben Sie Ihre Anmeldeinformationen ein, wenn Sie dazu aufgefordert werden.	Cloud-Architekt
Validieren Sie das Skript.	Vergewissern Sie sich, dass die VM-Migration initiiert wurde.	Cloud-Architekt

Führen Sie das Skript mit vollem Funktionsumfang aus, um mehrere zu migrieren VMs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die CSV-Datei und füllen Sie sie aus.	Erstellen Sie eine CSV-Datei namens `Import_VM_list.csv` auf Ihrem Computer und füllen Sie sie mit dem folgenden Beispielinhalt:
	`VM_NAME,DESTINATION_VM_FOLDER,DESTINATION_COMPUTE,DESTINATION_DATASTORE,SOURCE_NETWORK,DESTINATION_NETWORK`
	`[enterValue],[enterValue],[enterValue],[enterValue],[enterValue],[enterValue]`
		Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ersetzen Sie jede Datei `[enterValue]` in der CSV-Datei durch die Informationen, die Sie zuvor gesammelt haben. **Note** Sie können die .csv-Datei mithilfe von VMware vRealize Network Insight (vRNI) oder einer anderen Methode auffüllen.	
Kopieren Sie das Skript.	Die Version des Skripts mit vollem Funktionsumfang verwendet Informationen aus einer externen CSV-Datei, um automatisch mehrere Dateien zu migrieren. VMs Kopieren Sie das zweite Skript aus dem Codeabschnitt dieses Musters und speichern Sie es auf dem Computer, auf dem das VMware PowerCLI-Modul installiert ist, im selben Ordner wie die CSV-Datei.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie das Skript.	Bearbeiten Sie das Skript, um die folgenden Änderungen vorzunehmen: • Zeile 7: Stellen Sie die HCX-Servervariable (`Connect-HCXServer`) ein. • Zeile 12: (Optional) Wenn Sie den CSV-Dateinamen anders festlegen, aktualisieren Sie ihn. • Zeilen 3-4: (Optional) Stellen Sie den Zeitplan ein. • Zeile 20: (Optional) Geben Sie die `New-HCXMigration` Einstellungen im `Migration` Abschnitt an. • Zeilen 9 und 11: (Optional) Wenn die Quelle oder das Ziel mehrere Standorte umfasst, geben Sie die gewünschten Standorte manuell an.	Cloud-Architekt
Führen Sie das Skript aus.	Führen Sie auf dem Server, auf dem PowerCLI installiert ist, in einem PowerShell Fenster mit erhöhten Rechten das Skript aus und geben Sie Ihre Anmeldeinformationen ein, wenn Sie dazu aufgefordert werden.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie das Skript.	Vergewissern Sie sich, dass die VM-Migration initiiert wurde.	Cloud-Architekt

Fehlerbehebung

Problem	Lösung
Das Skript schlägt mit der folgenden Fehlermeldung fehl: „Alle Quellnetzwerke sind nicht dem Ziel zugeordnet!“	Wenn das Quell-vCenter Cross-vCenter NSX verwendet, funktioniert das PowerCLI-Modul nicht. Verwenden Sie eine Skriptmethode (wie Python) mit der HCX-API anstelle von PowerCLI. Dies ist eine bekannte Einschränkung des PowerCLI-Skripts.
Das Skript schlägt mit der folgenden Fehlermeldung fehl: „HCXServer Verbindungsfehler: Nicht autorisiert“	Die von Ihnen eingegebenen Anmeldeinformationen bieten nicht die erforderlichen Berechtigungen.

Zugehörige Ressourcen

- Migration von Workloads zur VMware Cloud auf AWS mit Hybrid Cloud Extension (HCX) (AWS-Blogbeitrag)
- Auswahl eines Migrationsansatzes für die Verlagerung Ihrer VMware Anwendungen und Workloads in die AWS-Cloud (AWS Prescriptive Guidance)
- Migrieren Sie VMware SDDC mithilfe von VMware HCX zur VMware Cloud auf AWS (AWS Prescriptive Guidance)
- Erste Schritte mit dem HCX-Modul (Blogbeitrag) VMware

Migrieren Sie einen F5 BIG-IP-Workload zu F5 BIG-IP VE in der AWS-Cloud

Erstellt von Will Bauer (AWS)

Übersicht

Organizations möchten zur Amazon Web Services (AWS) Cloud migrieren, um ihre Agilität und Widerstandsfähigkeit zu erhöhen. Nachdem Sie Ihre F5 BIG-IP-Sicherheits - und Verkehrsmanagementlösungen in die AWS-Cloud migriert haben, können Sie sich auf die Agilität und die Einführung hochwertiger Betriebsmodelle in Ihrer gesamten Unternehmensarchitektur konzentrieren.

Dieses Muster beschreibt, wie ein F5 BIG-IP-Workload auf einen F5 BIG-IP Virtual Edition (VE) -Workload in der AWS-Cloud migriert wird. Der Workload wird migriert, indem die bestehende Umgebung neu gehostet und Aspekte der Plattformumstellung wie Service Discovery und API-Integrationen implementiert werden. CloudFormation AWS-Vorlagen beschleunigen die Migration Ihres Workloads zur AWS-Cloud.

Dieses Muster richtet sich an Techniker- und Architekturteams, die Sicherheits- und Verkehrsmanagementlösungen von F5 migrieren, und ist Teil des Leitfadens Migration von F5 BIG-IP zu F5 BIG-IP VE in der AWS-Cloud auf der AWS Prescriptive Guidance-Website.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein vorhandener lokaler F5 BIG-IP-Workload.
- Bestehende F5-Lizenzen für BIG-IP VE-Versionen.
- Ein aktives AWS-Konto.
- Eine bestehende Virtual Private Cloud (VPC), die mit einem Ausgang über ein NAT-Gateway oder eine Elastic IP-Adresse konfiguriert und mit Zugriff auf die folgenden Endpunkte konfiguriert ist: Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), AWS Security Token Service (AWS STS) und Amazon. CloudWatch Sie können auch die modulare und skalierbare VPC-Architektur Quick Start als Baustein für Ihre Bereitstellungen ändern.
- Eine oder zwei bestehende Availability Zones, je nach Ihren Anforderungen.
- Drei bestehende private Subnetze in jeder Availability Zone.
- CloudFormation AWS-Vorlagen, verfügbar im GitHub F5-Repository.

Während der Migration können Sie je nach Ihren Anforderungen auch Folgendes verwenden:

- Eine F5 Cloud Failover Extension zur Verwaltung der Elastic IP-Adresszuweisung, der sekundären IP-Zuordnung und der Änderungen an der Routentabelle.
- Wenn Sie mehrere Availability Zones verwenden, müssen Sie die F5 Cloud Failover Extensions verwenden, um die Elastic IP-Zuordnung zu virtuellen Servern zu verwalten.
- Sie sollten erwägen, F5 Application Services 3 (AS3), F5 Application Services Templates (FAST) oder ein anderes Infrastructure-as-Code-Modell (IaC) zur Verwaltung der Konfigurationen zu verwenden. Die Vorbereitung der Konfigurationen in einem IaC-Modell und die Verwendung von Code-Repositorys helfen Ihnen bei der Migration und Ihren laufenden Verwaltungsbemühungen.

Fachwissen

- Dieses Muster setzt voraus, dass Sie wissen, wie ein oder mehrere Rechenzentren mit vorhandenen Rechenzentren verbunden werden VPCs können. Weitere Informationen dazu finden Sie unter Network-to-Amazon VPC-Konnektivitätsoptionen in der Amazon VPC-Dokumentation.
- Außerdem sind Kenntnisse der Produkte und Module von F5 erforderlich, darunter Traffic Management Operating System (TMOS), Local Traffic Manager (LTM), Global Traffic Manager (GTM), Access Policy Manager (APM), Application Security Manager (ASM), Advanced Firewall Manager (AFM) und BIG-IQ.

Produktversionen

- Wir empfehlen, F5 BIG-IP Version 13.1 oder höher zu verwenden, obwohl das Muster F5 BIG-IP Version 12.1 oder höher unterstützt.

Architektur

Quelltechnologie-Stack

- F5 BIG-IP-Arbeitslast

Zieltechnologie-Stack

- Amazon CloudFront
- Amazon CloudWatch

- Amazon EC2
- Amazon S3
- Amazon VPC
- AWS Global Accelerator
- AWS STS
- AWS Transit Gateway
- F5 BIG-IP VE

Zielarchitektur

Tools

- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.
- Amazon CloudFront beschleunigt die Verteilung Ihrer Webinhalte, indem es sie über ein weltweites Netzwerk von Rechenzentren bereitstellt, was die Latenz senkt und die Leistung verbessert.
- Amazon CloudWatch hilft Ihnen dabei, die Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie auf AWS ausführen, in Echtzeit zu überwachen.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Security Token Service (AWS STS) hilft Ihnen dabei, temporäre Anmeldeinformationen mit eingeschränkten Rechten für Benutzer anzufordern.
- AWS Transit Gateway ist ein zentraler Hub, der virtuelle private Clouds (VPCs) und lokale Netzwerke verbindet.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen

Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.

Epen

Entdeckung und Bewertung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beurteilen Sie die Leistung von F5 BIG-IP.	Erfassen und notieren Sie die Leistungskennzahlen der Anwendungen auf dem virtuellen Server sowie die Messwerte der Systeme, die migriert werden sollen. Dies hilft dabei, die AWS-Zielinfrastruktur für eine bessere Kostenoptimierung richtig zu dimensionieren.	F5 Architekt, Ingenieur und Netzwerkarchitekt, Ingenieur
Evaluieren Sie das F5 BIG-IP-Betriebssystem und die Konfiguration.	Evaluieren Sie, welche Objekte migriert werden und ob eine Netzwerkstruktur beibehalten werden muss, z. B. VLANs	F5 Architekt, Ingenieur
Evaluieren Sie die F5-Lizenzoptionen.	Prüfen Sie, welches Lizenz- und Nutzungsmodell Sie benötigen. Diese Bewertung sollte auf Ihrer Bewertung des F5 BIG-IP-Betriebssystems und der Konfiguration basieren.	F5 Architekt, Ingenieur
Evaluieren Sie die öffentlichen Anwendungen.	Ermitteln Sie, für welche Anwendungen öffentliche IP-Adressen erforderlich sind. Ordnen Sie diese	F5-Architekt, Cloud-Architekt, Netzwerkarchitekt, Ingenieur, Anwendungsteams

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anwendungen den erforderl ichen Instanzen und Clustern zu, um die Leistungs- und SLA-Anforderungen (Service Level Agreement) zu erfüllen.	
Evaluieren Sie interne Anwendungen.	Evaluieren Sie, welche Anwendungen von internen Benutzern verwendet werden. Stellen Sie sicher, dass Sie wissen, wo sich diese internen Benutzer in der Organisat ion befinden und wie diese Umgebungen mit der AWS-Cloud verbunden sind. Sie sollten auch sicherstellen, dass diese Anwendungen das Domain Name System (DNS) als Teil der Standarddomain verwenden können.	F5-Architekt, Cloud-Architekt, Netzwerkarchitekt, Ingenieur, Anwendungsteams
Finalisieren Sie das AMI.	Nicht alle F5 BIG-IP-Ve rsionen werden als Amazon Machine Images () erstellt. AMIs Sie können das F5 BIG-IP Image Generator Tool verwenden, wenn Sie über spezielle QFE-Versi onen (Quick-Fix Engineering) verfügen. Weitere Informati onen zu diesem Tool finden Sie im Abschnitt „Verwandte Ressourcen“.	F5-Architekt, Cloud-Architekt, Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Finalisieren Sie die Instanzty pen und die Architektur.	Entscheiden Sie sich für die Instance-Typen, die VPC-Architektur und die vernetzte Architektur.	F5-Architekt, Cloud-Architekt, Netzwerkarchitekt, Ingenieur

Vollständige Aktivitäten im Zusammenhang mit Sicherheit und Compliance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Dokumentieren Sie die bestehenden F5-Sicher heitsrichtlinien.	Sammeln und dokumenti eren Sie die vorhandenen F5-Sicherheitsrichtlinien. Stellen Sie sicher, dass Sie eine Kopie davon in einem sicheren Code-Repository erstellen.	F5 Architekt, Ingenieur
Verschlüsseln Sie das AMI.	(Optional) Ihre Organisation benötigt möglicherweise die Verschlüsselung von Daten im Ruhezustand. Weitere Informationen zum Erstellen eines benutzerdefinierten BYOL-Images (Bring Your Own License) finden Sie im Abschnitt „Verwandte Ressourcen“.	F5-Architekt, Ingenieur, Cloud-Architekt, Ingenieur
Härten Sie die Geräte aus.	Dies trägt zum Schutz vor potenziellen Sicherheitslücken bei.	F5 Architekt, Ingenieur

Konfigurieren Sie Ihre neue AWS-Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Edge- und Sicherheitskonten.	Melden Sie sich bei der AWS-Managementkonsole an und erstellen Sie die AWS-Konten, die die Edge- und Sicherheitsservices bereitstellen und betreiben. Diese Konten können sich von den Konten unterscheiden, die VPCs für gemeinsame Dienste und Anwendungen verwendet werden. Dieser Schritt kann als Teil einer landing zone abgeschlossen werden.	Cloud-Architekt, Ingenieur
Stellen Sie Edge und Sicherheit bereit VPCs.	Richten Sie die für die Bereitstellung von Edge- und Sicherheitsdiensten VPCs erforderlichen Dienste ein und konfigurieren Sie sie.	Cloud-Architekt, Ingenieur
Connect zum Quellrechenzentrum her.	Connect zum Quellrechenzentrum her, das Ihren F5 BIG-IP-Workload hostet.	Cloud-Architekt, Netzwerkarchitekt, Ingenieur
Stellen Sie die VPC-Verbindungen bereit.	Connect den Edge- und Sicherheitsdienst VPCs mit der Anwendung VPCs.	Netzwerkarchitekt, Ingenieur
Stellen Sie die Instanzen bereit.	Stellen Sie die Instances mithilfe der CloudFormation AWS-Vorlagen aus dem Abschnitt „Verwandte Ressourcen“ bereit.	F5 Architekt, Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen und konfigurieren Sie den Instanz-Failover.	Stellen Sie sicher, dass die AWS Advanced HA iApp-Vorlage oder die F5 Cloud Failover Extension konfiguriert ist und ordnungsgemäß funktioniert.	F5 Architekt, Ingenieur

Netzwerk konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die VPC-Topologie vor.	Öffnen Sie die Amazon VPC-Konsole und stellen Sie sicher, dass Ihre VPC über alle erforderlichen Subnetze und Schutzmaßnahmen für die F5 BIG-IP VE-Bereitstellung verfügt.	Netzwerkarchitekt, F5-Architekt, Cloud-Architekt, Ingenieur
Bereiten Sie Ihre VPC-Endpoints vor.	Bereiten Sie die VPC-Endpunkte für Amazon EC2, Amazon S3 und AWS STS vor, falls ein F5 BIG-IP-Workload keinen Zugriff auf ein NAT-Gateway oder eine Elastic IP-Adresse auf einer TMM-Schnittstelle hat.	Cloud-Architekt, Ingenieur

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie die Konfigura tion.	Migrieren Sie die F5 BIG-IP-Konfiguration auf F5 BIG-IP VE in der AWS-Cloud.	F5 Architekt, Ingenieur
Ordnen Sie die Sekundarstufe IPs zu.	Die IP-Adressen virtuelle r Server stehen in einer Beziehung zu den sekundäre n IP-Adressen, die den Instanzen zugewiesen sind. Weisen Sie sekundäre IP-Adressen zu und stellen Sie sicher, dass „Neuzuordnung/ Neuzuweisung zulassen“ ausgewählt ist.	F5 Architekt, Ingenieur

Konfigurationen testen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die virtuellen Serverkonfigurationen.	Testen Sie die virtuellen Server.	F5-Architekt, Anwendung steams

Schließen Sie den Betrieb ab

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Backup-St rategie.	Die Systeme müssen heruntergefahren werden, um einen vollständigen Snapshot zu erstellen. Weitere Informati onen finden Sie unter „Aktualis ierung einer virtuellen F5 BIG-	F5-Architekt, Cloud-Architekt, Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	IP-Maschine“ im Abschnitt „Verwandte Ressourcen“.	
Erstellen Sie das Cluster-Failover-Runbook.	Stellen Sie sicher, dass der Failover-Runbook-Vorgang abgeschlossen ist.	F5 Architekt, Ingenieur
Richten Sie die Protokollierung ein und validieren Sie sie.	Konfigurieren Sie das F5-Telemetrie-Streaming so, dass Protokolle an die erforderlichen Ziele gesendet werden.	F5 Architekt, Ingenieur

Schließen Sie die Umstellung ab

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gehen Sie zur neuen Bereitstellung über.		F5-Architekt, Cloud-Architekt, Netzwerkarchitekt, Ingenieur, AppTeams

Zugehörige Ressourcen

Leitfaden zur Migration

- Migration von F5 BIG-IP zu F5 BIG-IP VE in der AWS-Cloud

F5-Ressourcen

- CloudFormation AWS-Vorlagen im F5-Repository GitHub
- F5 im AWS Marketplace
- Überblick über F5 BIG-IP VE
- Beispiel-Schnellstart — BIG-IP Virtual Edition mit WAF (LTM + ASM)
- F5-Anwendungsservices auf AWS: ein Überblick (Video)
- Benutzerhandbuch für die Erweiterung F5 Application Services 3

- F5 Cloud-Dokumentation
- F5 iControl REST-Wiki
- F5 Überblick über einzelne Konfigurationsdateien (11.x - 15.x)
- F5-Topologielabor
- F5-Whitepapers
- Das F5 BIG-IP-Bildgenerator-Tool
- Aktualisierung einer virtuellen F5 BIG-IP VE-Maschine
- Überblick über die Option „Plattform-Migrate“ für das UCS-Archiv

Migrieren Sie eine lokale Go-Webanwendung mithilfe der binären Methode zu AWS Elastic Beanstalk

Erstellt von Suhas Basavaraj (AWS) und Shumaz Mukhtar Kazi (AWS)

Übersicht

Dieses Muster beschreibt, wie eine lokale Go-Webanwendung zu AWS Elastic Beanstalk migriert wird. Nach der Migration der Anwendung erstellt Elastic Beanstalk die Binärdatei für das Quellpaket und stellt sie auf einer Amazon Elastic Compute Cloud (Amazon) -Instance bereit. EC2

Als Strategie für die Rehost-Migration ist dieses Muster schnell und erfordert keine Codeänderungen, was weniger Test- und Migrationszeit bedeutet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine lokale Go-Webanwendung.
- Ein GitHub Repository, das den Quellcode Ihrer Go-Anwendung enthält. Wenn Sie es nicht verwenden GitHub, gibt es andere Möglichkeiten, ein Anwendungsquellpaket für Elastic Beanstalk zu erstellen.

Produktversionen

- Die neueste Go-Version, die von Elastic Beanstalk unterstützt wird. Weitere Informationen finden Sie in der Elastic Beanstalk Beanstalk-Dokumentation.

Architektur

Quelltechnologie-Stack

- Eine lokale Go-Webanwendung

Zieltechnologie-Stack

- AWS Elastic Beanstalk
- Amazon CloudWatch

Zielarchitektur

Tools

- AWS Elastic Beanstalk stellt Anwendungen in der AWS-Cloud schnell bereit und verwaltet sie, ohne dass Benutzer sich mit der Infrastruktur vertraut machen müssen, auf der diese Anwendungen ausgeführt werden. Elastic Beanstalk vereinfacht die komplexe Verwaltung, ohne Einschränkungen in Bezug auf Auswahl oder Kontrolle nach sich zu ziehen.
- GitHubist ein verteiltes Open-Source-Versionskontrollsystem.

Epen

Erstellen Sie die ZIP-Datei mit dem Quellpaket für die Go-Webanwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Quellpaket für die Go-Anwendung.	Öffnen Sie das GitHub Repository, das den Quellcode Ihrer Go-Anwendung enthält, und bereiten Sie das Quellpaket vor. Das Quellpaket enthält eine `application.go` Quelldatei im Stammverzeichnis, die das Hauptpaket für Ihre Go-Anwendung hostet. Wenn Sie es nicht verwenden GitHub, finden Sie im Abschnitt Voraussetzungen weiter oben in diesem Muster weitere Möglichkeiten, Ihr Anwendungsquellpaket zu erstellen.	Systemadministrator, Anwendungsentwickler
Erstellen einer Konfigurationsdatei	Erstellen Sie einen `.ebextensions` Ordner in Ihrem Quellpaket und dann eine `options.config`	Systemadministrator, Anwendungsentwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Datei in diesem Ordner. Weitere Informationen finden Sie in der Elastic Beanstalk Beanstalk-Dokumentation.	
Erstellen Sie die ZIP-Datei des Quellpakets.	Führen Sie den folgenden Befehl aus. `git archive -o ../godemoapp.zip HEAD` Dadurch wird die .zip-Datei des Quellpakets erstellt. Laden Sie die ZIP-Datei herunter und speichern Sie sie als lokale Datei. **Important** Die ZIP-Datei darf 512 MB nicht überschreiten und darf keinen übergeordneten Ordner oder ein Verzeichnis der obersten Ebene enthalten.	Systemadministrator, Anwendungsentwickler

Migrieren Sie die Go-Webanwendung zu Elastic Beanstalk

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie die Elastic Beanstalk Beanstalk-Anwendung aus.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Elastic Beanstalk Beanstalk-Konsole. 2. Wählen Sie aus der Liste der Regionen Ihre AWS-Region aus. 3. Wählen Sie im Navigationsbereich Applications und dann eine bestehende Elastic Beanstalk Beanstalk-Anwendung aus oder erstellen Sie eine. Anweisungen zum Erstellen einer Elastic Beanstalk Beanstalk-Anwendung finden Sie in der Elastic Beanstalk Beanstalk-Dokumentation.	Systemadministrator, Anwendungsentwickler
Initiieren Sie die Elastic Beanstalk Beanstalk-Webserver-Umgebung.	1. Wählen Sie auf der Seite mit der Anwendungsübersicht die Option Neue Umgebung erstellen und anschließend Webserver-Umgebung aus. 2. Füllen Sie die Felder Umgebungsname und Domänenname aus.	Systemadministrator, Anwendungsentwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie Plattform version und anschließend Go als Plattform aus.	
Laden Sie die .zip-Datei des Quellpakets auf Elastic Beanstalk hoch.	1. Wählen Sie unter Anwendungscode die Option Code hochladen und dann Lokale Datei aus. 2. Wählen Sie die ZIP-Datei aus, die Ihr Quellpaket enthält. 3. Geben Sie der Datei unter Versionsbezeichnung einen eindeutigen Namen und wählen Sie dann Umgebung erstellen aus.	Systemadministrator, Anwendungsentwickler
Testen Sie die bereitgestellte Go-Webanwendung.	Sie werden zur Übersicht sseite der Elastic Beanstalk Beanstalk-Anwendung weitergeleitet. Wählen Sie oben in der Übersicht neben Environment ID die URL aus, die mit „Um zu Ihrer Anwendung `elasticbe anstalk.com` zu navigiere n“ endet. Ihre Anwendung muss diesen Namen in ihrer Konfigurationsdate i als Umgebungsvariable verwenden und ihn auf der Webseite anzeigen.	Systemadministrator, Anwendungsentwickler

Fehlerbehebung

Problem	Lösung
Auf die Anwendung kann nicht über einen Application Load Balancer zugegriffen werden.	Überprüfen Sie die Zielgruppe, die Ihre Elastic Beanstalk Beanstalk-Anwendung enthält. Wenn sie fehlerhaft ist, melden Sie sich bei Ihrer Elastic Beanstalk Beanstalk-Instance an und überprüfen Sie die `nginx.conf` Dateikonf iguration, um sicherzustellen, dass sie zur richtigen Integritätsstatus-URL weitergeleitet wird. Möglicherweise müssen Sie die URL für die Zustandsprüfung der Zielgruppe ändern.

Zugehörige Ressourcen

- Von Elastic Beanstalk unterstützte Go-Plattformversionen
- Verwenden von Konfigurationsdateien mit Elastic Beanstalk
- Eine Beispielanwendung in Elastic Beanstalk erstellen

Migrieren Sie einen lokalen SFTP-Server zur Verwendung von AWSAWS Transfer for SFTP

Erstellt von Akash Kumar (AWS)

Übersicht

Dieses Muster beschreibt, wie eine lokale Dateiübertragungslösung, die das Secure Shell (SSH) File Transfer Protocol (SFTP) verwendet, mithilfe des Dienstes auf den AWS Cloud migriert wird. AWS Transfer for SFTP Benutzer stellen in der Regel entweder über seinen Domainnamen oder eine feste IP-Adresse eine Verbindung zu einem SFTP-Server her. Dieses Muster deckt beide Fälle ab.

AWS Transfer for SFTP ist Mitglied der AWS Transfer Family. Es ist ein sicherer Übertragungsdienst, mit dem Sie Dateien über SFTP in und aus AWS Speicherdiensten übertragen können. Sie können es AWS Transfer for SFTP mit Amazon Simple Storage Service (Amazon S3) oder Amazon Elastic File System (Amazon EFS) verwenden. Dieses Muster verwendet Amazon S3 für die Speicherung.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto.
- Ein vorhandener SFTP-Domänenname oder eine feste SFTP-IP.

Einschränkungen

- Das größte Objekt, das Sie in einer Anfrage übertragen können, ist derzeit 5 GiB groß. Für Dateien, die größer als 100 MiB sind, sollten Sie den mehrteiligen Amazon S3 S3-Upload in Betracht ziehen.

Architektur

Quelltechnologie-Stack

- Lokale Flatfiles oder Datenbank-Dumpdateien.

Zieltechnologie-Stack

- AWS Transfer for SFTP
- Amazon S3

- Amazon Virtual Private Cloud (Amazon VPC)
- AWS Identity and Access Management (IAM) Rollen und Richtlinien
- Elastic-IP-Adressen
- Sicherheitsgruppen
- CloudWatch Amazon-Protokolle (optional)

Zielarchitektur

Automatisierung und Skalierung

Verwenden Sie die beigefügten AWS CloudFormation Vorlagen, um die Zielarchitektur für dieses Muster zu automatisieren:

- `amazon-vpc-subnets.yml`stellt eine Virtual Private Cloud (VPC) mit zwei öffentlichen und zwei privaten Subnetzen bereit.
- `amazon-sftp-server.yml`stellt den SFTP-Server bereit.
- `amazon-sftp-customer.yml`fügt Benutzer hinzu.

Tools

AWS-Services

- Amazon CloudWatch Logs hilft Ihnen dabei, die Protokolle all Ihrer Systeme und Anwendungen zu zentralisieren, AWS-Services sodass Sie sie überwachen und sicher archivieren können.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, sie zu verwenden.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt. Dieses Muster verwendet Amazon S3 als Speichersystem für Dateiübertragungen.
- AWS Transfer for SFTPhilft Ihnen bei der Übertragung von Dateien in und aus AWS Speicherdiensten über das SFTP-Protokoll.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk bereitzustellen. Dieses virtuelle Netzwerk entspricht einem

herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben würden, mit den Vorteilen der Verwendung der skalierbaren Infrastruktur von AWS.

Epen

Erstellen einer VPC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC mit Subnetzen.	Öffnen Sie die Amazon VPC-Konsole. Erstellen Sie eine Virtual Private Cloud (VPC) mit zwei öffentlichen Subnetzen. (Das zweite Subnetz bietet hohe Verfügbarkeit.) –oder– Sie können die angehängte CloudFormation Vorlage in der CloudFormation Konsole bereitstellen `amazon-vpc-subnets.yml` , um die Aufgaben in diesem Epos zu automatisieren.	Entwickler, Systemadministrator
Fügen Sie ein Internet-Gateway hinzu.	Stellen Sie ein Internet-Gateway bereit und verbinden Sie es mit der VPC.	Entwickler, Systemadministrator
Migrieren Sie eine bestehende IP.	Hängen Sie eine bestehende IP an die Elastic IP-Adresse an. Sie können eine Elastic IP-Adresse aus Ihrem Adresspool erstellen und verwenden.	Entwickler, Systemadministrator

Stellen Sie einen SFTP-Server bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen SFTP-Server.	Öffnen Sie die AWS Transfer Family -Konsole. Folgen Sie den Anweisungen unter Erstellen eines mit dem Internet verbundenen Endpunkts für Ihren Server in der AWS Transfer Family Dokumentation, um einen SFTP-Server mit einem mit dem Internet verbundenen Endpunkt zu erstellen. Wählen Sie als Endpunkttyp die Option VPC Hosted aus. Wählen Sie für Access die Option Internet Facing aus. Wählen Sie für VPC die VPC aus, die Sie im vorherigen Epos erstellt haben. –oder– Sie können die angehängte CloudFormation Vorlage in der CloudFormation Konsole bereitstellen`amazon-sftp-server.yml`, um die Aufgaben in diesem Epic zu automatisieren.	Entwickler, Systemadministrator
Migrieren Sie den Domainnamen.	Hängen Sie den vorhandenen Domainnamen an den benutzerdefinierten Hostnamen an. Wenn Sie einen neuen Domainnamen	Entwickler, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	verwenden, verwenden Sie den Amazon Route 53-DNS-Alias. Wählen Sie für einen vorhandenen Domainnam en „Anderes DNS“. Weitere Informationen finden Sie in der AWS Transfer Family Dokumentation unter Arbeiten mit benutzerdefinierten Hostnamen.	
Fügen Sie eine CloudWatch Logging-Rolle hinzu.	(Optional) Wenn Sie die CloudWatch Protokoll ierung aktivieren möchten, erstellen Sie eine `Transfer` Rolle mit den CloudWatc h Logs-API-Vorgängen `logs:CreateLogGrou p logs:CreateLogStre am` , `logs:Desc ribeLogStreams` , und`logs:PutLogEvents` . Weitere Informationen finden Sie CloudWatch in der AWS Transfer Family Dokumenta tion unter Aktivität protokoll ieren mit.	Entwickler, Systemadm inistrator
Speichern und abschicken.	Wählen Sie Speichern. Wählen Sie für Aktionen die Option Start und warten Sie, bis der SFTP-Server mit dem Status Online erstellt wurde.	Entwickler, Systemadm inistrator

Ordnen Sie dem SFTP-Server Elastic IP-Adressen zu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stoppen Sie den Server, damit Sie die Einstellungen ändern können.	Wählen Sie auf der AWS Transfer Family Konsole Server und dann den von Ihnen erstellten SFTP-Server aus. Wählen Sie für Actions (Aktionen) die Option Stop (Stopp). Wenn der Server offline ist, wählen Sie Bearbeiten, um seine Einstellungen zu ändern.	Entwickler, Systemadministrator
Wählen Sie Availability Zones und Subnetze.	Wählen Sie im Abschnitt Availability Zones die Availability Zones und Subnetze für Ihre VPC aus.	Entwickler, Systemadministrator
Fügen Sie Elastic IP-Adressen hinzu.	Wählen Sie unter IPv4 Adressen eine Elastic IP-Adresse für jedes Subnetz aus und klicken Sie dann auf Speichern.	Entwickler, Systemadministrator

Hinzufügen von Benutzern

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle, damit Benutzer auf den S3-Bucket zugreifen können.	Erstellen Sie eine IAM-Rolle für `Transfer` und fügen Sie `s3:ListBucket` `s3:GetBucketLocation` , und `s3:PutObject` mit dem S3-Bucket-Namen als Ressource	Entwickler, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	hinzu. Weitere Informationen finden Sie in der Dokumentation unter Erstellen einer IAM-Rolle und -Richtlinie. AWS Transfer Family –oder– Sie können die angehängte CloudFormation Vorlage in der CloudFormation Konsole bereitstellen `amazon-sftp-customer.yml` , um die Aufgaben in diesem Epos zu automatisieren.	
Erstellen Sie einen S3-Bucket.	Erstellen Sie einen S3-Bucket für die Anwendung.	Entwickler, Systemadministrator
Erstellen Sie optionale Ordner.	(Optional) Wenn Sie Dateien für Benutzer separat in bestimmten Amazon S3 S3-Ordnern speichern möchten, fügen Sie die entsprechenden Ordner hinzu.	Entwickler, Systemadministrator
Erstellen Sie einen öffentlichen SSH-Schlüssel.	Informationen zum Erstellen eines SSH-Schlüsselpaars finden Sie in der Dokumentation unter Generieren von SSH-Schlüsseln. AWS Transfer Family	Entwickler, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Hinzufügen von Benutzern.	Wählen Sie auf der AWS Transfer Family Konsole Server, wählen Sie den von Ihnen erstellten SFTP-Server aus und klicken Sie dann auf Benutzer hinzufügen. Wählen Sie für das Home-Verzeichnis den S3-Bucket aus, den Sie erstellt haben. Geben Sie für den öffentlichen SSH-Schlüssel den öffentlichen Schlüsselteil des SSH-Schlüsselpaars an. Fügen Sie Benutzer für den SFTP-Server hinzu und wählen Sie dann Hinzufügen.	Entwickler, Systemadministrator

Testen Sie den SFTP-Server

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Sicherheitsgruppe.	Fügen Sie im Abschnitt Sicherheitsgruppen Ihres SFTP-Servers die IP Ihres Testcomputers hinzu, um SFTP-Zugriff zu erhalten.	Developer
Verwenden Sie ein SFTP-Client-Hilfsprogramm, um den Server zu testen.	Testen Sie Dateiübertragungen mit einem beliebigen SFTP-Client-Hilfsprogramm. Eine Liste der Clients und Anweisungen finden Sie in der AWS Transfer Family Dokumentation unter	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Übertragen von Dateien mit einem Client.	

Zugehörige Ressourcen

- AWS Transfer Family Benutzerhandbuch
- Amazon S3 S3-Benutzerhandbuch
- Elastische IP-Adressen in der EC2 Amazon-Dokumentation

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Migrieren Sie eine lokale VM EC2 mithilfe des AWS Application Migration Service zu Amazon

Erstellt von Thanh Nguyen (AWS)

Übersicht

Wenn es um die Migration von Anwendungen geht, können Unternehmen verschiedene Ansätze verfolgen, um die Server der Anwendung von der lokalen Umgebung in die Amazon Web Services (AWS) Cloud neu zu hosten (Lift and Shift). Eine Möglichkeit besteht darin, neue Amazon Elastic Compute Cloud (Amazon EC2) -Instances bereitzustellen und die Anwendung dann von Grund auf neu zu installieren und zu konfigurieren. Ein anderer Ansatz besteht darin, native Migrationsdienste von Drittanbietern oder AWS zu verwenden, um mehrere Server gleichzeitig zu migrieren.

Dieses Muster beschreibt die Schritte für die Migration einer unterstützten virtuellen Maschine (VM) zu einer EC2 Amazon-Instance in der AWS-Cloud mithilfe des AWS Application Migration Service. Sie können den in diesem Muster beschriebenen Ansatz verwenden, um eine oder mehrere virtuelle Maschinen manuell, nacheinander oder automatisch zu migrieren, indem Sie auf der Grundlage der beschriebenen Schritte entsprechende Automatisierungsskripts erstellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto in einer der AWS-Regionen, die den Application Migration Service unterstützen
- Netzwerkkonnektivität zwischen dem EC2 Quellserver und dem Zielserver über ein privates Netzwerk mithilfe von AWS Direct Connect oder einem virtuellen privaten Netzwerk (VPN) oder über das Internet

Einschränkungen

- Die aktuelle Liste der unterstützten Regionen finden Sie unter Unterstützte AWS-Regionen.
- Eine Liste der unterstützten Betriebssysteme finden Sie in den Abschnitten Unterstützte Betriebssysteme und Allgemein von Amazon EC2 FAQs.

Architektur

Quelltechnologie-Stack

- Ein physischer, virtueller oder in der Cloud gehosteter Server, auf dem ein von Amazon unterstütztes Betriebssystem ausgeführt wird EC2

Zieltechnologie-Stack

- Eine EC2 Amazon-Instance, auf der dasselbe Betriebssystem wie die Quell-VM ausgeführt wird
- Amazon Elastic Block Store (Amazon EBS)

Quell- und Zielarchitektur

Das folgende Diagramm zeigt die allgemeine Architektur und die Hauptkomponenten der Lösung. Im lokalen Rechenzentrum gibt es virtuelle Maschinen mit lokalen Festplatten. Auf AWS gibt es einen Staging-Bereich mit Replikationsservern und einen Bereich für migrierte Ressourcen mit EC2 Instances für Tests und Cutover. Beide Subnetze enthalten EBS-Volumes.

1. Initialisieren Sie den AWS Application Migration Service.
2. Richten Sie die Serverkonfiguration und das Reporting für den Staging-Bereich ein, einschließlich der Ressourcen für den Staging-Bereich.
3. Installieren Sie Agenten auf Quellservern und verwenden Sie die kontinuierliche Datenreplikation auf Blockebene (komprimiert und verschlüsselt).
4. Automatisieren Sie Orchestrierung und Systemkonvertierung, um das Umstellungsfenster zu verkürzen.

Netzwerk-Architektur

Das folgende Diagramm zeigt die allgemeine Architektur und die Hauptkomponenten der Lösung aus Netzwerksicht, einschließlich der erforderlichen Protokolle und Ports für die Kommunikation zwischen den Hauptkomponenten im lokalen Rechenzentrum und auf AWS.

Tools

- Mit AWS Application Migration Service können Sie Anwendungen ohne Änderungen und mit minimalen Ausfallzeiten in die AWS-Cloud rehosten (Lift and Shift).

Bewährte Methoden

- Nehmen Sie den Quellserver nicht offline und führen Sie keinen Neustart durch, bis die Umstellung auf die EC2 Zielinstanz abgeschlossen ist.
- Bieten Sie den Benutzern ausreichend Gelegenheit, Benutzerakzeptanztests (UAT) auf dem Zielserver durchzuführen, um Probleme zu identifizieren und zu lösen. Idealerweise sollten diese Tests mindestens zwei Wochen vor der Umstellung beginnen.
- Überwachen Sie regelmäßig den Status der Serverreplikation auf der Application Migration Service-Konsole, um Probleme frühzeitig zu erkennen.
- Verwenden Sie temporäre AWS Identity and Access Management (IAM) -Anmeldeinformationen für die Agenteninstallation anstelle von permanenten IAM-Benutzeranmeldedaten.

Epen

AWS-Anmeldeinformationen generieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Rolle AWS Replication Agent.	Melden Sie sich mit Administratorberechtigungen für das AWS-Konto an. Erstellen Sie auf der AWS Identity and Access Management (IAM) -Konsole eine IAM-Rolle: 1. Wählen Sie auf der IAM-Konsole Rollen aus. 2. Wählen Sie Rolle erstellen aus. 3. Wählen Sie auf der Seite Vertrauenswürdige Entität auswählen im Abschnitt Vertrauenswürdige Entität die Option AWS-Konto aus.	AWS-Administrator, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie im Abschnitt Ein AWS-Konto die Option Dieses Konto (< Account-ID>) aus. 5. Wählen Sie Weiter aus. 6. Suchen Sie auf der Seite „Berechtigungen hinzufügen“ nach der `AWSApplicationMigrationAgentInstallationPolicy` Richtlinie und aktivieren Sie das Kontrollkästchen neben dem Richtlinnennamen. 7. Wählen Sie Weiter aus. 8. Geben Sie auf der Seite mit den Rollendetails MGN_Agent_Installation_Role als Rollennamen ein. 9. Vergewissern Sie sich, dass die Felder korrekt sind, und wählen Sie dann Rolle erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie temporäre Sicherheitsnachweise.	Melden Sie sich auf einem Computer, auf dem AWS Command Line Interface (AWS CLI) installiert ist, mit Administratorrechten an. Oder melden Sie sich alternativ (innerhalb einer unterstützten AWS-Region) in der AWS-Managementkonsole mit Administratorberechtigungen für das AWS-Konto an und öffnen Sie AWS CloudShell. Generieren Sie temporäre Anmeldeinformationen mit dem folgenden Befehl und ersetzen Sie `<account-id>` ihn durch die AWS-Konto-ID. `aws sts assume-role --role-arn arn:aws:iam::<account-id>:role/MGN_Agent_Installation_Role --role-session-name mgn_installation_session_role` Kopieren Sie aus der Ausgabe des Befehls die Werte für `AccessKeyId` **`SecretAccessKey`** , und **`SessionToken`** . Bewahren Sie sie für den späteren Gebrauch an einem sicheren Ort auf.	AWS-Administrator, Migration singenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Important Diese temporären Anmeldeinformationen laufen nach einer Stunde ab. Wenn Sie nach einer Stunde Anmeldeinformationen benötigen, wiederholen Sie die vorherigen Schritte.	

Initialisieren Sie den Application Migration Service und erstellen Sie die Vorlage für die Replikationseinstellungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initialisieren Sie den Dienst.	Melden Sie sich auf der Konsole mit Administratorberechtigungen für das AWS-Konto an. Wählen Sie Application Migration Service und dann Get started aus.	AWS-Administrator, Migrationsingenieur
Erstellen und konfigurieren Sie die Vorlage für die Replikationseinstellungen.	1. Geben Sie die folgenden Konfigurationsdetails an: a. Wählen Sie das Subnetz für den Staging-Bereich aus. b. Wählen Sie den Instanztyp des Replikationsservers aus	AWS-Administrator, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(`t3.small`standardm äßig). c. Wählen Sie den EBS-Volumetyp aus (standard mäßig gp3). d. Wählen Sie die EBS-Verschlüsselungsoption aus. e. Stellen Sie sicher, dass das Kontrollk ästchen Sicherhei tsgruppe des Application Migration Service immer verwenden aktiviert ist. f. Aktivieren Sie das Kontrollkästchen Private IP für Datenreplikation verwenden (VPN DirectConnect, VPC-Peering), wenn Sie private Netzwerkk onnektivität zwischen der lokalen Umgebung und AWS verwenden. g. Aktivieren Sie das Kontrollkästchen Netzwerkbandbreite drosseln (pro Server — in Mbit/s), wenn Sie die Netzwerkbandbreite für Application Migration Service einschränken möchten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie Create template (Vorlage erstellen) aus. Der Application Migration Service erstellt automatisch alle IAM-Rollen, die für die Datenreplikation und den Start migrierter Server erforderlich sind.	

Installieren Sie AWS Replication Agents auf Quellcomputern

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Halten Sie die erforderlichen AWS-Anmeldeinformationen bereit.	Wenn Sie die Installat ionsdatei auf einem Quellserv er ausführen, müssen Sie die temporären Anmeldein formationen eingeben, die Sie zuvor generiert haben, einschließlich `AccessKey Id SecretAccessKey` , und`SessionToken` .	Migrationsingenieur, AWS-Administrator
Installieren Sie den Agenten für Linux-Server.	Kopieren Sie den Installat ionsbefehl, melden Sie sich bei Ihren Quellservern an und führen Sie das Installat ionsprogramm aus. Eine ausführliche Anleitung finden Sie in der AWS-Dokum entation.	AWS-Administrator, Migration singenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den Agenten für Windows-Server.	Laden Sie die Installat ionsdatei auf jeden Server herunter und führen Sie dann den Installationsbefehl aus. Eine ausführliche Anleitung finden Sie in der AWS-Dokum entation.	AWS-Administrator, Migration singenieur
Warten Sie, bis die erste Datenreplikation abgeschlo ssen ist.	Wenn der Agent installiert wurde, wird der Quellserver auf der Application Migration Service-Konsole im Abschnitt Quellserver angezeigt. Warten Sie, bis der Server die erste Datenreplikation durchführt.	AWS-Administrator, Migration singenieur

Starteinstellungen konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie die Serverdetails an.	Wählen Sie in der Applicati on Migration Service-Konsole den Abschnitt Quellserver und dann einen Servernamen aus der Liste aus, um auf die Serverdetails zuzugreifen.	AWS-Administrator, Migration singenieur
Konfigurieren Sie die Starteins tellungen.	Wählen Sie die Registerkarte Starteinstellungen. Sie können eine Vielzahl von Einstellu ngen konfigurieren, darunter allgemeine Starteinstellungen und EC2 Startvorlageneinst ellungen. Eine ausführliche	AWS-Administrator, Migration singenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anleitung finden Sie in der AWS-Dokumentation.	

Führen Sie einen Test durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Quellserver.	1. Stellen Sie in der Application Migration Service-Konsole im Abschnitt Quellserver sicher, dass der Migrationszyklus der Quellserver bereit zum Testen ist und dass der Datenreplikationsstatus Fehlerfrei lautet. 2. Aktivieren Sie das Kontrollkästchen links neben jedem Quellserver. 3. Wählen Sie Test and Cutover und anschließend Launch Test Instance aus. 4. Wenn Sie dazu aufgefordert werden, wählen Sie Launch. Die Server werden gestartet.	AWS-Administrator, Migrationsingenieur
Stellen Sie sicher, dass der Test erfolgreich abgeschlossen wurde.	Nachdem der Testserver vollständig gestartet wurde, wird im Warnmeldungsstatus auf der Seite für jeden	AWS-Administrator, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Server die Meldung Gestartet angezeigt.	
Testen Sie den Server.	Führen Sie Tests auf dem Testserver durch, um sicherzustellen, dass er wie erwartet funktioniert.	AWS-Administrator, Migration singenieur

Planen und führen Sie eine Umstellung durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Planen Sie ein Zeitfenster für die Umstellung ein.	Vereinbaren Sie mit den zuständigen Teams einen angemessenen Zeitrahmen für die Umstellung.	AWS-Administrator, Migration singenieur
Führen Sie die Umstellung durch.	1. Aktivieren Sie in der Anwendungsmigratio nskonsole auf der Seite Quellserver das Kontrollk ästchen links neben jedem Quellserver. 2. Wählen Sie Test und Übernahme und dann Als „Bereit für die Übernahme“ markieren aus. 3. Stellen Sie sicher, dass der Migrationszyklus jedes Quellservers bereit für die Übernahme ist. 4. Wählen Sie Test and Cutover und anschließend	AWS-Administrator, Migration singenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Cutover-Instances starten aus. 5. Wenn Sie dazu aufgefordert werden, wählen Sie Launch. Die Server werden gestartet. Der Migrationszyklus des Quellservers wird zu „Umstellung läuft“ geändert.	
Stellen Sie sicher, dass die Umstellung erfolgreich abgeschlossen wurde.	Nachdem die Übernahmeserver vollständig gestartet wurden, zeigt der Status Alerts auf der Seite Quellserver für jeden Server den Status Gestartet an.	AWS-Administrator, Migrationsingenieur
Testen Sie den Server.	Führen Sie Tests mit dem Cutover-Server durch, um sicherzustellen, dass er wie erwartet funktioniert.	AWS-Administrator, Migrationsingenieur
Schließen Sie die Umstellung ab.	Wählen Sie Test und Übernahme und anschließend Übernahme abschließen aus, um den Migrationsprozess abzuschließen.	AWS-Administrator, Migrationsingenieur

Zugehörige Ressourcen

- AWS Application Migration Service
- AWS Application Migration Service — Benutzerhandbuch

Migrieren Sie kleine Datensätze mithilfe von AWS SFTP von der lokalen Infrastruktur zu Amazon S3

Erstellt von Charles Gibson (AWS) und Sergiy Shevchenko (AWS)

Übersicht

Dieses Muster beschreibt, wie kleine Datenmengen (5 TB oder weniger) von lokalen Rechenzentren zu Amazon Simple Storage Service (Amazon S3) mithilfe von AWS Transfer for SFTP (AWS SFTP) migriert werden. Bei den Daten kann es sich entweder um Datenbank-Dumps oder um Flatfiles handeln.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine AWS Direct Connect, die zwischen Ihrem Rechenzentrum und AWS hergestellt wurde

-Einschränkungen

- Die Datendateien müssen weniger als 5 TB groß sein. Für Dateien über 5 TB können Sie einen mehrteiligen Upload auf Amazon S3 durchführen oder eine andere Datenübertragungsmethode wählen.

Architektur

Quelltechnologie-Stack

- Lokale Flatfiles oder Datenbank-Dumps

Zieltechnologie-Stack

- Amazon S3

Quell- und Zielarchitektur

Tools

- AWS SFTP — Ermöglicht die direkte Übertragung von Dateien in und aus Amazon S3 mithilfe des Secure File Transfer Protocol (SFTP).
- AWS Direct Connect — Stellt eine dedizierte Netzwerkverbindung von Ihren lokalen Rechenzentren zu AWS her.
- VPC-Endpunkte — Ermöglicht es Ihnen, eine VPC privat mit unterstützten AWS-Services und VPC-Endpunktservices zu verbinden, die von AWS bereitgestellt werden, PrivateLink ohne dass ein Internet-Gateway, ein NAT-Gerät (Network Address Translation), eine VPN-Verbindung oder eine AWS Direct Connect-Verbindung erforderlich ist. Instances in einer VPC benötigen keine öffentlichen IP-Adressen, um mit Ressourcen im Service zu kommunizieren.

Epen

Bereite dich auf die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Dokumentieren Sie die aktuellen SFTP-Anfo rderungen.		Inhaber der Anwendung, SA
Identifizieren Sie die Authentif izierungsanforderungen.	Zu den Anforderungen können eine schlüssel basierte Authentifizierung, ein Benutzername oder ein Passwort oder ein Identität sanbieter (IdP) gehören.	Inhaber der Anwendung, SA
Identifizieren Sie die Anforderu ngen an die Anwendung sintegration.		Besitzer der Anwendung
Identifizieren Sie die Benutzer, die den Dienst benötigen.		Besitzer der Anwendung
Ermitteln Sie den DNS-Namen für den SFTP-Serverendpunkt.		Netzwerk

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie die Backup-Strategie.		SA, DBA (wenn Daten übertragen werden)
Identifizieren Sie die Strategie für die Anwendungsmigration oder -umstellung.		Inhaber der Anwendung, SA, DBA

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine oder mehrere virtuelle private Clouds (VPCs) und Subnetze in Ihrem AWS-Konto.		Inhaber der Anwendung, AMS
Erstellen Sie die Sicherheitsgruppen und die Network Access Control List (ACL).		Sicherheit, Netzwerke, AMS
Erstellen Sie den S3-Bucket.		Inhaber der Anwendung, AMS
Erstellen Sie die Rolle für Identitäts- und Zugriffsmanagement (IAM).	Erstellen Sie eine IAM-Richtlinie, die die Berechtigungen enthält, um AWS SFTP den Zugriff auf Ihren S3-Bucket zu ermöglichen. Diese IAM-Richtlinie bestimmt, welche Zugriffsebene Sie SFTP-Benutzern gewähren. Erstellen Sie eine weitere IAM-Richtlinie, um eine Vertrauensbeziehung mit AWS SFTP aufzubauen.	Sicherheit, AMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ordnen Sie eine registrierte Domain zu (optional).	Wenn Sie eine eigene registrierte Domain haben, können Sie diese mit dem SFTP-Server verknüpfen. Sie können SFTP-Verkehr von einer Domain oder von einer Subdomain an Ihren SFTP-Serverendpunkt weiterleiten.	Netzwerke, AMS
Erstellen Sie einen SFTP-Server.	Geben Sie den Identitätsanbietertyp an, den der Dienst zur Authentifizierung Ihrer Benutzer verwendet.	Inhaber der Anwendung, AMS
Öffnen Sie einen SFTP-Client.	Öffnen Sie einen SFTP-Client und konfigurieren Sie die Verbindung für die Verwendung des SFTP-Endpunkthosts. AWS SFTP unterstützt jeden Standard-SFTP-Client. Zu den häufig verwendeten SFTP-Clients gehören OpenSSH, WinSCP, Cyberduck und. FileZilla Sie können den Hostnamen des SFTP-Servers von der AWS-SFTP-Konsole abrufen.	Besitzer der Anwendung, AMS

Planen und testen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Planen Sie die Anwendungsmigration.	Planen Sie alle erforderlichen Änderungen an der Anwendungskonfiguration	Inhaber der Anwendung, AMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ein, legen Sie das Migration sdatum fest und legen Sie den Testplan fest.	
Testen Sie die Infrastruktur.	Testen Sie in einer Umgebung außerhalb der Produktio nsumgebung.	Inhaber der Anwendung, AMS

Zugehörige Ressourcen

Referenzen

- AWS Transfer for SFTP — Benutzerhandbuch
- AWS Direct Connect Connect-Ressourcen
- VPC-Endpunkte

Tutorials und Videos

- AWS Transfer for SFTP (Video)
- AWS Transfer for SFTP — Benutzerhandbuch
- AWS SA Whiteboarding — Direktverbindung (Video)

Migrieren Sie von Oracle GlassFish zu AWS Elastic Beanstalk

Erstellt von Sandeep Bondugula (AWS)

Übersicht

Dieses Muster beschreibt, wie eine Java-Anwendung, die auf einem lokalen GlassFish Oracle-Server ausgeführt wird, zu AWS Elastic Beanstalk in der AWS-Cloud migriert wird.

Auf AWS wird die Java-Anwendung auf einem GlassFish Docker-Server mit AWS Elastic Beanstalk bereitgestellt, der in einer Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppe ausgeführt wird.

Zusätzliche Funktionen:

- Amazon Elastic Beanstalk fungiert als Wrapper für mehrere zugrunde liegende Ressourcen. Es richtet Elastic Load Balancing ein (das den eingehenden Verkehr von Amazon Route 53 verarbeitet), verteilt den Datenverkehr auf eine oder mehrere EC2 Instances und dient auch als Bereitstellungstool.
- Um eine lokale Datenbank zu Amazon Relational Database Service (Amazon RDS) zu migrieren, aktualisieren Sie die Datenbankverbindungsdetails. In der Backend-Datenbank können Sie Amazon RDS Multi-AZ-Bereitstellungen konfigurieren und den Datenbank-Engine-Typ auswählen.
- Sie können die Multi-AZ-Bereitstellung für hohe Verfügbarkeit zusammen mit der Auto Scaling-Gruppe und der Skalierungsrichtlinie verwenden, um die Ausfallsicherheit zu verbessern.
- Sie können eine Skalierungsrichtlinie einrichten, die auf CloudWatch Amazon-Metriken basiert.
- In AWS Elastic Beanstalk können Sie die zugrunde liegenden Elastic Load Balancing Balancing-Einstellungen und Amazon EC2 Auto Scaling konfigurieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine lokale Java-Anwendung, die auf läuft GlassFish
- Eine WAR-Datei (Java Web Application Resource)

Produktversionen

- Oracle Glassfish 4.1.2 und 5.0
- Java 7 4.0 GlassFish
- Java 8 GlassFish 4.1 oder höher

Architektur

Quelltechnologie-Stack

- Anwendungen entwickelt in GlassFish

Zieltechnologie-Stack

- Elastic Beanstalk

Zielarchitektur

Arbeitsablauf bei der Bereitstellung

Tools

- Amazon Elastic Beanstalk — Ein Service für die Bereitstellung und Skalierung von Webanwendungen und Services, die mit Java, .NET, PHP, Node.js, Python, Ruby, Go und Docker auf Servern wie Apache, NGINX, Passenger und IIS entwickelt wurden.
- Amazon CloudWatch — Bietet Daten und umsetzbare Erkenntnisse zur Überwachung von Anwendungen, reagiert auf systemweite Leistungsänderungen, optimiert die Ressourcennutzung und bietet einen einheitlichen Überblick über den Betriebsstatus.
- Docker — Eine Plattform, die Software in standardisierte Einheiten verpackt, um Anwendungen schnell zu erstellen, zu testen und bereitzustellen.
- Java — Eine Allzweck-Programmiersprache. Java ist klassenbasiert, objektorientiert und so konzipiert, dass es weniger Implementierungsabhängigkeiten aufweist.

Epen

Richten Sie eine VPC ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Virtual Private Cloud (VPC) -Instanz mit den erforderlichen Informationen.		SysAdmin
Erstellen Sie mindestens zwei Subnetze innerhalb der VPC.		SysAdmin
Erstellen Sie eine Routing-T abelle gemäß den Anforderu ngen.		SysAdmin

Amazon S3 einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon-Si mple-Storage-Service-(Amazo n S3)-Bucket.		SysAdmin
Kopieren Sie die WAR-Datei in den S3-Bucket und laden Sie den Anwendungscode hoch.		SysAdmin

Erstellen einer IAM-Rolle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS Identity and Access Management (IAM) -Rolle.	Sie können das Standardprofil mit aws-elasticbeanstalk-ec 2 Rollen verwenden oder es von	SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Elastic Beanstalk automatisch erstellen lassen.	

Elastic Beanstalk einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Öffnen Sie das Elastic Beanstalk-Dashboard.		SysAdmin
Erstellen Sie eine neue Anwendung und wählen Sie die Webserver-Umgebung aus.		SysAdmin
Wählen Sie GlassFish Docker als vorkonfigurierte Plattform.		SysAdmin
Laden Sie den Code hoch.	Geben Sie die URL der S3-Bucket-Datei oder die ZIP-Datei aus den lokalen Systemdateien an.	SysAdmin
Wählen Sie den Umgebungstyp aus.	Wählen Sie in den Einstellungen für die Konfigurationskapazität entweder Single Instance oder Load Balancer aus.	SysAdmin
Konfigurieren Sie den Load Balancer.	Wenn Sie im vorherigen Schritt Load Balancer ausgewählt haben, konfigurieren Sie die Multi-AZ-Bereitstellung.	SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie unter Konfiguration und Sicherheitseinstellungen die zuvor erstellte IAM-Rolle aus.		SysAdmin
Wenn Sie unter Konfiguration und Sicherheitseinstellungen ein vorhandenes key pair haben, verwenden Sie es oder erstellen Sie ein neues EC2 Amazon-Schlüsselpaar.		SysAdmin
Konfigurieren Sie Amazon in den Einstellungen für die Konfigurationsüberwachung CloudWatch.		SysAdmin
Wählen Sie in den Einstellungen für die Konfigurationssicherheit die zuvor erstellte VPC aus.		SysAdmin
Wählen Sie Umgebung erstellen aus.		SysAdmin

Testen der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Anwendung mithilfe der URL, die in der erstellten Umgebung bereitgestellt wurde.		

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wenden Sie die DNS-Änderungen (Domain Name Service) in Amazon Route 53 an.		

Zugehörige Ressourcen

- GlassFish Oracle-Dokumentation
- GlassFish Open-Source-Java-EE-Referenzimplementierung
- Dokumentation zu AWS Elastic Beanstalk
- Elastic Beanstalk mit Amazon verwenden CloudWatch
- Preise für AWS Elastic Beanstalk
- EC2 Auto Scaling-Gruppe
- Skalieren Sie die Größe Ihrer Auto Scaling Scaling-Gruppe
- Amazon RDS Multi-AZ-Bereitstellungen

Migrieren Sie eine lokale Oracle-Datenbank zu Oracle auf Amazon EC2

Erstellt von Baji Shaik (AWS) und Pankaj Choudhary (AWS)

Übersicht

Dieses Muster führt Sie durch die Schritte zur Migration einer lokalen Oracle-Datenbank zu Oracle auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance. Es beschreibt zwei Optionen für die Migration: die Verwendung von AWS Data Migration Service (AWS DMS) oder die Verwendung nativer Oracle-Tools wie RMAN, Data Pump Import/Export, transportable Tablespaces und Oracle. GoldenGate

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle-Quelldatenbank in einem lokalen Rechenzentrum

Einschränkungen

- Das Zielbetriebssystem (OS) muss von Amazon unterstützt werden EC2. Eine vollständige Liste der unterstützten Systeme finden Sie bei Amazon EC2 FAQs.

Produktversionen

- Oracle-Versionen 10.2 und höher (für Versionen 10.x), 11g und bis zu 12.2 und 18c für die Editionen Enterprise, Standard, Standard One und Standard Two. Die aktuelle Liste der von AWS DMS unterstützten Versionen finden Sie unter „Lokale Datenbanken und EC2 Amazon-Instanzdatenbanken“ unter Quellen für die Datenmigration in der AWS DMS-Dokumentation.

Architektur

Quelltechnologie-Stack

- Eine lokale Oracle-Datenbank

Zieltechnologie-Stack

- Eine Oracle-Datenbank-Instance auf Amazon EC2

Zielarchitektur

Architektur der Datenmigration

Verwenden von AWS DMS:

Verwendung nativer Oracle-Tools:

Tools

- AWS DMS — AWS Database Migration Services (AWS DMS) unterstützt verschiedene Arten von Quell- und Zieldatenbanken. Informationen zu den unterstützten Datenbankversionen und -editionen finden Sie unter Using an Oracle Database as a Source for AWS DMS. Wir empfehlen Ihnen, die neueste Version von AWS DMS zu verwenden, um die umfassendste Version von Versionen und Funktionen zu erhalten.
- Systemeigene Oracle-Tools — RMAN, Data Pump-Import/Export, transportable Tablespaces, Oracle GoldenGate

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Versionen der Quell- und Zieldaten banken.		DBA
Identifizieren Sie die Version des Zielbetriebssystems.		DBA, SysAdmin
Identifizieren Sie die Hardwareanforderungen für die Zielserverinstanz auf		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
der Grundlage der Oracle-Kompatibilitätsliste und der Kapazitätsanforderungen.		
Identifizieren Sie die Speicheranforderungen (Speichertyp und Kapazität).		DBA, SysAdmin
Identifizieren Sie die Netzwerkanforderungen (Latenz und Bandbreite).		DBA, SysAdmin
Wählen Sie den richtigen Instanztyp auf der Grundlage von Kapazität, Speicherf unktionen und Netzwerkf unktionen aus.		DBA, SysAdmin
Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerk-/Hostzugriff für Quell- und Zieldatenbanken.		DBA, SysAdmin
Identifizieren Sie eine Liste der Betriebssystembenutzer, die für die Oracle-Softwareins tallation erforderlich sind.		DBA, SysAdmin
Laden Sie das AWS Schema Conversion Tool (AWS SCT) und die Treiber herunter.		DBA
Erstellen Sie ein AWS SCT-Projekt für den Workload und stellen Sie eine Verbindung zur Quelldatenbank her.		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie SQL-Dateien für die Erstellung von Objekten (Tabellen, Indizes, Sequenzen usw.).		DBA
Legen Sie eine Backup-St rategie fest.		DBA, SysAdmin
Ermitteln Sie die Verfügbar keitsanforderungen.		DBA
Identifizieren Sie die Strategie zur Anwendungsmigration/ Umstellung.		DBA, Besitzer der App SysAdmin

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Virtual Private Cloud (VPC) und Subnetze in Ihrem AWS-Konto .		SysAdmin
Erstellen Sie Sicherhei tsgruppen und Netzwerkz ugriffskontrolllisten ()ACLs.		SysAdmin
Konfigurieren und starten Sie die EC2 Instanz.		SysAdmin

Installieren Sie die Oracle-Software

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Betriebss ystembenutzer und -gruppen, die für die Oracle-Software erforderlich sind.		DBA, SysAdmin
Laden Sie die erforderliche Version der Oracle-Software herunter.		
Installieren Sie die Oracle-So ftware auf der EC2 Instanz.		DBA, SysAdmin
Erstellen Sie Objekte wie Tabellen, Primärschlüssel, Ansichten und Sequenzen mithilfe der von AWS SCT generierten Skripts.		DBA

Daten migrieren — Option 1

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie native Oracle-Tools oder Tools von Drittanbi etern, um Datenbankobjekte und Daten zu migrieren.	Zu den Oracle-Tools gehören der Import/Export von Data Pump, RMAN, transportable Tablespaces und. GoldenGate	DBA

Daten migrieren — Option 2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie die Migration smethode.		DBA
Erstellen Sie eine Replikati onsinstanz in der AWS DMS-Konsole.		DBA
Erstellen Sie Quell- und Zielendpunkte.		DBA
Erstellen Sie eine Replikati onsaufgabe.		DBA
Aktivieren Sie Change Data Capture (CDC), um Änderungen für eine kontinuie rliche Replikation zu erfassen.		DBA
Führen Sie die Replikati onsaufgabe aus und überwachen Sie die Protokoll e.		DBA
Erstellen Sie sekundäre Objekte wie Indizes und Fremdschlüssel, wenn der vollständige Ladevorgang abgeschlossen ist.		DBA

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Anwendungsmigration.		DBA SysAdmin, Besitzer der App

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Umstellung und Umstellung der Anwendung.		DBA, Besitzer der App SysAdmin

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre AWS Secrets Manager Manager-R essourcen herunter.		DBA, SysAdmin
Überprüfen und validieren Sie die Projektdokumente.		DBA SysAdmin, Besitzer der App
Erfassen Sie Kennzahlen zum Zeitpunkt der Migration, zum prozentualen Anteil manueller Daten im Vergleich zum Tool, zu Kosteneinsparungen usw.		DBA SysAdmin, Besitzer der App
Schließen Sie das Projekt ab und geben Sie Feedback.		

Zugehörige Ressourcen

Referenzen

- Strategien für die Migration von Oracle-Datenbanken zu AWS
- Migration von Oracle-Datenbanken in die AWS-Cloud
- EC2 Amazon-Webseite
- AWS DMS-Webseite
- AWS DMS-Blogbeiträge
- EC2 Amazon-Preisgestaltung
- Lizenzierung von Oracle-Software in der Cloud-Computing-Umgebung

Tutorials und Videos

- Erste Schritte mit Amazon EC2
- Erste Schritte mit AWS DMS
- Einführung in Amazon EC2 — Elastic Cloud Server und Hosting mit AWS (Video)

Migrieren Sie eine lokale Oracle-Datenbank mithilfe EC2 von Oracle Data Pump zu Amazon

Erstellt von Navakanth Talluri (AWS)

Übersicht

Bei der Migration von Datenbanken müssen Sie Faktoren wie die Quell- und Zieldatenbank-Engines und Versionen, Migrationstools und -services sowie akzeptable Ausfallzeiten berücksichtigen. Wenn Sie eine lokale Oracle-Datenbank zu Amazon Elastic Compute Cloud (Amazon EC2) migrieren, können Sie Oracle-Tools wie Oracle Data Pump und Oracle Recovery Manager (RMAN) verwenden. Weitere Informationen zu Strategien finden Sie unter Migration von Oracle-Datenbanken in die AWS-Cloud.

Oracle Data Pump hilft Ihnen dabei, die logische, konsistente Sicherung der Datenbank zu extrahieren und sie auf der EC2 Zielinstanz wiederherzustellen. Dieses Muster beschreibt, wie eine lokale Oracle-Datenbank mithilfe von Oracle Data Pump und dem `NETWORK_LINK` Parameter mit minimaler Ausfallzeit auf eine EC2 Instanz migriert wird. Der `NETWORK_LINK` Parameter startet einen Import über einen Datenbank-Link. Der Oracle Data Pump Import (impdp) -Client auf der EC2 Zielinstanz stellt eine Verbindung zur Quelldatenbank her, ruft Daten von dieser ab und schreibt die Daten direkt in die Datenbank auf der Zielinstanz. In dieser Lösung werden keine Backup- oder Dump-Dateien verwendet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine lokale Oracle-Datenbank, die:
  - Ist keine Oracle Real Application Clusters (RAC) -Datenbank
  - Ist keine Oracle Automatic Storage Management (Oracle ASM) -Datenbank
  - Befindet sich im Lese-/Schreibmodus.
- Sie haben einen AWS Direct Connect Connect-Link zwischen Ihrem lokalen Rechenzentrum und AWS erstellt. Weitere Informationen finden Sie unter Verbindung erstellen (Direct Connect-Dokumentation).

Produktversionen

- Oracle Database 10g Version 1 (10.1) und höher

Architektur

Quelltechnologie-Stack

- Ein eigenständiger Oracle-Datenbankserver (ohne RAC und ohne ASM) in einem lokalen Rechenzentrum

Zieltechnologie-Stack

- Eine Oracle-Datenbank, die auf Amazon läuft EC2

Zielarchitektur

Die Zuverlässigkeitssäule des AWS Well-Architected Framework empfiehlt die Erstellung von Datensicherungen, um eine hohe Verfügbarkeit und Ausfallsicherheit zu gewährleisten. Weitere Informationen finden Sie unter Architecting for High Availability in Best Practices for Running Oracle Database on AWS. Dieses Muster richtet mithilfe von Oracle Active Data Guard Primär- und Standby-Datenbanken auf EC2 Instances ein. Für eine hohe Verfügbarkeit sollten sich die EC2 Instances in verschiedenen Availability Zones befinden. Die Availability Zones können sich jedoch in derselben AWS-Region oder in verschiedenen AWS-Regionen befinden.

Active Data Guard bietet schreibgeschützten Zugriff auf eine physische Standby-Datenbank und wendet fortlaufend Redo-Änderungen von der Primärdatenbank aus an. Basierend auf Ihrem Recovery Point Objective (RPO) und Recovery Time Objective (RTO) können Sie zwischen synchronen und asynchronen Redo-Transport-Optionen wählen.

Die folgende Abbildung zeigt die Zielarchitektur, wenn sich die Primär- und EC2 Standby-Instances in unterschiedlichen AWS-Regionen befinden.

Architektur der Datenmigration

Nachdem Sie die Zielarchitektur eingerichtet haben, verwenden Sie Oracle Data Pump, um die lokalen Daten und Schemas auf die primäre EC2 Instanz zu migrieren. Während der Umstellung können Anwendungen nicht auf die lokale Datenbank oder die Zieldatenbank zugreifen. Sie fahren diese Anwendungen herunter, bis sie mit der neuen Zieldatenbank auf der primären EC2 Instanz verbunden werden können.

Die folgende Abbildung zeigt die Architektur während der Datenmigration. In dieser Beispielarchitektur befinden sich die Primär- und EC2 Standby-Instances in verschiedenen AWS-Regionen.

Tools

AWS-Services

- AWS Direct Connect verbindet Ihr internes Netzwerk über ein Standard-Ethernet-Glasfaserkabel mit einem Direct Connect-Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt zu öffentlichen AWS-Services erstellen und dabei Internetdienstanbieter in Ihrem Netzwerkpfad umgehen.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.

Andere Tools und Dienste

- Oracle Active Data Guard unterstützt Sie bei der Erstellung, Wartung, Verwaltung und Überwachung von Standby-Datenbanken.
- Oracle Data Pump hilft Ihnen, Daten und Metadaten mit hoher Geschwindigkeit von einer Datenbank in eine andere zu verschieben.

Bewährte Methoden

- Bewährte Methoden für die Ausführung von Oracle Database in AWS
- Daten mit NETWORK_LINK importieren

Epen

Richten Sie die EC2 Instanzen auf AWS ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Quellhard warekonfiguration für den	Überprüfen Sie die lokale Konfiguration, einschließlich	DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
lokalen Host und die Kernel-Parameter.	Speichergröße, Eingabe-/Ausgabeoperationen pro Sekunde (IOPS) und CPU. Dies ist wichtig für die Oracle-Lizenzierung, die auf CPU-Kernen basiert.	
Erstellen Sie die Infrastruktur auf AWS.	Erstellen Sie die virtuelle n privaten Clouds (VPCs), privaten Subnetze, Sicherhei tsgruppen, Netzwerkzugriffsko ntrolllisten (ACLs), Routing-Tabellen und das Internet-Gateway. Weitere Informati onen finden Sie hier: • VPCs und Subnetze • Tutorial: Eine VPC für die Verwendung mit einer Datenbank-Instance erstellen	DBA, AWS-Systemadminist rator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die EC2 Instanzen mithilfe von Active Data Guard ein.	Konfigurieren Sie EC2 AWS-Instanzen mithilfe einer Active Data Guard-Konfiguration, wie im AWS Well-Architected Framework beschrieben. Die Version von Oracle Database auf der EC2 Instance kann sich von der lokalen Version unterscheiden, da dieses Muster logische Backups verwendet. Beachten Sie Folgendes: • Versetzen Sie die Zieldaten bank in den Lese-/Sch reibmodus. • Geben Sie in der Zieldaten bank die TNS-Details (Transparent Network Substrate) für die Quelldate nbank an. Weitere Informationen finden Sie unter: • Eine Datenbank starten (Oracle-Dokumentation) • Eine Oracle-Datenbank erstellen und konfigurieren (Oracle-Dokumentation)	DBA, AWS-Systemadminist rator

Migrieren Sie die Datenbank zu Amazon EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie von der Instanz aus einen DBLink zur lokalen Datenbank. EC2	Erstellen Sie einen Datenbank -Link (dblink) zwischen der Oracle-Datenbank auf der EC2 Instanz und der lokalen Oracle-Datenbank. Weitere Informationen finden Sie unter Verwenden des Netzwerk-Link-Imports zum Verschieb en von Daten (Oracle-D okumentation).	DBA
Überprüfen Sie die Verbindun g zwischen der EC2 Instanz und dem lokalen Host.	Verwenden Sie den DBlink, um zu überprüfen, ob die Verbindung zwischen der EC2 Instanz und der lokalen Datenbank funktioniert. Anweisungen finden Sie unter CREATE DATABASE LINK (Oracle-Dokumentation).	DBA
Beenden Sie alle Anwendung en, die mit der lokalen Datenbank verbunden sind.	Nachdem die Datenbank ausfallzeit genehmigt wurde, fahren Sie alle Anwendung en und abhängigen Jobs herunter, die eine Verbindun g zu Ihrer lokalen Datenbank herstellen. Sie können dies entweder direkt von der Anwendung aus oder mithilfe von Cron aus der Datenbank tun. Weitere Informationen finden Sie unter Verwenden des Crontab-Dienstprogramms	DBA, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zur Planung von Aufgaben unter Oracle Linux.	
Planen Sie den Datenmigrationsjob.	Verwenden Sie auf dem Zielhost den Befehl, `impdb` um den Data Pump-Import zu planen. Dadurch wird die Zieldatenbank mit dem lokalen Host verbunden und die Datenmigration gestartet. Weitere Informationen finden Sie unter Data Pump Import und NETWORK_LINK (Oracle-Dokumentation).	DBA
Validieren Sie die Datenmigration.	Die Datenvalidierung ist ein entscheidender Schritt. Für die Datenvalidierung können Sie benutzerdefinierte Tools oder Oracle-Tools verwenden, z. B. eine Kombination aus DBLink- und SQL-Abfragen.	DBA

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Versetzen Sie die Quelldatenbank in den schreibgeschützten Modus.	Vergewissern Sie sich, dass die Anwendung heruntergefahren ist und keine Änderungen an der Quelldatenbank vorgenommen wurden. Öffnen Sie die Quelldatenbank im schreibgeschützten Modus. Auf diese Weise können	DBA, DevOps Ingenieur, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie offene Transaktionen vermeiden. Weitere Informationen finden Sie unter `ALTER DATABASE` SQL-Anweisungen (Oracle-Dokumentation).	
Überprüfen Sie die Objektanzahl und die Daten.	Verwenden Sie benutzerdefinierte Tools oder Oracle-Tools, z. B. eine Kombination aus DBLink- und SQL-Abfragen, um die Daten und das Objekt zu validieren.	DBA, App-Entwickler
Connect die Anwendungen mit der Datenbank auf der primären EC2 Instanz.	Ändern Sie das Verbindungsattribut der Anwendung so, dass es auf die neue Datenbank verweist, die Sie auf der primären EC2 Instanz erstellt haben.	DBA, App-Entwickler
Überprüfen Sie die Anwendungsleistung.	Starten Sie die Anwendung. Überprüfen Sie die Funktionalität und Leistung der Anwendung mithilfe von Automated Workload Repository (Oracle-Dokumentation).	App-Entwickler, DevOps Ingenieur, DBA

Zugehörige Ressourcen

AWS-Referenzen

- Migration von Oracle-Datenbanken in die AWS-Cloud
- Amazon EC2 für Oracle
- Migration umfangreicher Oracle-Datenbanken zu AWS für plattformübergreifende Umgebungen

- VPCs und Subnetze
- Tutorial: Eine VPC für die Verwendung mit einer Datenbank-Instance erstellen

Oracle-Referenzen

- Oracle Data Guard-Konfigurationen
- Import von Datenpumpen

Migrieren Sie RHEL-BYOL-Systeme mithilfe von AWS MGN zu Instances mit AWS-Lizenz

Erstellt von Mike Kuznetsov (AWS)

Übersicht

Wenn Sie Ihre Workloads mithilfe von AWS Application Migration Service (AWS MGN) zu AWS migrieren, müssen Sie möglicherweise Ihre Red Hat Enterprise Linux (RHEL) -Instances hochziehen (rehosten) und die Lizenz während der Migration vom Standardmodell Bring Your Own License (BYOL) auf ein AWS-Lizenzmodell (LI) ändern. AWS MGN unterstützt einen skalierbaren Ansatz, der Amazon Machine Image (AMI) IDs verwendet. Dieses Muster beschreibt, wie die Lizenzänderung auf RHEL-Servern während der Rehost-Migration in großem Umfang durchgeführt werden kann. Außerdem wird erklärt, wie Sie die Lizenz für ein RHEL-System ändern können, das bereits auf Amazon Elastic Compute Cloud (Amazon EC2) läuft.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zugriff auf das AWS-Zielkonto
- AWS MGN wurde im AWS-Zielkonto und in der Region für die Migration initialisiert (nicht erforderlich, wenn Sie bereits von Ihrem lokalen System zu AWS migriert haben)
- Ein RHEL-Quellserver mit einer gültigen RHEL-Lizenz

Architektur

Dieses Muster deckt zwei Szenarien ab:

- Migrieren Sie ein System mithilfe von AWS MGN direkt von einem lokalen System in eine AWS LI-Instance. Folgen Sie für dieses Szenario den Anweisungen im ersten Epic (Migration zur LI-Instance — Option 1) und im dritten Epic.
- Änderung des Lizenzmodells von BYOL auf LI für ein zuvor migriertes RHEL-System, das bereits auf Amazon läuft. EC2 Folgen Sie für dieses Szenario den Anweisungen im zweiten Epic (Migration zur LI-Instance — Option 2) und im dritten Epic.

> **Note**
>
> Das dritte Epic beinhaltet die Neukonfiguration der neuen RHEL-Instance für die Nutzung der von AWS bereitgestellten Red Hat Update Infrastructure (RHUI) -Server. Dieser Prozess ist für beide Szenarien derselbe.

Tools

AWS-Services

- Mit dem AWS Application Migration Service (AWS MGN) können Sie Anwendungen ohne Änderungen und mit minimalen Ausfallzeiten in die AWS-Cloud rehosten (Lift and Shift).

Epen

Zur LI-Instanz migrieren — Option 1 (für ein lokales RHEL-System)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Suchen Sie die AMI-ID der RHEL AWS LI-Instance in der Zielregion.	Besuchen Sie AWS Marketplace oder verwenden Sie die EC2 Amazon-Konsole, um die RHEL-AMI-ID zu finden, die der Version des RHEL-Quellsystems entspricht (z. B. RHEL-7.7), und notieren Sie sich die AMI-ID. Auf der EC2 Amazon-Konsole können Sie AMIs nach einem der folgenden Suchbegriffe filtern: • Beschreibung = Bereitgestellt von Red Hat, Inc. • AMI-Name = RHEL-7.7	Cloud-Administrator
Konfigurieren Sie die AWS MGN-Starteinstellungen.	1. Fügen Sie auf der AWS MGN-Konsole das RHEL-	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Quellsystem hinzu: Installieren Sie den AWS Replication Agent und fügen Sie den Quellserver hinzu, indem Sie den Anweisungen in der AWS MGN-Dokumentation folgen. 2. Wählen Sie auf der Seite Quellserver das RHEL-Quellsystem und dann die Registerkarte Starteinstellungen aus. 3. Wählen Sie im Abschnitt Allgemeine Starteinstellungen die Option Bearbeiten aus. Um die automatische Auswahl zu deaktivieren und den Zielinstanztyp manuell anzugeben, ändern Sie die Größe des Instanztyps auf Keine und wählen Sie dann Einstellungen speichern. Auf diese Weise können Sie den Instance-Typ verwenden, den Sie in Ihrer EC2 Amazon-Startvorlage konfigurieren. Weitere Informationen finden Sie in der AWS MGN-Dokumentation. 4. Wählen EC2 Sie im Abschnitt Launch Template die Option Modify aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wählen Sie im Dialogfeld „Informationen zum Ändern von EC2 Startvorlagen“ erneut die Option Ändern aus. Dadurch wird die EC2 Amazon-Konsole geöffnet, sodass Sie die Vorlage für diese Instance ändern können. 5. Lesen Sie die wichtigsten Überlegungen in der AWS MGN-Dokumentation. **Note** Sie können die Warnung vor der Wahl Ihres eigenen AMI ignorieren. 6. Ändern Sie auf der EC2 Amazon-Konsole in der neuen Startvorlage Folgendes: • Geben Sie für AMI die AMI-ID an, die Sie zuvor identifiziert haben, oder suchen Sie nach RHEL- x und geben Sie die Version an, die Sie benötigen (z. B. RHEL-7.7). • Stellen Sie unter Instance-Typ den	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	gewünschten Ziel-Instance-Typ ein. • Lassen Sie die folgenden Abschnitte unverändert: Schlüsselpaar (Anmeldung), Netzwerkeinstellungen (sofern Sie kein Zielsubnetz und Sicherheitsgruppen angeben möchten), Speicher, Ressourcen-Tags (sofern Sie keine Tags hinzufügen oder ändern möchten). • (Optional) Geben Sie im Abschnitt Erweiterte Details die Rolle des IAM-Instance-Profils an, falls dies für die future Verwaltung durch AWS Systems Manager erforderlich ist. 7. Wählen Sie Vorlagenversion erstellen und wählen Sie dann den Link in der Erfolgsmeldung, um die Startvorlage anzuzeigen. 8. Wählen Sie „Aktionen“, „Standardversion festlegen“. Wählen Sie unter Vorlagenversion die neueste Version aus (Version 2 für ein neues System) und wählen Sie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dann Als Standardversion festlegen aus. AWS MGN wird nun diese Version der Startvorlage verwenden, um Test- oder Cutover-Instances zu starten. Weitere Informationen finden Sie in der AWS MGN-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Einstellungen.	1. Wählen Sie in der AWS MGN-Konsole auf der Seite Quellserver Ihren Quellserver und dann die Registerkarte Starteinstellungen aus. 2. Vergewissern Sie sich im Abschnitt EC2 Launch Template, dass die Parameter Instance-Typ, Subnetz und Sicherheitsgruppen korrekt eingestellt sind. **Note** In diesem Abschnitt wird die von Ihnen ausgewählte AMI-ID nicht angezeigt. Um die ID zu sehen, können Sie die EC2 Amazon-Konsole in der Ansicht Vorlagen starten öffnen und nach der Vorlagen-ID suchen, die in diesem Abschnitt angezeigt wird.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die neue LI-Instanz.	1. Wenn die erste Synchronisierung abgeschlossen ist, ändert sich die Spalte Migrationslebenszyklus für den Server auf der Seite Quellserver der AWS-MGN-Konsole in Bereit zum Testen. Um die neue Test-Instance zu starten, wählen Sie Ihren Quellserver aus, öffnen Sie das Menü Test und Übernahme und wählen Sie dann Test-Instances starten. Wählen Sie Jobdetails anzeigen, um den Status des Startjobs zu überwachen. Weitere Informationen finden Sie in der AWS MGN-Dokumentation. 2. Warten Sie, bis der Startjob abgeschlossen ist, und öffnen Sie dann die Seite mit den Details der gestarteten EC2 Instance. Wählen Sie den Tab Details und vergewissern Sie sich, dass der Abschnitt mit den Instanzdetails Folgendes enthält: • Plattformdetails: „Red Hat Enterprise Linux“ • AMI-Name: Der Name des AMI, das Sie in	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der EC2 Startvorlage angegeben haben 3. Wechseln Sie zur neuen LI-Instance, indem Sie den Anweisungen in der AWS MGN-Dokumentation folgen. 4. Konfigurieren Sie die neue Instanz neu, um die von AWS bereitgestellten RHUI-Server zu verwenden, indem Sie die Schritte im letzten Epic befolgen.	

Zur LI-Instanz migrieren — Option 2 (für eine EC2 RHEL-BYOL-Instanz)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie Ihre RHEL EC2 BYOL-Instance zu einer AWS LI-Instance.	Sie können RHEL-Systeme, die Sie zuvor als BYOL zu AWS migriert haben, zu AWS LI-Instances wechseln, indem Sie ihre Festplatten (Amazon Elastic Block Store-Volumes) verschieben und sie an eine neue LI-Instance anhängen. Gehen Sie wie folgt vor, um diesen Wechsel vorzunehmen: 1. Starten Sie eine neue RHEL-Zielinstanz von einem RHEL LI AMI aus. Vergewissern Sie sich, dass	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	das von Ihnen gewählte AMI: • Verwendet dieselbe RHEL-Version wie Ihre aktuelle RHEL-Instance. • Hat denselben Startvorg ang (BIOS oder UEFI) wie Ihre aktuelle RHEL-Instanz. Wenn der Quellserver beispiels weise BIOS-basiert ist, verwenden Sie das AWS Marketplace RHEL AMI, das ebenfalls BIOS-basi ert ist. Wählen Sie für UEFI-basierte Systeme das UEFI-basierte AMI. 2. Stoppen Sie beide Instances: die neue LI-Instance und die ursprüngl iche Quell-Instance. 3. Trennen Sie alle EBS-Volumes (einschließlich der Root-Festplatte) von der neuen LI-Instanz und löschen Sie sie. 4. Trennen Sie alle EBS-Volumes (einschließlich der Root-Festplatte) von der alten Quell-Instance und fügen Sie sie der neuen LI-Instance hinzu. Behalten Sie die gleiche Zuordnung von Volumes zu Geräten	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bei. (Beispielsweise muss das EBS-Volume, das zuvor an das `/dev/sda` Laufwerk angeschlossen war, genauso wie das EBS-Volume `/dev/sda` an die neue Instanz angehängt werden.) 5. Löschen Sie die Quellinst anz (jetzt ohne Festplatte). 6. Starten Sie die neue LI-Instanz. Melden Sie sich bei der Instance an und konfigurieren Sie sie neu, um die von AWS bereitges tellten RHUI-Server zu verwenden, indem Sie die Schritte im nächsten Epic befolgen.	

Neukonfiguration von RHEL OS zur Verwendung von AWS-bereitgestelltem RHUI — beide Optionen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie das Betriebss ystem vom Red Hat Abonnement und der Lizenz ab.	Nach der Migration und der erfolgreichen Umstellung muss das RHEL-System aus dem Red Hat-Abonnement entfernt werden, um den Verbrauch der Red Hat-Lizen z zu beenden und Doppelabr echnungen zu vermeiden.	Linux oder Systemadm inistrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Um RHEL OS aus dem Red Hat-Abonnement zu entfernen, folgen Sie dem in der Dokumentation zu Red Hat Subscription Management (RHSM) beschriebenen Prozess. Verwendung des -CLI-Befehls: `subscription-manager unregister` Sie können das Subscription Manager-Plugin auch deaktivieren, um den Status des Abonnements nicht mehr bei jedem Yum-Anruf zu überprüfen. Bearbeiten Sie dazu die Konfigurationsdatei `/etc/yum/pluginconf.d/subscription-manager.conf` und ändern Sie den Parameter `enabled=1` auf `enabled=0`.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ersetzen Sie die alte Update-Konfiguration (RHUI, Red Hat Satellite Network, Yum-Repositorys) durch das von AWS bereitgestellte RHUI.	Sie müssen das migrierte RHEL-System neu konfigurieren, um die von AWS bereitgestellten RHUI-Server zu verwenden. Dadurch erhalten Sie Zugriff auf die RHUI-Server innerhalb der AWS-Regionen, ohne dass eine externe Update-Infrastruktur erforderlich ist. Die Änderung umfasst den folgenden Prozess: 1. Erstellen Sie eine Sicherungskopie der vorhandenen Yum-Konfiguration. 2. Entfernen Sie die alte RHUI-Konfiguration (Yum-Repositories) und die alten Pakete. 3. Fügen Sie die neuen von AWS bereitgestellten RHUI-Konfiguration und die Zertifikatspakete hinzu. Sie müssen diese von einer anderen RHEL-Instance auf AWS abrufen, da diese Konfigurationspakete nur auf von AWS bereitgestellten RHUI-Servern verfügbar sind.	Linux oder Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Hier sind die detaillierten Schritte und Befehle:
	
	1. Sichern Sie die bestehende Yum-Konfiguration und die Zertifikate, indem Sie alle `/etc/pki/*` Ordner `/etc/yum*` und an einen Backup-Speicherort kopieren. Zum Beispiel:
	
	`mkdir yum-backup`
	`cp -ra /etc/yum* /etc/pki ./yum-backup`
	`tar czf yum-backup.tgz ./yum-backup`
	
	2. Entfernen Sie die alte RHUI-Konfiguration und die Pakete:
	
	a. Finden Sie alle installierten RHUI-Pakete:
	
	`sudo rpm -qa | grep rhui`
	
	b. Löschen Sie diese Pakete:
	
	`sudo yum remove $(rpm -qa | grep rhui)`
	
	c. Entfernen Sie die `/etc/yum/vars/releasever` Datei, falls sie existiert.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Fügen Sie die neuen von AWS bereitgestellten RHUI- und Zertifikatspakete hinzu. Sie müssen diese von einer anderen RHEL-Instance auf AWS abrufen. Dazu stehen verschiedene Möglichke iten zur Verfügung. Sie können beispielsweise den Anweisungen im Red Hat Knowledgebase-Artikel folgen: a. Starten Sie eine weitere RHEL-Instance (RHEL-EC2) vom AWS Marketplace aus. b. Laden Sie zwei Pakete von dieser Instance herunter: das neueste RHUI-Client-Konfig urationspaket und die Zertifikate der Zertifizi erungsstelle (CA). Führen Sie beispiels weise diesen Befehl von Ihrem Desktop aus aus: `ssh RHEL-EC2 "sudo yumdownloader ca-certificates rh-amazon-rhui-client"` c. Kopieren Sie die Pakete von der EC2 RHEL-Instanz auf das neue	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	migrierte System. Zum Beispiel:
	`scp RHEL-EC2:rh-amazon-rhui-client\* RHEL-EC2:ca-certificates\* . ssh <migrated-instance> "mkdir /tmp/amazon" scp rh-amazon-rhui-client* ca-certificates* <migrated-instance>:/tmp/amazon`
	d. Installieren Sie die neuen RHUI- und CA-Konfigurationspakete auf der migrierten Instanz:
	`ssh <migrated-instance> "sudo rpm -Uhv /tmp/amazon/*"`	

Überprüfen Sie die Konfiguration.	Stellen Sie auf der migrierten Zielinstanz sicher, dass die neue Konfiguration korrekt ist: `sudo yum clean all sudo yum repolist`	Linux oder Systemadministrator

Zugehörige Ressourcen

- Benutzerhandbuch für den AWS Application Migration Service (AWS MGN)

- Holen Sie sich ein unterstützendes AWS-RHUI-Clientpaket IMDSv2 (Artikel in der Red Hat Knowledgebase)
- Vorlagen für die EC2 Markteinführung von Amazon (EC2 Amazon-Dokumentation)

Migrieren Sie eine lokale SAP ASE-Datenbank zu Amazon EC2

Erstellt von Sergey Dmitriev (AWS) und Gergely Cserdi (AWS)

Übersicht

Dieses Muster beschreibt, wie eine SAP Adaptive Server Enterprise (ASE) -Datenbank von einem lokalen Host zu einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance migriert wird. Das Muster deckt die Verwendung von AWS Database Migration Service (AWS DMS) oder nativen SAP ASE-Tools wie ASE Cockpit, Sybase Central for ASE und DBA Cockpit für die Migration ab.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine SAP ASE-Quelldatenbank in einem lokalen Rechenzentrum

-Einschränkungen

- Die Quelldatenbank muss weniger als 64 TB groß sein

Produktversionen

- SAP ASE Version 15.x und 16.x oder höher

Architektur

Quelltechnologie-Stack

- Lokale SAP ASE-Datenbank

Zieltechnologie-Stack

- SAP ASE-Datenbank auf einer EC2 Instanz

Architektur der Datenbankmigration

Verwenden von AWS DMS:

Verwendung nativer SAP ASE-Tools:

Tools

- AWS DMS — AWS Data Migration Service (AWS DMS) unterstützt mehrere verschiedene Quell- und Zieldatenbanken. Weitere Informationen finden Sie unter Quellen für die Datenmigration und Ziele für die Datenmigration. Wir empfehlen Ihnen, die neueste Version von AWS DMS zu verwenden, um die umfassendste Version von Versionen und Funktionen zu erhalten.
- SAP ASE — Zu den systemeigenen Tools gehören ASE Cockpit, Sybase Central für ASE und DBA Cockpit.

Epen

Analysieren Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversionen.		DBA
Identifizieren Sie die Zielversion des Betriebssystems.		DBA, SysAdmin
Identifizieren Sie die Hardwareanforderungen für die Zielserverinstanz auf der Grundlage der SAP ASE-Kompatibilitätsliste und der Kapazitätsanforderungen.		DBA, SysAdmin
Identifizieren Sie die Anforderungen für den Speichertyp und die Kapazität.		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Netzwerkanforderungen, einschließlich Latenz und Bandbreite.		DBA, SysAdmin
Wählen Sie den richtigen Instanztyp, die Kapazität, die Speicherfunktionen und die Netzwerkfunktionen aus.		DBA, SysAdmin
Identifizieren Sie die Netzwerk- und Hostzugri ffssicherheitsanforderungen für die Quell- und Zieldaten banken.		DBA, SysAdmin
Identifizieren Sie eine Liste der Betriebssystembenutzer, die für die SAP ASE-Softw areinstallation erforderlich sind.		DBA, SysAdmin
Bestimmen Sie die Backup-St rategie.		DBA
Ermitteln Sie die Verfügbar keitsanforderungen.		DBA
Identifizieren Sie die Strategie für Anwendungsmigration und Switchover.		DBA, Besitzer der SysAdmin App

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine virtuelle private Cloud (VPC) und Subnetze.		SysAdmin
Erstellen Sie Sicherhei tsgruppen und die Network Access Control List (ACL).		SysAdmin
Konfigurieren und starten Sie die EC2 Instanz.		SysAdmin

Installieren Sie die Software

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Betriebss ystembenutzer und -gruppen, die für das Funktionieren der SAP ASE-Software erforderl ich sind.		DBA, SysAdmin
Laden Sie die erforderliche Version der SAP ASE-Softw are herunter.		DBA, SysAdmin
Installieren Sie die SAP ASE-Datenbank, die Backup-Se rver-Software und die Replikati onsserversoftware auf der EC2 Instanz und konfigurieren Sie dann den Server.		DBA, SysAdmin

Migrieren Sie die Daten — Option 1

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie die Datenbank objekte und Daten mithilfe systemeigener SAP ASE-Tools oder Tools von Drittanbietern.	Informationen zu SAP ASE oder Tools von Drittanbietern finden Sie in der Dokumentation. Dazu gehören ASE Cockpit, Sybase Central für ASE und DBA Cockpit.	DBA

Migrieren Sie die Daten — Option 2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie die Daten mithilfe von AWS DMS.		DBA

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Anwendungsmigration.		DBA SysAdmin, Besitzer der App

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Umstellung oder Umstellung der Anwendung.		DBA, Besitzer der App SysAdmin

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die temporären AWS-Ressourcen herunter.		DBA, SysAdmin
Validieren und überprüfen Sie die Projektdokumente.		DBA SysAdmin, Besitzer der App
Erfassen Sie Kennzahlen zum Zeitpunkt der Migration, zu den prozentualen Einsparungen bei den manuellen Kosten im Vergleich zu den Werkzeugkosten usw.		DBA SysAdmin, Besitzer der App
Schließen Sie das Projekt und geben Sie Feedback.		DBA SysAdmin, Besitzer der App

Zugehörige Ressourcen

Referenzen

- Amazon EC2
- AWS DMS
- EC2 Amazon-Preisgestaltung

Tutorials und Videos

- Erste Schritte mit Amazon EC2
- Erste Schritte mit dem AWS Database Migration Service
- AWS-Datenmigrationsservice (Video)
- Einführung in Amazon EC2 — Elastic Cloud Server und Hosting mit AWS (Video)

Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Amazon EC2

Erstellt von Senthil Ramasamy (AWS)

Übersicht

Dieses Muster beschreibt, wie eine lokale Microsoft SQL Server-Datenbank auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance zu Microsoft SQL Server migriert wird. Es behandelt zwei Optionen für die Migration: die Verwendung von AWS Database Migration Service (AWS DMS) oder die Verwendung systemeigener Microsoft SQL Server-Tools wie Backup und Wiederherstellung, Assistent zum Kopieren von Datenbanken oder Kopieren und Anfügen von Datenbanken.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS Konto
- Ein von Amazon unterstütztes Betriebssystem EC2 (eine vollständige Liste der unterstützten Betriebssystemversionen finden Sie unter Amazon EC2 FAQs)
- Eine Microsoft SQL Server-Quelldatenbank in einem lokalen Rechenzentrum

Produktversionen

- AWS DMS Unterstützt für lokale Datenbanken und EC2 Amazon-Instance-Datenbanken:
  - SQL Server-Versionen 2005, 2008, 2008R2, 2012, 2014, 2016, 2017 und 2019
  - Enterprise-, Standard-, Workgroup-, Developer- und Web-Editionen
- Die aktuelle Liste der unterstützten Versionen finden Sie unter Using a Microsoft SQL Server Database as a Target for AWS DMS.

Architektur

Quelltechnologie-Stack

- Lokale Microsoft SQL Server-Datenbank

Zieltechnologie-Stack

- Microsoft SQL Server-Datenbank auf einer EC2 Instanz

Zielarchitektur

Architektur der Datenmigration

- Verwenden AWS DMS

- Verwendung systemeigener SQL Server-Tools

Tools

- AWS Database Migration Service (AWS DMS) hilft Ihnen bei der Migration Ihrer Daten zu und von weit verbreiteten kommerziellen und Open-Source-Datenbanken wie Oracle, SQL Server, MySQL und PostgreSQL. Sie können AWS DMS es verwenden, um Ihre Daten in die AWS Cloud, zwischen lokalen Instanzen (über ein AWS Cloud Setup) oder zwischen Kombinationen von Cloud- und lokalen Setups zu migrieren.
- AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist.
- Zu den systemeigenen Microsoft SQL Server-Tools gehören Sicherung und Wiederherstellung, der Assistent zum Kopieren von Datenbanken sowie das Kopieren und Anfügen von Datenbanken.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversionen.		DBA
Identifizieren Sie die Version des Zielbetriebssystems.		DBA, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Hardwareanforderungen für die Zielserverinstanz auf der Grundlage der Microsoft SQL Server-Kompatibilitätsliste und der Kapazitätsanforderungen.		DBA, Systemadministrator
Identifizieren Sie die Speicheranforderungen für Typ und Kapazität.		DBA, Systemadministrator
Identifizieren Sie die Netzwerkanforderungen, einschließlich Latenz und Bandbreite.		DBA, Systemadministrator
Wählen Sie den EC2 Instanztyp auf der Grundlage von Kapazität, Speicherfunktionen und Netzwerkfunktionen aus.		DBA, Systemadministrator
Identifizieren Sie die Sicherheitsanforderungen für das Netzwerk und den Hostzugriff für die Quell- und Zieldatenbanken.		DBA, Systemadministrator
Identifizieren Sie eine Liste der Benutzer, die für die Microsoft SQL Server-Softwareinstallation erforderlich sind.		DBA, Systemadministrator
Legen Sie die Backup-Strategie fest.		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie die Verfügbar keitsanforderungen.		DBA
Identifizieren Sie die Strategie für die Anwendungsmigration und -umstellung.		DBA, Systemadministrator

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine virtuelle private Cloud (VPC) und Subnetze.		Systemadministrator
Erstellen Sie Sicherhei tsgruppen und eine Network Access Control List (ACL).		Systemadministrator
Konfigurieren und starten Sie eine EC2 Instanz.		Systemadministrator

Installieren Sie die Software

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Benutzer und Gruppen, die für die Microsoft SQL Server-Software erforderl ich sind.		DBA, Systemadministrator
Laden Sie die Microsoft SQL Server-Software herunter.		DBA, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die Microsoft SQL Server-Software auf der EC2 Instanz und konfigurieren Sie den Server.		DBA, Systemadministrator

Migrieren Sie die Daten — Option 1

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie native Microsoft SQL Server-Tools oder Tools von Drittanbietern, um die Datenbankobjekte und -daten zu migrieren.	Zu den Tools gehören Sicherung und Wiederherstellung, der Assistent zum Kopieren von Datenbanken sowie das Kopieren und Anfügen von Datenbanken. Weitere Informationen finden Sie in der Anleitung Migrieren von Microsoft SQL Server-Datenbanken auf die AWS Cloud.	DBA

Migrieren Sie die Daten — Option 2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie die Daten mithilfe von AWS DMS.	Weitere Informationen zur Verwendung AWS DMS finden Sie unter den Links im Abschnitt Verwandte Ressourcen.	DBA

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Anwendungsmigration.	Verwenden Sie AWS Schema Conversion Tool (AWS SCT), um SQL-Code zu analysier en und zu ändern, der in den Quellcode der Anwendung eingebettet ist.	DBA, Besitzer der App

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Umstellung der Anwendung.		DBA, App-Besitzer, Systemadministrator

Schließen Sie das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie alle temporären AWS Ressourcen herunter.	Zu den temporären Ressource n gehören die AWS DMS Replikationsinstanz und die EC2 Instanz für AWS SCT.	DBA, Systemadministrator
Überprüfen und validieren Sie die Projektdokumente.		DBA, App-Besitzer, Systemadministrator
Erfassen Sie Kennzahlen zum Zeitpunkt der Migration, zu den prozentualen Einsparun gen bei den manuellen Kosten im Vergleich zu den Werkzeugkosten usw.		DBA, App-Besitzer, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schließen Sie das Projekt und geben Sie Feedback.		DBA, App-Besitzer, Systemadministrator

Zugehörige Ressourcen

Referenzen

- Migration von Microsoft SQL Server-Datenbanken auf die AWS Cloud
- Amazon EC2
- Amazon EC2 FAQs
- EC2 Amazon-Preisgestaltung
- AWS Database Migration Service
- Microsoft-Produkte auf AWS
- Microsoft-Lizenzierung am AWS
- Microsoft SQL Server auf AWS

Tutorials und Videos

- Erste Schritte mit Amazon EC2
- Erste Schritte mit AWS Database Migration Service
- Verbinden Sie eine EC2 Amazon-Instance mit Ihrem Simple AD Active Directory
- Fügen Sie Ihrem AWS Managed Microsoft AD Active Directory eine EC2 Amazon-Instance hinzu
- AWS Database Migration Service(Video)
- Einführung in Amazon EC2 — Elastic Cloud Server und Hosting mit AWS (Video)

Migrieren Sie eine lokale MySQL-Datenbank zu Amazon EC2

Erstellt von Lorenzo Mota (AWS)

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer lokalen MySQL-Datenbank zu einer MySQL-Datenbank auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance. Das Muster beschreibt die Verwendung von AWS Database Migration Service (AWS DMS) oder nativen MySQL-Tools wie mysqldump für die Migration. Es konzentriert sich auf die vollständige Datenbankmigration zu einer MySQL-DB-Instance.

Das Muster richtet sich in erster Linie an Lösungsarchitekten. DBAs Es kann in kleinen oder großen Projekten, in einer Test- oder Endmigrationsphase verwendet werden. Wir empfehlen, dass Sie mindestens einen Testzyklus ausführen, bevor Sie dieses Muster in einer Produktionsumgebung verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine MySQL-Quelldatenbank in einem lokalen Rechenzentrum

Produktversionen

- MySQL Version 5.5 und höher
- Ein von Amazon unterstütztes Zielbetriebssystem EC2; siehe Amazon EC2 FAQs

Architektur

Quelltechnologie-Stack

- Eine lokale MySQL-Datenbank

Zieltechnologie-Stack

- Eine MySQL-Datenbank-Instance auf Amazon EC2

AWS-Datenmigrationsmethoden

- AWS DMS
- Native MySQL-Tools wie mysqldump oder Tools von Drittanbietern wie Percona XtraBackup

Zielarchitektur

Das folgende Diagramm zeigt die EC2 Zielimplementierung von Amazon nach der Umstellung.

AWS-Datenmigrationsarchitektur

Verwenden von AWS DMS:

Das folgende Diagramm veranschaulicht den Datenmigrationsablauf, der auf dem AWS DMS Senden vollständiger und inkrementeller Änderungen an die MySQL-Zieldatenbank bis zur Übernahme basiert. Die Netzwerkverbindung von lokal zu AWS hängt von den Anforderungen des SQL-Clients ab und fällt nicht in den Anwendungsbereich dieses Musters.

Verwendung anderer MySQL-Tools:

Das folgende Diagramm veranschaulicht den Datenmigrationsablauf, der auf der Verwendung von MySQL-Tools zum Generieren von Export-Dumpdateien aus der lokalen Datenbank basiert. Diese Dateien werden in Amazon Simple Storage Service (Amazon S3) verschoben und vor der Übernahme in die MySQL-Zieldatenbank importiert. Die Netzwerkverbindung von lokal zu AWS hängt von den Anforderungen des SQL-Clients ab und liegt außerhalb des Geltungsbereichs dieses Musters.

Hinweise:

- Abhängig von den Ausfallzeiten und der Größe der Datenbank für die endgültige Umstellung können Sie ein anderes CDC-Tool (Change Data Capture) verwenden AWS DMS , um die Umstellungszeit zu minimieren. Wenn Sie ein CDC-Tool wie verwenden AWS DMS, können Sie innerhalb von Minuten zur Zieldatenbank migrieren.
- Eine Offline-Strategie mit mysqldump kann ausreichen, wenn die Größe der Datenbank und die Netzwerklatenz ein kurzes Umstellungsfenster zulassen. (Wir empfehlen, Tests durchzuführen, um eine ungefähre Zeit zu erhalten.)

- In der Regel AWS DMS erfordert eine durchgehende CDC-Strategie mehr Überwachung und Komplexität als eine Offline-Option.

Tools

AWS Dienste

- AWS Database Migration Service (AWS DMS) unterstützt mehrere Quell- und Zieldatenbanken. Hinweise zu MySQL-Quell- und Zieldatenbanken, die von unterstützt werden AWS DMS, finden Sie unter Verwenden einer MySQL-kompatiblen Datenbank als Quelle für AWS DMS und Verwenden einer MySQL-kompatiblen Datenbank als Ziel für. AWS DMS Wenn Ihre Quelldatenbank von nicht unterstützt wird AWS DMS, müssen Sie eine andere Methode für die Migration Ihrer Daten wählen.

Andere Tools

- mysqldump ist ein MySQL-Hilfsprogramm, das zu Sicherungs- oder Migrationszwecken eine Dump-Datei aus einer MySQL-Datenbank erstellt.
- Percona XtraBackup ist ein Open-Source-Hilfsprogramm für die Durchführung blockierungsfreier Backups auf MySQL-Datenbanken.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Datenbank versionen.	Validieren Sie die Versionen der Quell- und Zieldaten banken. Informationen zu den von AWS DMS unterstützten MySQL-Versionen finden Sie AWS DMS in der AWS DMS Dokumentation unter Sources for AWS DMS und Targets for.	DBA
Identifizieren Sie das Zielbetri ebssystem.	Ermitteln Sie die Version des Zielbetriebssystems.	DBA, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Eine Liste der von Amazon EC2 unterstützten Zielbetri ebssysteme finden Sie unter Amazon EC2 FAQs.	
Identifizieren Sie die Hardwareanforderungen.	Ermitteln Sie die Hardwarea nforderungen für die Zielserve rinstanz auf der Grundlage der MySQL-Kompatibilitätsliste und der Kapazitätsanforder ungen.	DBA, Systemadministrator
Identifizieren Sie die Speicheranforderungen.	Ermitteln Sie den Speichert yp und die Kapazität für die Zieldatenbank.	DBA, Systemadministrator
Identifizieren Sie die Netzwerkanforderungen.	Ermitteln Sie die Netzwerka nforderungen wie Latenz und Bandbreite.	DBA, Systemadministrator
Wählen Sie den Typ der Zielinstanz.	Wählen Sie den Zielinsta nztyp auf der Grundlage von Kapazität, Speicherfunktionen und Netzwerkfunktionen aus.	DBA, Systemadministrator
Identifizieren Sie die Sicherhei tsanforderungen.	Ermitteln Sie die Sicherhei tsanforderungen für den Netzwerk- oder Hostzugriff für die Quell- und Zieldaten banken.	DBA, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Benutzer.	Ermitteln Sie die Liste der Betriebssystembenutzer für die MySQL-Softwareinst allation. Weitere Informationen finden Sie in der MySQL-Dok umentation.	DBA, Systemadministrator
Legen Sie eine Backup-St rategie fest.		DBA
Ermitteln Sie die Verfügbar keitsanforderungen.		DBA
Identifizieren Sie die Strategie für die Anwendungsmigration oder den Umstieg.		DBA, Systemadministrator

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine virtuelle private Cloud (VPC) und Subnetze.	Konfigurieren Sie Routentab ellen, Internet-Gateways, NAT-Gateways und Subnetze. Weitere Informationen finden Sie unter VPC-Konfigurations optionen in der Amazon VPC-Dokumentation.	Systemadministrator
Erstellen Sie Sicherhei tsgruppen und Netzwerkz ugriffskontrolllisten (ACLs).	Konfigurieren Sie IPs je nach Ihren Anforderungen Ports (Standard für MySQL ist 3306) und CIDR-Bereiche oder spezifische.	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren und starten Sie eine EC2 Instanz.	Anweisungen finden Sie in der EC2 Amazon-Dokumentation unter Eine EC2 Instance starten.	Systemadministrator

Installieren Sie die MySQL-Software

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Benutzer und Gruppen.	Erstellen Sie die Betriebssystembenutzer und -gruppen, die Zugriff auf den Server und die Datenbank benötigen. Weitere Informationen finden Sie unter Access Control and Account Management in der MySQL-Dokumentation.	DBA, Systemadministrator
Laden Sie MySQL herunter.	Laden Sie die MySQL-Software herunter. Anweisungen und Binärdateien finden Sie unter Installation von MySQL in der MySQL-Dokumentation.	DBA, Systemadministrator
Installieren Sie MySQL auf der EC2 Instanz und konfigurieren Sie den Server.	Connect zu Ihrer EC2 Instance her und installieren Sie die MySQL-Software. Weitere Informationen finden Sie in der EC2 Amazon-Dokumentation unter Connect zu Ihrer EC2 Instance herstellen.	DBA, Systemadministrator

Daten migrieren — Option 1

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie Daten mit nativen MySQL- oder Drittanbieter-Tools.	Diese Option verwendet native MySQL-Tools oder Tools von Drittanbietern, um Datenbankobjekte und Daten zu migrieren. Anweisungen finden Sie in der Dokumentation für mysqldump oder Percona XtraBackup (für die physische Migration). Weitere Informationen zur Verwendung dieser Tools finden Sie im AWS Blogbeitrag Migrationsoptionen für MySQL zu Amazon RDS for MySQL oder Amazon Aurora MySQL.	DBA

Daten migrieren — Option 2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie Daten mit AWS DMS.	Weitere Informationen finden Sie AWS DMS in der AWS DMS Dokumentation unter Ansicht auf hoher Ebene von.	DBA

Bereite dich auf die Umstellung vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sammeln Sie die Anzahl der Objekte.	Sammeln Sie Objektzahlen aus der Quelldatenbank	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und neuen Zieldatenbanken. Korrigieren Sie alle Unstimmig keiten in der Zieldatenbank.	
Überprüfen Sie die Abhängigk eiten.	Vergewissern Sie sich, dass Abhängigkeiten (Links) zu und von anderen Datenbank en weiterhin gültig sind und ordnungsgemäß funktionieren.	DBA
Testen.	Wenn es sich um einen Testzyklus handelt, führen Sie Abfragetests durch, sammeln Sie Metriken und beheben Sie alle Probleme.	DBA

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kunden bewegen.	Stellen Sie die Anwendung sclients auf die neue Infrastru ktur um.	DBA, Besitzer der App, Systemadministrator
Bieten Sie Unterstützung an.	Bieten Sie Unterstützung bei Funktionstests von Anwendungen.	DBA

Schließt das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ressourcen herunterfahren.	Fahren Sie die AWS DMS Replikationsinstanz und	DBA, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	andere temporäre AWS Ressourcen herunter.	
Dokumente überprüfen und projizieren.	Überprüfen und validieren Sie die Projektdokumente.	DBA, App-Besitzer, Systemadministrator
Sammeln Sie Metriken.	Erfassen Sie Kennzahlen wie die Zeit bis zur Migration , den Prozentsatz manueller Änderungen im Vergleich zu toolgestützten Änderungen und Kosteneinsparungen.	DBA, App-Besitzer, Systemadministrator
Schließt das Projekt ab.	Schließen Sie das Migration sprojekt ab und geben Sie Feedback.	DBA, App-Besitzer, Systemadministrator
Quelldatenbank außer Betrieb nehmen.	Nehmen Sie die lokale MySQL-Datenbank außer Betrieb.	DBA, Systemadministrator

Zugehörige Ressourcen

Referenzen

- EC2 Amazon-Dokumentation
- AWS DMS Dokumentation
- EC2 Amazon-Preisgestaltung
- AWS DMS Step-by-Step Anleitungen
- mysqldump
- Percona XtraBackup

Tutorials und Videos

- Erste Schritte mit AWS DMS

- Einführung in Amazon EC2 — Elastic Cloud Server und Hosting mit AWS (Video)

Reduzieren Sie die Umstellungszeit für homogene SAP-Migrationen mithilfe des Application Migration Service

Erstellt von Pavel Rubin (AWS), Diego Valverde (AWS) und Sunil Yadav (AWS)

Übersicht

Dieses Muster beschreibt die Schritte für die Migration von SAP-Workloads mithilfe des AWS Application Migration Service. Der Application Migration Service erleichtert Übernahmen, indem er Replikation auf Blockebene verwendet, um Replikationsvolumes aufrechtzuerhalten, die kontinuierlich mit ihren Quellen synchronisiert werden.

Zu den SAP-Workloads gehören die Anwendungen SAP Customer Relationship Management (SAP CRM), SAP Enterprise Resource Planning (ERP) und SAP Business Warehouse (SAP BW).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit stabiler Netzwerkkonnektivität zwischen SAP-Quellservern und der Ziel-Virtual Private Cloud (VPC) auf AWS
- Eine SAP Adaptive Server Enterprise (ASE) -Quelldatenbank für Linux oder Windows in einem lokalen Rechenzentrum

Einschränkungen

- Das Zielbetriebssystem muss von Amazon Elastic Compute Cloud (Amazon EC2) unterstützt werden. Weitere Informationen finden Sie auf Amazon EC2 FAQs.

Architektur

Quelltechnologie-Stack

- Eine SAP ASE-Datenbank

Zieltechnologie-Stack

- Amazon EC2
- Amazon Elastic Block Store (Amazon EBS)

Quell- und Zielarchitektur

Das folgende Diagramm zeigt die Migration von den lokalen Servern über den Replication Agent zum Application Migration Service-Endpunkt. Ein Amazon Simple Storage Service (Amazon S3) -Endpunkt wird für den Zugriff auf Installations- und Konfigurationsdateien verwendet. Die Subnetze für den Staging-Bereich und die migrierten Ressourcen enthalten EC2 Instances mit Datenspeicher auf EBS-Volumes. Port TCP 443 wird verwendet, um das Quellmaschinennetzwerk mit dem Application Migration Service zu verbinden und um die Staging-Bereichs-Subnetze mit den regionalen Endpunkten Application Migration Service EC2, Amazon und Amazon S3 zu verbinden. Port TCP 1500 wird für die Datenreplikation zwischen dem lokalen Netzwerk und dem Staging-Bereich verwendet.

Tools

- Mit AWS Application Migration Service können Sie Anwendungen ohne Änderungen und mit minimaler Ausfallzeit in die AWS-Cloud rehosten (lift-and-shift).
- Amazon Elastic Block Store (Amazon EBS) bietet Speichervolumes auf Blockebene zur Verwendung mit Amazon Elastic Compute Cloud (Amazon EC2) -Instances.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Security Token Service (AWS STS) hilft Ihnen dabei, temporäre Anmeldeinformationen mit eingeschränkten Rechten für Benutzer anzufordern.

Epen

Initialisieren Sie den Anwendungsmigrationsdienst

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initialisieren Sie den Anwendungsmigrationsdienst.	Initialisieren Sie den Application Migration Service in der AWS-Region, in der Sie die SAP ASE-Datenbank bereitste	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	llen möchten. AWS bietet ein automatisiertes Setup, wenn Sie zum ersten Mal die Seite Application Migration Service in jeder Region aufrufen.	
Manuelles Erstellen von Servicerollen.	(Optional) Wenn Sie das Konto mithilfe von Automatisierung (z. B. AWS Control Tower) einrichten möchten, können Sie die sechs AWS Identity and Access Management (IAM) -Rollen, die für Installation, Replikation und Starts erforderlich sind, manuell erstellen. Anweisungen finden Sie in der AWS-Dokumentation.	AWS-Administrator
Erstellen Sie eine Vorlage für Replikationseinstellungen.	Die Vorlage für Replikationseinstellungen definiert das Subnetz, den Instance-Typ, die Amazon EBS-Verschlüsselung und die Art der Datenweiterleitung. Detaillierte Informationen zu den Einstellungen finden Sie in der AWS-Dokumentation.	Allgemeines AWS

Generieren Sie Anmeldeinformationen für die Agenteninstallation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine neue IAM-Rolle.	Navigieren Sie in der IAM-Konsole zu Rollen und wählen Sie Rolle erstellen aus. Wählen Sie für den Entitätstyp Vertrauenswürdig AWS-Konto und dann Weiter aus.	AWS-Systemadministrator
An AWSApplication Migration AgentPolicy die IAM-Rolle anhängen.	Die von AWS verwaltete `AWSApplicationMigrationAgentPolicy` Richtlinie enthält die erforderlichen Berechtigungen für die Installation des Application Migration Service Agents. Nachdem Sie die Richtlinie angehängt haben, wählen Sie Weiter.	AWS-Systemadministrator
Schließen Sie die Rollenerstellung ab.	Vergeben Sie einen benutzerfreundlichen Namen und wählen Sie Rolle erstellen.	AWS-Systemadministrator
Generieren Sie temporäre Anmeldeinformationen.	Folgen Sie den Anweisungen in der AWS STS STS-Dokumentation, um die Zugriffsschlüssel-ID, den geheimen Zugriffsschlüssel und das Sitzungstoken zu generieren. Diese Anmeldeinformationen werden bei der Installation des Agenten verwendet.	AWS-Systemadministrator

Installieren Sie den Application Migration Service Agent auf dem SAP-Quellcomputer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das Agent-Installationsprogramm auf den SAP-Quellcomputer herunter.	Laden Sie das Agent-Installationsprogramm herunter, das für Ihr Quellbetriebssystem geeignet ist: Windows oder Linux.	Besitzer der App
Installieren Sie den AWS Replication Agent.	Wenn Sie die Agent-Installationsdatei auf einem Quellcomputer ausführen, werden Sie zunächst aufgefordert, Ihren Zugriffsschlüssel, Ihren geheimen Zugriffsschlüssel, Ihr Sitzungstoken und die Region einzugeben, in die repliziert werden soll. Verwenden Sie die temporären Anmeldeinformationen der IAM-Rolle, die Sie zuvor erstellt haben, und dieselbe Region, die Sie bei der Initialisierung konfiguriert haben.	Besitzer der App
Warten Sie auf die erste Datenreplikation.	Nach der Installation des Agenten wird der Quellcomputer auf der Registerkarte Maschinen in der Application Migration Service-Konsole angezeigt.	Besitzer der App

Konfigurieren Sie die Startvorlage des Zielcomputers

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Launch-Vorlage für den Quellserver.	Jeder Quellserver verwendet eine eindeutige EC2 Startvorlage, die als Grundlage für die Konfiguration des EC2 Zielservers dient. Sie können diese Vorlage bearbeiten, wenn Sie die EC2 Amazon-Konfiguration Ihres migrierten Servers anpassen möchten.	Allgemeines AWS
Legen Sie die Standardversion der Launch-Vorlage fest.	Nachdem Sie die erforderlichen Änderungen an der Startvorlage vorgenommen haben, geben Sie an, dass diese aktualisierte Version als Standardvorlage für den Start verwendet werden soll. Weitere Informationen finden Sie in der AWS-Dokumentation.	Allgemeines AWS
Deaktivieren Sie den Instanztyp und die richtige Größe.	(Optional) Die richtige Dimensionierung des Instanztyps bietet automatische Empfehlungen für den Instanztyp auf der Grundlage der Konfiguration des SAP-Quellservers. Wir empfehlen, diese Einstellung zu deaktivieren, damit Sie benutzerdefinierte Instance-Typen in der Launch-Vorlage angeben können.	Allgemeines AWS

Führen Sie einen Test durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initiieren Sie einen Teststart.	Wählen Sie in der Applicati on Migration Service-Konsole einen oder mehrere Server aus und wählen Sie dann unter Test und Übernahme die Option Testinstanzen starten aus.	Allgemeines AWS, Migration singenieur, Migrationsleiter
Warten Sie, bis der Konvertie rungs- und Startvorgang abgeschlossen ist.	Sie können den Startvorgang auf der Registerkarte Startverl auf überprüfen. Nachdem der Computer erfolgreich als EC2 Instanz gestartet wurde, wird die Registerkarte „Benachric htigungen“ auf „Gestartet“ aktualisiert.	
Stellen Sie sicher, dass der Test erfolgreich abgeschlo ssen wurde.	Stellen Sie über Remote Desktop Protocol (RDP) oder SSH (Secure Shell) eine Connect zur gestartet en Instance her und führen Sie die entsprechenden Anwendungsprüfungen durch. Melden Sie sich beispiels weise bei der SAP-Schni ttstelle an und überprüfen Sie die Funktionalität.	Migrationsingenieur, App-Besit zer
Aktualisieren Sie den Quelllebenszyklus.	Wenn der Test erfolgreich war, aktualisieren Sie den Lebenszyklus des Quellcomp uters auf der Registerkarte Test und Übernahme auf Als	Migrationsingenieur, Migration sleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	„Bereit für die Übernahme“ markieren.	

Eine Umstellung auf das EC2 Amazon-Ziel planen und durchführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Planen Sie ein Umstellungsfenster ein.		Leiter der Umstellung, Leiter der Migration, Inhaber der App
Initiieren Sie einen Cutover-Start.	Wählen Sie einen oder mehrere Server aus. Wählen Sie auf der Registerkarte Test and Cutover in der Application Migration Service-Konsole unter Test und Übernahme die Option Übernahmeinstanzen starten aus.	Migrationsingenieur
Warten Sie, bis die Konvertierungs- und Startvorgänge abgeschlossen sind.	Sie können den Startvorgang auf der Registerkarte Startverlauf überprüfen. Nachdem der Computer erfolgreich als EC2 Instanz gestartet wurde, wird die Registerkarte „Benachrichtigungen“ auf „Gestartet“ aktualisiert.	
Stellen Sie sicher, dass die Umstellung erfolgreich abgeschlossen wurde.	Stellen Sie über RDP oder SSH eine Connect zur gestarteten Instance her und führen Sie die entsprechenden Anwendungsprüfungen durch.	App-Besitzer, Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie den Quelllebenszyklus.	Wenn die Übernahme erfolgreich war, aktualisieren Sie den Lebenszyklus der Quellmaschine, indem Sie auf der Registerkarte Test und Übernahme die Option Übernahme abschließen auswählen.	Ingenieur für Migration

Zugehörige Ressourcen

Referenzen

- AWS Application Migration Service
- Häufig gestellte Fragen zur AWS-Anwendungsmigration

Video

- Architektur des AWS-Anwendungsmigrationsdienstes

Rehosten Sie lokale Workloads in der AWS-Cloud: Migrationscheckliste

Erstellt von Srikanth Rangavajhala (AWS)

Übersicht

Das Rehosten von lokalen Workloads in der Amazon Web Services (AWS) -Cloud umfasst die folgenden Migrationsphasen: Planung, Pre-Discovery, Discovery, Build, Test und Cutover. Dieses Muster beschreibt die Phasen und die damit verbundenen Aufgaben. Die Aufgaben werden ausführlich beschrieben und unterstützen etwa 75% aller Anwendungsworkloads. Sie können diese Aufgaben über einen Zeitraum von zwei bis drei Wochen in einem agilen Sprintzyklus implementieren.

Sie sollten diese Aufgaben mit Ihrem Migrationsteam und Ihren Beratern besprechen und überprüfen. Nach der Überprüfung können Sie die Informationen sammeln, Aufgaben streichen oder neu bewerten, falls dies Ihren Anforderungen entspricht, und andere Aufgaben so ändern, dass sie mindestens 75% der Anwendungs-Workloads in Ihrem Portfolio unterstützen. Anschließend kannst du ein agiles Projektmanagement-Tool wie Atlassian Jira oder Rally Software verwenden, um die Aufgaben zu importieren, sie Ressourcen zuzuweisen und deine Migrationsaktivitäten zu verfolgen.

Das Muster geht davon aus, dass Sie AWS Cloud Migration Factory verwenden, um Ihre Workloads neu zu hosten, aber Sie können das Migrationstool Ihrer Wahl verwenden.

Amazon Macie kann Ihnen helfen, sensible Daten in Ihren Wissensdatenbanken zu identifizieren, die als Datenquellen gespeichert sind, Aufrufprotokolle modellieren und Eingabeaufforderungsspeicher in Amazon Simple Storage Service (Amazon S3) -Buckets speichern. Weitere Informationen finden Sie in der Macie-Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Projektmanagement-Tool zur Nachverfolgung von Migrationsaufgaben (z. B. Atlassian Jira oder Rally Software)
- Migrationstool zum Rehosten Ihrer Workloads auf AWS (z. B. Cloud Migration Factory)

Architektur

Quellplattform

- Lokaler Quellstapel (einschließlich Technologien, Anwendungen, Datenbanken und Infrastruktur)

Zielplattform

- AWS-Cloud-Zielstapel (einschließlich Technologien, Anwendungen, Datenbanken und Infrastruktur)

Architektur

Das folgende Diagramm veranschaulicht das Rehosting (Erkennung und Migration von Servern aus einer lokalen Quellumgebung zu AWS) mithilfe von Cloud Migration Factory und AWS Application Migration Service.

Tools

- Sie können ein Migrations- und Projektmanagement-Tool Ihrer Wahl verwenden.

Epen

Planungsphase

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Pflegen Sie den Rückstand vor der Entdeckung.	Führen Sie die Arbeitssitzung mit Abteilungsleitern und Anwendungsbesitzern durch, bevor der Rückstand erkannt wird.	Projektmanager, Leiter von Agile Scrum
Führen Sie die Arbeitssitzung zur Sprint-Planung durch.	Verteilen Sie die Anwendung en, die Sie migrieren möchten, als Übung für den Umfang auf mehrere Sprints und Wellen.	Projektmanager, Leiter von Agile Scrum

Phase vor der Entdeckung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie die Anwendungskenntnisse.	Bestätigen und dokumentieren Sie den Inhaber der Anwendung und dessen Kenntnisse über die Anwendung. Stellen Sie fest, ob es einen anderen Ansprechpartner für technische Fragen gibt.	Migrationsspezialist (Interviewer)
Ermitteln Sie die Compliance-Anforderungen für Anwendungen.	Erkundigen Sie sich beim Eigentümer der Anwendung, dass die Anwendung nicht den Anforderungen des Payment Card Industry Data Security Standard (PCI DSS), des Sarbanes-Oxley Act (SOX), personenbezogener Daten (PII) oder anderer Standards entsprechen muss. Wenn Compliance-Anforderungen bestehen, müssen die Teams ihre Konformitätsprüfungen auf den Servern abschließen, die migriert werden sollen.	Migrationsspezialist (Interviewer)
Bestätigen Sie die Anforderungen für die Produktionsfreigabe.	Bestätigen Sie die Anforderungen für die Freigabe der migrierten Anwendung für die Produktion (z. B. Veröffentlichungsdatum und Dauer der Ausfallzeit) mit dem Eigentümer der Anwendung	Migrationsspezialist (Interviewer)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	oder dem technischen Ansprechpartner.	
Serverliste abrufen.	Ruft die Liste der Server ab, die der Zielanwendung zugeordnet sind.	Migrationsspezialist (Interviewer)
Holen Sie sich das logische Diagramm, das den aktuellen Status zeigt.	Rufen Sie das aktuelle Statusdiagramm für die Anwendung vom Unternehmensarchitekten oder dem Anwendungsbesitzer ab.	Migrationsspezialist (Interviewer)
Erstellen Sie ein logisches Diagramm, das den Zielstatus zeigt.	Erstellen Sie ein logisches Diagramm der Anwendung, das die Zielarchitektur auf AWS zeigt. Dieses Diagramm sollte Server, Konnektivität und Zuordnungsfaktoren veranschaulichen.	Unternehmensarchitekt, Geschäftsinhaber
Serverinformationen abrufen.	Sammeln Sie Informationen über die Server, die der Anwendung zugeordnet sind, einschließlich ihrer Konfigurationsdetails.	Migrationsspezialist (Interviewer)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Serverinformationen zur Discovery-Vorlage hinzu.	Fügen Sie der Vorlage für die Anwendungserkennung detaillierte Serverinformationen hinzu (dieses Muster finden Sie `mobilize-application-questionnaire.xlsx` im Anhang). Diese Vorlage enthält alle anwendungsbezogenen Sicherheits-, Infrastruktur-, Betriebssystem- und Netzwerkdetails.	Migrationsspezialist (Interviewer)
Veröffentlichen Sie die Vorlage für die Anwendungserkennung.	Teilen Sie die Vorlage für die Anwendungserkennung mit dem Anwendungseigentümer und dem Migrationsteam, damit sie gemeinsam darauf zugreifen und sie verwenden können.	Migrationsspezialist (Interviewer)

Entdeckungsphase

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie die Serverliste.	Bestätigen Sie die Serverliste und den Zweck der einzelnen Server mit dem Besitzer der Anwendung oder dem technischen Leiter.	Spezialist für Migration
Identifizieren und fügen Sie Servergruppen hinzu.	Identifizieren Sie Servergruppen wie Webserver oder Anwendungsserver und fügen	Spezialist für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie diese Informationen der Vorlage für die Anwendung serkennung hinzu. Wählen Sie die Ebene der Anwendung (Web, Anwendung, Datenbank) aus, zu der jeder Server gehören soll.	
Füllen Sie die Vorlage für die Anwendungserkennung aus.	Vervollständigen Sie die Details der Vorlage für die Anwendungserkennung mit Hilfe des Migrationsteams, des Anwendungsteams und AWS.	Spezialist für Migration
Fügen Sie fehlende Serverdet ails hinzu (Middleware- und Betriebssystemteams).	Bitten Sie Middleware- und Betriebssystemteams (OS), die Vorlage für die Anwendung serkennung zu überprüfen und alle fehlenden Serverdet ails, einschließlich Datenbank informationen, hinzuzufügen.	Spezialist für Migration
Holen Sie sich die Regeln für eingehenden/ausgehenden Verkehr (Netzwerkteam).	Bitten Sie das Netzwerkteam, die Regeln für eingehenden/ ausgehenden Verkehr für die Quell- und Zielserver zu ermitteln. Das Netzwerkteam sollte außerdem bestehend e Firewallregeln hinzufüge n, diese in ein Sicherhei tsgruppenformat exportier en und bestehende Load Balancer zur Vorlage für die Anwendungserkennung hinzufügen.	Spezialist für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie das erforderliche Tagging.	Ermitteln Sie die Tagging-Anforderungen für die Anwendung.	Spezialist für Migration
Erstellen Sie Details zur Firewall-Anforderung.	Erfassen und filtern Sie die Firewallregeln, die für die Kommunikation mit der Anwendung erforderlich sind.	Migrationsspezialist, Lösungsarchitekt, Netzwerkleiter
Aktualisieren Sie den EC2 Instanztyp.	Aktualisieren Sie den Amazon Elastic Compute Cloud (Amazon EC2) -Instanztyp, der in der Zielumgebung verwendet werden soll, basierend auf Infrastruktur- und Serveranforderungen.	Migrationsspezialist, Lösungsarchitekt, Netzwerkleiter
Identifizieren Sie das aktuelle Statusdiagramm.	Identifizieren oder erstellen Sie das Diagramm, das den aktuellen Status der Anwendung zeigt. Dieses Diagramm wird in der Anfrage zur Informationssicherheit (InfoSec) verwendet.	Migrationsspezialist, Lösungsarchitekt
Finalisieren Sie das future Zustandsdiagramm.	Finalisieren Sie das Diagramm, das den future (Ziel-) Status der Anwendung zeigt. Dieses Diagramm wird auch in der InfoSec Anfrage verwendet.	Migrationsspezialist, Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Serviceanfragen für Firewalls oder Sicherheitsgruppen.	Erstellen Sie Firewall- oder Sicherheitsgruppen-Serviceanfragen (für Entwicklung/Qualitätssicherung, Vorproduktion und Produktion). Wenn Sie Cloud Migration Factory verwenden, fügen Sie replikationsspezifische Ports hinzu, sofern diese noch nicht geöffnet sind.	Migrationsspezialist, Lösungsarchitekt, Netzwerkleiter
Überprüfen Sie die Anfragen von Firewalls oder Sicherheitsgruppen (InfoSec Team).	In diesem Schritt überprüft und genehmigt das InfoSec Team die Firewall- oder Sicherheitsgruppenanfragen, die im vorherigen Schritt erstellt wurden.	InfoSec Ingenieur, Migrationsspezialist
Implementieren Sie Firewall-Sicherheitsgruppenanfragen (Netzwerkteam).	Nachdem das InfoSec Team die Firewallanfragen genehmigt hat, implementiert das Netzwerkteam die erforderlichen Firewallregeln für eingehende/ausgehende Verbindungen.	Migrationsspezialist, Lösungsarchitekt, Netzwerkleiter

Erstellungsphase (Wiederholung für Entwicklungs- und QA-, Vorproduktions- und Produktionsumgebungen)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Importieren Sie die Anwendungs- und Serverdaten.	1. Stellen Sie sicher, dass Sie bei Ihrem Server für die Ausführung der Migration als Domänenbenutzer mit	Migrationsspezialist, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	lokalen Administratorrechten auf den Quellservern im Geltungsbereich angemeldet sind. 2. Verwenden Sie das Eingabeformular für die Migration, um die Attribute für die Quellserver im Geltungsbereich zu importieren. Weitere Informationen finden Sie im Cloud Migration Factory-Implementierungsleitfaden. Wenn Sie Cloud Migration Factory nicht verwenden, folgen Sie den Anweisungen zur Einrichtung Ihres Migration stools.	
Überprüfen Sie die Voraussetzungen für Quellserver.	Connect mit den Quellservern im Geltungsbereich her, um Voraussetzungen wie TCP-Port 1500, TCP-Port 443, freien Speicherplatz auf dem Stammvolume, .NET Framework-Version und andere Parameter zu überprüfen. Diese sind für die Replikation erforderlich. Weitere Informationen finden Sie im Cloud Migration Factory-Implementierungsleitfaden.	Migrationsspezialist, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Servicean frage zur Installation von Replikationsagenten.	Erstellen Sie eine Servicean frage zur Installation von Replikationsagenten auf den im Lieferumfang enthaltenen Servern für Entwicklung/Qualit ätssicherung, Vorproduktion oder Produktion.	Migrationsspezialist, Cloud-Administrator
Installieren Sie die Replikati onsagenten.	Installieren Sie die Replikati onsagenten auf den Quellserv ern im Leistungsumfang auf den Entwicklungs-, QA-, Vorproduktions- oder Produktionsrechnern. Weitere Informationen finden Sie im Cloud Migration Factory-I mplementierungsleitfaden.	Migrationsspezialist, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Veröffentlichen Sie die Skripte nach dem Start.	Der Application Migration Service unterstützt Skripts nach dem Start, mit denen Sie Aktivitäten auf Betriebssystemebene automatisieren können, z. B. das Installieren oder Deinstallieren von Software nach dem Start von Ziel-Instances. In diesem Schritt werden die Skripts nach dem Start auf Windows- oder Linux-Computer übertragen, je nachdem, welche Server für die Migration identifiziert wurden. Anweisungen finden Sie im Cloud Migration Factory-Implementierungsleitfaden.	Migrationsspezialist, Cloud-Administrator
Überprüfen Sie den Replikationsstatus.	Bestätigen Sie den Replikationsstatus für die Quellserver im Geltungsbereich automatisch mithilfe des bereitgestellten Skripts. Das Skript wird alle fünf Minuten wiederholt, bis sich der Status aller Quellserver in der angegebenen Welle auf Fehlerfrei ändert. Anweisungen finden Sie im Cloud Migration Factory-Implementierungsleitfaden.	Migrationsspezialist, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Admin-Benutzer.	Möglicherweise ist ein lokaler Administrator oder Sudo-Benutzer auf den Quellcomputern erforderlich, um Probleme nach der Umstellung von den Quellservern im Geltungsbereich auf AWS zu beheben. Das Migrationsteam verwendet diesen Benutzer, um sich beim Zielserver anzumelden, wenn der Authentifizierungsserver (z. B. der DC- oder LDAP-Server) nicht erreichbar ist. Anweisungen für diesen Schritt finden Sie im Cloud Migration Factory-Implementierungsleitfaden.	Migrationsspezialist, Cloud-Administrator
Validieren Sie die Startvorlage.	Überprüfen Sie die Server-Metadaten, um sicherzustellen, dass sie erfolgreich funktionieren und keine ungültigen Daten enthalten. In diesem Schritt werden sowohl die Test- als auch die Cutover-Metadaten validiert. Anweisungen finden Sie im Cloud Migration Factory-Implementierungsleitfaden.	Migrationsspezialist, Cloud-Administrator

Testphase (Wiederholung für Entwicklungs- und QA-, Vorproduktions- und Produktionsumgebungen)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Servicean frage.	Erstellen Sie eine Servicean frage für das Infrastrukturteam und andere Teams, um die Anwendung auf Entwicklu ngs-/QA-, Vorproduktions- oder Produktionsinstanzen umzustellen.	Migrationsspezialist, Cloud-Administrator
Konfigurieren Sie einen Load Balancer (optional).	Konfigurieren Sie die erforderl ichen Load Balancer, z. B. einen Application Load Balancer oder einen F5-Load Balancer, mit iRules.	Migrationsspezialist, Cloud-Administrator
Starten Sie Instanzen zum Testen.	Startet alle Zielcomputer für eine bestimmte Welle im Application Migration Service im Testmodus. Weitere Informationen finden Sie im Cloud Migration Factory-I mplementierungsleitfaden.	Migrationsspezialist, Cloud-Administrator
Überprüfen Sie den Status der Zielinstanz.	Überprüfen Sie den Status der Zielinstanz, indem Sie den Startvorgang für alle Quellserver im Geltungsb ereich in derselben Welle überprüfen. Es kann bis zu 30 Minuten dauern, bis die Ziel-Instances hochgefahren sind. Sie können den Status manuell überprüfen, indem Sie sich bei der EC2 Amazon-Konsole anmelden, nach	Migrationsspezialist, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dem Namen des Quellservers suchen und die Spalte Statusprüfung überprüfen. Die bestandenen Statusprüfungen 2/2 deuten darauf hin, dass die Instance aus Sicht der Infrastruktur fehlerfrei ist.	
DNS-Einträge ändern.	Ändern Sie DNS-Einträge (Domain Name System). (Verwenden Sie `resolv.conf` oder `host.conf` für eine Microsoft Windows-Umgebung.) Konfigurieren Sie jede EC2 Instanz so, dass sie auf die neue IP-Adresse dieses Hosts verweist. **Note** Stellen Sie sicher, dass es keine DNS-Konflikte zwischen lokalen Servern und AWS-Cloud-Servern gibt. Dieser Schritt und die folgenden Schritte sind optional, abhängig von der Umgebung, in der der Server gehostet wird.	Migrationsspezialist, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Konnektivität zu Backend-Hosts von EC2 Instanzen aus.	Überprüfen Sie die Anmeldungen anhand der Domänenanmeldedaten für die migrierten Server.	Migrationsspezialist, Cloud-Administrator
Aktualisieren Sie den DNS-A-Eintrag.	Aktualisieren Sie den DNS-A-Eintrag für jeden Host so, dass er auf die neue EC2 private Amazon-IP-Adresse verweist.	Migrationsspezialist, Cloud-Administrator
Aktualisieren Sie den DNS-CNAME-Eintrag.	Aktualisieren Sie den DNS-CNAME-Eintrag für virtuelle Server IPs (Load Balancer-Namen) so, dass er auf den Cluster für Web- und Anwendungsserver verweist.	Migrationsspezialist, Cloud-Administrator
Testen Sie die Anwendung in den entsprechenden Umgebungen.	Melden Sie sich bei der neuen EC2 Instanz an und testen Sie die Anwendung in den Entwicklungs-, QA-, Vorproduktions- und Produktionsumgebungen.	Migrationsspezialist, Cloud-Administrator
Als bereit für die Umstellung markieren.	Wenn der Test abgeschlossen ist, ändern Sie den Status des Quellservers, um anzuzeigen, dass er bereit für die Übernahme ist, sodass Benutzer eine Übernahmeinstanz starten können. Anweisungen finden Sie im Cloud Migration Factory-Implementierungsleitfaden.	Migrationsspezialist, Cloud-Administrator

Umstellungsphase

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Bereitstellungsplan für die Produktion.	Erstellen Sie einen Bereitstellungsplan für die Produktion (einschließlich eines Notfallplans).	Migrationsspezialist, Cloud-Administrator
Informieren Sie das Betriebsteam über Ausfallzeiten.	Informieren Sie das Betriebsteam über den Zeitplan für die Ausfallzeiten der Server. Einige Teams benötigen für diese Benachrichtigung möglicherweise eine Änderungsanfrage oder ein Ticket für eine Serviceanfrage (CR/SR).	Migrationsspezialist, Cloud-Administrator
Replizieren Sie Produktionsmaschinen.	Replizieren Sie Produktionsmaschinen mithilfe des Application Migration Service oder eines anderen Migrationstools.	Migrationsspezialist, Cloud-Administrator
Fahren Sie die Quellserver im Geltungsbereich herunter.	Nachdem Sie den Replikationsstatus der Quellserver überprüft haben, können Sie die Quellserver herunterfahren, um Transaktionen von Client-Anwendungen zu den Servern zu stoppen. Sie können die Quellserver im Übernahmefenster herunterfahren. Weitere Informationen finden Sie im Cloud Migration	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Factory-Implementierungsleitfaden.	
Starten Sie Instanzen für die Umstellung.	Startet alle Zielcomputer für eine bestimmte Welle im Application Migration Service im Übernahmemodus. Weitere Informationen finden Sie im Cloud Migration Factory-Implementierungsleitfaden.	Migrationsspezialist, Cloud-Administrator
Zielinstanz abrufen IPs.	Rufen Sie die IPs vier Zielinstanzen ab. Wenn das DNS-Update in Ihrer Umgebung ein manueller Prozess ist, müssten Sie die neuen IP-Adressen für alle Zielinstanzen abrufen. Weitere Informationen finden Sie im Cloud Migration Factory-Implementierungsleitfaden.	Migrationsspezialist, Cloud-Administrator
Überprüfen Sie die Verbindungen zum Zielserver.	Nachdem Sie die DNS-Einträge aktualisiert haben, stellen Sie mit dem Hostnamen eine Verbindung zu den Zielinstanzen her, um die Verbindungen zu überprüfen. Weitere Informationen finden Sie im Cloud Migration Factory-Implementierungsleitfaden.	Migrationsspezialist, Cloud-Administrator

Zugehörige Ressourcen

- Wie migriert man

- Implementierungsleitfaden für AWS Cloud Migration Factory
- Automatisierung umfangreicher Servermigrationen mit Cloud Migration Factory
- AWS Application Migration Service — Benutzerhandbuch
- AWS Migration Acceleration Program

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Richten Sie mithilfe von Amazon eine Multi-AZ-Infrastruktur für einen SQL Server Always On FCI ein FSx

Erstellt von Manish Garg (AWS), T.V.R.L.Phani Kumar Dadi (AWS), Nishad Mankar (AWS) und RAJNEESH TYAGI (AWS)

Übersicht

Wenn Sie eine große Anzahl von Microsoft SQL Server AlwaysOn-Failoverclusterinstanzen (FCIs) schnell migrieren müssen, kann Ihnen dieses Muster dabei helfen, die Bereitstellungszeit zu minimieren. Durch die Verwendung von Automatisierung und Amazon FSx for Windows File Server werden manueller Aufwand, von Menschen verursachte Fehler und der Zeitaufwand für die Bereitstellung einer großen Anzahl von Clustern reduziert.

Dieses Muster richtet die Infrastruktur für SQL Server FCIs in einer Multi-Availability Zone (Multi-AZ) -Bereitstellung auf Amazon Web Services (AWS) ein. Die Bereitstellung der für diese Infrastruktur erforderlichen AWS-Services wird mithilfe von CloudFormationAWS-Vorlagen automatisiert. Die Installation von SQL Server und die Erstellung von Clusterknoten auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance werden mithilfe von PowerShell Befehlen durchgeführt.

Diese Lösung verwendet ein hochverfügbares Multi-AZ Amazon FSx for Windows-Dateisystem als gemeinsamen Zeugen für die Speicherung der SQL Server-Datenbankdateien. Das FSx Amazon-Dateisystem und EC2 Windows-Instances, die SQL Server hosten, sind mit derselben AWS Directory Service for Microsoft Active Directory-Domäne (AWS Managed Microsoft AD) verknüpft.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein AWS-Benutzer mit ausreichenden Berechtigungen zur Bereitstellung von Ressourcen mithilfe von CloudFormation AWS-Vorlagen
- AWS Directory Service für Microsoft Active Directory
- Anmeldeinformationen in AWS Secrets Manager zur Authentifizierung bei AWS Managed Microsoft AD in einem Schlüssel-Wert-Paar:
  - `ADDomainName`: <Domain Name>
  - `ADDomainJoinUserName`: <Domain Username>

- `ADDomainJoinPassword`: <Domain User Password>
- `TargetOU`: <Target OU Value>

> **Note**
>
> Sie verwenden denselben Schlüsselnamen in der AWS Systems Manager Manager-Automatisierung für die AWS Managed Microsoft AD-Join-Aktivität.

- SQL Server-Mediendateien für die SQL Server-Installation und die Erstellung von Windows-Service- oder Domänenkonten, die bei der Clustererstellung verwendet werden
- Eine virtuelle private Cloud (VPC) mit zwei öffentlichen Subnetzen in separaten Availability Zones, zwei privaten Subnetzen in den Availability Zones, einem Internet-Gateway, NAT-Gateways, Routentabellenzuordnungen und einem Jump-Server

Produktversionen

- Windows Server 2012 R2 und Microsoft SQL Server 2016

Architektur

Quelltechnologie-Stack

- Lokaler SQL Server mit FCIs Verwendung eines gemeinsam genutzten Laufwerks

Zieltechnologie-Stack

- EC2 AWS-Instanzen
- Amazon FSx für Windows-Dateiserver
- Runbook zur AWS Systems Manager Automation
- Netzwerkkonfigurationen (VPC, Subnetze, Internet-Gateway, NAT-Gateways, Jump-Server, Sicherheitsgruppen)
- AWS Secrets Manager
- AWS Managed Microsoft AD
- Amazon EventBridge
- AWS Identity and Access Management (IAM)

Zielarchitektur

Das folgende Diagramm zeigt ein AWS-Konto in einer einzelnen AWS-Region mit einer VPC, die zwei Availability Zones umfasst, zwei öffentliche Subnetze mit NAT-Gateways, einem Jump-Server im ersten öffentlichen Subnetz, zwei privaten Subnetzen mit jeweils einer EC2 Instance für einen SQL Server-Knoten in einer Knotensicherheitsgruppe und einem FSx Amazon-Dateisystem, das eine Verbindung zu jedem der SQL Server-Knoten herstellt. AWS Directory Service, Amazon EventBridge, AWS Secrets Manager und AWS Systems Manager sind ebenfalls enthalten.

Automatisierung und Skalierung

- Sie können AWS Systems Manager verwenden, um AWS Managed Microsoft AD beizutreten und die SQL Server-Installation durchzuführen.

Tools

AWS-Services

- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.
- AWS Directory Service bietet mehrere Möglichkeiten, Microsoft Active Directory (AD) mit anderen AWS-Services wie Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS) für SQL Server und Amazon FSx für Windows File Server zu verwenden.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS-Lambda-Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen AWS-Konten.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.

- AWS Secrets Manager hilft Ihnen dabei, hartcodierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Geheimnis programmgesteuert abzurufen.
- AWS Systems Manager unterstützt Sie bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der AWS-Cloud ausgeführt werden. Es vereinfacht das Anwendungs- und Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme und hilft Ihnen, Ihre AWS-Ressourcen sicher und skalierbar zu verwalten.

Andere Tools

- PowerShellist ein Automatisierungs- und Konfigurationsverwaltungsprogramm von Microsoft, das unter Windows, Linux und macOS läuft. Dieses Muster verwendet PowerShell Skripts.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub aws-windows-failover-cluster-automation verfügbar.

Bewährte Methoden

- Die IAM-Rollen, die für die Bereitstellung dieser Lösung verwendet werden, sollten dem Prinzip der geringsten Rechte entsprechen. Weitere Informationen finden Sie in der IAM-Dokumentation.
- Folgen Sie den CloudFormation bewährten Methoden von AWS.

Epen

Stellen Sie die Infrastruktur bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Systems Manager CloudFormation Manager-Stack bereit.	1. Melden Sie sich bei Ihrem AWS-Konto an und öffnen Sie die AWS-Manag ementkonsole. 2. Navigieren Sie zur CloudFormation Konsole und erstellen Sie den	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Systems Manager CloudFormation Manager-Stack, indem Sie die `ssm.yaml` Vorlage hochladen. Geben Sie Werte für die folgenden Parameter an: • StateUnJoinAssociationLoggingBucketName— Geben Sie einen Namen für den S3-Bucket an, den die Vorlage zu Protokollierungszwecken erstellt. • SSMAssociationADUnjoinName — Geben Sie einen Namen für die `AWS::SSM::Association` Ressource ein. • SSMAutomationDocumentName— Geben Sie einen Namen für das Systems Manager Automation-Runbook ein. • EventBridgeName— Geben Sie einen Namen für den EventBridge Event-Bus ein. 3. Stellen Sie den Systems Manager CloudFormation Manager-Stack bereit, indem Sie die `ssm.yaml` CloudFormation Vorlage starten. Die Vorlage erstellt	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	das Systems Manager Atomation Runbook, das initiiert wird, wenn eine neue EC2 Instanz mit dem Tag gestartet wird. `ADJoined: FSXADD` Das Automation-Runbook fügt die Instance dem AWS Managed Microsoft AD-Verzeichnis hinzu.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Infrastruktur-Stack bereit.	Erstellen Sie nach erfolgreicher Bereitstellung des Systems Manager `infra` Manager-Stacks den Stack, der EC2 Instanzknoten, Sicherheitsgruppen, das Dateisystem Amazon FSx for Windows File Server und die IAM-Rolle umfasst. 1. Navigieren Sie zur CloudFormation Konsole und starten Sie die `infra-cf.yaml` Vorlage. Um diesen Stack bereitzustellen, sind die folgenden Parameter erforderlich: • `ActiveDirectoryId` — ID für AWS Managed Microsoft AD • `ADDnsIpAddresses1` — Primäre DNS-IP-Adresse von AWS Managed Microsoft AD • `ADDnsIpAddresses2` — Sekundäre DNS-IP-Adresse von AWS Managed Microsoft AD • `FSxSecurityGroupName` — Name der FSx	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon-Sicherheits gruppe • `FSxWindowsFileSystemName` — Name des FSx Amazon-Laufwerks • `ImageID`— ID des Windows 2012 R2-Basisimages oder Amazon Machine Image (AMI), das zur Erstellung des SQL Server-Instanzknotens verwendet wurde • `KeyPairName` — Schlüssel-Wert-Paar, das für den Zugriff an die EC2 Instanzknoten angehängt werden soll • `Node1SecurityGroupName` — Name der ersten Knoten-Sicherheitsgruppe • `Node2SecurityGroupName` — Name der Sicherheitsgruppe für den zweiten Knoten • `OUSecretName` — Name des Geheimnisses, das die AWS Managed Microsoft AD-Informationen enthält • `PrivateSubnet1` — ID des ersten privaten Subnetzes	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `PrivateSubnet2` — ID des zweiten privaten Subnetzes • `SqlFSxFCIName` — Name des Tags, das auf die primären und sekundären Knoten und auf Amazon angewendet wurde FSx. • `SqlFSxServerNetBIOSName1` — Name des primären EC2 Instance-Knotens (maximal 15 Zeichen) • `SqlFSxServerNetBIOSName2` — Name des sekundären EC2 Instanzknotens (maximal 15 Zeichen) • `VPC`— VPC-ID • `WorkloadInstanceType` — Art der Instanz EC2 Stellen Sie den `infra` Stack bereit. Der Stapel erstellt alle Infrastru kturkomponenten, die für die Einrichtung von Windows SQL Server FCI erforderlich sind. 2. Nachdem die EC2 Instanzknoten gestartet wurden, wird das Systems	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Manager Automation-Dokument aufgerufen, um diese Instances mit AWS Managed Microsoft AD zu verbinden. Sie können den Fortschritt auf der Automationsseite der Systems Manager Manager-Konsole verfolgen .	

Richten Sie den Windows SQL Server Always On FCI ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie die Windows-Tools.	1. Melden Sie sich bei der primären EC2 Instanz an, bei der es sich um Knoten 1 handelt. Führen Sie das folgende PowerShell Skript aus, um die Windows-Funktionen (Active Directory und FCI Tools) zu installieren.
	`Install-WindowsFeature -Name RSAT-AD-Powershell,Failover-Clustering -IncludeManagementTools`
	`Install-WindowsFeature -Name RSAT-Clustering,RSAT-ADDS-Tools,RSAT-AD-Powershell,RSAT-DHCP,RSAT-DNS-Server`
		AWS DevOps, DevOps Ingenieur, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Melden Sie sich bei der sekundären EC2 Instanz an, bei der es sich um Knoten 2 handelt, und führen Sie dasselbe Skript aus, um Funktionen auf Knoten 2 zu aktivieren.	
Stellen Sie die Cluster-Computerobjekte in den Active Directory-Domänendiensten vorab bereit.	Folgen Sie den Anweisungen in der Windows Server-Dokumentation, um das Clusternamenobjekt (CNO) in den Active Directory-Domänendiensten (AD DS) und ein virtuelles Computerobjekt (VCO) für eine Clusterrolle vorab bereitzustellen.	AWS DevOps, DBA, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das WSFC.	Gehen Sie wie folgt vor, um den Windows Server Failover Clustering (WSFC) -Cluster zu erstellen: 1. Melden Sie sich bei der primären EC2 Instanz an, bei der es sich um Knoten 1 handelt. Führen Sie den folgenden Code aus, um die FSx Amazon-Dateifreigabe zu erstellen und vollen Zugriff auf das aufgeführte AD-Servicekonto zu gewähren. `Invoke-Command -ComputerName "<FSx Windows Remote PowerShell Endpoint>" -ConfigurationName FSxRemoteAdmin -scriptblock { New-FSxSmbShare -Name "SQLDB" -Path "D:\share" -Description "SQL Databases Share" -ContinuouslyAvailable $true -FolderEnumerationMode AccessBased -EncryptData $true grant-fsxsmbshareaccess -name SQLDB -AccountName "<domain\user>" -accessRight Full }`	AWS DevOps, DBA, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Mit diesem Befehl wird auch die kontinuierlich verfügbare Dateifreigabe (CA) erstellt, die für die Verwendung durch Microsoft SQL Server optimiert ist. 2. Führen Sie den folgenden Befehl aus, um den Failovercluster auf der primären Instanz (Knoten 1) zu erstellen. `New-Cluster -Name <CNO Name> -Node <Node1 Name>, <Node2 Name> -StaticAddress <Node1 Secondary Private IP>, <Node2 Secondary Private IP>` Der Befehl erfordert die folgenden Parameter: • `Name`— Der Name des Clusters (CNO) • `Node`— Die Namen der primären bzw. sekundären Knoten • `StaticAddress` — Die sekundären IP-Adressen der primären bzw. sekundären Knoten	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Important Ein Domänenadministrator oder ein regulärer Benutzer muss auf beiden Knoten über Administratorrechte verfügen, um den Windows Server Failover Clustering (WSFC) - Cluster zu erstellen. Andernfalls schlägt der vorherige Befehl fehl und gibt die Meldung, zurück. `You do not have administrator privilege on servers` 3. Führen Sie nach der Erstellung des Clusters den folgenden Befehl aus, um den File Share Witness anzuhängen. `Set-ClusterQuorum -FileShareWitness \ \<FSx Windows Remote PowerShell Endpoint> \share\witness`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den SQL Server-Failover-Cluster.	Nachdem der WSFC-Cluster eingerichtet ist, installieren Sie den SQL Server-Cluster auf der primären Instanz (node1). 1. Erstellen Sie im Laufwerk T auf beiden Knoten Ordner `tempdb`. `log` Die Ordner werden in den PowerShell Befehlen verwendet. 2. Nachdem Sie die SQL Server-Mediendateien für die SQL Server-Installation auf beiden Knoten kopiert haben, führen Sie den folgenden PowerShell Befehl auf Knoten 1 aus, um SQL Server auf Knoten 1 zu installieren. `D:\setup.exe /Q ` `/ACTION=InstallFailoverCluster ` `/IACCEPTSQLSERVERLICENSETERMS ` `/FEATURES="SQL,IS,BC,Conn" ` `/INSTALLSHAREDDIR="C:\Program Files\Microsoft SQL Server” ` `/INSTALLSHAREDWOWDIR="C:\Program Files (x86)\Microsoft SQL Server" ` `/RSINSTALLMODE="FilesOnlyMode" `	AWS DevOps, DBA, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`/INSTANCEID="MSSQLSERVER" ` `/INSTANCENAME="MSSQLSERVER" ` `/FAILOVERCLUSTERGROUP="SQL Server (MSSQLSERVER)" ` `/FAILOVERCLUSTERIPADDRESSES="IPv4;<2nd Sec Private Ip node1>;Cluster Network 1;<subnet mask>" ` `/FAILOVERCLUSTERNETWORKNAME="<Fail over cluster Network Name>" ` `/INSTANCEDIR="C:\Program Files\Microsoft SQL Server" ` `/ENU="True" ` `/ERRORREPORTING=0 ` `/SQMREPORTING=0 ` `/SAPWD="<Domain User password>" ` `/SQLCOLLATION="SQL_Latin1_General_CP1_CI_AS" ` `/SQLSYSADMINACCOUNTS="<domain\username>" ` `/SQLSVCACCOUNT="<domain\username>" /SQLSVCPASSWORD="<Domain User password>" ` `/AGTSVCACCOUNT="<domain\username>" /AGTSVCPASSWORD="<Domain User password>" ` `/ISSVCACCOUNT="<domain\username>" /ISSVCPAS`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SWORD="<Domain User password>" ` /FTSVCACCOUNT="NT Service\MSSQLFDLauncher" ` /INSTALLSQLDATADIR="\\<FSX DNS name>\share\Program Files\Microsoft SQL Server" ` /SQLUSERDBDIR="\\<FSX DNS name>\share\data" ` /SQLUSERDBLOGDIR="\\<FSX DNS name>\share\log" ` /SQLTEMPDBDIR="T:\tempdb" ` /SQLTEMPDBLOGDIR="T:\log" ` /SQLBACKUPDIR="\\<FSX DNS name>\share\SQLBackup" ` /SkipRules=Cluster_VerifyForErrors ` /INDICATEPROGRESS	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie dem Cluster einen sekundären Knoten hinzu.	Führen Sie den folgenden PowerShell Befehl aus, um SQL Server zum sekundären Knoten (Knoten 2) hinzuzufügen. `D:\setup.exe /Q ` `/ACTION=AddNode ` `/IACCEPTSQLSERVERLICENSETERMS ` `/INSTANCENAME="MSSQLSERVER" ` `/FAILOVERCLUSTERGROUP="SQL Server (MSSQLSERVER)" ` `/FAILOVERCLUSTERIPADDRESSES="IPv4;<2nd Sec Private Ip node2>;Cluster Network 2;<subnet mask>" ` `/FAILOVERCLUSTERNETWORKNAME="<Fail over cluster Network Name>" ` `/CONFIRMIPDEPENDENCYCHANGE=1 ` `/SQLSVCACCOUNT="<domain\username>" /SQLSVCPASSWORD="<Domain User password>" ` `/AGTSVCACCOUNT="domain\username>" /AGTSVCPASSWORD="<Domain User password>" ` `/FTSVCACCOUNT="NT Service\MSSQLFDLauncher" ` `/SkipRules=Cluster_VerifyForErrors `	AWS DevOps, DBA, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`/INDICATEPROGRESS`	
Testen Sie den SQL Server FCI.	1. Starten Sie auf der Windows-Instanz für einen der Knoten in den Verwaltungstools den Failovercluster-Manager. 2. Navigieren Sie zu Knoten und vergewissern Sie sich, dass der Knotenstatus Status Running lautet. 3. Wählen Sie Rollen aus, öffnen Sie das Kontextmenü (mit der rechten Maustaste) für SQL Server (MSSQLSERVER) und wählen Sie Move and Select Node aus. 4. Nach der Knotenauswahl sollte SQL Server auf dem anderen Knoten ausgeführt werden.	DBA, Ingenieur DevOps

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen von Ressourcen.	Verwenden Sie den CloudFormation AWS-Stack -Löschvorgang, um die Ressourcen zu bereinigen: 1. Öffnen Sie die CloudFormation AWS-Konsole.	AWS DevOps, DBA, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie auf der Seite Stacks den `infra` Stack aus. Der Stack muss aktuell ausgeführt werden. 3. Wählen Sie im Stack-Detailbereich Delete (Löschen) aus. 4. Wählen Sie Delete stack (Stack löschen) aus, wenn Sie dazu aufgefordert werden. 5. Wiederholen Sie die Schritte 2 bis 4 für den `ssm` Stapel. Nachdem das Löschen des Stacks abgeschlossen ist, befinden sich die Stapel im `DELETE_COMPLETE` Status. Stapel im `DELETE_COMPLETE` Status werden standardmäßig nicht in der CloudFormation Konsole angezeigt. Um gelöschte Stacks anzuzeigen, müssen Sie den Stack-Ansichtsfilter ändern, wie unter Gelöschte Stacks auf der CloudFormation AWS-Konsole anzeigen beschrieben. Wenn das Löschen fehlgeschlagen ist, befindet sich ein Stack im `DELETE_FAILED`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Status. Lösungen finden Sie in der CloudFormation Dokumentation unter Fehler beim Löschen des Stacks.	

Fehlerbehebung

Problem	Lösung
CloudFormation AWS-Vorlagenfehler	Wenn die CloudFormation Vorlage während der Bereitstellung fehlschlägt, gehen Sie wie folgt vor: 1. Öffnen Sie die CloudFormation AWS-Konsole. 2. Wählen Sie auf der Seite Stacks in der CloudFormation Konsole den Stack aus. 3. Wählen Sie Ereignisse und überprüfen Sie den Stack-Status.
Fehler beim Verbinden mit AWS Managed Microsoft AD	Gehen Sie wie folgt vor, um die Verbindungsprobleme zu beheben: 1. Öffnen Sie die Systems Manager-Konsole. 2. Wählen Sie die Bereitstellungsregion aus. 3. Wählen Sie im linken Bereich Automation aus und suchen Sie das ausgefallene Automatisierungs-Runbook. 4. Öffnen Sie das Automatisierungs-Runbook und suchen Sie nach dem Ausführungsstatus und den Ausführungsschritten. 5. Untersuchen Sie die Details des fehlgeschlagenen Schritts, um den genauen Fehler oder Misserfolg zu ermitteln.

Zugehörige Ressourcen

- Vereinfachen Sie Ihre Hochverfügbarkeitsbereitstellungen von Microsoft SQL Server mit Amazon FSx for Windows File Server
- FSx Für Windows File Server mit Microsoft SQL Server verwenden

Verwenden Sie BMC Discovery-Abfragen, um Migrationsdaten für die Migrationsplanung zu extrahieren

Erstellt von Ben Tailor-Hamblin (AWS), Simon Cunningham (AWS), Emma Baldry (AWS) und Shabnam Khan (AWS)

Übersicht

Dieses Handbuch enthält Abfragebeispiele und Schritte, mit denen Sie mithilfe von BMC Discovery Daten aus Ihrer lokalen Infrastruktur und Ihren Anwendungen extrahieren können. Das Muster zeigt Ihnen, wie Sie BMC Discovery-Abfragen verwenden, um Ihre Infrastruktur zu scannen und Software-, Service- und Abhängigkeitsinformationen zu extrahieren. Die extrahierten Daten werden für die Bewertungs- und Mobilisierungsphasen einer groß angelegten Migration zur Amazon Web Services (AWS) Cloud benötigt. Sie können diese Daten verwenden, um wichtige Entscheidungen darüber zu treffen, welche Anwendungen im Rahmen Ihres Migrationsplans gemeinsam migriert werden sollen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Lizenz für BMC Discovery (ehemals BMC ADDM) oder die SaaS-Version (Software as a Service) von BMC Helix Discovery
- On-Premise- oder SaaS-Version von BMC Discovery, installiert

> **Note**
>
> Bei lokalen Versionen von BMC Discovery müssen Sie die Anwendung in einem Client-Netzwerk mit Zugriff auf alle Netzwerk- und Servergeräte installieren, die für eine Migration zwischen mehreren Rechenzentren in Frage kommen. Der Zugriff auf das Client-Netzwerk muss gemäß den Installationsanweisungen der Anwendung gewährt werden. Wenn das Scannen von Windows Server-Informationen erforderlich ist, müssen Sie ein Windows-Proxy-Manager-Gerät im Netzwerk einrichten.

- Netzwerkzugriff, damit die Anwendung Geräte in mehreren Rechenzentren scannen kann, wenn Sie BMC Helix Discovery verwenden

Versionen der Produkte

- BMC Discovery 22.2 (12.5)

- BMC Discovery 22,1 (12,4)
- BMC Discovery 21,3 (12,3)
- BMC Discovery 21,05 (12,2)
- BMC Discovery 20,08 (12,1)
- BMC Discovery 20,02 (12,0)
- BMC Discovery 11.3
- BMC Discovery 11.2
- BMC Discovery 11.1
- BMC Discovery 11.0
- BMC Atrium Discovery 10.2
- BMC Atrium Discovery 10.1
- BMC Atrium Discovery 10.0

Architektur

Das folgende Diagramm zeigt, wie Vermögensverwalter BMC Discovery-Abfragen verwenden können, um BMC-modellierte Anwendungen sowohl in SaaS- als auch in lokalen Umgebungen zu scannen.

Das Diagramm zeigt den folgenden Arbeitsablauf: Ein Asset Manager verwendet BMC Discovery oder BMC Helix Discovery, um Datenbank- und Softwareinstanzen zu scannen, die auf virtuellen Servern laufen, die auf mehreren physischen Servern gehostet werden. Das Tool kann Anwendungen mit Komponenten modellieren, die sich über mehrere virtuelle und physische Server erstrecken.

Technologie-Stack

- BMC Discovery
- BMC Helix Discovery

Tools

- BMC Discovery ist ein Tool zur Erkennung von Rechenzentren, mit dem Sie Ihr Rechenzentrum automatisch ermitteln können.

- BMC Helix Discovery ist ein SaaS-basiertes Erkennungs- und Abhängigkeitsmodellierungssystem, mit dem Sie Ihre Datenbestände und deren Abhängigkeiten dynamisch modellieren können.

Bewährte Methoden

Es ist eine bewährte Methode, Anwendungs-, Abhängigkeits- und Infrastrukturdaten abzubilden, wenn Sie in die Cloud migrieren. Die Zuordnung hilft Ihnen dabei, die Komplexität Ihrer aktuellen Umgebung und die Abhängigkeiten zwischen den verschiedenen Komponenten zu verstehen.

Die Inventarinformationen, die diese Abfragen liefern, sind aus mehreren Gründen wichtig:

1. Planung — Wenn Sie die Abhängigkeiten zwischen den Komponenten verstehen, können Sie den Migrationsprozess effektiver planen. Beispielsweise müssen Sie möglicherweise zuerst bestimmte Komponenten migrieren, um sicherzustellen, dass andere erfolgreich migriert werden können.
2. Risikobewertung — Durch die Zuordnung der Abhängigkeiten zwischen den Komponenten können Sie potenzielle Risiken oder Probleme identifizieren, die während des Migrationsprozesses auftreten können. Sie könnten beispielsweise feststellen, dass bestimmte Komponenten auf veralteten oder nicht unterstützten Technologien basieren, was zu Problemen in der Cloud führen könnte.
3. Cloud-Architektur — Die Zuordnung Ihrer Anwendungs- und Infrastrukturdaten kann Ihnen auch dabei helfen, eine geeignete Cloud-Architektur zu entwerfen, die Ihren organisatorischen Anforderungen entspricht. Beispielsweise müssen Sie möglicherweise eine mehrstufige Architektur entwerfen, um Hochverfügbarkeits- oder Skalierbarkeitsanforderungen zu erfüllen.

Insgesamt ist die Zuordnung von Anwendungs-, Abhängigkeits- und Infrastrukturdaten ein entscheidender Schritt im Cloud-Migrationsprozess. Die Kartierung kann Ihnen helfen, Ihre aktuelle Umgebung besser zu verstehen, potenzielle Probleme oder Risiken zu identifizieren und eine geeignete Cloud-Architektur zu entwerfen.

Epen

Identifizieren und bewerten Sie Discovery-Tools

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die ITSM-Besitzer.	Identifizieren Sie die Eigentümer des IT Service	Leiter der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Management (ITSM) (in der Regel, indem Sie sich an die operativen Support-Teams wenden).	
Überprüfen Sie CMDB.	Identifizieren Sie die Anzahl der Konfigurationsmanagement-Datenbanken (CMDBs), die Asset-Informationen enthalten, und identifizieren Sie dann die Quellen dieser Informationen.	Leiter der Migration
Identifizieren Sie Discovery-Tools und prüfen Sie, ob BMC Discovery verwendet wird.	Wenn Ihr Unternehmen BMC Discovery verwendet, um Daten über Ihre Umgebung an das CMDB-Tool zu senden, überprüfen Sie den Umfang und die Reichweite der Scans. Überprüfen Sie beispielsweise, ob BMC Discovery alle Rechenzentren scannt und ob sich die Access-Server in Perimeterzonen befinden.	Leiter der Migration
Prüfen Sie den Stand der Anwendungsmodellierung.	Prüfen Sie, ob Anwendungen in BMC Discovery modelliert wurden. Wenn nicht, empfehlen Sie die Verwendung des BMC Discovery-Tools, um zu modellieren, welche laufenden Softwareinstanzen eine Anwendung und einen Geschäftsdienst bereitstellen.	Migrationsingenieur, Migrationsleiter

Extrahieren Sie Infrastrukturdaten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Extrahieren Sie Daten auf physischen und virtuellen Servern.	Um Daten auf den von BMC Discovery gescannten physischen und virtuellen Servern zu extrahieren, verwenden Sie Query Builder, um die folgende Abfrage auszuführen: `search Host show key as 'Serverid', virtual, name as 'HOSTNAME', os_type as 'osName', os_version as 'OS Version', num_logical_processors as 'Logical Processor Counts', cores_per_processor as 'Cores per Processor', logical_ram as 'Logical RAM', #Consumer:StorageUse:Provider:DiskDrive.size as 'Size'` **Note** Sie können die extrahierten Daten verwenden, um die geeigneten Instanzgrößen für die Migration zu ermitteln.	Migrationsingenieur, Migrationsleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Extrahieren Sie Daten aus modellierten Anwendungen.	Wenn Ihre Anwendungen in BMC Discovery modelliert werden, können Sie Daten über die Server extrahieren, auf denen die Anwendung ssoftware ausgeführt wird. Um die Servernamen abzurufen, verwenden Sie Query Builder, um die folgenden Abfragen auszuführen: `search SoftwareInstance show key as 'ApplicationID', #RunningSoftware:HostedSoftware:Host:Host.key as 'ReferenceID', type, name` **Note** Anwendungen werden in BMC Discovery anhand einer Sammlung laufender Softwareinstanzen modelliert. Die Anwendung ist von allen Servern abhängig, auf denen die Anwendung ssoftware ausgeführt wird.	Besitzer der BMC Discovery-Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Extrahieren Sie Daten aus Datenbanken.	Um eine Liste aller gescannten Datenbanken und der Server, auf denen diese Datenbanken laufen, zu erhalten, verwenden Sie Query Builder, um die folgende Abfrage auszuführen: `search Database show key as 'Key', name, type as 'Source Engine Type', #Detail:Detail:ElementWithDetail:SoftwareInstance.name as 'Software Instance', #Detail:Detail:ElementWithDetail:SoftwareInstance.product_version as 'Product Version', #Detail:Detail:ElementWithDetail:SoftwareInstance.edition as 'Edition', #Detail:Detail:ElementWithDetail:SoftwareInstance.#RunningSoftware:HostedSoftware:Host:Host.key as 'ServerID'`	Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Extrahieren Sie Daten zur Serverkommunikation.	Um Informationen über die gesamte Netzwerkkommunikation zwischen Servern abzurufen, die von BMC Discovery aus historischen Netzwerkkommunikationsprotokollen gesammelt wurden, verwenden Sie Query Builder, um die folgende Abfrage auszuführen: `search Host TRAVERSE InferredElement:Inference:Associate:DiscoveryAccess TRAVERSE DiscoveryAccess:DiscoveryAccessResult:DiscoveryResult:NetworkConnectionList TRAVERSE List:List:Member:DiscoveredNetworkConnection PROCESS WITH networkConnectionInfo`	Besitzer der BMC Discovery-Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Extrahieren Sie Daten zur Anwendungserkennung.	Um Informationen zu Anwendungsabhängigkeiten zu erhalten, verwenden Sie Query Builder, um die folgende Abfrage auszuführen: `search SoftwareInstance show key as 'SRC App ID', #Dependant:Dependency:DependedUpon:SoftwareInstance.key as 'DEST App ID'`	Besitzer der BMC Discovery-Anwendung
Extrahieren Sie Daten zu Unternehmensdiensten.	Um Daten zu Unternehmensdiensten zu extrahieren, die von Hosts bereitgestellt werden, verwenden Sie Query Builder, um die folgende Abfrage auszuführen: `search Host show name, #Host:HostedSoftware:AggregateSoftware:BusinessService.name as 'Name'`	Besitzer der BMC Discovery-Anwendung

Fehlerbehebung

Problem	Lösung
Eine Abfrage kann nicht ausgeführt werden oder enthält nicht aufgefüllte Spalten.	Überprüfen Sie die Asset-Datensätze in BMC Discovery und ermitteln Sie, welche Felder Sie benötigen. Ersetzen Sie dann diese Felder in der Abfrage mithilfe des Abfrage-Generators.

Problem	Lösung
Die Details einer abhängigen Anlage werden nicht ausgefüllt.	Dies ist wahrscheinlich auf Zugriffsberechtigungen oder Netzwerkkonnektivität zurückzuführen. Das Discovery-Tool verfügt möglicherweise nicht über die erforderlichen Berechtigungen für den Zugriff auf bestimmte Ressourcen, insbesondere wenn sie sich in verschiedenen Netzwerken oder in unterschiedlichen Umgebungen befinden. Wir empfehlen Ihnen, eng mit Experten für die Datenermittlung zusammenzuarbeiten, um sicherzustellen, dass alle relevanten Ressourcen identifiziert werden.

Zugehörige Ressourcen

Referenzen

- Anspruch auf BMC Discovery-Lizenzierung (BMC-Dokumentation)
- Funktionen und Komponenten von BMC Discovery (BMC-Dokumentation)
- BMC Discovery-Benutzerhandbuch (BMC-Dokumentation)
- Suchen nach Daten (auf BMC Discovery) (BMC-Dokumentation)
- Portfolioerkennung und -analyse für die Migration (AWS Prescriptive Guidance)

Anleitungen und Videos

- BMC Discovery: Webinar — Bewährte Methoden für Berichtsabfragen (Teil 1) (YouTube)

Umziehen

Themen

- Migrieren Sie eine Amazon RDS for Oracle Oracle-Datenbank zu einer anderen AWS-Konto und AWS-Region verwenden Sie sie AWS DMS für die laufende Replikation
- Migrieren Sie VMware SDDC mithilfe von VMware HCX zur Cloud auf AWS VMware
- Migrieren Sie eine Amazon RDS-DB-Instance zu einer anderen VPC oder einem anderen Konto
- Migrieren Sie eine Amazon RDS for Oracle DB-Instance zu einer anderen VPC
- Migrieren Sie einen Amazon Redshift Redshift-Cluster in eine AWS-Region in China
- Transportieren Sie PostgreSQL-Datenbanken zwischen zwei Amazon RDS-DB-Instances mithilfe von pg_transport

Migrieren Sie eine Amazon RDS for Oracle Oracle-Datenbank zu einer anderen AWS-Konto und AWS-Region verwenden Sie sie AWS DMS für die laufende Replikation

Erstellt von Durga Prasad Cheepuri (AWS) und Eduardo Valentim (AWS)

Übersicht

> **Warning**
>
> IAM-Benutzer verfügen über langfristige Anmeldeinformationen, was ein Sicherheitsrisiko darstellt. Um dieses Risiko zu minimieren, empfehlen wir, diesen Benutzern nur die Berechtigungen zu gewähren, die sie für die Ausführung der Aufgabe benötigen, und diese Benutzer zu entfernen, wenn sie nicht mehr benötigt werden.

Dieses Muster führt Sie durch die Schritte zur Migration einer Quelldatenbank von Amazon Relational Database Service (Amazon RDS) für Oracle zu einer anderen AWS-Konto und. AWS-Region Das Muster verwendet einen DB-Snapshot für eine einmalige vollständige Datenladung und aktiviert AWS Database Migration Service (AWS DMS) für die fortlaufende Replikation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine aktive Datenbank AWS-Konto , die die Amazon RDS for Oracle Oracle-Quelldatenbank enthält, die mit einem anderen Schlüssel AWS Key Management Service (AWS KMS) verschlüsselt wurde
- Aktiv AWS-Konto in einer anderen Datenbank als AWS-Region der Quelldatenbank, die für die Amazon RDS for Oracle Oracle-Zieldatenbank verwendet werden soll
- Virtual Private Cloud (VPC) -Peering zwischen Quelle und Ziel VPCs
- Vertrautheit mit der Verwendung einer Oracle-Datenbank als Quelle für AWS DMS
- Vertrautheit mit der Verwendung einer Oracle-Datenbank als Ziel für AWS DMS

Produktversionen

- Oracle-Versionen 11g (Versionen 11.2.0.3.v1 und höher) und bis zu 12.2 und 18c. Die aktuelle Liste der unterstützten Versionen und Editionen finden Sie in der Dokumentation unter Verwenden

einer Oracle-Datenbank als Quelle für AWS DMS und mit Verwenden einer Oracle-Datenbank als Ziel für. AWS DMS AWS Informationen zu Oracle-Versionen, die von Amazon RDS unterstützt werden, finden Sie unter Oracle auf Amazon RDS.

Architektur

Quell- und Zieltechnologie-Stacks

- Amazon RDS for Oracle Oracle-DB-Instance

Architektur für fortlaufende Replikation

Tools

Tools, die für das einmalige vollständige Laden von Daten verwendet werden

- Amazon Relational Database Service (Amazon RDS) erstellt einen Speicher-Volume-Snapshot Ihrer DB-Instance und sichert dabei die gesamte DB-Instance und nicht nur einzelne Datenbanken. Beim Erstellen eines DB-Snapshots wählen Sie die DB-Instance aus, die gesichert werden soll, und benennen den DB-Snapshot, damit Sie später mit diesem eine Wiederherstellung ausführen können. Die Zeit, die für die Erstellung eines Snapshots benötigt wird, hängt von der Größe Ihrer Datenbanken ab. Da der Snapshot das gesamte Speichervolume umfasst, wirkt sich die Größe von Dateien, wie z. B. temporäre Dateien, auch auf die Zeit aus, die zum Erstellen des Snapshots benötigt wird. Weitere Informationen zur Verwendung von DB-Snapshots finden Sie unter Erstellen eines DB-Snapshots in der Amazon RDS-Dokumentation.
- AWS Key Management Service (AWS KMS) erstellt einen Schlüssel für die Amazon RDS-Verschlüsselung. Wenn Sie eine verschlüsselte DB-Instance erstellen, können Sie auch die AWS KMSSchlüssel-ID für Ihren Verschlüsselungsschlüssel angeben. Wenn Sie keine AWS KMSSchlüssel-ID angeben, verwendet Amazon RDS Ihren Standard-Verschlüsselungsschlüssel für Ihre neue DB-Instance. AWS KMSerstellt Ihren Standard-Verschlüsselungsschlüssel für Ihre AWS-Konto. Ihr AWS-Konto hat für jeden einen anderen Standard-Verschlüsselungsschlüssel AWS-Region. Für dieses Muster sollte die Amazon RDS-DB-Instance mit dem nicht standardmäßigen AWS KMSSchlüssel verschlüsselt werden. Weitere Informationen zur Verwendung von AWS KMSSchlüsseln für die Amazon RDS-Verschlüsselung finden Sie unter Verschlüsseln von Amazon RDS-Ressourcen in der Amazon RDS-Dokumentation.

Tools, die für die laufende Replikation verwendet werden

- AWS Database Migration Service (AWS DMS) wird verwendet, um laufende Änderungen zu replizieren und die Quell- und Zieldatenbank synchron zu halten. Weitere Informationen zur Verwendung AWS DMS für die laufende Replikation finden Sie in der AWS DMS Dokumentation unter Arbeiten mit einer AWS DMS Replikationsinstanz.

Epen

Konfiguriere deine Quelle AWS-Konto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Oracle-DB-Quellinstanz vor.	Lassen Sie die Amazon RDS for Oracle DB-Instance im ARCHIVELOG-Modus laufen und legen Sie den Aufbewahrungszeitraum fest. Einzelheiten finden Sie unter Arbeiten mit einer AWS verwalteten Oracle-Datenbank als Quelle für. AWS DMS	DBA
Legen Sie die zusätzliche Protokollierung für die Oracle-DB-Quellinstanz fest.	Legen Sie die zusätzliche Protokollierung auf Datenbank- und Tabellenebene für die Amazon RDS for Oracle Oracle-DB-Instance fest. Einzelheiten finden Sie unter Arbeiten mit einer AWS verwalteten Oracle-Datenbank als Quelle für. AWS DMS	DBA
Aktualisieren Sie die AWS KMS Schlüsselrichtlinie im Quellkonto.	Aktualisieren Sie die AWS KMS Schlüsselrichtlinie in der Quelle AWS-Konto , damit das Ziel AWS-Konto den verschlüsselten Amazon AWS KMS	SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	RDS-Schlüssel verwenden kann. Einzelheiten finden Sie in der AWS KMS Dokumentation.	
Erstellen Sie einen manuellen Amazon RDS-DB-Snapshot der Quell-DB-Instance.		AWS-IAM-Benutzer
Teilen Sie den manuellen, verschlüsselten Amazon RDS-Snapshot mit dem Ziel AWS-Konto.	Einzelheiten finden Sie unter Einen DB-Snapshot teilen.	AWS-IAM-Benutzer

Konfigurieren Sie Ihr Ziel AWS-Konto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie eine Richtlinie bei.	Fügen Sie im Ziel AWS-Konto dem Root-IAM-Benutzer eine AWS Identity and Access Management (IAM-) Richtlinie hinzu, damit der IAM-Benutzer mithilfe des gemeinsamen Schlüssels einen verschlüsselten DB-Snapshot kopieren kann. AWS KMS	SysAdmin
Wechseln Sie zur Quelle. AWS-Region		AWS-IAM-Benutzer
Kopieren Sie den geteilten Snapshot.	Wählen Sie in der Amazon RDS-Konsole im Bereich Snapshots die Option Für mich freigegeben und	AWS-IAM-Benutzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wählen Sie den geteilten Snapshot aus. Kopieren Sie den Snapshot in dieselbe Datenbank AWS-Region wie die Quelldatenbank, indem Sie den Amazon-Ressourcennamen (ARN) für den von der Quelldatenbank verwendeten AWS KMS Schlüssel verwenden. Einzelheiten finden Sie unter Kopieren eines DB-Snapshots.	
Wechseln Sie zum Ziel AWS-Region und erstellen Sie einen neuen AWS KMS Schlüssel.		AWS-IAM-Benutzer
Kopieren Sie den Snapshot.	Wechseln Sie zur Quelle AWS-Region. Wählen Sie auf der Amazon RDS-Konsole im Bereich Snapshots die Option Owned by Me und wählen Sie den kopierten Snapshot aus. Kopieren Sie den Snapshot auf das Ziel, AWS-Region indem Sie den AWS KMS Schlüssel für das neue Ziel AWS-Region verwenden.	AWS-IAM-Benutzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Snapshot wieder her.	Wechseln Sie zum Ziel AWS-Region. Wählen Sie auf der Amazon RDS-Konsole im Bereich Snapshots die Option Owned by Me aus. Wählen Sie den kopierten Snapshot aus und stellen Sie ihn in einer Amazon RDS for Oracle DB-Instance wieder her. Einzelheiten finden Sie unter Aus einem DB-Snapshot wiederherstellen.	AWS-IAM-Benutzer

Bereiten Sie Ihre Quelldatenbank für die laufende Replikation vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Oracle-Benutzer mit den entsprechenden Berechtigungen.	Erstellen Sie einen Oracle-Benutzer mit den erforderlichen Rechten für Oracle als Quelle für AWS DMS. Einzelheiten finden Sie in der AWS DMS Dokumentation.	DBA
Konfigurieren Sie die Quelldatenbank für Oracle LogMiner oder Oracle Binary Reader.		DBA

Bereiten Sie Ihre Zieldatenbank für die laufende Replikation vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Oracle-Benutzer mit den entsprechenden Berechtigungen.	Erstellen Sie einen Oracle-Benutzer mit den erforderlichen Rechten für Oracle als Ziel für AWS DMS. Einzelheiten finden Sie in der AWS DMS Dokumentation.	DBA

Komponenten erstellen AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Replikationsinstanz im Ziel AWS-Region.	Erstellen Sie eine Replikationsinstanz in der VPC des Ziels AWS-Region. Einzelheiten finden Sie in der AWS DMS Dokumentation.	AWS-IAM-Benutzer
Erstellen Sie Quell- und Zielendpunkte mit der erforderlichen Verschlüsselung und testen Sie Verbindungen.	Einzelheiten finden Sie in der AWS DMS Dokumentation.	DBA
Erstellen Sie Replikationsaufgaben.	1. Wählen Sie als Migrationstyp die Option Laufende Replikation aus. 2. Verwenden Sie für den Startpunkt der Change Data Capture (CDC) die Oracle-Systemänderungsnummer (SCN), als der Amazon RDS-Snapshot vollständig geladen wurde, oder den Zeitstempel, als der	IAM-Benutzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Vollladevorgang ausgeführt wurde. 3. Wählen Sie für **`TargetTablePrepMode`** DO_NOTHING. Wenn die Aufgabe LOB-Daten tabellen (Large Binary Object) enthält, wählen Sie den Modus Limitiert aus und legen Sie die maximale LOB-Größe auf die maximale Größe der LOB-Daten in der Tabelle fest. 4. Aktivieren Sie die Protokollierung. 5. Gruppieren Sie Tabellen, die über Schlüssel miteinander verknüpft sind, zu einer einzigen Aufgabe. Wenn es Tabellen mit einer großen Menge an LOB-Daten gibt und die Tabelle keine Beziehung zu anderen Tabellen hat, erstellen Sie dafür eine separate Aufgabe mit den zuvor beschriebenen LOB-Einstellungen. Einzelheiten finden Sie in der AWS DMS Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Aufgaben und überwachen Sie sie.	Einzelheiten finden Sie in der AWS DMS Dokumentation.	AWS-IAM-Benutzer
Aktivieren Sie bei Bedarf die Validierung der Aufgabe.	Beachten Sie, dass die Aktivierung der Validierung Auswirkungen auf die Leistung der Replikation hat. Einzelheiten finden Sie in der AWS DMS Dokumentation.	AWS-IAM-Benutzer

Zugehörige Ressourcen

- Änderung einer wichtigen Richtlinie
- Manuellen Amazon RDS-DB-Snapshot erstellen
- Einen manuellen Amazon RDS-DB-Snapshot teilen
- Einen Snapshot kopieren
- Wiederherstellung aus einem Amazon RDS-DB-Snapshot
- Erste Schritte mit AWS DMS
- Verwenden einer Oracle-Datenbank als Quelle für AWS DMS
- Verwendung einer Oracle-Datenbank als Ziel für AWS DMS
- AWS DMS Einrichtung mit VPC-Peering
- Wie teile ich manuelle Amazon RDS-DB-Snapshots oder DB-Cluster-Snapshots mit anderen? AWS-Konto (Artikel im AWS Knowledge Center)

Migrieren Sie VMware SDDC mithilfe von VMware HCX zur Cloud auf AWS VMware

Erstellt von Deepak Kumar (AWS)

Übersicht

> Hinweis: Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

Dieses Muster beschreibt die Verwendung von VMware Hybrid Cloud Extension (HCX) zur Migration Ihrer lokalen virtuellen Maschinen (VMs) und Anwendungen zu VMware Cloud on Amazon Web Services (AWS). Bei der Migration wird SDDC-Software (Software-Defined Data Center) der VMware Enterprise-Klasse in der AWS-Cloud verwendet, um einen optimierten Zugriff auf AWS-Services zu ermöglichen.

VMware Cloud on AWS integriert Rechen-, Speicher- und Netzwerkvirtualisierungsprodukte (vSphere, vSAN und VMware NSX) in das VMware vCenter Servermanagement, das für die Ausführung auf einer dedizierten, elastischen Bare-Metal-AWS-Infrastruktur optimiert ist. Die daraus resultierende Infrastruktur ist wartungsarm, vereinfacht und hyperkonvergiert.

Mit diesem Service können IT-Teams ihre Cloud-Ressourcen mit vertrauten Tools verwalten. VMware Weitere Informationen finden Sie auf der VMware Website unter VMware Cloud on AWS.

VMware HCX unterstützt drei Arten von Cloud-Migrationen:

- Hybridität (Rechenzentrumserweiterung): Erweiterung eines vorhandenen, lokalen VMware SDDC auf AWS, um eine Erweiterung des Platzbedarfs, On-Demand-Kapazität, eine Test-/Entwicklungsumgebung und virtuelle Desktops bereitzustellen.
- Cloud-Evakuierung (Aktualisierung der Infrastruktur im gesamten Rechenzentrum): Konsolidierung von Rechenzentren und vollständige Umstellung auf die AWS-Cloud (einschließlich der Verwaltung der Rechenzentrumszusammenlegung oder der Beendigung des Leasingvertrags).
- Anwendungsspezifische Migration: Verschieben einzelner Anwendungen in die AWS-Cloud, um spezifische Geschäftsanforderungen zu erfüllen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eröffnen Sie ein AWS-Konto (erforderlich für die VMware Cloud-SDDC-Erstellung).
- Eröffnen Sie ein Mein VMware Konto. Registrieren Sie sich bei https://my.vmware.com/web/vmware/ und füllen Sie alle Felder aus.
- Überprüfen Sie die Version von vCenter und Hosts und erfassen Sie die Anzahl der VMs. Bitten Sie nach Möglichkeit um einen RVToolsExport, um Informationen zu Ihren virtuellen Umgebungen anzuzeigen. Wir empfehlen vCenter Version 6.0 oder höher.
- Sie müssen verteilte virtuelle Switches bereitstellen, wenn Sie Rechenzentrumsnetzwerke (L2) erweitern, vMotion mithilfe von HCX testen oder Anwendungsabhängigkeiten mithilfe von vRealize Network Insight analysieren möchten.
- Wählen Sie ein konfliktfreies lokales aktuelles Management-Subnetzwerk aus, um das SDDC on Cloud on AWS zu erstellen. VMware
- Überprüfen Sie die HCX-Anforderungen, indem Sie die Voraussetzungen im HCX-Benutzerhandbuch überprüfen. VMware
- Identifizieren und gruppieren Sie VMs die Migrationswellen. Prüfen Sie VMs , ob Sie das für Tests verwenden können.
- Sammeln Sie alle Daten über den relativen Bandbreitenverbrauch, die WAN-Komprimierung und die Datenübertragungsgeschwindigkeit.

Hinweise

- VMware NSX-V oder NSX-T vor Ort sind nicht erforderlich.
- Keine zusätzlichen Kosten für HCX (es ist in VMware Cloud on AWS enthalten).

Architektur

Das folgende Diagramm zeigt die HCX-Lösung, die auf Services aus mehreren Komponenten basiert. Jede Komponente unterstützt eine bestimmte Funktion in der HCX-Lösung. Weitere Informationen zu den einzelnen HCX-Komponenten finden Sie im Blogbeitrag Migrieren von Workloads zur VMware Cloud auf AWS mit Hybrid Cloud Extension (HCX).

Quelltechnologie-Stack

- Lokal VMs und von vSphere VMware verwaltete Anwendungen

Zieltechnologie-Stack

- VMware Cloud auf AWS

Tools

- VMware HCX — VMware HCX ist ein Tool, mit dem Sie Ihre Anwendungen und Workloads zwischen Rechenzentren und Cloud-Umgebungen migrieren können. Es ist in VMware Cloud on AWS enthalten.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie eine Migration sstrategie.	Entscheiden Sie, ob Sie Ihr Rechenzentrum erweitern (Hybridität), alle Ihre Rechenzentren verlagern (Cloud-Evakuierung) oder bestimmte Anwendungen zu AWS verlagern möchten.	SysAdmin, Besitzer der App
Überprüfen Sie die HCX-Anforderungen.	Informationen zur Migration finden Sie im VMware HCX-Benutzerhandbuch.	SysAdmin, Besitzer der App

Migrieren Sie zur VMware Cloud auf AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie Ihre VMs PR-Anwendungen.	Weitere Informationen finden Sie in der VMware Dokumentation unter Hybridmigration mit VMware HCX.	SysAdmin, Besitzer der App

Zugehörige Ressourcen

- VMware Cloud auf AWS: Erste Schritte
- Hybride Migration mit VMware HCX
- VMware HCX-Benutzerhandbuch
- VMware Preise für Cloud on AWS
- VMware Roadmap für Cloud auf AWS

Migrieren Sie eine Amazon RDS-DB-Instance zu einer anderen VPC oder einem anderen Konto

Erstellt von Dhrubajyoti Mukherjee (AWS)

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer Amazon Relational Database Service (Amazon RDS) -DB-Instance von einer Virtual Private Cloud (VPC) zu einer anderen im selben AWS-Konto oder von einem AWS-Konto zu einem anderen AWS-Konto.

Dieses Muster ist nützlich, wenn Sie Ihre Amazon RDS-DB-Instances aus Trennungs- oder Sicherheitsgründen auf eine andere VPC oder ein anderes Konto migrieren möchten (z. B. wenn Sie Ihren Anwendungsstapel und Ihre Datenbank in unterschiedlichen Ordnern platzieren möchten VPCs).

Die Migration einer DB-Instance auf ein anderes AWS-Konto umfasst Schritte wie das Erstellen eines manuellen Snapshots, dessen gemeinsame Nutzung und das Wiederherstellen des Snapshots im Zielkonto. Dieser Vorgang kann je nach Datenbankänderungen und Transaktionsraten zeitaufwändig sein. Außerdem führt er zu Datenbankausfällen. Planen Sie die Migration daher im Voraus. Ziehen Sie eine blaue/grüne Bereitstellungsstrategie in Betracht, um Ausfallzeiten zu minimieren. Alternativ können Sie den AWS Data Migration Service (AWS DMS) testen, um die Ausfallzeiten für die Änderung zu minimieren. Dieses Muster deckt diese Option jedoch nicht ab. Weitere Informationen finden Sie in der AWS DMS-Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS Identity and Access Management (IAM) -Berechtigungen, die für die VPC, Subnetze und die Amazon RDS-Konsole erforderlich sind

Einschränkungen

- Änderungen an einer VPC führen zu einem Neustart der Datenbank, was zu Anwendungsausfällen führt. Wir empfehlen, die Migration in Zeiten geringer Spitzenzeiten durchzuführen.
- Einschränkungen bei der Migration von Amazon RDS zu einer anderen VPC:

  - Bei der DB-Instance, die Sie migrieren, muss es sich um eine einzelne Instance ohne Standby handeln. Sie darf kein Mitglied eines Clusters sein.
  - Amazon RDS darf sich nicht in mehreren Availability Zones befinden.
  - Amazon RDS darf keine Read Replicas haben.
  - Die in der Ziel-VPC erstellte Subnetzgruppe muss Subnetze aus der Availability Zone haben, in der die Quelldatenbank läuft.
- Einschränkungen bei der Migration von Amazon RDS auf ein anderes AWS-Konto:
  - Das Teilen von Snapshots, die mit dem Standard-Serviceschlüssel für Amazon RDS verschlüsselt sind, wird derzeit nicht unterstützt.

Architektur

Migration zu einer VPC im selben AWS-Konto

Das folgende Diagramm zeigt den Workflow für die Migration einer Amazon RDS-DB-Instance zu einer anderen VPC im selben AWS-Konto.

Die Schritte bestehen aus den folgenden Schritten. Ausführliche Anweisungen finden Sie im Abschnitt Epics.

1. Erstellen Sie eine DB-Subnetzgruppe in der Ziel-VPC. Eine DB-Subnetzgruppe ist eine Sammlung von Subnetzen, mit denen Sie beim Erstellen von DB-Instances eine bestimmte VPC angeben können.
2. Konfigurieren Sie die Amazon RDS-DB-Instance in der Quell-VPC für die Verwendung der neuen DB-Subnetzgruppe.
3. Wenden Sie die Änderungen an, um die Amazon RDS-Datenbank auf die Ziel-VPC zu migrieren.

Zu einem anderen AWS-Konto migrieren

Das folgende Diagramm zeigt den Arbeitsablauf für die Migration einer Amazon RDS-DB-Instance auf ein anderes AWS-Konto.

Die Schritte bestehen aus den folgenden Schritten. Ausführliche Anweisungen finden Sie im Abschnitt Epics.

1. Greifen Sie im AWS-Quellkonto auf die Amazon RDS-DB-Instance zu.
2. Erstellen Sie einen Amazon RDS-Snapshot im AWS-Quellkonto.
3. Teilen Sie den Amazon RDS-Snapshot mit dem AWS-Zielkonto.
4. Greifen Sie auf den Amazon RDS-Snapshot im AWS-Zielkonto zu.
5. Erstellen Sie eine Amazon RDS-DB-Instance im AWS-Zielkonto.

Tools

AWS-Services

- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der AWS-Cloud.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.

Bewährte Methoden

- Wenn Datenbankausfälle bei der Migration einer Amazon RDS-DB-Instance auf ein anderes Konto ein Problem darstellen, empfehlen wir Ihnen, AWS DMS zu verwenden. Dieser Service bietet Datenreplikation, was zu einer Ausfallzeit von weniger als fünf Minuten führt.

Epen

Migrieren Sie zu einer anderen VPC im selben AWS-Konto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer neuen VPC.	Erstellen Sie auf der Amazon VPC-Konsole eine neue VPC und Subnetze mit den gewünschten Eigenschaften und IP-Adressbereichen. Eine ausführliche Anleitung finden	Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie in der Amazon VPC-Dokumentation.	
Erstellen Sie eine DB-Subnetzgruppe.	Auf der Amazon RDS-Konsole: 1. Wählen Sie Subnetzgruppen, DB-Subnetzgruppe erstellen. 2. Geben Sie den Namen, die Beschreibung und die VPC-ID der Subnetzgruppe ein. 3. Fügen Sie die Subnetze hinzu, die zur Subnetzgruppe gehören. Fügen Sie Subnetze hinzu, um mindestens zwei Availability Zones abzudecken. 4. Wählen Sie Erstellen aus. Weitere Informationen finden Sie in der Amazon RDS-Dokumentation.	Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Amazon RDS-DB-Instance so, dass sie die neue Subnetzgruppe verwendet.	Auf der Amazon RDS-Konsole: 1. Wählen Sie im Navigationsbereich Datenbanken und dann die Amazon RDS-DB-Instance aus, die migriert werden soll. 2. Wählen Sie im Abschnitt Konnektivität die Subnetzgruppe aus, die der Ziel-VPC zugeordnet ist. 3. Wählen Sie im Abschnitt Änderungen planen die Option Sofort anwenden aus. Wenn die Migration zur Ziel-VPC abgeschlossen ist, wird die Standardsicherheitsgruppe der Ziel-VPC der Amazon RDS-DB-Instance zugewiesen. Sie können eine neue Sicherheitsgruppe für diese VPC mit den erforderlichen eingehenden und ausgehenden Regeln für Ihre DB-Instance konfigurieren. Alternativ können Sie die AWS-Befehlszeilenschnittstelle (AWS CLI) verwenden, um die Migration zur Ziel-VPC durchzuführen, indem Sie	Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die neue VPC-Sicherheitsgruppen-ID explizit angeben. Zum Beispiel: `aws rds modify-db-instance \ --db-instance-identifier testrds \ --db-subnet-group-name new-vpc-subnet-group \ --vpc-security-group-ids sg-idxxxx \ --apply-immediately`	

Zu einem anderen AWS-Konto migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine neue VPC und Subnetzgruppe im AWS-Zielkonto.	1. Erstellen Sie auf der Amazon VPC-Konsole eine neue VPC mit den gewünschten Eigenschaften und IP-Adressbereichen. Eine ausführliche Anleitung finden Sie in der Amazon VPC-Dokumentation. 2. Erstellen Sie Subnetze für die neue VPC, indem Sie den Anweisungen in der Amazon VPC-Dokumentation folgen. 3. Erstellen Sie auf der Amazon RDS-Konsole	Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	DB-Subnetzgruppen. Anweisungen finden Sie in der Amazon RDS-Dokumentation.	
Teilen Sie einen manuellen Snapshot der Datenbank und teilen Sie ihn mit dem Zielkonto.	1. Erstellen Sie einen manuellen Snapshot der Quelldatenbank, indem Sie den Anweisungen in der Amazon RDS-Dokumentation folgen. 2. Teilen Sie den Snapshot mit dem AWS-Zielkonto, indem Sie die Zielkonto-ID angeben. Anweisungen finden Sie im re:POST-Artikel über das Teilen von DB-Snapshots mit anderen Konten.	Administrator
Starten Sie eine neue Amazon RDS-DB-Instance.	Starten Sie eine neue Amazon RDS-DB-Instance aus dem gemeinsam genutzten Snapshot im AWS-Zielkonto. Anweisungen finden Sie in der Amazon RDS-Dokumentation.	Administrator

Zugehörige Ressourcen

- Amazon VPC-Dokumentation
- Dokumentation zu Amazon RDS
- Wie ändere ich die VPC für eine RDS-DB-Instance? (AWS re:POST-Artikel)
- Wie übertrage ich das Eigentum an Amazon RDS-Ressourcen auf ein anderes AWS-Konto? (AWS re:POST-Artikel)

- Wie teile ich manuelle Amazon RDS-DB-Snapshots oder Aurora-DB-Cluster-Snapshots mit einem anderen AWS-Konto? (AWS re:POST-Artikel)
- AWS DMS-Dokumentation

Migrieren Sie eine Amazon RDS for Oracle DB-Instance zu einer anderen VPC

Erstellt von Pinesh Singal (AWS)

Übersicht

Dieses Migrationsmuster bietet step-by-step Anleitungen für die Migration einer Amazon Relational Database Service (Amazon RDS) for Oracle Database (DB) -Instance von einer Virtual Private Cloud (VPC) zu einer anderen VPC im selben Amazon Web Services (AWS) -Konto. Sie können dieses Muster beispielsweise verwenden, wenn Ihr Unternehmen verlangt, dass sich die Datenbank und der Amazon Elastic Compute Cloud (Amazon EC2) -Anwendungsserver in derselben VPC befinden.

Das Muster beschreibt eine Online-Migrationsstrategie mit fast keinen Ausfallzeiten für eine Oracle-Quelldatenbank mit mehreren Terabyte und einer hohen Anzahl von Transaktionen.

Um eine Amazon RDS for Oracle DB-Instance auf eine andere VPC zu verschieben, müssen Sie die Amazon RDS-Subnetzgruppe ändern. Diese Subnetzgruppe muss mit der neuen VPC und den erforderlichen Subnetzen vorkonfiguriert werden. Während des VPC-Wechsels von einem Netzwerk zu einem anderen wird die Amazon RDS-Instance neu gestartet, sodass während der Übertragung nicht auf die Datenbank zugegriffen werden kann.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Zwei VPCs mit privaten Subnetzen
- Eine Amazon RDS for Oracle-Datenbank-Instance (läuft), konfiguriert mit Sicherheitsgruppen für eingehenden und ausgehenden Datenverkehr

Einschränkungen

- Eine DB-Instance, die sich über mehrere Availability Zones (Multi-AZ) erstreckt, wird nicht unterstützt. Dieses Muster bietet jedoch eine Möglichkeit, diese Einschränkung zu umgehen.
- Die DB-Instance kann nicht migriert werden, solange eine Read Replica aktiviert ist.
- Die Subnetzgruppe in der neuen VPC sollte sich in derselben Availability Zone wie die Datenbank befinden.

- Die Migration sollte während der geplanten Wartungsperiode oder zu Zeiten mit geringem Datenverkehr erfolgen, da das Verschieben der Datenbank in eine andere VPC einen Neustart der Datenbank verursacht, was zu Anwendungsausfällen für einige Minuten führt.

Produktversionen

- Amazon RDS for Oracle Oracle-DB-Instance, 12.1.0.2 und höher

Architektur

Quelltechnologie-Stack

- Eine Amazon RDS for Oracle 12.1.0.2.v22-DB-Instance in einer VPC
- Eine VPC, die in einer separaten Routentabelle konfiguriert ist
- In einer VPC konfigurierte Amazon RDS-Subnetzgruppen
- Amazon RDS-Optionsgruppen (falls erforderlich)

Zieltechnologie-Stack

- Amazon RDS for Oracle Oracle-Datenbank-Instance mit Version 12.1.0.2.v22 in einer anderen VPC
- Amazon VPC auf separater Route konfiguriert
- Amazon RDS-Subnetzgruppen, die in einer neuen VPC konfiguriert sind
- Amazon RDS-Optionsgruppen (falls erforderlich)

Quell- und Zielarchitektur

Das folgende Diagramm zeigt, wie Amazon RDS for Oracle DB mithilfe der Konsole von einem privaten Subnetz in einer VPC in ein privates Subnetz in einer anderen VPC verschoben wird.

1. Verwenden Sie die Konsole, um die Amazon RDS for Oracle Oracle-DB-Quell-Instance zu ändern.
2. Ändern Sie in der Ziel-VPC die Subnetzgruppe und ändern Sie die Optionsgruppe, falls sie verwendet wird.

Tools

- Amazon RDS — Amazon Relational Database Service (Amazon RDS) ist ein Webservice, der die Einrichtung, den Betrieb und die Skalierung einer relationalen Datenbank in der AWS-Cloud erleichtert. Er bietet kosteneffiziente, anpassbare Kapazität für eine relationale Datenbank und verwaltet allgemeine Datenbankverwaltungsaufgaben. Dieses Muster verwendet Amazon RDS for Oracle.

Epen

Ändern Sie die Konfiguration der Amazon RDS for Oracle Oracle-Datenbank in der vorhandenen VPC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Subnetzgruppe.	Konfigurieren Sie eine Subnetzgruppe in Amazon RDS.	Allgemeines AWS
Erstellen Sie eine Optionsgruppe.	(Optional) Konfigurieren Sie eine Optionsgruppe in Amazon RDS.	Allgemeines AWS
Ändern Sie die Amazon RDS for Oracle DB-Instance.	Ändern Sie die Datenbank mit der Subnetzgruppe und der Optionsgruppe.	Allgemein AWS, DBA
Aktualisieren Sie die Oracle-Datenbank, falls erforderlich.	Um die Amazon RDS for Oracle Oracle-Quelldatenbank zu migrieren, nehmen Sie die folgenden Änderungen vor: • Entfernen Sie Read Replicas, falls sie existieren. • Schalten Sie die Multi-AZ-Funktion aus, falls sie aktiviert ist.	Allgemeines AWS

Konfiguration der Amazon RDS for Oracle Oracle-Datenbank in der Ziel-VPC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Subnetzgruppe.	Konfigurieren Sie in Amazon RDS eine Subnetzgruppe mithilfe des Subnetzes der neuen VPC und der Availability Zone der Datenbank.	Allgemeines AWS
Erstellen Sie eine Optionsgruppe.	(Optional) Konfigurieren Sie eine Optionsgruppe in Amazon RDS.	Allgemeines AWS
Ändern Sie die Amazon RDS for Oracle Oracle-Datenbank.	Ändern Sie die Datenbank mit der neuen Subnetzgruppe und der Optionsgruppe der neuen VPC. Sie können diese Änderungen sofort oder in einem Wartungsfenster anwenden. Es kann mehrere Minuten dauern, bis die Änderung abgeschlossen ist. Während der Änderung werden Sie die folgenden Statusänderungen sehen: • moving-to-vpc • C onfiguring-enhanced-monitoring • Ändern • Verfügbar Durch die Änderung wird die Standardsicherheitsgruppe	Allgemein AWS, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der neuen VPC angehängt. Fügen Sie je nach Bedarf von Amazon RDS for Oracle eine neue Sicherheitsgruppe hinzu.	
Aktualisieren Sie die Amazon RDS for Oracle Oracle-Datenbank, falls erforderlich.	Nehmen Sie nach der Migration zur Amazon RDS for Oracle Oracle-Zieldatenbank in der neuen VPC bei Bedarf die folgenden Änderungen vor: • Aktivieren Sie Read Replicas, falls sie in der Quelldatenbank vorhanden waren. • Schalten Sie die Multi-AZ-Funktion ein, wenn sie in der Quelldatenbank aktiviert war.	Allgemeines AWS
Testen Sie die Anwendungskonnektivität.	Führen Sie von einer beliebigen Anwendung aus einen Datenbankverbindungstest durch. Vergewissern Sie sich, dass die geänderte Amazon RDS for Oracle DB in der neuen VPC verbunden ist und von der Anwendung aus darauf zugegriffen werden kann.	Besitzer der App

Zugehörige Ressourcen

- Amazon VPC-Dokumentation
- VPCs und Subnetze

- Arbeiten mit einer DB-Instance in einer VPC
- Dokumentation zu Amazon RDS
- Oracle auf Amazon RDS
- Amazon RDS-Konsole
- Wie ändere ich die VPC einer Amazon RDS-DB-Instance?

Migrieren Sie einen Amazon Redshift Redshift-Cluster in eine AWS-Region in China

Erstellt von Jing Yan (AWS)

Übersicht

Dieses Muster bietet einen step-by-step Ansatz zur Migration eines Amazon Redshift Redshift-Clusters aus einer anderen AWS-Region in China.

Dieses Muster verwendet SQL-Befehle, um alle Datenbankobjekte neu zu erstellen, und verwendet den Befehl UNLOAD, um diese Daten von Amazon Redshift in einen Amazon Simple Storage Service (Amazon S3) -Bucket in der Quellregion zu verschieben. Die Daten werden dann in einen S3-Bucket in der AWS-Region in China migriert. Der COPY-Befehl wird verwendet, um Daten aus dem S3-Bucket zu laden und in den Amazon Redshift Redshift-Zielcluster zu übertragen.

Amazon Redshift unterstützt derzeit keine regionsübergreifenden Funktionen wie das Kopieren von Snapshots in AWS-Regionen in China. Dieses Muster bietet eine Möglichkeit, diese Einschränkung zu umgehen. Sie können die Schritte in diesem Muster auch rückgängig machen, um Daten von einer AWS-Region in China in eine andere AWS-Region zu migrieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Aktive AWS-Konten sowohl in einer Region China als auch in einer AWS-Region außerhalb China
- Bestehende Amazon Redshift Redshift-Cluster sowohl in einer Region China als auch in einer AWS-Region außerhalb China

Einschränkungen

- Dies ist eine Offline-Migration, was bedeutet, dass der Amazon Redshift Redshift-Quellcluster während der Migration keine Schreibvorgänge ausführen kann.

Architektur

Quelltechnologie-Stack

- Amazon Redshift Redshift-Cluster in einer AWS-Region außerhalb China

Zieltechnologie-Stack

- Amazon Redshift Redshift-Cluster in einer AWS-Region in China

Zielarchitektur

Tools

Tools

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice, der Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet. Sie können Amazon S3 verwenden, um Daten aus Amazon Redshift zu speichern, und Sie können Daten aus einem S3-Bucket nach Amazon Redshift kopieren.
- Amazon Redshift — Amazon Redshift ist ein vollständig verwalteter Data-Warehouse-Service im Petabyte-Bereich in der Cloud.
- psql — psql ist ein terminalbasiertes Frontend für PostgreSQL.

Epen

Bereiten Sie sich auf die Migration in der Quellregion vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten und konfigurieren Sie eine EC2 Instanz in der Quellregion.	Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon Elastic Compute Cloud (Amazon EC2) -Konsole. Ihre aktuelle Region wird in der Navigationsleiste oben auf dem Bildschirm angezeigt . Diese Region kann keine AWS-Region in China sein. Wählen Sie im Dashboard der EC2 Amazon-Konsole „Instanz starten“ und erstellen und konfigurieren Sie eine	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	EC2 Instance. Wichtig: Stellen Sie sicher, dass Ihre EC2 Sicherheitsgruppen für eingehende Nachrichten uneingeschränkten Zugriff auf den TCP-Port 22 von Ihrem Quellcomputer aus zulassen. Anweisungen zum Starten und Konfigurieren einer EC2 Instanz finden Sie im Abschnitt „Verwandte Ressourcen“.	
Installieren Sie das PSQL-Tool .	Downloaden und installieren Sie PostgreSQL. Amazon Redshift stellt das psql-Tool nicht bereit, es wird mit PostgreSQL installiert. Weitere Informationen zur Verwendung von psql und zur Installation von PostgreSQL-Tools finden Sie im Abschnitt „Verwandte Ressourcen“.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Notieren Sie die Amazon Redshift Redshift-Clusterdetails.	Öffnen Sie die Amazon Redshift Redshift-Konsole und wählen Sie im Navigationsbereich „Clusters“ aus. Wählen Sie dann den Namen des Amazon Redshift Redshift-Clusters aus der Liste aus. Notieren Sie sich auf der Registerkarte „Eigenschaften“ im Abschnitt „Datenbankkonfigurationen“ den „Datenbanknamen“ und den „Port“. Öffnen Sie den Abschnitt „Verbindungsdetails“ und notieren Sie den „Endpunkt“ im <port><databasename>Format „Endpoint:/“. Wichtig: Stellen Sie sicher, dass Ihre Amazon Redshift Redshift-Sicherheitsgruppen für eingehende Nachrichten uneingeschränkten Zugriff auf den TCP-Port 5439 von Ihrer Instance aus zulassen. EC2	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Connect psql mit dem Amazon Redshift Redshift-Cluster.	<userid><databasename><port>Geben Sie an einer Befehlszeile die Verbindungsinformationen an, indem Sie den Befehl „psql -h <endpoint>-U -d -p“ ausführen. <userid>Geben Sie an der psql-Passwort-Eingabeaufforderung das Passwort für den Benutzer „“ ein. Sie sind dann mit dem Amazon Redshift Redshift-Cluster verbunden und können interaktiv Befehle eingeben.	DBA
Erstellen Sie einen S3-Bucket.	Öffnen Sie die Amazon S3 S3-Konsole und erstellen Sie einen S3-Bucket für die aus Amazon Redshift exportierten Dateien. Anweisungen zum Erstellen eines S3-Buckets finden Sie im Abschnitt „Verwandte Ressourcen“.	DBA, AWS Allgemein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Richtlinie, die das Entladen von Daten unterstützt.	Öffnen Sie die AWS Identity and Access Management (IAM) -Konsole und wählen Sie „Richtlinien“. Wählen Sie „Richtlinie erstellen“ und dann die Registerkarte „JSON“. Kopieren Sie die IAM-Richtlinie für das Entladen von Daten aus dem Abschnitt „Zusätzliche Informationen“ und fügen Sie sie ein. Wichtig: Ersetzen Sie „s3_bucket_name“ durch den Namen Ihres S3-Buckets. Wählen Sie „Richtlinie überprüfen“ und geben Sie einen Namen und eine Beschreibung für die Richtlinie ein. Wählen Sie „Richtlinie erstellen“.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle, um den UNLOAD-Vorgang für Amazon Redshift zu ermöglichen.	Öffnen Sie die IAM-Konsole und wählen Sie „Rollen“. Wählen Sie „Rolle erstellen“ und wählen Sie „AWS-Service“ unter „Typ der vertrauenswürdigen Entität auswählen“. Wählen Sie „Redshift“ für den Service, wählen Sie „Redshift — Customizable“ und dann „Next“. Wählen Sie die Richtlinie „Entladen“, die Sie zuvor erstellt haben, und klicken Sie auf „Weiter“. Geben Sie einen „Rollennamen“ ein und wählen Sie „Rolle erstellen“.	DBA
Ordnen Sie die IAM-Rolle dem Amazon Redshift Redshift-Cluster zu.	Öffnen Sie die Amazon Redshift Redshift-Konsole und wählen Sie „IAM-Rollen verwalten“. Wählen Sie im Dropdownmenü „Verfügbare Rollen“ und wählen Sie die Rolle aus, die Sie zuvor erstellt haben. Wählen Sie „Änderungen übernehmen“. Wenn der „Status“ für die IAM-Rolle unter „IAM-Rollen verwalten“ als „Sync“ angezeigt wird, können Sie den Befehl UNLOAD ausführen.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beenden Sie Schreibvorgänge in den Amazon Redshift Redshift-Cluster.	Sie müssen daran denken, alle Schreibvorgänge in den Amazon Redshift Redshift-Quellcluster zu beenden, bis die Migration abgeschlossen ist.	DBA

Bereiten Sie sich auf die Migration in der Zielregion vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten und konfigurieren Sie eine EC2 Instanz in der Zielregion.	Melden Sie sich bei der AWS-Managementkonsole für eine Region in China an, entweder Peking oder Ningxia. Wählen Sie in der EC2 Amazon-Konsole „Launch Instance“ und erstellen und konfigurieren Sie eine EC2 Instance. Wichtig: Stellen Sie sicher, dass Ihre EC2 Amazon-Sicherheitsgruppen für eingehende Nachrichten uneingeschränkten Zugriff auf TCP-Port 22 von Ihrem Quellcomputer aus zulassen. Weitere Anweisungen zum Starten und Konfigurieren einer EC2 Instance finden Sie im Abschnitt „Verwandte Ressourcen“.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Notieren Sie die Amazon Redshift Redshift-Clusterdetails.	Öffnen Sie die Amazon Redshift Redshift-Konsole und wählen Sie im Navigationsbereich „Clusters“ aus. Wählen Sie dann den Namen des Amazon Redshift Redshift-Clusters aus der Liste aus. Notieren Sie sich auf der Registerkarte „Eigenschaften“ im Abschnitt „Datenbankkonfigurationen“ den „Datenbanknamen“ und den „Port“. Öffnen Sie den Abschnitt „Verbindungsdetails“ und notieren Sie den „Endpunkt“ im <port><databasename>Format „Endpoint:/“. Wichtig: Stellen Sie sicher, dass Ihre Amazon Redshift Redshift-Sicherheitsgruppen für eingehende Nachrichten uneingeschränkten Zugriff auf den TCP-Port 5439 von Ihrer Instance aus zulassen. EC2	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Connect psql mit dem Amazon Redshift Redshift-Cluster.	<userid><databasename><port>Geben Sie an einer Befehlszeile die Verbindungsinformationen an, indem Sie den Befehl „psql -h <endpoint>-U -d -p“ ausführen. <userid>Geben Sie an der psql-Passwort-Eingabeaufforderung das Passwort für den Benutzer „“ ein. Sie sind dann mit dem Amazon Redshift Redshift-Cluster verbunden und können interaktiv Befehle eingeben.	DBA
Erstellen Sie einen S3-Bucket.	Öffnen Sie die Amazon S3 S3-Konsole und erstellen Sie einen S3-Bucket für die exportierten Dateien aus Amazon Redshift. Hilfe zu dieser und anderen Geschichten finden Sie im Abschnitt „Verwandte Ressourcen“.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Richtlinie, die das Kopieren von Daten unterstützt.	Öffnen Sie die IAM-Konsole und wählen Sie „Richtlinien“. Wählen Sie „Richtlinie erstellen“ und dann den Tab „JSON“. Kopieren Sie die IAM-Richtlinie zum Kopieren von Daten aus dem Abschnitt „Zusätzliche Informationen“ und fügen Sie sie ein. Wichtig: Ersetzen Sie „s3_bucket_name“ durch den Namen Ihres S3-Buckets. Wählen Sie „Richtlinie überprüfen“ und geben Sie einen Namen und eine Beschreibung für die Richtlinie ein. Wählen Sie „Richtlinie erstellen“.	DBA
Erstellen Sie eine IAM-Rolle, um den COPY-Vorgang für Amazon Redshift zu ermöglichen.	Öffnen Sie die IAM-Konsole und wählen Sie „Rollen“. Wählen Sie „Rolle erstellen“ und wählen Sie „AWS-Service“ unter „Typ der vertrauenswürdigen Entität auswählen“. Wählen Sie „Redshift“ für den Service, wählen Sie „Redshift — Customizable“ und dann „Next“. Wählen Sie die Richtlinie „Kopieren“, die Sie zuvor erstellt haben, und klicken Sie auf „Weiter“. Geben Sie einen „Rollennamen“ ein und wählen Sie „Rolle erstellen“.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ordnen Sie die IAM-Rolle dem Amazon Redshift Redshift-Cluster zu.	Öffnen Sie die Amazon Redshift Redshift-Konsole und wählen Sie „IAM-Rollen verwalten“. Wählen Sie im Dropdownmenü „Verfügba re Rollen“ und wählen Sie die Rolle aus, die Sie zuvor erstellt haben. Wählen Sie „Änderungen übernehme n“. Wenn der „Status“ für die IAM-Rolle unter „IAM-Rollen verwalten“ als „Sync“ angezeigt wird, können Sie den Befehl „COPY“ ausführen.	DBA

Überprüfen Sie die Quelldaten und Objektinformationen, bevor Sie mit der Migration beginnen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Zeilen in den Amazon Redshift Redshift-Quelltabellen.	Verwenden Sie die Skripts im Abschnitt „Zusätzliche Informationen“, um die Anzahl der Zeilen in den Amazon Redshift Redshift-Quelltabellen zu überprüfen und aufzuzeichnen. Denken Sie daran, die Daten für die UNLOAD- und COPY-Skri pten gleichmäßig aufzuteilen. Dies verbessert die Effizienz beim Entladen und Laden von Daten, da die Datenmenge, die von den einzelnen Skripten	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	abgedeckt wird, ausgewogen ist.	
Überprüfen Sie die Anzahl der Datenbankobjekte im Amazon Redshift Redshift-Quellcluster.	Verwenden Sie die Skripts im Abschnitt „Zusätzliche Informationen“, um die Anzahl der Datenbanken, Benutzer, Schemas, Tabellen, Ansichten und benutzerdefinierten Funktionen (UDFs) in Ihrem Amazon Redshift Redshift-Quellcluster zu überprüfen und aufzuzeichnen.	DBA
Überprüfen Sie die Ergebnisse der SQL-Anweisung vor der Migration.	Einige SQL-Anweisungen für die Datenvalidierung sollten nach den tatsächlichen Geschäfts- und Datensituationen sortiert werden. Dies dient dazu, die importierten Daten zu überprüfen, um sicherzustellen, dass sie konsistent sind und korrekt angezeigt werden.	DBA

Migrieren Sie Daten und Objekte in die Zielregion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie Amazon Redshift DDL-Skripts.	Generieren Sie Data Definition Language (DDL) -Skripts, indem Sie die Links aus dem Abschnitt „SQL-Anweisungen zur Abfrage von Amazon Redshift“ im Abschnitt	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	„Zusätzliche Informationen“ verwenden. Diese DDL-Skripts sollten die Abfragen „Benutzer erstellen“, „Schema erstellen “, „Schemaprivilegien für Benutzer“, „Tabelle/Ansicht erstellen“, „Benutzerrechte für Objekte“ und „Funktion erstellen“ enthalten.	
Erstellen Sie Objekte im Amazon Redshift Redshift-Cluster für die Zielregion.	Führen Sie die DDL-Skrip ts mithilfe der AWS-Befeh lszeilenschnittstelle (AWS CLI) in der AWS-Region in China aus. Diese Skripts erstellen Objekte im Amazon Redshift Redshift-Cluster für die Zielregion.	DBA
Entladen Sie die Amazon Redshift Redshift-Quellclus terdaten in den S3-Bucket.	Führen Sie den Befehl UNLOAD aus, um Daten aus dem Amazon Redshift Redshift-Cluster in der Quellregion in den S3-Bucket zu entladen.	DBA, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Übertragen Sie die Bucket-Daten der Quellregion S3 in den Ziel-Bucket der Region S3.	Übertragen Sie die Daten aus Ihrem S3-Bucket der Quellregion in den S3-Bucket der Zielregion. Da der Befehl „$ aws s3 sync“ nicht verwendet werden kann, stellen Sie sicher, dass Sie den Prozess verwenden, der im Artikel „Übertragung von Amazon S3 S3-Daten von AWS-Regionen zu AWS-Regionen in China“ im Abschnitt „Verwandte Ressourcen“ beschrieben ist.	Developer
Laden Sie Daten in den Amazon Redshift Redshift-Zielcluster.	Führen Sie im psql-Tool für Ihre Zielregion den Befehl COPY aus, um Daten aus dem S3-Bucket in den Amazon Redshift Redshift-Zielcluster zu laden.	DBA

Überprüfen Sie die Daten in den Quell- und Zielregionen nach der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen und vergleichen Sie die Anzahl der Zeilen in den Quell- und Zieltabellen.	Überprüfen und vergleichen Sie die Anzahl der Tabellenzeilen in den Quell- und Zielregionen, um sicherzustellen, dass alle migriert wurden.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen und vergleichen Sie die Anzahl der Quell- und Zieldatenbankobjekte.	Überprüfen und vergleichen Sie alle Datenbankobjekte in den Quell- und Zielregionen, um sicherzustellen, dass alle migriert wurden.	DBA
Überprüfen und vergleichen Sie die SQL-Skriptergebnisse in den Quell- und Zielregionen.	Führen Sie die vor der Migration vorbereiteten SQL-Skripts aus. Überprüfen und vergleichen Sie die Daten, um sicherzustellen, dass die SQL-Ergebnisse korrekt sind.	DBA
Setzen Sie die Passwörte r aller Benutzer im Amazon Redshift Redshift-Zielcluster zurück.	Nachdem die Migration abgeschlossen und alle Daten verifiziert wurden, sollten Sie alle Benutzerkennwörter für den Amazon Redshift Redshift-Cluster in der AWS-Region in China zurücksetzen.	DBA

Zugehörige Ressourcen

- Übertragung von Amazon S3 S3-Daten von AWS-Regionen in AWS-Regionen in China
- Erstellen eines S3-Buckets
- Zurücksetzen eines Amazon Redshift Redshift-Benutzerkennworts
- PSQL-Dokumentation

Zusätzliche Informationen

IAM-Richtlinie für das Entladen von Daten

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::s3_bucket_name"]
    },
    {
      "Effect": "Allow",
      "Action": ["s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::s3_bucket_name/*"]
    }
  ]
}
```

IAM-Richtlinie für das Kopieren von Daten

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::s3_bucket_name"]
    },
    {
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": ["arn:aws:s3:::s3_bucket_name/*"]
    }
  ]
}
```

SQL-Anweisungen zur Abfrage von Amazon Redshift

```
##Database

select * from pg_database where datdba>1;

##User

select * from pg_user where usesysid>1;

##Schema
```

```
SELECT n.nspname AS "Name",

  pg_catalog.pg_get_userbyid(n.nspowner) AS "Owner"

FROM pg_catalog.pg_namespace n

WHERE n.nspname !~ '^pg_' AND n.nspname <> 'information_schema'

ORDER BY 1;

##Table

select count(*) from pg_tables where schemaname not in
 ('pg_catalog','information_schema');

select schemaname,count(*) from pg_tables where schemaname not in
 ('pg_catalog','information_schema') group by schemaname order by 1;

##View

SELECT

    n.nspname AS schemaname,c.relname AS
 viewname,pg_catalog.pg_get_userbyid(c.relowner) as "Owner"

FROM

    pg_catalog.pg_class AS c

INNER JOIN

    pg_catalog.pg_namespace AS n

    ON c.relnamespace = n.oid

WHERE relkind = 'v' and n.nspname not in ('information_schema','pg_catalog');

##UDF

SELECT

   n.nspname AS schemaname,

   p.proname AS proname,
```

```
   pg_catalog.pg_get_userbyid(p.proowner) as "Owner"

FROM pg_proc p

LEFT JOIN pg_namespace n on n.oid = p.pronamespace

WHERE p.proowner != 1;
```

SQL-Skripts zum Generieren von DDL-Anweisungen

- Get_Schema_Priv_by_User-Skript
- Generate_TBL_DDL-Skript
- Generate_View_DDL
- Generate_User_Grant_Revoke_DDL
- Generieren_UDF_DDL

Transportieren Sie PostgreSQL-Datenbanken zwischen zwei Amazon RDS-DB-Instances mithilfe von pg_transport

Erstellt von Raunak Rishabh (AWS) und Jitender Kumar (AWS)

Übersicht

Dieses Muster beschreibt die Schritte für die Migration extrem großer Datenbanken zwischen zwei Amazon Relational Database Service (Amazon RDS) für PostgreSQL-DB-Instances mithilfe der Erweiterung pg_transport. Diese Erweiterung bietet einen physischen Transportmechanismus, um jede Datenbank zu verschieben. Durch das Streaming der Datenbankdateien mit minimaler Verarbeitung bietet es eine extrem schnelle Methode für die Migration großer Datenbanken zwischen DB-Instances mit minimaler Ausfallzeit. Diese Erweiterung verwendet ein Pull-Modell, bei dem die Ziel-DB-Instance die Datenbank aus der Quell-DB-Instance importiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Beide DB-Instances müssen dieselbe Hauptversion von PostgreSQL ausführen.
- Die Datenbank darf auf dem Ziel nicht existieren. Andernfalls schlägt der Transport fehl.
- In der Quelldatenbank darf keine andere Erweiterung als pg_transport aktiviert sein.
- Alle Quelldatenbankobjekte müssen sich im Standard-Tablespace pg_default befinden.
- Die Sicherheitsgruppe der Quell-DB-Instance sollte Traffic von der Ziel-DB-Instance zulassen.
- Installieren Sie einen PostgreSQL-Client wie psql oder PgAdminum mit der Amazon RDS PostgreSQL-DB-Instance zu arbeiten. Sie können den Client entweder in Ihrem lokalen System installieren oder eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance verwenden. In diesem Muster verwenden wir psql auf einer EC2 Instance.

Einschränkungen

- Sie können Datenbanken nicht zwischen verschiedenen Hauptversionen von Amazon RDS for PostgreSQL transportieren.
- Die Zugriffsrechte und der Besitz von der Quelldatenbank werden nicht auf die Zieldatenbank übertragen.
- Sie können Datenbanken nicht auf Read Replicas oder auf übergeordneten Instanzen von Read Replicas transportieren.

- Sie können Reg-Datentypen nicht in Datenbanktabellen verwenden, die Sie mit dieser Methode transportieren möchten.
- Sie können insgesamt bis zu 32 Transporte (einschließlich Importe und Exporte) gleichzeitig auf einer DB-Instance ausführen.
- Sie können Tabellen nicht umbenennen oder einschließen/ausschließen. Alles wird unverändert migriert.

Vorsicht

- Erstellen Sie Sicherungskopien, bevor Sie die Erweiterung entfernen, da durch das Entfernen der Erweiterung auch abhängige Objekte und einige Daten entfernt werden, die für den Betrieb der Datenbank von entscheidender Bedeutung sind.
- Berücksichtigen Sie die Instanzklasse und die Prozesse, die in anderen Datenbanken auf der Quell-Instance ausgeführt werden, wenn Sie die Anzahl der Worker und `work_mem` Werte für pg_transport bestimmen.
- Wenn der Transport beginnt, werden alle Verbindungen in der Quelldatenbank beendet und die Datenbank wird in den schreibgeschützten Modus versetzt.

> **Note**
>
> Wenn der Transport in einer Datenbank ausgeführt wird, hat er keine Auswirkungen auf andere Datenbanken auf demselben Server.

Versionen der Produkte

- Amazon RDS for PostgreSQL 10.10 und höher und Amazon RDS for PostgreSQL 11.5 und höher. Aktuelle Versionsinformationen finden Sie unter Transport von PostgreSQL-Datenbanken zwischen DB-Instances in der Amazon RDS-Dokumentation.

Architektur

Tools

- pg_transport bietet einen physischen Transportmechanismus zum Verschieben jeder Datenbank. Durch das Streamen der Datenbankdateien mit minimaler Verarbeitung werden Daten beim physischen Transport viel schneller übertragen als bei herkömmlichen Dump- und Ladeprozessen und es sind nur minimale Ausfallzeiten erforderlich. PostgreSQL-Transportdatenbanken verwenden ein Pull-Modell, bei dem die Ziel-DB-Instance die Datenbank aus der Quell-DB-Instance importiert. Sie installieren diese Erweiterung auf Ihren DB-Instances, wenn Sie die Quell- und Zielumgebungen vorbereiten, wie in diesem Muster erklärt.
- Mit psql können Sie eine Verbindung zu Ihren PostgreSQL-DB-Instances herstellen und mit ihnen arbeiten. Informationen zur Installation von psql auf Ihrem System finden Sie auf der PostgreSQL-Downloadseite.

Epen

Erstellen Sie die Zielparametergruppe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Parameter gruppe für das Zielsystem.	Geben Sie einen Gruppenna men an, der sie als Zielparam etergruppe identifiziert, zum Beispiel`pgtarget-param-group` . Anweisungen finden Sie in der Amazon RDS-Dokumentation.	DBA
Ändern Sie die Parameter für die Parametergruppe.	Legen Sie die folgenden Parameter fest: 1. Fügen `pg_transport` Sie dem `shared_pr eload_libraries` Parameter hinzu. `shared_preload_lib raries = pg_stat_s`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`tatements, pg_transp ort` 2. Legen Sie den Parameter `pg_transport.num_w orkers` fest. Wählen Sie die Anzahl der Mitarbeit er aus, mit denen Sie den Transport durchführen möchten. Der von Ihnen festgelegte Wert bestimmt die Anzahl der `transport .send_file` Mitarbeit er, die in der Quelle erstellt werden. 3. Erhöhen Sie den Wert von `max_worke r_processes` auf mehr als das Dreifache des Werts von`pg_transp ort.num_workers` . Wenn Sie beispielsweise den Wert `pg_transp ort.num_workers` auf 4 setzen, sollte der `max_worker_process es` Wert mindestens 13 sein. Wenn dies fehlschlä gt, empfiehlt pg_transport einen Mindestwert. 4. Auf 1 gesetzt`pg_transp ort.timing` . Diese Einstellung ermöglicht die Meldung von Zeitinfor	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	mationen während des Transports. 5. Legen Sie den Parameter `pg_transport.work_mem` fest. Dieser Parameter gibt den maximalen Arbeitsspeicher an, der jedem Worker zugewiesen werden soll. Der Standardwert lautet 128 MB. Weitere Informationen zu diesen Parametern finden Sie in der Amazon RDS-Dokumentation.	

Erstellen Sie die Quellparametergruppe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Parametergruppe für das Quellsystem.	Geben Sie einen Gruppennamen an, der sie als Quellparametergruppe identifiziert, z. B. `pgsource-param-group`. Anweisungen finden Sie in der Amazon RDS-Dokumentation.	DBA
Ändern Sie die Parameter für die Parametergruppe.	Legen Sie die folgenden Parameter fest: 1. Fügen `pg_transport` Sie dem `shared_pr`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`eload_libraries` Parameter hinzu. `shared_preload_libraries = pg_stat_statements, pg_transport` 2. Legen Sie den Parameter `pg_transport.num_workers` fest. Der Wert dieses Parameters, der im Ziel definiert ist, bestimmt die Anzahl der zu verwendenden `transport.send_file` Arbeitskräfte. Wenn auf dieser Instanz ein Import ausgeführt wird, erhöhen Sie diesen Wert, berücksichtigen Sie jedoch die Anzahl der Worker, die bereits ausgeführt werden. 3. Erhöhen Sie den Wert von `max_worker_processes` auf mehr als das Dreifache des Werts von `pg_transport.num_workers` auf dem Ziel. Wenn Sie beispielsweise den Wert 4 für das Ziel `pg_transport.num_workers` auf 4 setzen, sollte der `max_worker_processes` Wert in	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Quelle mindestens 13 sein. Wenn dies fehlschlägt, empfiehlt pg_transport einen Mindestwert. 4. Legen Sie den Parameter `pg_transport.work_mem` fest. Dieser Parameter gibt den maximalen Speicher an, der jedem Worker zugewiesen werden soll. Der Standardwert lautet 128 MB. Weitere Informationen zu diesen Parametern finden Sie in der Amazon RDS-Dokumentation.	

Bereiten Sie die Zielumgebung vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine neue Amazon RDS for PostgreSQL PostgreSQL-DB-Instance, in die Sie Ihre Quelldatenbank transportieren möchten.	Ermitteln Sie die Instanzklasse und die PostgreSQL-Version auf der Grundlage Ihrer Geschäftsanforderungen.	DBA, Systemadministrator, Datenbankarchitekt
Ändern Sie die Sicherheitsgruppe des Ziels, um Verbindungen über den DB-Instance-Port von der EC2 Instance aus zuzulassen.	Standardmäßig ist der Port für die PostgreSQL-Instanz 5432. Wenn Sie einen anderen Port verwenden, müssen Verbindungen zu diesem Port	DBA, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	für die Instanz geöffnet sein. EC2	
Ändern Sie die Instanz und weisen Sie die neue Zielparam etergruppe zu.	Beispiel, `pgtarget-param-group` .	DBA
Starten Sie die Amazon RDS-DB-Zielinstanz neu.	Die Parameter `shared_preload_libraries` und `max_worker_processes` sind statische Parameter und erfordern einen Neustart der Instance.	DBA, Systemadministrator
Stellen Sie mit psql von der EC2 Instanz aus eine Connect zur Datenbank her.	Verwenden Sie den -Befehl: `psql -h <rds_end_point> -p PORT -U username -d database -W`	DBA
Erstellen Sie die Erweiterung pg_transport.	Führen Sie die folgende Abfrage als Benutzer mit der `rds_superuser` Rolle aus: `create extension pg_transport;`	DBA

Bereiten Sie die Quellumgebung vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Sicherhei tsgruppe der Quelle, um Verbindungen auf dem DB-Instance-Port von der	Standardmäßig ist der Port für die PostgreSQL-Instanz 5432. Wenn Sie einen anderen Port verwenden, müssen	DBA, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Amazon-Instance und der EC2 Ziel-DB-Instance aus zuzulassen	Verbindungen zu diesem Port für die Instanz geöffnet sein. EC2	
Ändern Sie die Instanz und weisen Sie die neue Quellpara metergruppe zu.	Beispiel, `pgsource-param-group` .	DBA
Starten Sie die Amazon RDS-DB-Quell-Instance neu.	Die Parameter `shared_pr eload_libraries` und `max_worker_processes` sind statische Parameter und erfordern einen Neustart der Instance.	DBA
Stellen Sie mit psql von der EC2 Instanz aus eine Connect zur Datenbank her.	Verwenden Sie den -Befehl: `psql -h <rds_end_point> -p PORT -U username -d database -W`	DBA
Erstellen Sie die Erweiterung pg_transport und entfernen Sie alle anderen Erweiteru ngen aus den zu transport ierenden Datenbanken.	Der Transport schlägt fehl, wenn in der Quelldatenbank andere Erweiterungen als pg_transport installiert sind. Dieser Befehl muss von einem Benutzer mit der `rds_super user` Rolle ausgeführt werden.	DBA

Führen Sie den Transport durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie einen Probelauf durch.	Verwenden Sie die `transport.import_from_server` Funktion, um zuerst einen Probelauf durchzuführen: `SELECT transport.import_from_server( 'source-db-instance-endpoint', source-db-instance-port, 'source-db-instance-user', 'source-user-password', 'source-database-name', 'destination-user-password', 'true');` Der letzte Parameter dieser Funktion (gesetzt auf`true`) definiert den Probelauf. Diese Funktion zeigt alle Fehler an, die beim Ausführen des Haupttransports auftreten würden. Beheben Sie die Fehler, bevor Sie den Haupttransport ausführen.	DBA
Wenn der Probelauf erfolgreich ist, initiieren Sie den Datenbanktransport.	Führen Sie die `transport.import_from_server` Funktion aus, um den Transport durchzuführen. Sie stellt eine Verbindung zur	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Quelle her und importiert die Daten. `SELECT transport .import_from_serve r( 'source-db-instanc e-endpoint', source- db-instance-port, 'source-db-instance- user', 'source-user- password', 'source- database-name', 'destination-user- password', false);` Der letzte Parameter dieser Funktion (gesetzt auf`false`) gibt an, dass es sich nicht um einen Probelauf handelt.	
Führen Sie die Schritte nach dem Transport durch.	Nachdem der Datenbank transport abgeschlossen ist: • Überprüfen Sie die Daten in der Zielumgebung. • Fügen Sie dem Ziel alle Rollen und Berechtigungen hinzu. • Aktivieren Sie bei Bedarf alle erforderlichen Erweiteru ngen im Ziel und in der Quelle. • Setzt den Wert des `max_worker_process es` Parameters zurück.	DBA

Zugehörige Ressourcen

- Dokumentation zu Amazon RDS
- pg_transport-Dokumentation
- Migrieren von Datenbanken mit RDS PostgreSQL Transportable Databases (Blogbeitrag)
- PostgreSQL wird heruntergeladen
- psql-Hilfsprogramm
- Erstellen einer DB-Parametergruppe
- Parameter in einer DB-Parametergruppe ändern
- PostgreSQL wird heruntergeladen

Plattformwechsel

Themen

- Exportieren Sie eine Microsoft SQL Server-Datenbank mithilfe von AWS DMS nach Amazon S3
- Migrieren Sie ML-Workloads zum Erstellen, Trainieren und Bereitstellen zu Amazon SageMaker mithilfe der AWS-Entwicklertools
- Migrieren Sie OpenText TeamSite Workloads in die AWS-Cloud
- Migrieren Sie Oracle CLOB-Werte in einzelne Zeilen in PostgreSQL auf AWS
- Migrieren Sie eine lokale Oracle-Datenbank zu Amazon RDS for Oracle, indem Sie den direkten Oracle Data Pump-Import über einen Datenbank-Link verwenden
- Migrieren Sie die Oracle E-Business Suite zu Amazon RDS Custom
- Migrieren Sie Oracle PeopleSoft zu Amazon RDS Custom
- Migrieren Sie die Oracle ROWID-Funktionalität zu PostgreSQL auf AWS
- Migrieren Sie Oracle-Datenbank-Fehlercodes in eine Amazon Aurora PostgreSQL-kompatible Datenbank
- Migrieren Sie Redis-Workloads zu Redis Enterprise Cloud auf AWS
- Migrieren Sie SAP ASE auf Amazon EC2 zu Amazon Aurora PostgreSQL-kompatibel mit AWS SCT und AWS DMS
- Migrieren Sie Windows-SSL-Zertifikate mithilfe von ACM zu einem Application Load Balancer
- Migrieren Sie eine Messaging-Warteschlange von Microsoft Azure Service Bus zu Amazon SQS
- Migrieren Sie eine relationale Datenbank zu MongoDB Atlas am AWS
- Migrieren Sie eine selbst gehostete MongoDB-Umgebung zu MongoDB Atlas am AWS
- Migrieren Sie eine Oracle JD EnterpriseOne Edwards-Datenbank mithilfe von Oracle Data Pump und AWS DMS zu AWS
- Migrieren Sie eine PeopleSoft Oracle-Datenbank mithilfe von AWS DMS zu AWS
- Migrieren Sie eine lokale MySQL-Datenbank zu Amazon RDS for MySQL
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Amazon RDS for SQL Server
- Migrieren Sie Daten mithilfe von Rclone von Microsoft Azure Blob zu Amazon S3
- Migrieren Sie von Couchbase Server zu Couchbase Capella auf AWS
- Migrieren Sie von IBM WebSphere Application Server zu Apache Tomcat auf Amazon EC2
- Migrieren Sie EC2 mit Auto Scaling von IBM WebSphere Application Server zu Apache Tomcat auf Amazon

- Migrieren Sie eine.NET-Anwendung von Microsoft Azure App Service zu AWS Elastic Beanstalk
- Migrieren Sie von Oracle WebLogic zu Apache Tomcat (ToMEE) auf Amazon ECS
- Migrieren Sie mithilfe von AWS DMS eine Oracle-Datenbank von Amazon EC2 zu Amazon RDS for Oracle
- Migrieren Sie eine lokale Oracle-Datenbank mit Logstash zu Amazon OpenSearch Service
- Migrieren Sie eine lokale Oracle-Datenbank zu Amazon RDS for Oracle
- Migrieren Sie eine lokale Oracle-Datenbank mit Oracle Data Pump zu Amazon RDS for Oracle
- Migrieren Sie mit pglogical von PostgreSQL auf Amazon EC2 zu Amazon RDS for PostgreSQL
- Migrieren Sie eine lokale PostgreSQL-Datenbank zu Aurora PostgreSQL
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Microsoft SQL Server auf Amazon EC2 unter Linux
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mithilfe von Verbindungsservern zu Amazon RDS for SQL Server
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mit systemeigenen Sicherungs- und Wiederherstellungsmethoden zu Amazon RDS for SQL Server
- Migrieren Sie eine Microsoft SQL Server-Datenbank mithilfe von AWS DMS und AWS SCT zu Aurora MySQL
- Migrieren Sie eine lokale MariaDB-Datenbank mit nativen Tools zu Amazon RDS for MariaDB
- Migrieren Sie eine lokale MySQL-Datenbank zu Aurora MySQL
- Migrieren Sie lokale MySQL-Datenbanken mit Percona XtraBackup, Amazon EFS und Amazon S3 zu Aurora MySQL
- Migrieren Sie lokale Java-Anwendungen mit AWS App2Container zu AWS
- Migrieren Sie gemeinsam genutzte Dateisysteme in einer großen AWS-Migration
- Migrieren Sie eine Oracle-Datenbank mithilfe von GoldenGate Oracle-Flatfile-Adaptern zu Amazon RDS for Oracle
- Ändern Sie Python- und Perl-Anwendungen, um die Datenbankmigration von Microsoft SQL Server zur Amazon Aurora PostgreSQL-Compatible Edition zu unterstützen
- Streamen Sie Daten von IBM Db2, SAP, Sybase und anderen Datenbanken nach MongoDB Atlas auf AWS

Exportieren Sie eine Microsoft SQL Server-Datenbank mithilfe von AWS DMS nach Amazon S3

Erstellt von Sweta Krishna (AWS)

Übersicht

Organizations müssen für Datenbankmigration, Sicherung und Wiederherstellung, Datenarchivierung und Datenanalyse häufig Datenbanken auf Amazon Simple Storage Service (Amazon S3) kopieren. Dieses Muster beschreibt, wie Sie eine Microsoft SQL Server-Datenbank nach Amazon S3 exportieren können. Die Quelldatenbank kann vor Ort oder auf Amazon Elastic Compute Cloud (Amazon EC2) oder Amazon Relational Database Service (Amazon RDS) für Microsoft SQL Server in der Amazon Web Services (AWS) Cloud gehostet werden.

Die Daten werden mithilfe des AWS Database Migration Service (AWS DMS) exportiert. Standardmäßig schreibt AWS DMS Volllast- und CDC-Daten (Change Data Capture) im Format mit kommagetrennten Werten (.csv). Für kompaktere Speicher- und schnellere Abfrageoptionen verwendet dieses Muster die Formatoption Apache Parquet (.parquet).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine AWS Identity and Access Management (IAM) -Rolle für das Konto mit Schreib-, Lösch- und Tag-Zugriff auf den Ziel-S3-Bucket und AWS DMS (`dms.amazonaws.com`), das dieser IAM-Rolle als vertrauenswürdige Entität hinzugefügt wurde
- Eine lokale Microsoft SQL Server-Datenbank (oder Microsoft SQL Server auf einer EC2 Instance oder eine Amazon RDS for SQL Server Server-Datenbank)
- Netzwerkkonnektivität zwischen der Virtual Private Cloud (VPC) auf AWS und dem von AWS Direct Connect bereitgestellten lokalen Netzwerk oder einem virtuellen privaten Netzwerk (VPN)

Einschränkungen

- Ein VPC-fähiger (Gateway-VPC) S3-Bucket wird derzeit in AWS DMS-Versionen vor 3.4.7 nicht unterstützt.
- Änderungen an der Quelltabellenstruktur während des vollständigen Ladevorgangs werden nicht unterstützt.

- Der vollständige LOB-Modus (Large Binary Object) von AWS DMS wird nicht unterstützt.

Produktversionen

- Microsoft SQL Server-Versionen 2005 oder höher für die Enterprise-, Standard-, Workgroup- und Developer-Editionen.
- Support für Microsoft SQL Server Version 2019 als Quelle ist in den AWS-DMS-Versionen 3.3.2 und höher verfügbar.

Architektur

Quelltechnologie-Stack

- Eine lokale Microsoft SQL Server-Datenbank (oder Microsoft SQL Server auf einer EC2 Instance oder eine Amazon RDS for SQL Server Server-Datenbank)

Zieltechnologie-Stack

- AWS Direct Connect
- AWS DMS
- Amazon S3

Zielarchitektur

Tools

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS-Cloud oder zwischen Kombinationen von Cloud- und lokalen Setups.
- AWS Direct Connect verbindet Ihr internes Netzwerk über ein Standard-Ethernet-Glasfaserkabel mit einem Direct Connect-Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt zu öffentlichen AWS-Services erstellen und dabei Internetdienstanbieter in Ihrem Netzwerkpfad umgehen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Epen

Bereite dich auf die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Datenbank version.	Überprüfen Sie die Version der Quelldatenbank und stellen Sie sicher, dass sie von AWS DMS unterstützt wird. Informationen zu unterstüt zten SQL Server-Datenbankve rsionen finden Sie unter Verwenden einer Microsoft SQL Server-Datenbank als Quelle für AWS DMS.	DBA
Erstellen Sie eine VPC und eine Sicherheitsgruppe.	Erstellen Sie in Ihrem AWS-Konto eine VPC und eine Sicherheitsgruppe. Weitere Informationen finden Sie in der Amazon VPC-Dokumentation.	Systemadministrator
Erstellen Sie einen Benutzer für die AWS DMS-Aufgabe.	Erstellen Sie einen AWS DMS-Benutzer in der Quelldatenbank und gewähren Sie ihm READ-Berechtigunge n. Dieser Benutzer wird von AWS DMS verwendet.	DBA
Testen Sie die DB-Konnek tivität.	Testen Sie die Konnektivität des AWS DMS-Benutzers mit der SQL Server-DB-Instance.	DBA
Erstellen Sie einen S3-Bucket.	Erstellen Sie den Ziel-S3-Bucket. Dieser Bucket wird die migrierten Tabellendaten enthalten.	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Richtlinie und -Rolle.	1. Verwenden Sie den Code im Abschnitt Zusätzliche Informationen, um eine IAM-Richtlinie mit Bucket-Berechtigungen zu erstellen. 2. Erstellen Sie die Rolle für AWS DMS und fügen Sie die Richtlinie der Rolle hinzu.	Systemadministrator

Migrieren Sie Daten mithilfe von AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS DMS-Replikations-Instance.	Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS DMS-Konsole. Wählen Sie im Navigationsbereich Replikationsinstanzen, Replikationsinstanz erstellen aus. Anweisungen finden Sie in Schritt 1 in der AWS DMS-Dokumentation.	DBA
Erstellen Sie Quell- und Zielendpunkte.	Erstellen Sie Quell- und Zielendpunkte. Testen Sie die Verbindung von der Replikationsinstanz zu den Quell- und Zielendpunkten. Anweisungen finden Sie in Schritt 2 in der AWS DMS-Dokumentation.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Replikationsaufgabe.	Erstellen Sie eine Replikationsaufgabe und wählen Sie Volllast oder Volllast mit Change Data Capture (CDC) aus, um Daten von SQL Server in den S3-Bucket zu migrieren. Anweisungen finden Sie in Schritt 3 in der AWS DMS-Dokumentation.	DBA
Starten Sie die Datenreplikation.	Starten Sie die Replikationsaufgabe und überwachen Sie die Protokolle auf Fehler.	DBA

Validieren Sie die Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die migrierten Daten.	Navigieren Sie auf der Konsole zu Ihrem Ziel-S3-Bucket. Öffnen Sie den Unterordner, der denselben Namen wie die Quelldatenbank hat. Vergewissern Sie sich, dass der Ordner alle Tabellen enthält, die aus der Quelldatenbank migriert wurden.	DBA

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre AWS-Ressourcen herunter und löschen Sie sie.	Fahren Sie temporäre AWS-Ressourcen herunter, die Sie für die Datenmigration erstellt haben, z. B. die AWS DMS-Replikationsinstanz, und löschen Sie sie, nachdem Sie den Export validiert haben.	DBA

Zugehörige Ressourcen

- AWS Database Migration Service — Benutzerhandbuch
- Verwendung einer Microsoft SQL Server-Datenbank als Quelle für AWS DMS
- Verwendung von Amazon S3 als Ziel für AWS Database Migration Service
- Verwenden eines S3-Buckets als AWS-DMS-Ziel (AWS re:POST)

Zusätzliche Informationen

Verwenden Sie den folgenden Code, um eine IAM-Richtlinie mit S3-Bucket-Berechtigungen für die AWS-DMS-Rolle hinzuzufügen. Ersetzen Sie `bucketname` durch den Namen von Ihrem Bucket.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Effect": "Allow",
             "Action": [
                 "s3:PutObject",
                 "s3:DeleteObject"
             ],
             "Resource": [
                 "arn:aws:s3:::bucketname*"
             ]
         },
         {
```

```
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucketname*"
            ]
        }
    ]
}
```

Migrieren Sie ML-Workloads zum Erstellen, Trainieren und Bereitstellen zu Amazon SageMaker mithilfe der AWS-Entwicklertools

Erstellt von Mustafa Waheed (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Dieses Muster bietet Anleitungen für die Migration einer lokalen Machine Learning-Anwendung (ML), die auf Unix- oder Linux-Servern ausgeführt wird, um mithilfe von Amazon auf AWS geschult und bereitgestellt zu werden. SageMaker Diese Bereitstellung verwendet eine Pipeline für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD). Das Migrationsmuster wird mithilfe eines CloudFormation AWS-Stacks bereitgestellt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto mit AWS Landing Zone
- AWS Command Line Interface (AWS CLI) ist auf Ihrem Unix- oder Linux-Server installiert und konfiguriert
- Ein in AWS bereitgestelltes ML-Quellcode-Repository CodeCommit

Einschränkungen

- In einer AWS-Region können nur 300 einzelne Pipelines bereitgestellt werden.
- Dieses Muster ist für überwachte ML-Workloads mit train-and-deploy Code in Python vorgesehen.

Produktversionen

- Docker-Version 19.03.5, Build 633a0ea, mit Python 3.6x

Architektur

Quelltechnologie-Stack

- Lokale Linux-Recheninstanz mit Daten entweder im lokalen Dateisystem oder in einer relationalen Datenbank

Quellarchitektur

Zieltechnologie-Stack

- AWS wurde mit Amazon S3 für die Datenspeicherung und Amazon DynamoDB als Metadatenspeicher für die Nachverfolgung oder Protokollierung von Pipeline-Läufen CodePipeline bereitgestellt

Zielarchitektur

Architektur für die Anwendungsmigration

- Natives Python-Paket und CodeCommit AWS-Repository (und ein SQL-Client für lokale Datensätze auf einer Datenbankinstanz)

Tools

- Python3
- Git
- AWS CLI — Die AWS-CLI stellt den CloudFormation AWS-Stack bereit und verschiebt Daten in den S3-Bucket. Der S3-Bucket wiederum führt zum Ziel.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie den Quellcode und die Datensätze.		Data Scientist
Identifizieren Sie die Typen und Größen der gewünschten Build-, Train- und Deployment-Instances.		Dateningenieur, Datenwissenschaftler
Erstellen Sie eine Liste der Fähigkeiten und Kapazität sanforderungen.		
Identifizieren Sie die Netzwerkanforderungen.		DBA, Systemadministrator
Identifizieren Sie die Sicherheitsanforderungen für den Netzwerk- oder Hostzugriff für die Quell- und Zielanwendungen.		Dateningenieur, ML-Ingenieur, Systemadministrator
Bestimmen Sie die Backup-Strategie.		ML-Ingenieur, Systemadministrator
Ermitteln Sie die Verfügbarkeitsanforderungen.		ML-Ingenieur, Systemadministrator
Identifizieren Sie die Strategie für die Anwendungsmigration oder den Umstieg.		Datenwissenschaftler, ML-Ingenieur

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC).		ML-Ingenieur, Systemadministrator
Erstellen Sie Sicherheitsgruppen.		ML-Ingenieur, Systemadministrator
Richten Sie einen Amazon S3 S3-Bucket und CodeCommit AWS-Repository-Zweige für ML-Code ein.		ML-Ingenieur

Laden Sie die Daten und den Code hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie native MySQL-Tools oder Tools von Drittanbietern, um Datensätze in den bereitgestellten S3-Bucket zu migrieren, zu validieren und zu testen.	Dies ist für die CloudFormation AWS-Stack-Bereitstellung erforderlich.	Dateningenieur, ML-Ingenieur
Package Sie den ML-Zug und den Hosting-Code als Python-Pakete und übertragen Sie sie in das bereitgestellte Repository in AWS CodeCommit oder GitHub.	Sie benötigen den Branch-Namen des Repositorys, um die CloudFormation AWS-Vorlage für die Migration bereitzustellen.	Datenwissenschaftler, ML-Ingenieur

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Migration von ML-Workloads.		Inhaber der Anwendung, ML-Ingenieur
Stellen Sie den CloudFormation AWS-Stack bereit.	Verwenden Sie die AWS-CLI, um den Stack zu erstellen, der in der mit dieser Lösung bereitgestellten YAML-Vorlage deklariert ist.	Datenwissenschaftler, ML-Ingenieur

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendungsclients auf die neue Infrastruktur um.		Anwendungsinhaber, Datenwissenschaftler, ML-Ingenieur

Schließen Sie das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die temporären AWS-Ressourcen herunter.	Fahren Sie alle benutzerdefinierten Ressourcen aus der CloudFormation AWS-Vorlage herunter (z. B. alle AWS Lambda-Funktionen, die nicht verwendet werden).	Datenwissenschaftler, ML-Ingenieur
Überprüfen und validieren Sie die Projektdokumente.		Inhaber der Anwendung, Datenwissenschaftler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Ergebnisse und die Bewertungsmetriken des ML-Modells mit Operatoren.	Stellen Sie sicher, dass die Modellleistung den Erwartungen der Anwendungsbenutzer entspricht und mit dem Status vor Ort vergleichbar ist.	Inhaber der Anwendung, Datenwissenschaftler
Schließen Sie das Projekt ab und geben Sie Feedback.		Inhaber der Anwendung, ML-Ingenieur

Zugehörige Ressourcen

- AWSCodePipeline
- AWS CodeCommit
- AWSCodeBuild
- AmazonSageMaker
- Amazon S3
- Amazon-DynamoDB
- AWS Lambda

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Migrieren Sie OpenText TeamSite Workloads in die AWS-Cloud

Erstellt von Battulga Purevragchaa (AWS), Michael Stewart und Carlos Marruenda Molina

Übersicht

> **Warning**
>
> Für dieses Szenario sind IAM-Benutzer mit programmatischem Zugriff und langfristigen Anmeldeinformationen erforderlich, was ein Sicherheitsrisiko darstellt. Um dieses Risiko zu minimieren, empfehlen wir, diesen Benutzern nur die Berechtigungen zu gewähren, die sie für die Ausführung der Aufgabe benötigen, und diese Benutzer zu entfernen, wenn sie nicht mehr benötigt werden. Zugriffsschlüssel können bei Bedarf aktualisiert werden. Weitere Informationen finden Sie unter Aktualisieren von Zugriffsschlüsseln im IAM-Benut zerhandbuch.

Viele OpenText Experience Platform-Instanzen werden vor Ort oder auf herkömmlichen Hosting-Lösungen mit fester Kapazität und älteren Kostenmodellen gehostet. Die Migration Ihrer OpenText Experience Platform-Workloads in die Amazon Web Services (AWS) Cloud bietet zusätzliche Funktionen und Mehrwert, indem Sie Ihre geschäftliche Flexibilität und Integrationsmöglichkeiten erhöhen und gleichzeitig Ihre Gesamtbetriebskosten senken.

Dieses Muster enthält Schritte und eine Vorlage für die Migration von OpenText TeamSiteWorkloads in die AWS-Cloud. Das Muster hilft Ihnen, den Umfang und die Budgetierung Ihrer Migrationsprojekte zu verstehen, indem es einen detaillierten Abschnitt zu Epics enthält, der Sie durch den OpenText TeamSite Migrationsprozess führt.

Dieses Muster wurde von AWS und TBSCG, einem AWS-Partner, entwickelt und liegt dem Leitfaden Migration OpenText TeamSite und Medienmanagement von Workloads in die AWS-Cloud auf der AWS Prescriptive Guidance-Website bei.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Mindestens ein aktives AWS-Konto
- Ein OpenText Workload, der in einem lokalen Rechenzentrum oder bei einem anderen Cloud-Anbieter gehostet wird

- Aktive Lizenzen OpenText

Der Migrationsprozess erfordert auch die Rollen und Verantwortlichkeiten, die in der folgenden Tabelle beschrieben sind.

Rolle	Verantwortlichkeiten
Sponsor	Internes Sponsoring
Liefermanager	Lieferung der Migration
Architekt für Lösungen	Definieren Sie die aktuelle und neue Architektur
DevOps Ingenieur	DevOps Aktivitäten
Ein Tester	Testen auf Systemebene
Eigentümer des Produkts	Priorisierung von Aufgaben auf der Grundlage von Geschäftsanforderungen
TeamSite Autoren	Benutzerakzeptanztests für Migration (UAT)
TeamSite Administrator	UAT-Migration
OpenText führen	OpenText Produktspezialist
OpenText Entwickler	OpenText Produktspezialist
Spezialist für Preisgestaltung	AWS und OpenText Lizenzierung
IT-Sicherheit	Grundzüge der IT-Sicherheit
Integrationsentwickler eines Drittanbieters	Überarbeiten Sie bestehende Integrationen
Frontend-Entwickler	Nehmen Sie Änderungen am migrierten Frontend-Code vor
Datenbankadministrator	Konfiguration der Datenbank

Einschränkungen

- Stellen Sie die Kompatibilität mit Ihren Zielbetriebssystemen sicher (OSs). Sie können die Kompatibilitätsmatrix aus den Versionshinweisen der OpenText Produktversion verwenden, die Sie migrieren.

Architektur

Quelltechnologie-Stack

- OpenText Kundenerlebnislösungen, die vor Ort oder bei einem anderen Cloud-Anbieter gehostet werden:
  - OpenText TeamSite
  - OpenText LiveSite
  - OpenText Medienmanagement
  - OpenText MediaBin

Zieltechnologie-Stack

- Eine OpenText Customer Experience-Plattform, die in der AWS-Cloud gehostet wird und die folgenden AWS-Services verwendet:
  - Amazon Elastic Compute Cloud (Amazon EC2)
  - Amazon Elastic Container Service (Amazon ECS)
  - OpenSearch Amazon-Dienst
  - Elastic Load Balancing
  - AWS Lambda
  - Amazon API Gateway
  - Amazon Relational Database Service (Amazon RDS)
  - Amazon Elastic Block Store (Amazon EBS)
  - Amazon Simple Storage Service (Amazon-S3)

Zielarchitektur

Tools

- AWS Database Migration Service (AWS DMS) ist ein Cloud-Service, der die Migration von relationalen Datenbanken, Data Warehouses, NoSQL-Datenbanken und anderen Arten von Datenspeichern vereinfacht.
- AWS Application Migration Service automatisiert die Konvertierung Ihrer Quellserver, sodass sie nativ auf AWS ausgeführt werden. Er vereinfacht außerdem die Modernisierung von Anwendungen mit integrierten und benutzerdefinierten Optimierungsoptionen.

Epen

Entdeckung und Bewertung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Halten Sie Workshops zu Entdeckungsanforderungen ab.	Halten Sie Workshops mit Geschäfts- und Technikteams ab, um die aktuelle Situation zu ermitteln, Anforderungen zu sammeln und die Migration sstrategie zu validieren. Je nach Komplexität und Umfang Ihrer Migration benötigt Ihr Unternehmen möglicherweise mehrere Workshops. Dauer: Zwei Wochen	Sponsor (optional), Delivery Manager, Lösungsarchitekt, OpenText Leiter, Product Owner
Analysieren Sie die Lösungs- und Migrationsanforderungen.	Analysieren und dokumenti eren Sie die geschäftlichen, funktionalen und technisch en Anforderungen, die das Design der geplanten Lösung und den Migrationsprozess beeinflussen. Dauer: Eine Woche	Lösungsarchitekt, OpenText Leiter, Produkteigentümer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Dokumentieren Sie Ihre bestehende OpenText Architektur.	Dokumentieren Sie Ihre bestehende OpenText Architektur, einschließlich der Kernkomponenten und aller zugehörigen Anwendungen und Dienste. Dauer: Eine Woche	Lösungsarchitekt, OpenText Leiter, Produkteigentümer
Definieren Sie die geplante AWS-Architektur.	Definieren Sie Ihre geplante AWS-Architektur auf der Grundlage der identifiz ierten Komponenten und Anforderungen und mithilfe der OpenText Kompatibi litätsmatrix. Die OpenText Kompatibilitätsmatrix finden Sie in den Versionshinweisen Ihrer OpenText TeamSite Version. Dauer: Eine Woche	Lösungsarchitekt, OpenText Leiter, Produkteigentümer, IT-Sicherheit
Beurteilen Sie die Größe Ihrer geplanten AWS-Architektur.	Die Größenanforderungen variieren je nach Arbeitslast und anderen nicht funktionalen Anforderungen für verschied ene Architekturkomponenten. Dauer: Zwei Tage	Lösungsarchitekt, OpenText Leiter
Berechnen Sie die Gesamtbet riebskosten.	Berechnen Sie die Gesamtbet riebskosten (TCO) für Ihre vorgeschlagene Lösung. Dauer: Zwei Tage	Lösungsarchitekt, Preisspez ialist

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie die Migrationsstrategie für jede Komponente.	Definieren und dokumentieren Sie, welche der sieben gängigen Migrationsstrategien (7 Rs) für jeden Kern oder jede zusätzliche Komponente, die in die AWS-Cloud migriert werden muss, verwendet werden soll. Dauer: Eine Woche	Lösungsarchitekt, OpenText Leiter, Produkteigentümer
Definieren Sie den Migrationsprozess für die Komponenten.	Definieren Sie den detaillierten Migrationsprozess für jede Komponente Ihres Workloads. Dauer: Eine Woche	Lösungsarchitekt, OpenText Leiter, Produkteigentümer, IT-Sicherheit
Definieren Sie den globalen Migrationsprozess und die Abhängigkeiten.	Erstellen Sie einen globalen Migrationsprozess und einen Kalender, der die Migrationsdetails für Komponenten, Abhängigkeiten und Geschäftskontinuität enthält. Dauer: Drei Tage	Lösungsarchitekt, OpenText Leiter, Produkteigentümer, IT-Sicherheit

Sicherheits- und Compliance-Aktivitäten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Sicherheitsrichtlinien.	Konfigurieren Sie die vom Kunden verwalteten Sicherheitsrichtlinien in Ihren AWS-Konten. Diese sollten die Komplexität und Rotation von Passwörtern sowie die	Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	automatische Deaktivierung ungenutzter Konten beinhalten. Weitere Informationen zu vom Kunden verwalteten Richtlinien finden Sie unter Vom Kunden verwaltete Richtlinien in der Dokumentation zu AWS Identity and Access Management (IAM).	
Erstellen Sie IAM-Benutzer.	Erstellen Sie die IAM-Benutzer, die Zugriff auf die AWS-Managementkonsole, die AWS-Befehlszeilenschnittstelle (AWS CLI) und das AWS-SDK benötigen. Weitere Informationen zum Erstellen von IAM-Benutzern finden Sie in der IAM-Dokumentation unter Erstellen eines IAM-Benutzers in Ihrem AWS-Konto.	Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie IAM-Gruppen.	Erstellen Sie die erforderlichen IAM-Benutzergruppen (z. B. Administrator- oder Entwicklergruppen) und fügen Sie diesen Gruppen IAM-Benutzer hinzu. Weitere Informationen zu IAM-Benutzergruppen finden Sie unter IAM-Benutzergruppen in der IAM-Dokumentation.	Lösungsarchitekt
Fügen Sie Sicherheitsrichtlinien hinzu.	Fügen Sie den IAM-Gruppen oder -Rollen Sicherheitsrichtlinien hinzu. Weitere Informationen dazu finden Sie in der IAM-Dokumentation unter Eine Richtlinie an eine IAM-Benutzergruppe anhängen.	Lösungsarchitekt
Aktivieren Sie die detaillierte Abrechnung.	Weitere Informationen zur Abrechnung finden Sie unter Überwachung Ihrer Nutzung und Kosten in der Dokumentation zu AWS Billing and Cost Management.	Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Kontaktdaten Ihrer Konten.	Stellen Sie sicher, dass die Kontaktdaten für Ihre Konten aktuell sind und mehr als einer Person in Ihrer Organisation zugeordnet sind. Weitere Informationen finden Sie unter Verwaltung eines AWS-Kontos in der Dokumentation zu AWS Billing and Cost Management.	Lösungsarchitekt, Produkteigentümer
Kontaktinformationen für Sicherheitsfragen hinzufügen.	Konfigurieren Sie Ihre Kontaktinformationen mit Ihren Sicherheitskontaktinformationen. Weitere Informationen dazu finden Sie unter Verwaltung eines AWS-Kontos in der Dokumentation zu AWS Billing and Cost Management.	Lösungsarchitekt, IT-Sicherheit
Richten Sie IAM-Rollen für EC2 Instanzen ein.	Konfigurieren Sie die IAM-Rollen für die EC2 Instanzen. Weitere Informationen dazu finden Sie unter IAM-Rollen für Amazon EC2 in der EC2 Amazon-Dokumentation.	Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Zugriff auf den AWS-Support.	Fügen Sie eine IAM-Richtlinie für IAM-Benutzer hinzu, die Zugriff auf das AWS Support for Support Center benötigen , und um Supportfälle zu erstellen. Weitere Informationen dazu finden Sie unter Zugriffsb erechtigungen für AWS Support in der AWS-Support-Dokumentation.	Lösungsarchitekt
Aktivieren CloudTrail.	Aktivieren Sie AWS automatis ch CloudTrail in all Ihren AWS-Regionen. Weitere Informationen dazu finden Sie `create-trail` in der CloudTrail AWS-Dokum entation unter Verwenden.	Lösungsarchitekt
Aktivieren CloudTrail Sie die Überprüfung der Protokoll datei.	Aktivieren Sie die Validieru ng von CloudTrail Protokoll dateien. Weitere Informationen dazu finden Sie CloudTrail in der CloudTrail AWS-Dokum entation unter Aktivieren der Protokolldatei-Integritätsp rüfung für.	Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beschränken Sie den Zugriff auf alle S3-Buckets, die CloudTrail Protokolle enthalten .	Wenden Sie eine Bucket-Richtlinie an, die den Zugriff auf S3-Buckets einschränkt, die Protokolldateien enthalten CloudTrail . Weitere Informationen dazu finden Sie unter Amazon S3 S3-Bucket-Richtlinie für CloudTrail in der CloudTrail AWS-Dokumentation.	Lösungsarchitekt
Integrieren Sie CloudTrail mit CloudWatch Protokollen	Integrieren Sie CloudTrail mit Amazon CloudWatch Logs generierte Trails. Weitere Informationen dazu finden Sie in der CloudTrail AWS-Dokumentation unter Ereignisse an CloudWatch Logs senden	Lösungsarchitekt
Aktivieren Sie AWS Config in allen erforderlichen Regionen.	Aktivieren Sie AWS Config automatisch in allen erforderlichen Regionen. Sie können AWS Config mithilfe der AWS-CLI einrichten. Weitere Informationen finden Sie unter Einrichten von AWS Config mit der AWS-CLI in der AWS Config-Dokumentation.	Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie die Protokollierung des S3-Bucket-Zugriffs.	Automatisieren Sie die Protokollierung des S3-Bucket-Zugriffs mit CloudTrail. Weitere Informationen dazu finden Sie in der Amazon S3-Dokumentation unter Aktivieren der CloudTrail Ereignisprotokollierung für S3-Buckets und -Objekte.	Lösungsarchitekt
Konfigurieren Sie die AWS KMS KMS-Schlüsselrichtlinien für CloudTrail.	Automatisieren Sie die Konfiguration der wichtigsten Richtlinien des AWS Key Management Service (AWS KMS) für CloudTrail. Weitere Informationen dazu finden Sie CloudTrail in der CloudTrail AWS-Dokumentation unter Configure AWS KMS key policies for.	Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verschlüsseln Sie CloudTrail Protokolle im Ruhezustand.	Konfigurieren Sie die serversei tige Verschlüsselung von CloudTrail Protokollen mithilfe von kundenverwalteten Schlüsseln, die in AWS KMS gespeichert sind. Weitere Informationen dazu finden Sie in der AWS-Dokum entation unter Verschlüs seln von CloudTrail Protokoll dateien mit verwalteten AWS-Schlüsseln (SSE-KMS). CloudTrail	Lösungsarchitekt
Automatisches Rotieren von KMS-Schlüsseln.	Konfigurieren Sie die Rotation von AWS-KMS-Schlüsseln. Weitere Informationen dazu finden Sie in der AWS KMS KMS-Dokumentation unter So aktivieren und deaktivieren Sie die automatische Schlüssel rotation.	Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
CloudWatch Alarme konfiguri eren.	Konfigurieren Sie die CloudWatch Amazon-Alarme, die durch bestimmte Ereigniss e ausgelöst werden. Zum Beispiel unbefugte Anfragen an das Root-Konto APIs oder dessen Nutzung. Weitere Informationen dazu finden Sie im AWS-Siche rheitsblog unter So erhalten Sie Benachrichtigungen, wenn die Root-Zugriffsschlüssel Ihres AWS-Kontos verwendet werden.	Lösungsarchitekt
Konfigurieren Sie Sicherhei tsgruppen.	Konfigurieren Sie Sicherhei tsgruppen, um sicherzus tellen, dass uneingeschränkter eingehender Datenverkehr auf den Ports 22 und 3389 nicht zulässig ist.	Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie die VPC-Flow-Protokollierung.	Erfassen Sie abgelehnt en IP-Verkehr zu und von Netzwerkschnittstellen in Ihrer Virtual Private Cloud (VPC) und konfigurieren Sie ihn so CloudWatch , dass er erfasst wird. Weitere Informationen dazu finden Sie unter Erstellen eines Flow-Protokolls in der Amazon VPC-Dokumentation.	Lösungsarchitekt
Ändern Sie die Standards icherheitsgruppe, um den gesamten Datenverkehr einzuschränken.	Ändern Sie die Standards icherheitsgruppe jeder VPC so, dass der Datenverkehr standardmäßig verweigert wird und der Zugriff explizit über Ihre Sicherheitsgruppen gewährt wird. Weitere Informationen dazu finden Sie unter Sicherhei tsgruppen für Ihre VPC in der Amazon VPC-Dokumentation.	Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Routingta bellen zwischen den VPCs.	Konfigurieren Sie die Routingtabellen für VPC-Peering mit dem geringsten erforderlichen Zugriff. Weitere Informationen dazu finden Sie unter Aktualisieren Ihrer Routing-Tabellen für eine VPC-Peering-Verbindung in der Amazon VPC-Dokum entation.	Lösungsarchitekt

Einrichtungsaktivitäten für die neue AWS-Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die AWS-Infra struktur bereit.	Erstellen Sie die AWS-Konten und Ressourcen. Dauer: Zwei Wochen	DevOps Ingenieur, Lösungsar chitekt
Richten Sie DevOps Tools und Prozesse ein.	Richten Sie DevOps Tools und Verfahren ein, z. B. CI/CD-Pip elines (Continuous Integrati on and Continuous Delivery) und automatisierte Test-Fram eworks.	DevOps Ingenieur, Lösungsar chitekt
Automatisieren Sie die Migration von Kernkompo nenten.	Verwenden Sie vorhanden e Vorlagen oder Skripts, um die Installation und Konfigura tion von OpenText Produkten wie TeamSite LiveSite, OpenDeploy und zu automatis ieren MediaBin.	DevOps Ingenieur, Lösungsar chitekt, OpenText Leiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dauer: Eine Woche	
Automatisieren Sie die Migration zusätzlicher Komponenten.	Analysieren und automatisieren Sie die Migration zusätzlicher Anwendungen, die in OpenText Kernkomponenten integriert sind (z. B. zusätzliche Datenbanken, Kommunikations-, Überwachungs- oder Cache-Komponenten). Dauer: Zwei Wochen	DevOps Ingenieur, Lösungsarchitekt, OpenText Leiter
Passen Sie die Kernkomponenten an.	Nehmen Sie alle erforderlichen Änderungen an den Anpassungen der OpenText Kernkomponenten vor (z. B. Integrationen).	Lösungsarchitekt, OpenText Leiter, OpenText Entwickler, Integrationsentwickler eines Drittanbieters, Frontend-Entwickler
Implementieren und konfigurieren Sie zusätzliche Dienste.	Stellen Sie alle neuen AWS-Services wie AWS Lambda-Funktionen oder Amazon API Gateway bereit, konfigurieren und implementieren.	DevOps Ingenieur, Lösungsarchitekt, Integrationsentwickler eines Drittanbieters, Frontend-Entwickler
Migrieren oder überarbeiten Sie andere Komponenten.	Migrieren Sie zusätzliche Komponenten, einschließlich aller erforderlichen Umgestaltungen. Dazu gehören externe Anwendungen wie maßgeschneiderte Berichtsportale oder bestehende API-Integrationsebenen.	DevOps Ingenieur, Lösungsarchitekt, Integrationsentwickler eines Drittanbieters, Frontend-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Migration in der Entwicklungsumgebung durch.	Automatisierte Migration saktivitäten für die Entwicklungsumgebung, einschließlich Systembereitstellung, Datenmigration, Anwendungsmigration, Installation und Konfiguration.	DevOps Ingenieur
Führen Sie die Migration in der Produktionsumgebung durch.	Automatisierte Migration saktivitäten für die Produktionsumgebung, einschließlich Systembereitstellung, Datenmigration, Anwendungsmigration, Installation und Konfiguration.	DevOps Ingenieur

Netzwerkaktivitäten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie CIDR-Blöcke für jede VPC.	Definieren Sie den CIDR-Block (Classless Inter-Domain Routing) (IP-Bereich und Maske) für jede nicht standardmäßige VPC. Dauer: Weniger als eine Woche	DevOps Ingenieur, Lösungsarchitekt
Definieren Sie Subnetze und Availability Zones.	Definieren Sie die Subnetze und Availability Zones, die in jeder nicht standardmäßigen VPC verwendet werden.	DevOps Ingenieur, Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dauer: Weniger als eine Woche	
Definieren Sie Sicherhei tsgruppen.	Definieren Sie Sicherhei tsgruppen und Sicherhei tsgruppenregeln für die Steuerung der Sicherheit auf AWS-Ressourcen. Dauer: Weniger als eine Woche	DevOps Ingenieur, Lösungsar chitekt
Definieren Sie Netzwerk ACLs.	Definieren Sie die Netzwerkz ugriffskontrolllisten (ACLs), um die Sicherheit an den Subnetzgrenzen zu kontrolli eren. Dauer: Weniger als eine Woche	DevOps Ingenieur, Lösungsar chitekt

Datenbanken migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Quelldate nbanken vor.	Verwenden Sie AWS DMS, um jede Quelldatenbank für die laufende Replikation in die AWS-Cloud vorzubereiten.	DevOps Ingenieur, Lösungsar chitekt
Erstellen Sie die Datenbanken für die OpenText Kernkompo nenten.	Erstellen Sie die Datenbank en, die für die Komponenten Opentext TeamSite LiveSite, und MediaBin erforderlich sind. Stellen Sie sicher, dass Benutzer und Zugriffsrechte	Lösungsarchitekt, OpenText Leiter, OpenText Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	gemäß der OpenText Installationsdokumentation korrekt konfiguriert sind.	
Kopieren Sie Daten von Quelldatenbankservern.	Automatisieren Sie den Vorgang des Kopierens von Daten für OpenText Kernkomponenten vom Quelldatenbankserver auf den Zieldatenbankserver.	Lösungsarchitekt, OpenText Leiter, OpenText Entwickler
Synchronisieren Sie Daten von den Datenbankservern.	Automatisieren Sie den Prozess der regelmäßigen Datensynchronisierung von den Quelldatenbanken zu den Zieldatenbanken.	OpenText Entwickler

Aktivitäten zur Migration von Inhalten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopieren Sie die OpenText TeamSite Inhaltsspeicher.	Automatisieren Sie den Vorgang des Kopierens der Inhaltsspeicher vom OpenText TeamSite Quellserver auf den OpenText TeamSite Zielserver.	Lösungsarchitekt, OpenText Leiter, OpenText Entwickler
Ordnen Sie Benutzer und Gruppen zu.	Interne Zuordnung des internen OpenText TeamSite Benutzers IDs zum Zielsystem IDs.	OpenText führen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Synchronisieren Sie die OpenText TeamSite Inhaltsspeicher.	Automatisieren Sie den Prozess der regelmäßigen Synchronisierung von Quell- und Zielinhaltsspeichern. Dies wird im Rahmen des Migrations- und Qualitätssicherungsprozesses implementiert.	OpenText Entwickler
Daten von Webservern kopieren.	Automatisieren Sie den Vorgang des Kopierens von Daten von den Quell-Webservern auf die Ziel-Webserver.	Lösungsarchitekt, OpenText Leiter, OpenText Entwickler
Synchronisieren Sie die Webserver-Daten.	Automatisieren Sie den Prozess der regelmäßigen Synchronisierung von Quell- und Ziel-Webserverdaten.	OpenText Entwickler
Kopieren Sie Daten aus dem Dateisystem des Webservers.	Automatisieren Sie das Kopieren von Inhalten und anderen Web-Assets aus dem Dateisystem des Quell-Webservers auf die Ziel-Webserver.	Lösungsarchitekt, OpenText Leiter, OpenText Entwickler
Synchronisieren Sie die Dateisysteme des Webservers.	Automatisieren Sie den Prozess der regelmäßigen Synchronisierung von Inhalten und anderen Web-Assets vom Dateisystem des Quell-Webservers mit den Ziel-Webservern.	OpenText Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie Feeds und Indizes.	Automatisieren Sie die Ausführung aller Prozesse, die Feeds oder andere Indizes generieren (z. B. Websuche) , die unsere OpenText TeamSite Webserver-Inhalte als Datenquelle verwenden.	Lösungsarchitekt, OpenText Leiter, Entwickler OpenText
Synchronisieren Sie die Generierung von Feeds und Indizes.	Automatisieren Sie den Prozess der regelmäßigen Neuerstellung von Feeds und Indizes nach Datensync hronisationen.	OpenText Entwickler

Test- und QA-Aktivitäten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Migrations-QA durch.	Testen Sie die AWS-Zielu mgebung, -anwendungen und -Services, um sicherzus tellen, dass die automatis ierten Migrationsprozesse korrekt erstellt und konfiguriert sind.	DevOps Ingenieur, OpenText Leiter, QA-Tester
Führen Sie Leistungstests durch.	Testen Sie die Leistung im Hinblick auf Reaktions fähigkeit und Stabilität unter einer bestimmten Arbeitsla st. Untersuchen, messen, validieren oder verifizieren Sie andere Qualitätsmerkmale des Zielsystems, wie Skalierbarkeit und Zuverlässigkeit.	DevOps Ingenieur, OpenText Leiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Damit dieser Test nützlich ist, müssen Sie über eine Testumgebung verfügen, die dieselbe Größe wie Ihre Produktionsumgebung hat. Dauer: Zwischen einer und zwei Wochen	
Sicherheitstests.	Schwachstellenscans und Penetrationstests zur Aufdeckung potenzieller Schwachstellen in den Sicherheitsmechanismen einer Anwendung, die Daten schützt und die Funktionalität nach Bedarf aufrechterhält. Damit dieser Test nützlich ist, müssen Sie über eine Testumgebung verfügen, die in Bezug auf Netzwerk und Sicherheit Ihrer Produktio nsumgebung entspricht. Dauer: Zwischen einer und zwei Wochen	DevOps Ingenieur, OpenText Leiter

Aktivitäten zur betrieblichen Integration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Betriebsb ereitschaft.	Erfahren Sie, wie Sie derzeit IT-Operationen durchführen und wie Sie in der AWS-Cloud arbeiten werden. Sie können	DevOps Ingenieur, OpenText Leiter, Leiter der Servicebe reitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dieses Geschäftsergebnis erzielen, indem Sie ein Cloud-Betriebsmodell definieren. Dauer: Eine Woche	
Investieren Sie in die Betriebsautomatisierung.	Investieren Sie in Automatisierung, um ein AWS-Betriebsmodell bereitzustellen.	DevOps Ingenieur, OpenText Leiter, Leiter der Servicebereitstellung
Integrieren Sie den Betrieb.	Verwenden Sie weiterhin aktuelle IT-Tools und erweitern Sie sie durch die Integration in die AWS-Cloud.	DevOps Ingenieur, OpenText Leiter, Leiter der Servicebereitstellung

Umstellungsaktivitäten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
DNS wechseln.	Wechseln Sie das Domain Name System (DNS) manuell von vorhandenen Hosts zu Hosts, die in der AWS-Cloud basieren. Dauer: Eine Stunde	DevOps Ingenieur, OpenText Leiter
Testen Sie die Notfallwiederherstellung.	Testen Sie Disaster Recovery, Backup und Wiederherstellung und führen Sie Ihre automatisierten Tests durch. Dauer: Ein Tag	DevOps Ingenieur, OpenText Leiter, QA-Tester

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie Überwachung und Analytik.	Stellen Sie sicher, dass die Überwachung und Analyse funktionieren. Dauer: Zwei Stunden	DevOps Ingenieur, OpenText Leiter
Schalten Sie die alte Umgebung aus und fordern Sie das Herunterfahren des Servers an.	Dauer: Drei Tage	DevOps Ingenieur, OpenText Leiter

Zugehörige Ressourcen

- Kundenverwaltete Richtlinien
- Einen IAM-Benutzer in Ihrem AWS-Konto erstellen
- IAM-Benutzergruppen
- Einer IAM-Benutzergruppe eine Richtlinie zuordnen
- Überwachung Ihrer Nutzung und Ihrer Kosten
- Verwaltung eines AWS-Kontos
- IAM-Rollen für Amazon EC2
- Zugriffsberechtigungen für den AWS-Support
- Verwenden von Create-Trail
- Aktivierung der Integritätsprüfung der Protokolldatei für CloudTrail
- Amazon S3 S3-Bucket-Richtlinie für CloudTrail
- Ereignisse an CloudWatch Logs senden
- AWS Config mit der AWS-CLI einrichten
- Aktivieren der CloudTrail Ereignisprotokollierung für S3-Buckets und -Objekte
- Konfiguration von AWS KMS KMS-Schlüsselrichtlinien für CloudTrail
- Verschlüsselung von CloudTrail Protokolldateien mit verwalteten AWS KMS KMS-Schlüsseln (SSE-KMS)
- Wie aktiviere und deaktiviere ich die automatische Schlüsselrotation

- So erhalten Sie Benachrichtigungen, wenn die Root-Zugriffsschlüssel Ihres AWS-Kontos verwendet werden
- Ein Flow-Protokoll erstellen
- Sicherheitsgruppen für Ihre VPC
- Aktualisierung Ihrer Routentabellen für eine VPC-Peering-Verbindung

Migrieren Sie Oracle CLOB-Werte in einzelne Zeilen in PostgreSQL auf AWS

Erstellt von Sai Krishna Namburu (AWS) und Sindhusha Paturu (AWS)

Übersicht

Dieses Muster beschreibt, wie die Werte von Oracle Character Large Object (CLOB) in Amazon Aurora PostgreSQL-Compatible Edition und Amazon Relational Database Service (Amazon RDS) für PostgreSQL in einzelne Zeilen aufgeteilt werden. PostgreSQL unterstützt den CLOB-Datentyp nicht.

Tabellen mit Intervallpartitionen werden in der Oracle-Quelldatenbank identifiziert, und der Tabellenname, der Partitionstyp, das Partitionsintervall und andere Metadaten werden erfasst und in die Zieldatenbank geladen. Sie können CLOB-Daten mit einer Größe von weniger als 1 GB mithilfe von AWS Database Migration Service (AWS DMS) als Text in Zieltabellen laden, oder Sie können die Daten im CSV-Format exportieren, in einen Amazon Simple Storage Service (Amazon S3) -Bucket laden und in Ihre PostgreSQL-Zieldatenbank migrieren.

Nach der Migration können Sie den benutzerdefinierten PostgreSQL-Code, der mit diesem Muster bereitgestellt wird, verwenden, um die CLOB-Daten basierend auf der neuen Zeilenzeichen-ID (`CHR(10)`) in einzelne Zeilen aufzuteilen und die Zieltabelle aufzufüllen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Oracle-Datenbanktabelle mit Intervallpartitionen und Datensätzen mit einem CLOB-Datentyp.
- Eine Aurora PostgreSQL-kompatible oder Amazon RDS for PostgreSQL PostgreSQL-Datenbank mit einer Tabellenstruktur, die der Quelltabelle ähnelt (dieselben Spalten und Datentypen).

Einschränkungen

- Der CLOB-Wert darf 1 GB nicht überschreiten.
- Jede Zeile in der Zieltabelle muss eine neue Zeilenzeichen-ID haben.

Versionen der Produkte

- Oracle 12c
- Aurora Postgres 11.6

Architektur

Das folgende Diagramm zeigt eine Oracle-Quelltabelle mit CLOB-Daten und die entsprechende PostgreSQL-Tabelle in Aurora PostgreSQL-kompatibler Version 11.6.

Tools

AWS-Services

- Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt.
- Amazon Relational Database Service (Amazon RDS) für PostgreSQL unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen PostgreSQL-Datenbank in der AWS-Cloud.
- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS-Cloud oder zwischen Kombinationen von Cloud- und lokalen Setups.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere Tools

Sie können die folgenden Client-Tools verwenden, um eine Verbindung zu Ihren Aurora PostgreSQL-kompatiblen Datenbanken und Amazon RDS for PostgreSQL PostgreSQL-Datenbanken herzustellen, darauf zuzugreifen und diese zu verwalten. (Diese Tools werden in diesem Muster nicht verwendet.)

- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL. Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, verwalten und verwenden können.
- DBeaverist ein Open-Source-Datenbanktool für Entwickler und Datenbankadministratoren. Sie können das Tool verwenden, um Ihre Daten zu manipulieren, zu überwachen, zu analysieren, zu verwalten und zu migrieren.

Bewährte Methoden

Bewährte Methoden für die Migration Ihrer Datenbank von Oracle zu PostgreSQL finden Sie im AWS-Blogbeitrag Bewährte Methoden für die Migration einer Oracle-Datenbank zu Amazon RDS

PostgreSQL oder Amazon Aurora PostgreSQL: Überlegungen zum Migrationsprozess und zur Infrastruktur.

Bewährte Methoden für die Konfiguration der AWS DMS-Aufgabe für die Migration großer binärer Objekte finden Sie unter Migrieren großer binärer Objekte (LOBs) in der AWS DMS-Dokumentation.

Epen

Identifizieren Sie die CLOB-Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie die CLOB-Daten.	Analysieren Sie in der Oracle-Quelldatenbank die CLOB-Daten, um festzustellen, ob sie Spaltenüberschriften enthalten , sodass Sie die Methode zum Laden der Daten in die Zieltabelle festlegen können. Verwenden Sie die folgende Abfrage, um die Eingabedaten zu analysieren. `SELECT * FROM clobdata_or;`	Developer
Laden Sie die CLOB-Daten in die Zieldatenbank.	Migrieren Sie die Tabelle mit CLOB-Daten in eine Zwischentabelle (Staging) in der Aurora- oder Amazon RDS-Zieldatenbank. Sie können AWS DMS verwenden oder die Daten als CSV-Datei in einen Amazon S3 S3-Bucket hochladen. Informationen zur Verwendun g von AWS DMS für diese	Migrationsingenieur, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Aufgabe finden Sie unter Verwenden einer Oracle-Datenbank als Quelle und Verwenden einer PostgreSQL-Datenbank als Ziel in der AWS DMS-Dokumentation. Informationen zur Verwendung von Amazon S3 für diese Aufgabe finden Sie unter Amazon S3 als Ziel verwenden in der AWS DMS-Dokumentation.	

Validieren Sie die PostgreSQL-Zieltabelle.	Überprüfen Sie die Zieldaten, einschließlich der Header, anhand der Quelldaten, indem Sie die folgenden Abfragen in der Zieldatenbank verwenden.
	
	`SELECT * FROM clobdata_pg;`
	`SELECT * FROM clobdatatarget;`
	
	Vergleichen Sie die Ergebnisse mit den Abfrageergebnissen aus der Quelldatenbank (ab dem ersten Schritt).
		Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Teilen Sie die CLOB-Daten in separate Zeilen auf.	Führen Sie den benutzerd efinierten PostgreSQL-Code aus, der im Abschnitt Zusätzlic he Informationen bereitges tellt wird, um die CLOB-Daten aufzuteilen und sie in separate Zeilen in der PostgreSQL-Zieltabelle einzufügen.	Developer

Überprüfen Sie die Daten.

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Daten in der Zieltabelle.	Überprüfen Sie die in die Zieltabelle eingefügten Daten mithilfe der folgenden Abfragen.
	`SELECT * FROM clobdata_pg;`
	`SELECT * FROM clobdatatarget;`
		Developer

Zugehörige Ressourcen

- CLOB-Datentyp (Oracle-Dokumentation)
- Datentypen (PostgreSQL-Dokumentation)

Zusätzliche Informationen

PostgreSQL-Funktion zum Aufteilen von CLOB-Daten

```
do
```

```
$$
declare
totalstr varchar;
str1 varchar;
str2 varchar;
pos1 integer := 1;
pos2 integer ;
len integer;


begin
        select rawdata||chr(10) into totalstr from clobdata_pg;
        len :=  length(totalstr) ;
        raise notice 'Total length : %',len;
        raise notice 'totalstr : %',totalstr;
        raise notice 'Before while loop';


        while pos1 < len  loop


                  select position (chr(10) in totalstr) into pos2;
                 raise notice '1st position of new line : %',pos2;


                str1 := substring (totalstr,pos1,pos2-1);
                raise notice 'str1 : %',str1;


                   insert into clobdatatarget(data) values (str1);
                   totalstr := substring(totalstr,pos2+1,len);
                   raise notice 'new totalstr :%',totalstr;
                len :=  length(totalstr) ;


        end loop;
end
$$
LANGUAGE 'plpgsql' ;
```

Beispiele für Eingabe und Ausgabe

Sie können die folgenden Beispiele verwenden, um den PostgreSQL-Code auszuprobieren, bevor Sie Ihre Daten migrieren.

Erstellen Sie eine Oracle-Datenbank mit drei Eingabezeilen.

```
CREATE TABLE clobdata_or (
id INTEGER GENERATED ALWAYS AS IDENTITY,
rawdata clob  );


insert into clobdata_or(rawdata) values (to_clob('test line 1') || chr(10) ||
 to_clob('test line 2') || chr(10) || to_clob('test line 3') || chr(10));
COMMIT;


SELECT * FROM clobdata_or;
```

Dadurch wird die folgende Ausgabe angezeigt.

id	Rohdaten
1	Testlinie 1 Testlinie 2 Testlinie 3

Laden Sie die Quelldaten zur Verarbeitung in eine PostgreSQL-Staging-Tabelle (`clobdata_pg`).

```
SELECT * FROM clobdata_pg;

CREATE TEMP TABLE clobdatatarget (id1 SERIAL,data VARCHAR );

<Run the code in the additional information section.>

SELECT * FROM clobdatatarget;
```

Dadurch wird die folgende Ausgabe angezeigt.

id1	data
1	Testlinie 1

2	Testlinie 2
3	Testlinie 3

Migrieren Sie eine lokale Oracle-Datenbank zu Amazon RDS for Oracle, indem Sie den direkten Oracle Data Pump-Import über einen Datenbank-Link verwenden

Erstellt von Rizwan Wangde (AWS)

Übersicht

Zahlreiche Muster behandeln die Migration von lokalen Oracle-Datenbanken zu Amazon Relational Database Service (Amazon RDS) for Oracle mithilfe von Oracle Data Pump, einem systemeigenen Oracle-Hilfsprogramm, das die bevorzugte Methode zur Migration großer Oracle-Workloads darstellt. Diese Muster beinhalten in der Regel das Exportieren von Anwendungsschemas oder Tabellen in Dump-Dateien, das Übertragen der Dump-Dateien in ein Datenbankverzeichnis auf Amazon RDS for Oracle und das anschließende Importieren der Anwendungsschemas und Daten aus den Dumpdateien.

Bei diesem Ansatz kann eine Migration länger dauern, abhängig von der Größe der Daten und der Zeit, die für die Übertragung der Dumpdateien auf die Amazon RDS-Instance benötigt wird. Darüber hinaus befinden sich die Dumpdateien auf dem Amazon Elastic Block Store (Amazon EBS) -Volume der Amazon RDS-Instance, das groß genug für die Datenbank und die Dumpdateien sein muss. Wenn die Dump-Dateien nach dem Import gelöscht werden, kann der leere Speicherplatz nicht abgerufen werden. Sie zahlen also weiterhin für ungenutzten Speicherplatz.

Dieses Muster mildert diese Probleme, indem ein direkter Import in die Amazon RDS-Instance mithilfe der Oracle Data Pump API (`DBMS_DATAPUMP`) über einen Datenbank-Link durchgeführt wird. Das Muster initiiert eine gleichzeitige Export- und Import-Pipeline zwischen der Quell- und Zieldatenbank. Dieses Muster erfordert keine Größenänderung eines EBS-Volumes für die Dumpdateien, da keine Dumpdateien auf dem Volume erstellt oder gespeichert werden. Durch diesen Ansatz werden die monatlichen Kosten für ungenutzten Festplattenspeicher eingespart.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Amazon Web Services (AWS) -Konto.
- Eine virtuelle private Cloud (VPC), die mit privaten Subnetzen in mindestens zwei Availability Zones konfiguriert ist, um die Netzwerkinfrastruktur für die Amazon RDS-Instance bereitzustellen.
- Eine Oracle-Datenbank in einem lokalen Rechenzentrum oder selbstverwaltete Datenbank in Amazon Elastic Compute Cloud (Amazon EC2).

- Eine bestehende Amazon RDS for Oracle Oracle-Instance in einer einzigen Availability Zone. Die Verwendung einer einzelnen Availability Zone verbessert die Schreibleistung während der Migration. Eine Multi-AZ-Bereitstellung kann 24—48 Stunden vor der Umstellung aktiviert werden.

  Diese Lösung kann auch Amazon RDS Custom for Oracle als Ziel verwenden.
- AWS Direct Connect (empfohlen für große Datenbanken).
- Lokale Netzwerkkonnektivität und Firewallregeln, die so konfiguriert sind, dass sie eine eingehende Verbindung von der Amazon RDS-Instance zur lokalen Oracle-Datenbank ermöglichen.

Einschränkungen

- Die Datenbankgrößenbeschränkung für Amazon RDS for Oracle beträgt 64 Tebibyte (TiB) (Stand Dezember 2022).
- Die maximale Größe einer einzelnen Datei auf einer Amazon RDS for Oracle Oracle-DB-Instances beträgt 16 TiB. Dies ist wichtig zu wissen, da Sie möglicherweise Tabellen auf mehrere Tablespaces verteilen müssen.

Produktversionen

- Quelldatenbank: Oracle Database Version 10g Release 1 und höher.
- Zieldatenbank: Die aktuelle Liste der unterstützten Versionen und Editionen auf Amazon RDS finden Sie in der AWS-Dokumentation unter Amazon RDS for Oracle.

Architektur

Quelltechnologie-Stack

- Selbstverwaltete Oracle-Datenbank vor Ort oder in der Cloud

Zieltechnologie-Stack

- Amazon RDS for Oracle oder Amazon RDS Custom für Oracle

Zielarchitektur

Das folgende Diagramm zeigt die Architektur für die Migration von einer lokalen Oracle-Datenbank zu Amazon RDS for Oracle in einer Single-AZ-Umgebung. Die Pfeilrichtungen stellen den Datenfluss in der Architektur dar. Das Diagramm zeigt nicht, welche Komponente die Verbindung initiiert.

1. Die Amazon RDS for Oracle Oracle-Instance stellt eine Verbindung zur lokalen Oracle-Quelldatenbank her, um eine Volllastmigration über den Datenbank-Link durchzuführen.
2. AWS Database Migration Service (AWS DMS) stellt eine Verbindung zur lokalen Oracle-Quelldatenbank her, um mithilfe von Change Data Capture (CDC) eine fortlaufende Replikation durchzuführen.
3. CDC-Änderungen werden auf die Amazon RDS for Oracle Oracle-Datenbank angewendet.

Tools

AWS-Services

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS Cloud oder zwischen Kombinationen von Cloud- und lokalen Setups. Dieses Muster verwendet CDC und die Einstellung Nur Datenänderungen replizieren.
- AWS Direct Connectverbindet Ihr internes Netzwerk über ein Standard-Ethernet-Glasfaserkabel mit einem AWS Direct Connect Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt zur Öffentlichkeit einrichten AWS-Services und dabei Internetdienstanbieter in Ihrem Netzwerkpfad umgehen.
- Amazon Relational Database Service unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Oracle-Datenbank in der AWS-Cloud.

Andere Tools

- Mit Oracle Data Pump können Sie Daten und Metadaten mit hoher Geschwindigkeit von einer Datenbank in eine andere verschieben.
- Client-Tools wie Oracle Instant Client oder SQL Developer werden verwendet, um eine Verbindung herzustellen und SQL-Abfragen in der Datenbank auszuführen.

Bewährte Methoden

Es werden zwar dedizierte, private Netzwerkverbindungen zwischen dem lokalen Netzwerk AWS Direct Connect verwendet und AWS dennoch sollten Sie die folgenden Optionen für zusätzliche Sicherheit und Datenverschlüsselung bei der Übertragung von Daten in Betracht ziehen:

- Ein virtuelles privates Netzwerk (VPN) AWS Site-to-Site VPN oder eine IPsec VPN-Verbindung vom lokalen Netzwerk zum Netzwerk AWS
- Oracle Database Native Network Encryption, konfiguriert in der lokalen Oracle-Datenbank
- Verschlüsselung mit TLS

Epen

Bereiten Sie die lokale Oracle-Quelldatenbank vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Netzwerkk onnektivität von der Zieldaten bank zur Quelldatenbank ein.	Konfigurieren Sie das lokale Netzwerk und die Firewall so, dass eingehende Verbindun gen von der Amazon RDS-Zielinstanz zur lokalen Oracle-Quelldatenbank zugelassen werden.	Netzwerkadministrator, Sicherheitsingenieur

Erstellen Sie einen Datenbank benutzer mit den entsprech enden Rechten.	Erstellen Sie einen Datenbank benutzer in der lokalen Oracle-Quelldatenbank mit Rechten zur Migration von Daten zwischen der Quelle und dem Ziel mithilfe von Oracle Data Pump:
	`GRANT CONNECT to <migration_user>;`
	`GRANT DATAPUMP_EXP_FULL_DATABASE to <migration_user>;`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`GRANT SELECT ANY TABLE to <migration_user>;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bereiten Sie die lokale Quelldatenbank für die AWS DMS CDC-Migration vor.	(Optional) Bereiten Sie die lokale Oracle-Quelldatenbank für die AWS DMS CDC-Migration nach Abschluss von Oracle Data Pump Full Load vor:
	1. Konfigurieren Sie die zusätzlichen Rechte, die für die Verwaltung von FLASHBACK während der Oracle Data Pump-Migration erforderlich sind:
	`GRANT FLASHBACK ANY TABLE to <migration_user>;`
	`GRANT FLASHBACK ARCHIVE ADMINISTER to <migration_user>;`
	2. Informationen zur Konfiguration der Benutzerkontenberechtigungen, die für eine selbstverwaltete Oracle-Quelle für erforderlich sind AWS DMS, finden Sie in der AWS DMS Dokumentation.
	3. Informationen zur Vorbereitung einer selbstverwalteten Oracle-Quelldatenbank für die Verwendung mit CDC finden Sie in der AWS DMS Dokumentation.AWS DMS
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren und konfigurieren Sie SQL Developer.	Installieren und konfigurieren Sie SQL Developer, um eine Verbindung herzustellen und SQL-Abfragen in der Quell- und Zieldatenbank auszuführ en.	DBA, Migrationsingenieur
Generieren Sie ein Skript, um die Tablespaces zu erstellen.	Verwenden Sie die folgende Beispiel-SQL-Abfrage, um das Skript in der Quelldatenbank zu generieren: `SELECT 'CREATE TABLESPACE ' tablespace_name ' DATAFILE SIZE 1G AUTOEXTEND ON MAXSIZE UNLIMITED;' from dba_tablespaces where tablespace_name not in ('SYSTEM', 'SYSAUX','TEMP','UNDOTBS1') order by 1;` Das Skript wird auf die Zieldatenbank angewendet.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie ein Skript zum Erstellen von Benutzern, Profilen, Rollen und Rechten.	Um ein Skript zur Erstellung der Datenbankbenutzer, Profile, Rollen und Rechte zu generieren, verwenden Sie die Skripten aus dem Oracle Support-Dokument How to Extract DDL for User including Privileges and Roles Using dbms_metadata.get_ddl (Doc ID 2739952.1) (Oracle-Konto erforderlich). Das Skript wird auf die Zieldatenbank angewendet.	DBA

Bereiten Sie die Amazon RDS-Zielinstanz für Oracle vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Datenbank-Link zur Quelldatenbank und überprüfen Sie die Konnektivität.	Um einen Datenbank-Link zur lokalen Quelldatenbank zu erstellen, können Sie den folgenden Beispielbefehl verwenden: `CREATE DATABASE LINK link2src CONNECT TO <migration_user_account> IDENTIFIED BY <password> USING '(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=<dns or ip address of remote db>)`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(PORT=<li stener port>))(C ONNECT_DATA=(SID=< remote SID>)))'; Führen Sie den folgenden SQL-Befehl aus, um die Konnektivität zu überprüfen: select * from dual@link 2src; Die Konnektivität ist erfolgrei ch, wenn die X Antwort	
Führen Sie die Skripts aus, um die Zielinstanz vorzubereiten.	Führen Sie die zuvor generiert en Skripts aus, um die Amazon RDS for Oracle Oracle-Zielinstanz vorzubere iten: 1. Tablespaces 2. Profile 3. Rollen Dadurch wird sichergestellt, dass die Oracle Data Pump-Migration die Schemas und ihre Objekte erstellen kann.	DBA, Migrationsingenieur

Führen Sie eine Volllastmigration durch, indem Sie Oracle Data Pump Import über einen Datenbank-Link verwenden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie die erforderlichen Schemas.	Verwenden Sie den Code im Abschnitt Zusätzliche Informationen, um die erforderlichen Schemas von der lokalen Quelldatenbank zur Amazon RDS-Zielinstanz zu migrieren: • Um ein einzelnes Schema zu migrieren, führen Sie Code 1 im Abschnitt Zusätzliche Informationen aus. • Um mehrere Schemas zu migrieren, führen Sie Code 2 im Abschnitt Zusätzliche Informationen aus. Um die Leistung der Migration zu optimieren, können Sie die Anzahl der parallel Prozesse anpassen, indem Sie den folgenden Befehl ausführen: `DBMS_DATAPUMP.SET_ PARALLEL (handle => v_hdnl, degree => 4);`	DBA
Sammeln Sie Schemastatistiken, um die Leistung zu verbessern.	Der Befehl Gather Schema Statistics gibt die für Datenbankobjekte gesammelten Statistiken des Oracle Query Optimizers zurück.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Mithilfe dieser Informationen kann der Optimierer den besten Ausführungsplan für jede Abfrage anhand dieser Objekte auswählen: `EXECUTE DBMS_STATS.GATHER_SCHEMA_STATS(ownname => '<schema_name>');`	

Führen Sie eine Volllastmigration und CDC-Replikation mithilfe von Oracle Data Pump durch und AWS DMS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erfassen Sie das SCN in der lokalen Oracle-Quelldatenbank.	Erfassen Sie die Systemänderungsnummer (SCN) in der lokalen Oracle-Quelldatenbank. Sie verwenden die SCN für den Volllast-Import und als Ausgangspunkt für die CDC-Replikation. Führen Sie die folgende SQL-Anweisung aus, um die aktuelle SCN in der Quelldatenbank zu generieren: `SELECT current_scn FROM V$DATABASE;`	DBA
Führen Sie die Volllastmigration der Schemas durch.	Gehen Sie wie folgt vor, um die erforderlichen Schemas (`FULL LOAD`) von der lokalen	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Quelldatenbank zur Amazon RDS-Zielinstanz zu migrieren: • Um ein einzelnes Schema zu migrieren, führen Sie Code 3 im Abschnitt Zusätzliche Informationen aus. • Um mehrere Schemas zu migrieren, führen Sie Code 4 im Abschnitt Zusätzliche Informationen aus. Ersetzen Sie den Code `<CURRENT_SCN_VALUE _IN_SOURCE_DATABAS E>` durch die SCN, die Sie aus der Quelldatenbank erfasst haben: `DBMS_DATAPUMP.SET_ PARAMETER (handle => v_hdnl, name => 'FLASHBACK_SCN', value => <CURRENT_SCN_VALUE _IN_SOURCE_DATABAS E>);` Um die Leistung der Migration zu optimieren, können Sie die Anzahl der parallel Prozesse anpassen:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);`	
Deaktivieren Sie die Trigger unter den migrierten Schemas.	Bevor Sie mit der reinen AWS DMS CDC-Aufgabe beginnen, deaktivieren Sie die `TRIGGERS` unter den migrierten Schemas aufgeführten.	DBA
Sammeln Sie Schemasta tistiken, um die Leistung zu verbessern.	Der Befehl Gather Schema Statistics gibt die für Datenbankobjekte gesammelten Statistiken des Oracle Query Optimizers zurück: `EXECUTE DBMS_STATS.GATHER_SCHEMA_STATS(ownname => '<schema_name>');` Mithilfe dieser Informationen kann der Optimierer den besten Ausführungsplan für jede Abfrage anhand dieser Objekte auswählen.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wird verwendet AWS DMS , um eine fortlaufende Replikation von der Quelle zum Ziel durchzuführen.	Wird verwendet AWS DMS , um eine fortlaufende Replikation von der Oracle-Quelldatenbank zur Amazon RDS for Oracle Oracle-Zielinstanz durchzuführen. Weitere Informationen finden Sie unter Erstellen von Aufgaben für die laufende Replikation mithilfe von AWS DMS und im Blogbeitrag How to work with native CDC support in AWS DMS.	DBA, Migrationsingenieur

Wechseln Sie zu Amazon RDS for Oracle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie Multi-AZ auf der Instance 48 Stunden vor der Umstellung.	Wenn es sich um eine Produktionsinstanz handelt, empfehlen wir, die Multi-AZ-Bereitstellung auf der Amazon RDS-Instance zu aktivieren, um die Vorteile von Hochverfügbarkeit (HA) und Disaster Recovery (DR) nutzen zu können.	DBA, Migrationsingenieur
Beenden Sie die AWS DMS reine CDC-Aufgabe (falls CDC aktiviert war).	1. Stellen Sie sicher, dass die Quelllatenz und die Ziellatenz in den CloudWatch Amazon-Metriken der AWS DMS Aufgabe 0 Sekunden anzeigen.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Beenden Sie die AWS DMS reine CDC-Aufgabe.	
Aktivieren Sie die Auslöser.	Aktivieren Sie die`TRIGGERS`, die Sie vor der Erstellung der CDC-Aufgabe deaktiviert haben.	DBA

Zugehörige Ressourcen

AWS

- Vorbereiten einer selbstverwalteten Oracle-Quelldatenbank für CDC mit AWS DMS
- Aufgaben für die laufende Replikation erstellen mit AWS DMS
- Multi-AZ-Bereitstellungen für hohe Verfügbarkeit
- Wie arbeitet man mit nativer CDC-Unterstützung in AWS DMS(Blogbeitrag)

Oracle-Dokumentation

- DBMS_DATAPUMP

Zusätzliche Informationen

Code 1: Nur Volllastmigration, einzelnes Anwendungsschema

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE( handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'SCHEMA_EXPR','IN (''<schema_name>'')');  --
 To migrate one selected schema
    DBMS_DATAPUMP.METADATA_FILTER (hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')'); --
 To prevent gathering Statistics during the import
```

```
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Code 2: Nur Volllastmigration, mehrere Anwendungsschemas

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE( handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'SCHEMA_LIST',
 '''<SCHEMA_1>'',''<SCHEMA_2>'', ''<SCHEMA_3>'''); -- To migrate multiple schemas
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')');
 -- To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Code 3: Volllastmigration vor einer reinen CDC-Aufgabe, einzelnes Anwendungsschema

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE( handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'SCHEMA_EXPR','IN (''<schema_name>'')');  --
 To migrate one selected schema
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')');
 -- To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARAMETER (handle => v_hdnl, name => 'FLASHBACK_SCN', value =>
 <CURRENT_SCN_VALUE_IN_SOURCE_DATABASE>); -- SCN required for AWS DMS CDC only task.
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
    DBMS_DATAPUMP.START_JOB(v_hdnl);
```

```
END;
/
```

Code 4: Volllastmigration vor einer reinen CDC-Aufgabe, mehrere Anwendungsschemas

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN (operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE (handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'SCHEMA_LIST',
 '''<SCHEMA_1>'',''<SCHEMA_2>'', ''<SCHEMA_3>'''); -- To migrate multiple schemas
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')');
 -- To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARAMETER (handle => v_hdnl, name => 'FLASHBACK_SCN', value =>
 <CURRENT_SCN_VALUE_IN_SOURCE_DATABASE>); -- SCN required for AWS DMS CDC only task.
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Szenario, in dem ein gemischter Migrationsansatz besser funktionieren kann

In seltenen Szenarien, in denen die Quelldatenbank Tabellen mit Millionen von Zeilen und sehr großen LOBSEGMENT-Spalten enthält, verlangsamt dieses Muster die Migration. Oracle migriert nacheinander LOBSEGMENTs über die Netzwerkverbindung. Es extrahiert eine einzelne Zeile (zusammen mit den LOB-Spaltendaten) aus der Quelltabelle und fügt die Zeile in die Zieltabelle ein. Dabei wird der Vorgang wiederholt, bis alle Zeilen migriert sind. Oracle Data Pump über den Datenbank-Link unterstützt keine Massenlademechanismen oder direkte Pfadlademechanismen für. LOBSEGMENTs

In dieser Situation empfehlen wir Folgendes:

- Überspringen Sie die identifizierten Tabellen während der Oracle Data Pump-Migration, indem Sie den folgenden Metadatenfilter hinzufügen:

```
dbms_datapump.metadata_filter(handle =>h1, name=>'NAME_EXPR', value => 'NOT IN
 (''TABLE_1'',''TABLE_2'')');
```

- Verwenden Sie eine AWS DMS Aufgabe (Volllastmigration, bei Bedarf mit CDC-Replikation), um die identifizierten Tabellen zu migrieren. AWS DMS extrahiert mehrere Zeilen aus der Oracle-Quelldatenbank und fügt sie in einem Batch in die Amazon RDS-Zielinstanz ein, wodurch die Leistung verbessert wird.

Migrieren Sie die Oracle E-Business Suite zu Amazon RDS Custom

Erstellt von Simon Cunningham (AWS), Jaydeep Nandy (AWS), Nitin Saxena (AWS) und Vishnu Vinnakota (AWS)

Übersicht

Die Oracle E-Business Suite ist eine ERP-Lösung (Enterprise Resource Planning) zur Automatisierung unternehmensweiter Prozesse wie Finanzen, Personalwesen, Lieferketten und Fertigung. Sie hat eine dreistufige Architektur: Client, Anwendung und Datenbank. Bisher mussten Sie Ihre Oracle E-Business Suite-Datenbank auf einer selbst verwalteten Amazon Elastic Compute Cloud (Amazon EC2) -Instance ausführen, aber jetzt können Sie von Amazon Relational Database Service (Amazon RDS) Custom profitieren.

Amazon RDS Custom for Oracle ist ein verwalteter Datenbankservice für ältere, benutzerdefinierte und verpackte Anwendungen, die Zugriff auf das zugrunde liegende Betriebssystem und die Datenbankumgebung benötigen. Er automatisiert Aufgaben und Operationen der Datenbankverwaltung und ermöglicht es Ihnen als Datenbankadministrator gleichzeitig, auf Ihre Datenbankumgebung und Ihr Betriebssystem zuzugreifen und diese anzupassen. Wenn Sie Ihre Oracle-Datenbank zu Amazon RDS Custom migrieren, kümmert sich Amazon Web Services (AWS) um schwere Aufgaben wie Backup-Aufgaben und die Sicherstellung einer hohen Verfügbarkeit, während Sie sich auf die Wartung Ihrer Oracle E-Business Suite-Anwendung und Funktionalität konzentrieren können. Wichtige Faktoren, die bei einer Migration zu berücksichtigen sind, finden Sie unter Strategien zur Oracle-Datenbankmigration in AWS Prescriptive Guidance.

Dieses Muster konzentriert sich auf die Schritte zur Migration einer eigenständigen Oracle-Datenbank EC2 auf Amazon RDS Custom mithilfe eines Oracle Recovery Manager (RMAN) -Backups und eines gemeinsam genutzten Amazon Elastic File System (Amazon EFS) -Dateisystems zwischen der EC2 Instance und Amazon RDS Custom. Das Muster verwendet ein vollständiges RMAN-Backup (das manchmal auch als Level-0-Backup bezeichnet wird). Der Einfachheit halber wird ein Cold-Backup verwendet, bei dem die Anwendung heruntergefahren und die Datenbank eingebunden und nicht geöffnet wird. (Sie können auch Oracle Data Guard oder RMAN-Duplication für die Sicherung verwenden. Dieses Muster deckt diese Optionen jedoch nicht ab.)

Informationen zur Architektur der Oracle E-Business Suite auf AWS für Hochverfügbarkeit und Disaster Recovery finden Sie im Muster Einrichten einer HA/DR-Architektur für Oracle E-Business Suite auf Amazon RDS Custom mit einer aktiven Standby-Datenbank.

> **Note**
>
> Dieses Muster enthält Links zu Support-Hinweisen von Oracle. Sie benötigen ein Oracle Support-Konto, um auf diese Dokumente zugreifen zu können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Oracle-Quelldatenbank der Version 12.1.0.2 oder 19c (mindestens 19.3), die auf Amazon EC2 mit Oracle Linux 7 oder Red Hat Enterprise Linux (RHEL) Version 7.x ausgeführt wird. Bei diesem Muster wird davon ausgegangen, dass der Name der Quelldatenbank `VIS` und der Name der zusätzlichen Container-Datenbank für Oracle 19c lauten. Sie können `VISCDB` jedoch auch andere Namen verwenden.

  > **Note**
  >
  > Sie können dieses Muster auch mit lokalen Oracle-Quelldatenbanken verwenden, sofern Sie über die entsprechende Netzwerkkonnektivität zwischen dem lokalen Netzwerk und Amazon Virtual Private Cloud (Amazon VPC) verfügen.

- Eine Anwendung der Oracle E-Business Suite Version 12.2.x (Vision-Instance). Dieses Verfahren wurde auf Version 12.2.11 getestet.
- Eine einzige Oracle E-Business Suite-Anwendungsebene. Sie können dieses Muster jedoch so anpassen, dass es mit mehreren Anwendungsebenen funktioniert.
- Für Oracle 12.1.0.2 wurde Amazon RDS Custom mit mindestens 16 GB Swap-Speicherplatz konfiguriert. Andernfalls wird auf der 12c Examples CD eine Warnung angezeigt. (Oracle 19c benötigt die Beispiel-CD nicht, wie später in diesem Dokument erwähnt wird.)

Führen Sie die folgenden Schritte aus, bevor Sie mit der Migration beginnen:

1. Erstellen Sie auf der Amazon RDS-Konsole eine Amazon RDS Custom for Oracle DB-Instance mit dem Datenbanknamen `VIS` (oder dem Namen Ihrer Quelldatenbank). Anweisungen finden Sie unter Arbeiten mit Amazon RDS Custom in der AWS-Dokumentation und im Blogbeitrag Amazon RDS Custom for Oracle — New Control Capabilities in Database Environment. Dadurch wird sichergestellt, dass der Datenbankname auf denselben Namen wie die Quelldatenbank

gesetzt ist. (Wenn das Feld leer gelassen wird, werden die EC2 Instanz und der Datenbankname auf gesetzt`ORCL`.) Stellen Sie sicher, dass Sie Ihre benutzerdefinierte Engine-Version (CEV) mindestens mit den Patches erstellen, die auf die Quelle angewendet wurden. Weitere Informationen finden Sie unter Vorbereitung der Erstellung eines CEV in der Amazon RDS-Dokumentation.

Hinweis für Oracle 19c: Derzeit kann für Oracle 19c der Name der Amazon RDS-Container-Datenbank angepasst werden. Der Standardwert ist `RDSCDB`. Stellen Sie sicher, dass Sie die benutzerdefinierte RDS-Oracle-Instance mit derselben System-ID (SID) wie auf der EC2 Quell-Instance erstellen. In diesem Muster wird beispielsweise davon ausgegangen, dass sich die Oracle 19c-SID `VISCDB` auf der Quell-Instance befindet. Daher sollte auch die Ziel-SID Oracle 19c auf Amazon RDS Custom sein. `VISCDB`

2. Konfigurieren Sie die Amazon RDS Custom DB-Instance mit ausreichend Speicher, vCPU und Arbeitsspeicher, um der EC2 Amazon-Quelldatenbank zu entsprechen. Zu diesem Zweck können Sie die EC2 Amazon-Instance-Typen auf der Grundlage von vCPU und Arbeitsspeicher abgleichen.
3. Erstellen Sie ein Amazon EFS-Dateisystem und mounten Sie es auf den Amazon EC2 - und Amazon RDS-Custom-Instances. Anweisungen finden Sie im Blogbeitrag Integrate Amazon RDS Custom for Oracle with Amazon EFS. Bei diesem Muster wird davon ausgegangen, dass Sie das Amazon EFS-Volume sowohl `/RMAN` auf der Amazon EC2 RDS-Quell-Instance als auch auf der benutzerdefinierten Amazon RDS-Ziel-Instance bereitgestellt haben und dass Netzwerkkonnektivität zwischen Quell- und Zielinstanz möglich ist. Sie können dieselbe Methode auch verwenden, indem Sie Amazon FSx oder ein beliebiges Shared Drive verwenden.

Annahmen

Bei diesem Muster wird davon ausgegangen, dass Ihre Anwendung und Datenbank logische Hostnamen verwenden, wodurch die Anzahl der Migrationsschritte reduziert wird. Sie können diese Schritte so anpassen, dass physische Hostnamen verwendet werden, aber logische Hostnamen reduzieren die Komplexität des Migrationsprozesses. Informationen zu den Vorteilen der Verwendung logischer Hostnamen finden Sie in den folgenden Support-Hinweisen:

- Für 12c, Oracle Support Note 2246690.1
- Für 19c, Oracle Support Note 2617788.1

Dieses Muster deckt das Upgrade-Szenario von Oracle 12c auf 19c nicht ab und konzentriert sich auf die Migration derselben Version der Oracle-Datenbank, die auf Amazon ausgeführt wird, EC2 zu Amazon RDS Custom for Oracle.

Amazon RDS Custom for Oracle unterstützt die Anpassung von Oracle Home. (Oracle Home speichert die Oracle-Binärdateien.) Sie können den Standardpfad von `/rdsdbbin/oracle` in einen von Ihnen angegebenen Pfad ändern, z. B. `/d01/oracle/VIS/19c` Der Einfachheit halber gehen die Anweisungen in diesem Muster vom Standardpfad aus`/rdsdbbin/oracle`.

Einschränkungen

Dieses Muster unterstützt die folgenden Funktionen und Konfigurationen nicht:

- Setzen des `ARCHIVE_LAG_TARGET` Datenbankparameters auf einen Wert außerhalb des Bereichs von 60—7200
- Deaktivierung des Protokollmodus der DB-Instance () `NOARCHIVELOG`
- Das `EBS-optimized` Attribut der Instance ausschalten EC2
- Ändern der ursprünglichen Amazon Elastic Block Store (Amazon EBS) -Volumes, die an die EC2 Instance angehängt sind
- Neue EBS-Volumes hinzufügen oder den Volume-Typ von bis ändern `gp2` `gp3`
- Support für das TNS-ifile
- Änderung des `control_file` Speicherorts und des Namens (muss sein`/rdsdbdata/db/VISCDB_A/controlfile/control-01.ctl`, wo `VISCDB` ist der CDB-Name)

Weitere Informationen zu diesen und anderen nicht unterstützten Konfigurationen finden Sie unter Reparieren nicht unterstützter Konfigurationen in der Amazon RDS-Dokumentation.

Produktversionen

Informationen zu Oracle-Datenbankversionen und Instance-Klassen, die von Amazon RDS Custom unterstützt werden, finden Sie unter Verfügbarkeit und Anforderungen für Amazon RDS Custom for Oracle.

Architektur

Das folgende Architekturdiagramm stellt ein Oracle E-Business Suite-System dar, das in einer einzigen Availability Zone auf AWS ausgeführt wird. Auf die Anwendungsebene wird über einen Application Load Balancer zugegriffen, sowohl die Anwendung als auch die Datenbanken befinden

sich in privaten Subnetzen, und die Amazon RDS Custom- und EC2 Amazon-Datenbankebene verwenden ein gemeinsam genutztes Amazon EFS-Dateisystem, um die RMAN-Backupdateien zu speichern und darauf zuzugreifen.

Tools

AWS-Services

- Amazon RDS Custom for Oracle ist ein verwalteter Datenbankservice für ältere, benutzerdefinierte und verpackte Anwendungen, die Zugriff auf das zugrunde liegende Betriebssystem und die Datenbankumgebung benötigen. Er automatisiert Aufgaben und Operationen der Datenbankverwaltung und ermöglicht es Ihnen als Datenbankadministrator gleichzeitig, auf Ihre Datenbankumgebung und Ihr Betriebssystem zuzugreifen und diese anzupassen.
- Amazon Elastic File System (Amazon EFS) ist ein einfaches, serverloses, elastisches Dateisystem zum Hinzufügen und Entfernen von Dateien, ohne dass eine Verwaltung oder Bereitstellung erforderlich ist. Dieses Muster verwendet ein gemeinsam genutztes Amazon EFS-Dateisystem, um die RMAN-Backup-Dateien zu speichern und darauf zuzugreifen.
- AWS Secrets Manager ist ein von AWS verwalteter Service, mit dem Sie Datenbankanmeldedaten, API-Schlüssel und andere geheime Informationen einfach rotieren, verwalten und abrufen können. Amazon RDS Custom speichert das key pair und die Anmeldeinformationen des Datenbankbenutzers bei der Datenbankerstellung in Secrets Manager. In diesem Muster rufen Sie die Datenbankbenutzerkennwörter aus Secrets Manager ab, um die `ADMIN` Benutzer `RDSADMIN` und zu erstellen und die Kennwörter sys und system zu ändern.

Andere Tools

- RMAN ist ein Tool, das Backup und Recovery für Oracle-Datenbanken unterstützt. Dieses Muster verwendet RMAN, um ein Cold-Backup der Oracle-Quelldatenbank auf Amazon durchzuführen EC2 , die auf Amazon RDS Custom wiederhergestellt wird.

Bewährte Methoden

- Verwenden Sie logische Hostnamen. Dadurch wird die Anzahl der Post-Clone-Skripts, die Sie ausführen müssen, erheblich reduziert. Weitere Informationen finden Sie in der Oracle Support Note 2246690.1.

- Amazon RDS Custom verwendet standardmäßig Oracle Automatic Memory Management (AMM). Wenn Sie den Hugemem-Kernel verwenden möchten, können Sie Amazon RDS Custom so konfigurieren, dass stattdessen Automatic Shared Memory Management (ASMM) verwendet wird.
- Lassen Sie den `memory_max_target` Parameter standardmäßig aktiviert. Das Framework verwendet diesen Parameter im Hintergrund, um Read Replicas zu erstellen.
- Aktivieren Sie Oracle Flashback Database. Diese Funktion ist in Failover-Testszenarien (nicht in Switchover-Testszenarien) nützlich, um den Standbymodus wiederherzustellen.
- Passen Sie für Datenbankinitialisierungsparameter das Standard-PFILE an, das von der Amazon RDS Custom DB-Instance für Oracle E-Business Suite bereitgestellt wird, anstatt das SPFILE aus der Oracle-Quelldatenbank zu verwenden. Dies liegt daran, dass Leerzeichen und Kommentare Probleme beim Erstellen von Read Replicas in Amazon RDS Custom verursachen. Weitere Informationen zu Datenbankinitialisierungsparametern finden Sie in der Oracle Support Note 396009.1.

Im folgenden Abschnitt Epics haben wir separate Anweisungen für Oracle 12.1.0.2 und 19c bereitgestellt, wobei sich die Details unterscheiden.

Epen

Fahren Sie die Quellanwendung herunter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fahren Sie die Anwendung herunter.	Verwenden Sie die folgenden Befehle, um die Quellanwendung herunterzufahren:
	`$ su - applmgr`
	`$ cd $INST_TOP/admin/scripts`
	`$ ./adstpall.sh`
		DBA

Erstellen Sie die ZIP-Datei.	Erstellen Sie die `appsutil.zip` Datei auf der Ebene der Quellanwendung. Sie werden diese Datei später verwenden, um den benutzerdefinierten	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon RDS-Datenbankknoten zu konfigurieren. `$ perl $AD_TOP/bin/admkappsutil.pl`	
Kopieren Sie die ZIP-Datei nach Amazon EFS.	Kopieren Sie `appsutil.zip` von `$INST_TOP/admin/out` auf Ihr gemeinsam genutztes Amazon EFS-Volume (`/RMAN/appsutil`). Sie können die Datei manuell übertragen, indem Sie Secure Copy (SCP) oder einen anderen Übertragungsmechanismus verwenden.	DBA

Klonen Sie die Quelldatenbank vorab

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Klonen Sie die Datenbankebene auf Amazon EC2 vorab.	Melden Sie sich als Oracle-Benutzer an und führen Sie Folgendes aus:
	`$ cd $ORACLE_HOME/appsutil/scripts/$CONTEXT_NAME`
	`$ perl adpreclone.pl dbTier`
	Überprüfen Sie anhand der generierten Protokolldatei,
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ob der Vorgang erfolgreich abgeschlossen wurde.	

Kopieren Sie appsutil.zip in das gemeinsam genutzte Amazon EFS-Dateisystem.	Erstellen Sie ein TAR-Backup und kopieren `$ORACLE_HOME/appsutil` Sie es in das gemeinsam genutzte Amazon EFS-Dateisystem (zum Beispiel `/RMAN/appsutil`):
	`$ cd $ORACLE_HOME`
	`$ tar cvf sourceappsutil.tar appsutil`
	`$ cp sourceappsutil.tar /RMAN/appsutil`
		DBA

Führen Sie eine kalte RMAN-Vollsicherung der EC2 Amazon-Quelldatenbank durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Backup-Skript.	Führen Sie eine vollständige RMAN-Backup der Quelldatenbank im gemeinsam genutzten Amazon EFS-Dateisystem durch. Der Einfachheit halber führt dieses Muster ein kaltes RMAN-Backup durch. Sie können diese Schritte jedoch ändern, um ein Hot-RMAN-Backup mit Oracle Data Guard	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	durchzuführen, um Ausfallze iten zu reduzieren.
	
	1. Starten Sie die EC2 Amazon-Quelldatenbank im Mount-Modus:
	
	`$ sqlplus / as sysdba`
	`$ SQL> shutdown immediate`
	`$ SQL> startup mount`
	
	2. Erstellen Sie ein RMAN-Backup-Skript (verwenden Sie eines der folgenden Beispiele , abhängig von Ihrer Oracle-Version, oder führen Sie eines Ihrer vorhandenen RMAN-Skri pts aus), um die Datenbank im Amazon EFS-Dateisystem zu sichern, das Sie bereitges tellt haben (`/RMAN`in diesem Beispiel).
	
	Für Oracle 12.1.0.2:
	
	`$ vi FullRMANColdBackup .sh`
	`#!/bin/bash`
	`. /home/oracle/.bash _profile`
	
	`export ORACLE_SID=VIS`
	`export ORACLE_HOME=/ d01/oracle/VIS/12.1.0`
	`export DATE=$(date + %y-%m-%d_%H%M%S)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
rman target / log=/RMAN
/VISDB_${DATE}.log <<
 EOF
run
{
allocate channel ch1
 device type disk format
 '/RMAN/visdb_full_
bkp_%u';
allocate channel ch2
 device type disk format
 '/RMAN/visdb_full_
bkp_%u';
crosscheck backup;
delete noprompt
 obsolete;
BACKUP AS COMPRESSED
 BACKUPSET DATABASE PLUS
 ARCHIVELOG;
backup archivelog all;
release channel ch1;
release channel ch2;
}
EOF
```

Für Oracle 19c:

```
$ vi FullRMANColdBackup
.sh
#!/bin/bash
. /home/oracle/.bash
_profile

export ORACLE_SI
D=VISCDB
export ORACLE_HOME=/
d01/oracle/VIS/19c
export DATE=$(date +
%y-%m-%d_%H%M%S)
```

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`rman target / log=/RMAN /VISDB_${DATE}.log << EOF run { allocate channel ch1 device type disk format '/RMAN/visdb_full_ bkp_%u'; allocate channel ch2 device type disk format '/RMAN/visdb_full_ bkp_%u'; crosscheck backup; delete noprompt obsolete; BACKUP AS COMPRESSED BACKUPSET DATABASE PLUS ARCHIVELOG; backup archivelog all; backup current controlfile format '/ RMAN/cntrl.bak'; release channel ch1; release channel ch2; } EOF`	
Führen Sie das Backup-Skript aus.	Ändern Sie die Berechtigungen, melden Sie sich als Oracle-Benutzer an und führen Sie das Skript aus: `$ chmod 755 FullRMANC oldBackup.sh $ ./FullRMANColdBack up.sh`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Suchen Sie nach Fehlern und notieren Sie sich den Namen der Sicherungsdatei.	Überprüfen Sie die RMAN-Protokolldatei auf Fehler. Wenn alles in Ordnung aussieht, listen Sie die Sicherungskopie der Steuerdatei auf. Notieren Sie sich den Namen der Ausgabedatei.
	
	Für Oracle 12.1.0.2:
	
	`RMAN> connect target /`
	
	`RMAN> list backup of controlfile;`
	
	`BS Key Type LV Size Device Type Elapsed Time Completion Time`
	`------- ---- -- ---------- --------- ---------- ---------- ---

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Sie werden die Sicherungsdatei `/RMAN/visdb_full_bkp_100rlsbt` später verwenden, wenn Sie die Datenbank auf Amazon RDS Custom wiederherstellen.
	
	Für Oracle 19c:
	
	`RMAN> connect target /`
	
	`RMAN> list backup of controlfile;`
	
	`BS Key Type LV Size Device Type Elapsed Time Completion Time`
	`------- ---- -- ---------- --------- ---------- ---------- ---

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Datenbank auf Amazon RDS Custom wiederherstellen.	

Konfiguration der benutzerdefinierten Amazon RDS-Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Ändern Sie die Hosts-Datei und legen Sie den Hostnamen fest.	**Note**
	Die Befehle in diesem Abschnitt müssen als Root-Benutzer ausgeführt werden.
	
	1. Bearbeiten Sie die `/etc/hosts` Datei auf der Amazon RDS Custom DB-Instance. Eine einfache Möglichkeit, dies zu tun, besteht darin, die Datenbank- und Anwendung s-Host-Einträge aus der EC2 Amazon-Datenbank-Hosts-Quelldatei zu kopieren.
	
	`<IP-address> OEBS-app01.localdomain OEBS-app01 OEBS-app01log.localdomain OEBS-app01log`
	`<IP-address> OEBS-db01.localdomain OEBS-db01 OEBS-db01log.localdomain OEBS-db01log`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	wo `<IP-address>` ist die IP-Adresse des Datenbank knotens, die Sie durch die benutzerdefinierte Amazon RDS-IP-Adresse ersetzen sollten. Die logischen Hostnamen werden mit angehängt. `*log`
	
	2. Ändern Sie den Datenbank -Hostnamen, indem Sie den folgenden Befehl ausführen: `hostnamectl`
	
	`$ sudo hostnamectl set-hostname --static persistent-hostname`
	
	Zum Beispiel:
	
	`$ sudo hostnamectl set-hostname --static OEBS-db01log`
	
	Weitere Informationen finden Sie im Knowledge Center-Artikel zum Zuweisen statischer Hostnamen.
	
	3. Starten Sie die Amazon RDS Custom DB-Instance neu. Machen Sie sich keine Gedanken über das Herunterfahren der Datenbank, da Sie sie in einem späteren Schritt löschen werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`$ reboot`
	
	4. Wenn die Amazon RDS Custom DB-Instance wieder verfügbar ist, melden Sie sich an und überprüfen Sie, ob sich der Hostname geändert hat:
	
	`$ hostname`
	`oebs-db01`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie die Oracle E-Business Suite-Software.	Installieren Sie die empfohlene RPMs Oracle E-Business Suite im Oracle-Standardverzeichnis auf der Amazon RDS Custom DB-Instance. Einzelheiten finden Sie in Oracle Support Note #1330701 .1. Die folgende Liste ist unvollständig. Die RPM-Liste ändert sich mit jeder Version. Stellen Sie daher sicher, dass alle erforderlichen Versionen installiert RPMs sind.
	
	Führen Sie als Root-Benutzer Folgendes aus:
	
	`$ sudo yum -y update`
	`$ sudo yum install -y elfutils-libelf-devel*`
	`$ sudo yum install -y libXp-1.0.2-2.1*.i686`
	`$ sudo yum install -y libXp-1.0.2-2.1*`
	`$ sudo yum install -y compat-libstdc++-*`
	
	Stellen Sie sicher, dass alle erforderlichen Patches installiert sind, bevor Sie mit dem nächsten Schritt fortfahren.
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie den VNC-Server.	**Note**
	Sie können diesen Schritt für Oracle 19c auslassen, da die Beispiel-CD nicht mehr benötigt wird; siehe Oracle Support Note 2782085.1.
	
	Für Oracle 12.1.0.2:
	
	Installieren Sie den VNC-Server und seine abhängigen Desktop-Pakete. Dies ist eine Voraussetzung für die Installation der 12c-Beispiel-CD im nächsten Schritt.
	
	1. Führen Sie als Root-Benutzer Folgendes aus:
	
	`$ sudo yum install -y tigervnc-server`
	`$ sudo yum install -y *kde*`
	`$ sudo yum install -y *xorg*`
	
	2. Starten Sie den VNC-Server für den `rdsdb` Benutzer und legen Sie das Passwort für VNC fest:
	
	`$ su - rdsdb`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`$ vncserver :1` `$ vncpassword`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die 12c-Beispiel-CD.	**Note** Sie können diesen Schritt für Oracle 19c auslassen, da die Beispiel-CD nicht mehr benötigt wird; siehe Oracle Support Note 2782085.1. Für Oracle 12.1.0.2: 1. Laden Sie die Installationsdateien vonhttps://edelivery.oracle.com/herunter. Suchen Sie für Oracle E-Business Suite 12.2.11 — Oracle Database 12c Release 1 (12.1.0.2) nach Beispielen für Linux x86-64 V100102-01.zip. 2. Erstellen Sie ein Verzeichnis zum Speichern der Beispiel-CD: `$ mkdir /RMAN/12c examples` 3. Kopieren Sie die ZIP-Datei der Beispiel-CD in dieses Verzeichnis, indem Sie den Übertragungsmechanismus	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Ihrer Wahl verwenden (z. B. SCP):
	`V100102-01.zip`
	4. Eigentümerschaft ändern in: `rdsdb`
	`$ chown -R rdsdb:rdsdb /RMAN/12cexamples`
	5. Entpacken Sie als `rdsdb` Benutzer die Datei:
	`$ unzip V10010201.zip`
	6. Stellen Sie eine Connect von einem Client her, der Zugriff auf den VNC-Client und Amazon RDS Custom hat. Stellen Sie sicher, dass Sie die erforderlichen Netzwerkkonnektivität und die Firewall-Ports geöffnet haben, um den Zugriff für VNC zu ermöglichen. Beispielsweise muss für einen VNC-Server, der auf läuft, Port 5901 in der Sicherheitsgruppe geöffnet `display :1` werden, die dem Amazon EC2 RDS-Custom-Host zugeordnet ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	7. Wechseln Sie in das Verzeichnis, in das Sie die Beispiel-CD kopiert haben:
	`$ cd /RMAN/12cexamples/examples`
	8. Führen Sie das Installationsprogramm aus. Stellen Sie sicher, dass Sie den Speicherort der `oraInst.loc` Datei überprüfen.
	`./runInstaller -invPtrLoc /rdsdbbin/oracle.12.1.custom.r1.EE.1/oraInst.loc`
	9. Verwenden Sie bei der Installation der Beispiel-CD die folgenden Parameter:
	`Skip Software Update Downloads`
	`Select Oracle Home 12.1.0.2 (Oracle Base = /rdsdbbin)`
	`(Software Location = /rdsdbbin/oracle/12.1.custom.r1.EE.1)`
	10. Das Installationsprogramm umfasst fünf Schritte mit Eingabeaufforderungen. Folgen Sie den Schritten, bis	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Installation abgeschlossen ist.	

Löschen Sie die Startdatenbank und erstellen Sie die Verzeichnisse zum Speichern der Datenbankdateien

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Den Automatisierungsmodus unterbrechen.	Sie müssen den Automatisierungsmodus auf Ihrer Amazon RDS Custom DB-Instance anhalten, bevor Sie mit den nächsten Schritten fortfahren, um sicherzustellen, dass die Automatisierung die RMAN-Aktivität nicht beeinträchtigt. Unterbrechen Sie die Automatisierung, indem Sie den folgenden AWS-Befehlszeilenschnittstellen-Befehl (AWS CLI) verwenden. (Stellen Sie sicher, dass Sie zuerst die AWS-CLI konfiguriert haben.) `aws rds modify-db-instance \ --db-instance-identifier VIS \ --automation-mode all-paused \ --resume-full-automation-mode-minute 360 \`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--region eu-west-1` Wenn Sie die Dauer der Pause angeben, stellen Sie sicher, dass Sie genügend Zeit für die RMAN-Wied erherstellung einplanen. Dies hängt von der Größe der Quelldatenbank ab. Ändern Sie daher den 360-Wert entsprechend.	

Löschen Sie die Starter-D atenbank.	Löschen Sie die bestehend e Amazon RDS-Custom-Datenbank.
	
	Führen Sie als Oracle-He imanwender die folgenden Befehle aus. (Der Standardb enutzer ist`rdsdb`, sofern Sie ihn nicht angepasst haben.)
	
	`$ sqlplus / as sysdba`
	`SQL> shutdown immediate ;`
	`SQL> startup nomount restrict;`
	`SQL> alter database mount;`
	`SQL> drop database;`
	`SQL> exit`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie Verzeichnisse zum Speichern der Datenbank dateien.	Für Oracle 12.1.0.2:
	
	Erstellen Sie Verzeichnisse für die Datenbank, die Kontrolld atei, die Datendateien und das Online-Protokoll. Verwenden Sie das übergeordnete Verzeichnis des `control_f iles` Parameters im vorherigen Befehl (in diesem Fall`VIS_A`). Führen Sie die folgenden Befehle als Oracle-Heimanwender aus (standard mäßig`rdsdb`).
	
	`$ mkdir -p /rdsdbdata/ db/VIS_A/controlfile`
	`$ mkdir -p /rdsdbdata/ db/VIS_A/datafile`
	`$ mkdir -p /rdsdbdata/ db/VIS_A/onlinelog`
	
	Für Oracle 19c:
	
	Erstellen Sie Verzeichnisse für die Datenbank, die Kontrolld atei, die Datendateien und das Online-Protokoll. Verwenden Sie das übergeordnete Verzeichnis des `control_f iles` Parameters im vorherigen Befehl (in diesem Fall`VISCDB_A`). Führen Sie die folgenden Befehle als Oracle-Heimanwender aus (standardmäßig`rdsdb`).
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`$ mkdir -p /rdsdbdata/db/cdb/VISCDB_A/controlfile`
	`$ mkdir -p /rdsdbdata/db/cdb/VISCDB_A/datafile`
	`$ mkdir -p /rdsdbdata/db/cdb/VISCDB_A/onlinelog`
	`$ mkdir -p /rdsdbdata/db/cdb/VISCDB_A/onlinelog/arch`
	`$ mkdir /rdsdbdata/db/pdb/VISCDB_A`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und ändern Sie die Parameterdatei für Oracle E-Business Suite.	In diesem Schritt kopieren Sie die Serverparameterdatei (SPFILE) nicht aus der Quelldatenbank. Stattdessen verwenden Sie die Standardparameterdatei (PFILE), die mit der Amazon RDS Custom DB-Instance erstellt wurde, und fügen die Parameter hinzu, die Sie für Oracle E-Business Suite benötigen. Wenn Sie die Datenbank löschen, erstellt Amazon RDS Automation eine Sicherungskopie der `init.ora` Datei, die mit der Amazon RDS-Custom-Datenbank verknüpft ist. Diese Datei heißt `oracle_pfile` und befindet sich in `/rdsdbdata/config` . Für Oracle 12.1.0.2: 1. Kopieren Sie `/rdsdbdata/config/oracle_pfile` in `$ORACLE_HOME` . `$ cp /rdsdbdata/config/oracle_pfile $ORACLE_HOME/dbs/initVIS.ora` 2. Bearbeiten Sie die `initVIS.ora` Datei auf der Amazon RDS Custom	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	DB-Instance. Überprüfen Sie alle Parameter in der Quelle und fügen Sie bei Bedarf alle Parameter hinzu. Einzelheiten finden Sie in der Oracle Support Note 396009.1.
	
	Important
	Stellen Sie sicher, dass die Parameter, die Sie hinzufügen, keine Kommentare enthalten. Kommentare führen zu Problemen bei der Automatisierung, z. B. beim Erstellen von Read Replicas und beim Ausstellen von point-in-time Wiederherstellungen (). PITRs
	
	3. Fügen Sie der `initVIS.ora` Datei je nach Ihren Anforderungen Parameter hinzu, die den folgenden ähneln:
	
	`*.workarea_size_policy='AUTO'`
	`*.plsql_code_type='INTERPRETED'`
	`*.cursor_sharing='EXACT'`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	*._b_tree_bitmap_plan s=FALSE *.session_cached_cu rsors=500 *.optimizer_adapt ive_features=false *.optimizer_secur e_view_merging=false *.SQL92_SECURITY=TRUE *.temp_undo_enabled= true _system_trig_enabled = TRUE nls_language = american nls_territory = america nls_numeric_charact ers = "." nls_comp = binary nls_sort = binary nls_date_format = DD- MON-RR nls_length_semantics = BYTE aq_tm_processes = 1 _sort_eliminatio n_cost_ratio =5 _like_with_bind _as_equality = TRUE _fast_full_scan_enable d = FALSE _b_tree_bitmap_plans = FALSE optimizer_secure_view _merging = FALSE _optimizer_autostats_ job = FALSE parallel_max_servers = 8 parallel_min_servers = 0	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`parallel_degree_policy = MANUAL`
	`sec_case_sensitive_logon = FALSE`
	`compatible = 12.1.0`
	`o7_dictionary_accessibility = FALSE`
	`utl_file_dir =/tmp`
	
	4. Ändern Sie Folgendes. Die Werte hängen von Ihrem Quellsystem ab. Überarbeiten Sie sie daher auf der Grundlage Ihrer aktuellen Konfiguration.
	
	`*.open_cursors=500`
	`*.undo_tablespace='APPS_UNDOTS1`
	
	5. Entfernen Sie die SPFILE-Referenz.
	
	`*.spfile='/rdsdbbin/oracle/dbs/spfileVIS.ora'`
	
	Hinweise:
	
	• Ändern Sie nicht die Werte, die von Amazon RDS Custom PFILE für `control_files` und `db_unique_name` bereitgestellt werden. Amazon RDS erwartet diese Werte. Wenn Sie von ihnen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	abweichen, kann dies zu Problemen führen, wenn Sie in future versuchen, eine Read Replica zu erstellen. • Amazon RDS Custom verwendet standardm äßig Automatic Memory Management (AMM). Wenn Sie Hugemem verwenden möchten, können Sie Amazon RDS Custom so konfigurieren, dass Automatic Shared Memory Management (ASMM) verwendet wird. • Lassen Sie den `memory_ma x_target` Parameter standardmäßig aktiviert. Das Amazon RDS-Frame work verwendet dies im Hintergrund, um Read Replicas zu erstellen. 6. Vergewissern Sie sich, dass keine Probleme mit der `initVIS.ora` Datei vorliegen, indem Sie den `startup nomount` folgenden Befehl ausführen: `SQL> startup nomount pfile=/rdsdbbin/or acle/dbs/initVIS.ora; SQL> create spfile='/ rdsdbdata/admin/VIS/`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	pfile/spfileVIS.ora'
	from pfile;
	SQL> exit
	
	7. Erstellen Sie einen symbolischen Link für SPFILE.
	
	$ ln -s /rdsdbdat
	a/admin/VIS/pfile/
	spfileVIS.ora
	$ORACLE_HOME/dbs/
	
	Für Oracle 19c:
	
	1. Kopieren Sie `/rdsdbdat a/config/oracle_pf ile` in `$ORACLE_HOME` .
	
	$ cp /rdsdbdata/config/
	oracle_pfile $ORACLE_H
	OME/dbs/initVISCDB
	.ora
	
	2. Bearbeiten Sie die `initVISCDB.ora` Datei auf der Amazon RDS Custom DB-Instance. Überprüfen Sie alle Parameter in der Quelle und fügen Sie bei Bedarf alle Parameter hinzu. Einzelhei ten finden Sie in der Oracle Support Note 396009.1.
	
	Important
	Stellen Sie sicher, dass die Parameter	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	, die Sie hinzufüge n, keine Kommentar e enthalten. Wenn Kommentare vorhanden sind, führen diese zu Problemen bei der Automatisierung, z. B. beim Erstellen von Read Replicas und beim Ausgeben von point-in-time Wiederherstellungen (). PITRs
	
	3. Fügen Sie der `initVISCD B.ora` Datei je nach Ihren Anforderungen Parameter hinzu, die den folgenden ähneln.
	
	`*.instance_name=VI SCDB`
	`*.sec_case_sensit ive_logon= FALSE`
	`*.result_cache_ma x_size = 600M`
	`*.optimizer_adaptive_p lans =TRUE`
	`*.optimizer_adaptive_ statistics = FALSE`
	`*.pga_aggregate_limit = 0`
	`*.temp_undo_enabled = FALSE`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	*._pdb_name_case_sens itive = TRUE *.event='10946 trace name context forever, level 8454144' *.workarea_size_p olicy='AUTO' *.plsql_code_t ype='INTERPRETED' *.cursor_sharing=' EXACT' *._b_tree_bitmap_pla ns=FALSE *.session_cached_c ursors=500 *.optimizer_secu re_view_merging=false *.SQL92_SECURITY=TRUE _system_trig_enabled = TRUE nls_language = american nls_territory = america nls_numeric_charact ers = "." nls_comp = binary nls_sort = binary nls_date_format = DD- MON-RR nls_length_semantics = BYTE aq_tm_processes = 1 _sort_eliminatio n_cost_ratio =5 _like_with_bind _as_equality = TRUE _fast_full_scan_enable d = FALSE _b_tree_bitmap_plans = FALSE optimizer_secure_view _merging = FALSE	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`_optimizer_autostats_ job = FALSE parallel_max_servers = 8 parallel_min_servers = 0 parallel_degree_policy = MANUAL`
	
	4. Ändern Sie Folgendes. Die Werte hängen von Ihrem Quellsystem ab. Überarbeiten Sie sie daher auf der Grundlage Ihrer aktuellen Konfiguration.
	
	`*.open_cursors=500 *.undo_tablespace ='UNDOTBS1'`
	
	5. Entfernen Sie die SPFILE-Referenz:
	
	`*.spfile='/rdsdbbin/oracle/dbs/spfileVISCDB.ora'`
	
	Hinweise:
	
	• Ändern Sie nicht die Werte, die von Amazon RDS Custom PFILE für `control_files` und `db_unique_name` bereitgestellt werden. Amazon RDS erwartet diese Werte. Wenn Sie von ihnen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	abweichen, kann dies zu Problemen führen, wenn Sie in future versuchen, eine Read Replica zu erstellen. • Amazon RDS Custom verwendet standardm äßig Automatic Memory Management (AMM). Wenn Sie Hugemem verwenden möchten, können Sie Amazon RDS Custom so konfigurieren, dass Automatic Shared Memory Management (ASMM) verwendet wird. • Lassen Sie den `memory_ma x_target` Parameter standardmäßig aktiviert. Das Amazon RDS-Frame work verwendet dies im Hintergrund, um Read Replicas zu erstellen. 6. Vergewissern Sie sich, dass keine Probleme mit der `initVISCDB.ora` Datei vorliegen, indem Sie den `startup nomount` folgenden Befehl ausführen: `SQL> startup nomount pfile=/rdsdbbin/or acle/dbs/initVISCD B.ora;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`SQL> create spfile='/rdsdbdata/admin/VISCDB/pfile/spfileVISCDB.ora' from pfile;`
	`SQL> exit`
	
	7. Erstellen Sie einen symbolischen Link für SPFILE.
	
	`$ ln -s /rdsdbdata/admin/VISCDB/pfile/spfileVISCDB.ora $ORACLE_HOME/dbs/`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die benutzerd efinierte Amazon RDS-Daten bank aus dem Backup wieder her.	Für Oracle 12.1.0.2:
	
	1. Stellen Sie die Kontrolldatei mithilfe der Sicherungsdatei wieder her, die Sie zuvor auf der Quelle erfasst haben:
	
	`RMAN> connect target /`
	`RMAN> RESTORE CONTROLFI`
	`LE FROM '/RMAN/vi`
	`sdb_full_bkp_100rl`
	`sbt';`
	
	`Starting restore at 10-`
	`APR-22`
	`using target database`
	` control file instead of`
	` recovery catalog`
	`allocated channel:`
	` ORA_DISK_1`
	`channel ORA_DISK_`
	`1: SID=201 device`
	` type=DISK`
	
	`channel ORA_DISK_1:`
	` restoring control file`
	`channel ORA_DISK_`
	`1: restore complete,`
	` elapsed time: 00:00:01`
	`output file name=/rds`
	`dbdata/db/VIS_A/co`
	`ntrolfile/control-`
	`01.ctl`
	`Finished restore at 10-`
	`APR-22`
	
	2. Katalogisieren Sie die Sicherungskopien, sodass
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Sie Folgendes ausstellen könnenRMAN `restore`:
	
	`RMAN> alter database mount;`
	`RMAN> catalog start with '/RMAN/visdb';`
	
	3. Erstellen Sie ein Skript zum Wiederherstellen der Datenbank:
	
	`$ vi restore.sh`
	`rman target / log=/home /rdsdb/rman.log << EOF`
	`run`
	`{`
	`set newname for database to '/rdsdbdata/db/VIS _A/datafile/%b';`
	`restore database;`
	`switch datafile all;`
	`switch tempfile all;`
	`}`
	`EOF`
	
	4. Stellen Sie die Quelle in der benutzerdefinierten Amazon RDS-Zieldatenbank wieder her. Sie müssen die Berechtigungen des Skripts ändern, um es ausführen zu können, und dann das `restore.sh` Skript ausführen, um die Datenbank wiederherzustellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`$ chmod 755 restore.sh`
	`$ nohup ./restore.sh &`
	
	Für Oracle 19c:
	
	1. Stellen Sie die Kontrolldatei mithilfe der Sicherungsdatei wieder her, die Sie zuvor auf der Quelle erfasst haben:
	
	`RMAN> connect target /`
	`RMAN> RESTORE CONTROLFI LE FROM '/RMAN/cn trl.bak';`
	`Starting restore at 07- JUN-23`
	`using target database control file instead of recovery catalog`
	`allocated channel: ORA_DISK_1`
	`channel ORA_DISK_ 1: SID=201 device type=DISK`
	`channel ORA_DISK_1: restoring control file`
	`channel ORA_DISK_ 1: restore complete, elapsed time: 00:00:01`
	`output file name=/rds dbdata/db/cdb/VISC DB_A/controlfile/c ontrol-01.ctl`
	`Finished restore at 07- JUN-23`
	
	2. Katalogisieren Sie die Sicherungskopien, sodass	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Sie Folgendes ausstellen könnenRMAN `restore`:
	
	`RMAN> alter database mount;`
	`RMAN> catalog start with '/RMAN/visdb';`
	
	Wenn Sie Probleme mit dem `start with` Befehl haben, können Sie die Sicherung skopien einzeln hinzufügen. Beispiel:
	
	`RMAN> catalog backuppiece '/RMAN/visdb_full_bkp_1d1e507m';`
	
	und wiederholen Sie dann den Befehl für jedes Sicherung sstück.
	
	3. Erstellen Sie ein Skript, um die Datenbank wiederher zustellen. Ändern Sie den Namen der austauschbaren Datenbank entsprechend Ihren Anforderungen. Weisen Sie parallel Kanäle basierend auf der Anzahl der CPUs verfügbaren V zu, um den Wiederherstellungsprozess zu beschleunigen.
	
	`$ vi restore.sh`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`rman target / log=/home /rdsdb/rmancdb.log << EOF run { allocate channel c1 type disk; allocate channel c2 type disk; .... allocate channel c<N> type disk; set newname for database to '/rdsdbdata/db/cdb /VISCDB_A/datafile/ %b'; set newname for database root to '/rdsdbda ta/db/cdb/VISCDB_A/ datafile/%f_%b'; set newname for database "PDB$SEED" to '/rdsdbdata/db/cdb/ pdbseed/%f_%b'; set newname for pluggable database VIS to '/rdsdbdata/db/pdb /VISCDB_A/%f_%b'; restore database; switch datafile all; switch tempfile all; release channel c1; release channel c2; release channel c3; .... release channel c<N>; } EOF` 4. Stellen Sie die Quelle in der benutzerdefinierten Amazon RDS-Zieldatenbank wieder	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	her. Sie müssen die Berechtigungen des Skripts ändern, um es ausführen zu können, und dann das `restore.sh` Skript ausführen, um die Datenbank wiederherzustellen.
	`$ chmod 755 restore.sh`
	`$ nohup ./restore.sh &`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Protokoll dateien auf Probleme.	Für Oracle 12.1.0.2:
	
	1. Vergewissern Sie sich, dass keine Probleme vorliegen , indem Sie die `rman.log` Datei überprüfen:
	
	`$ cat /home/rdsdb/ rman.log`
	
	2. Bestätigen Sie den Pfad der Protokolldateien, die in der Kontrolldatei registriert sind:
	
	`SQL> select member from v$logfile; MEMBER ---------- ---------- ---------- ---------- -------- /d01/oracle/VIS/data/ log1.dbf /d01/oracle/VIS/data/ log2.dbf /d01/oracle/VIS/data/ log3.dbf`
	
	3. Benennen Sie die Protokoll dateien so um, dass sie dem Dateipfad des Ziels entsprech en. Ersetzen Sie den Pfad so, dass er mit der Ausgabe aus dem vorherigen Schritt übereinstimmt:
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`SQL> ALTER DATABASE RENAME FILE '/d01/oracle/VIS/data/log1.dbf' TO '/rdsdbdata/db/VIS_A/onlinelog/log1.dbf';`
	`SQL> ALTER DATABASE RENAME FILE '/d01/oracle/VIS/data/log2.dbf' TO '/rdsdbdata/db/VIS_A/onlinelog/log2.dbf';`
	`SQL> ALTER DATABASE RENAME FILE '/d01/oracle/VIS/data/log3.dbf' TO '/rdsdbdata/db/VIS_A/onlinelog/log3.dbf';`
	
	Für Oracle 19c:
	
	1. Vergewissern Sie sich, dass keine Probleme vorliegen, indem Sie die `rmancdb.log` Datei überprüfen:
	
	`$ cat /home/rdsdb/rmancdb.log`
	
	2. Bestätigen Sie den Pfad der Protokolldateien, die in der Kontrolldatei registriert sind:
	
	`SQL> select member from v$logfile;`
	`MEMBER`
	`----------`
	`----------`
	`----------`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	``` ------------------ -------- /d01/oracle/VIS/or adata/VISCDB/redo0 3.log /d01/oracle/VIS/orada ta/VISCDB/redo02.log /d01/oracle/VIS/ oradata/VISCDB/re do01.log ```	
	3. Benennen Sie die Protokoll dateien so um, dass sie dem Dateipfad des Ziels entsprech en. Ersetzen Sie den Pfad so, dass er mit der Ausgabe aus dem vorherigen Schritt übereinstimmt: ``` SQL> ALTER DATABASE RENAME FILE '/d01/ora cle/VIS/oradata/VI SCDB/redo01.log' TO '/rdsdbdata/db/cdb/ VISCDB_A/onlinelog/ log1.dbf'; SQL> ALTER DATABASE RENAME FILE '/d01/ora cle/VIS/oradata/VI SCDB/redo02.log' TO '/rdsdbdata/db/cdb/ VISCDB_A/onlinelog/ log2.dbf'; SQL> ALTER DATABASE RENAME FILE '/d01/ora cle/VIS/oradata/VI SCDB/redo03.log' TO '/rdsdbdata/db/cdb/ ```	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`VISCDB_A/onlinelog/log3.dbf';`
	
	4. Bestätigen Sie den Pfad, den Status der Protokoll dateien und die Gruppennu mmer, die in der Kontrolldatei registriert ist:
	
	`SQL> column REDOLOG_F ILE_NAME format a50`
	`SQL> SELECT a.GROUP#, a.status, b.MEMBER AS REDOLOG_FILE_NAME, (a.BYTES/1024/1024) AS SIZE_MB FROM v$log a JOIN v$logfile b ON a.Group#=b.Group# ORDER BY a.GROUP#;`
	
	`GROUP# STATUS REDOLOG_F ILE_NAME SIZE_MB`
	`1 CURRENT /rdsdbdat a/db/cdb/VISCDB_A/ onlinelog/log1.dbf 512`
	`2 INACTIVE /rdsdbdat a/db/cdb/VISCDB_A/ onlinelog/log2.dbf 512`
	`3 INACTIVE /rdsdbdat a/db/cdb/VISCDB_A/ onlinelog/log3.dbf 512`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vergewissern Sie sich, dass Sie die Amazon RDS-Custom-Datenbank öffnen und OMF-Protokolldateien erstellen können.	Amazon RDS Custom for Oracle verwendet Oracle Managed Files (OMF), um den Betrieb zu vereinfachen. Sie können Read Replicas zu eigenständigen Instances heraufstufen, müssen jedoch zuerst die Protokolldateien mithilfe von OMF erstellen . Dadurch wird sicherges tellt, dass beim Heraufstu fen der Instanz der richtige Pfad verwendet wird. Weitere Informationen darüber, wie Sie Read Replicas bewerben können, finden Sie in der Amazon RDS-Dokumentation. Wenn Sie OMF-Dateien nicht verwenden, kann dies möglicherweise zu Problemen führen, wenn Sie versuchen, Read Replicas hochzustufen. 1. Öffnen Sie die Datenbank mit: `resetlogs` `SQL> alter database open resetlogs;` **Note** Wenn Sie den Fehler ORA-00392: Protokoll xx von Thread 1 wird gelöscht, Vorgang	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	nicht erlaubt erhalten, folgen Sie den Schritten im Abschnitt Problembehandlung für ORA-00392.
	
	2. Vergewissern Sie sich, dass die Datenbank geöffnet ist:
	
	`SQL> select open_mode from v$database;`
	`OPEN_MODE`
	`----------`
	`READ WRITE`
	
	3. Erstellen Sie die OMF-Protokolldateien. Ändern Sie die Gruppennummern, die Anzahl der Gruppen und die Größe je nach Ihren Anforderungen, indem Sie die Ausgabe der vorherigen Protokolldateiabfrage verwenden. Das folgende Beispiel beginnt bei Gruppe 4 und fügt der Einfachheit halber drei Gruppen hinzu.
	
	`SQL> alter database add logfile group 4 size 512M;`
	`Database altered.`
	`SQL> alter database add logfile group 5 size 512M;`
	`Database altered.`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`SQL> alter database add logfile group 6 size 512M;`
	`Database altered.`
	
	4. Löscht die vorherigen Nicht-OMF-Dateien. Hier ist ein Beispiel, das Sie je nach Ihren Anforderungen und der Ausgabe der Abfrage in den vorherigen Schritten anpassen können:
	
	`SQL> alter database drop logfile group 1;`
	`System altered.`
	`SQL> alter database drop logfile group 2;`
	`System altered.`
	`SQL> alter database drop logfile group 3;`
	`System altered.`
	
	Note
	Wenn Sie beim Versuch, die Protokolldateien zu löschen, eine ORA-01624 -Fehlermeldung erhalten, finden Sie weitere Informationen im Abschnitt Fehlerbehebung.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	5. Vergewissern Sie sich, dass Sie die OMF-Dateien sehen können, die erstellt wurden. (Der Verzeichnispfad variiert für Oracle 12.1.0.2 und 19c, aber das Konzept ist dasselbe.)
	`SQL> select member from v$logfile;`
	`MEMBER`
	`----------`
	`/rdsdbdata/db/cdb/VISCDB_A/onlinelog/o1_mf_4_ksrbslny_.log`
	`/rdsdbdata/db/cdb/VISCDB_A/onlinelog/o1_mf_5_ksrchw0k_.log`
	`/rdsdbdata/db/cdb/VISCDB_A/onlinelog/o1_mf_6_ksrcnl9v_.log`
	6. Starten Sie die Datenbank neu und vergewissern Sie sich, dass SPFILE von der Instanz verwendet wird:
	`SQL> shutdown immediate`
	`SQL> startup`
	`SQL> show parameter spfile`
	Für Oracle 12.1.0.2 gibt diese Abfrage Folgendes zurück:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`spfile /rdsdbbin /oracle/dbs/spfile VIS.ora`
	
	Für Oracle 19c gibt die Abfrage Folgendes zurück:
	
	`spfile /rdsdbbin /oracle/dbs/spfile VISCDB.ora`
	
	7. Nur für Oracle 19c überprüfen Sie den Status der Container-Datenbank und öffnen Sie sie bei Bedarf:
	
	`SQL> show pdbs CON_ID CON_NAME OPEN MODE RESTRICTED ---------- --------- ---------- --------- - 2 PDB$SEED READ ONLY NO 3 VIS MOUNTED NO`
	
	`SQL> alter session set container=VIS; Session altered.`
	
	`SQL> alter database open; Database altered.`
	
	`SQL> alter database save state; Database altered.`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>SQL> show pdbs
	    CON_ID CON_NAME
	          OPEN MODE
	 RESTRICTED
	---------- ---------
	--------------------- 	
	 ---------- -----
	         3 VIS
	                   READ
	 WRITE NO
	
	SQL> exit</pre>
	8. Löschen Sie die `init.ora` Datei von`$ORACLE_HOME/dbs`, weil Sie das PFILE nicht verwenden:
	<pre>$ cd $ORACLE_HOME/dbs</pre>
	Verwenden Sie für Oracle 12.1.0.2 den folgenden Befehl:
	<pre>$ pwd
	/rdsdbbin/oracle/dbs
	$ rm initVIS.ora</pre>
	Verwenden Sie für Oracle 19c den folgenden Befehl:
	<pre>$ pwd
	/rdsdbbin/oracle/dbs
	$ rm initVISCDB.ora</pre>	

Passwörter aus Secrets Manager abrufen, Benutzer erstellen und Passwörter ändern

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie Passwörter aus Secrets Manager ab.	Sie können diese Schritte in der Konsole oder mithilfe der AWS-CLI ausführen. Die folgenden Schritte enthalten Anweisungen für die Konsole. 1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon RDS-Konsole unter https://console.aws.amazon.com/rds/. 2. Wählen Sie im Navigationsbereich Datenbanken und dann die Amazon RDS-Datenbank aus. 3. Wählen Sie Konfiguration und notieren Sie sich die Ressourcen-ID für die Instance (sie hat das folgende Format:`db-WZ4WLCK6AOQ6TJGZKMGRCDCI3Y`). 4. Öffnen Sie die AWS Secrets Manager Manager-Konsole unter https://console.aws.amazon.com/secretsmanager/. 5. Wählen Sie das Geheimnis aus, das denselben Namen	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	hat wie`do-not-delete-custom-<resource_id>` , wobei es `resource-id` sich auf die ID für die Instance bezieht, die Sie in Schritt 3 notiert haben. 6. Wählen Sie Retrieve secret value (Secret-Wert abrufen) aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den RDSADMIN-Benutzer.	`RDSADMIN`ist ein Überwachungs- und Orchestrator-Datenbankbenutzer in der Amazon RDS Custom DB-Instance. Da die Startdatenbank gelöscht und die Zieldatenbank mithilfe von RMAN aus der Quelle wiederhergestellt wurde, müssen Sie diesen Benutzer nach dem Wiederherstellungsvorgang neu erstellen, um sicherzustellen, dass die benutzerdefinierte Amazon RDS-Überwachung wie erwartet funktioniert. Sie müssen außerdem ein separates Profil und einen separaten Tablespace für den Benutzer erstellen. `RDSADMIN` Die Anweisungen für Oracle 12.1.0.2 und 19c unterscheiden sich geringfügig.
	
	Für Oracle 12.1.0.2:
	
	1. Geben Sie an einer SQL-Eingabeaufforderung die folgenden Befehle ein:
	
	`SQL> set echo on`
	`feedback on serverout`
	`on`
	`SQL> @?/rdbms/admin/utl`
	`pwdmg.sql`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SQL> ALTER PROFILE DEFAULT LIMIT FAILED_LOGIN_ATTEMPTS UNLIMITED PASSWORD_LIFE_TIME UNLIMITED PASSWORD_VERIFY_F UNCTION NULL; 2. Erstellen Sie das Profil`RDSADMIN`: SQL> create profile RDSADMIN LIMIT COMPOSITE_LIMIT UNLIMITED SESSIONS_PER_USER UNLIMITED CPU_PER_SESSION UNLIMITED CPU_PER_CALL UNLIMITED LOGICAL_READS_PER _SESSION UNLIMITED LOGICAL_READS_PER_CALL UNLIMITED IDLE_TIME UNLIMITED CONNECT_TIME UNLIMITED PRIVATE_SGA UNLIMITED FAILED_LOGIN_ATTEMPTS 10 PASSWORD_LIFE_TIME UNLIMITED PASSWORD_REUSE_TIME UNLIMITED PASSWORD_REUSE_MAX UNLIMITED PASSWORD_VERIFY_F UNCTION NULL	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`PASSWORD_LOCK_TIME 86400/86400 PASSWORD_GRACE_TIME 604800/86400;`
	
	3. Stellen Sie die `DBSNMP` Benutzerprofile `SYS` `SYSTEM`, und wie folgt ein`RDSADMIN`:
	
	`SQL> set echo on feedback on serverout on SQL> alter user SYS profile RDSADMIN; SQL> alter user SYSTEM profile RDSADMIN; SQL> alter user DBSNMP profile RDSADMIN;`
	
	4. Erstellen Sie den `RDSADMIN` Tablespace:
	
	`SQL> create bigfile tablespace rdsadmin datafile size 7M autoextend on next 1m Logging online permanent blocksize 8192 extent managemen t local autoallocate default nocompress segment space managemen t auto;`
	
	5. Erstellen Sie den `RDSADMIN` Benutzer. Ersetzen Sie das `RDSADMIN` Passwort durch das Passwort, das Sie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	zuvor von Secrets Manager erhalten haben:
	
	`SQL> create user rdsadmin identified by xxxxxxxxxx Default tablespace rdsadmin Temporary tablespace temp profile rdsadmin ;`
	
	6. Gewähren Sie folgende Rechte`RDSADMIN`:
	
	`SQL> grant select on sys.v_$instance to rdsadmin; SQL> grant select on sys.v_$archived_log to rdsadmin; SQL> grant select on sys.v_$database to rdsadmin; SQL> grant select on sys.v_$database_in carnation to rdsadmin; SQL> grant select on dba_users to rdsadmin; SQL> grant alter system to rdsadmin; SQL> grant alter database to rdsadmin; SQL> grant connect to rdsadmin with admin option; SQL> grant resource to rdsadmin with admin option;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`SQL> alter user rdsadmin account unlock identified by xxxxxxxxxxx;`
	`SQL> @?/rdbms/admin/userlock.sql`
	`SQL> @?/rdbms/admin/utlrp.sql`
	
	Für Oracle 19c:
	
	1. Geben Sie an einer SQL-Eingabeaufforderung die folgenden Befehle ein:
	
	`SQL> set echo on feedback on serverout on`
	`SQL> @?/rdbms/admin/utlpwdmg.sql`
	
	`SQL> alter profile default LIMIT FAILED_LOGIN_ATTEMPTS UNLIMITED PASSWORD_LIFE_TIME UNLIMITED PASSWORD_VERIFY_FUNCTION NULL;`
	
	2. Erstellen Sie das Profil`RDSADMIN`.
	
	Note
	`RDSADMIN`hat `C##` in Oracle 19c das Präfix. Das liegt daran,	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dass der Datenbank parameter auf C## gesetzt common_user_prefix ist. RDSADMINhat kein Präfix in Oracle 12.1.0.2. SQL> create profile C##RDSADMIN LIMIT COMPOSITE_LIMIT UNLIMITED SESSIONS_PER_USER UNLIMITED CPU_PER_SESSION UNLIMITED CPU_PER_CALL UNLIMITED LOGICAL_READS_PER _SESSION UNLIMITED LOGICAL_READS_PER_CALL UNLIMITED IDLE_TIME UNLIMITED CONNECT_TIME UNLIMITED PRIVATE_SGA UNLIMITED FAILED_LOGIN_ATTEMPTS 10 PASSWORD_LIFE_TIME UNLIMITED PASSWORD_REUSE_TIME UNLIMITED PASSWORD_REUSE_MAX UNLIMITED PASSWORD_VERIFY_F UNCTION NULL PASSWORD_LOCK_TIME 86400/86400	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`PASSWORD_GRACE_TIME 604800/86400;`
	
	3. Setzen Sie die `DBSNMP` Benutzerprofile `SYSSYSTEM`, und auf: `RDSADMIN`
	
	`SQL> alter user SYS profile C##RDSADMIN;`
	`SQL> alter user SYSTEM profile C##RDSADMIN;`
	`SQL> alter user DBSNMP profile C##RDSADMIN;`
	
	4. Erstellen Sie den `RDSADMIN` Tablespace:
	
	`SQL> create bigfile tablespace rdsadmin datafile size 7M autoextend on next 1m Logging online permanent blocksize 8192 extent management local autoallocate default nocompress segment space management auto;`
	
	5. Erstellen Sie den `RDSADMIN` Benutzer. Ersetzen Sie das `RDSADMIN` Passwort durch das Passwort, das Sie zuvor von Secrets Manager erhalten haben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`SQL> create user C##rdsadmin identified by xxxxxxxxxx profile C##rdsadmin container=all;`
	
	6. Gewähren Sie folgende Rechte`RDSADMIN`:
	
	`SQL> grant select on sys.v_$instance to c##rdsadmin;`
	`SQL> grant select on sys.v_$archived_log to c##rdsadmin;`
	`SQL> grant select on sys.v_$database to c##rdsadmin;`
	`SQL> grant select on sys.v_$database_incarnation to c##rdsadmin;`
	`SQL> grant select on dba_users to c##rdsadmin;`
	`SQL> grant alter system to C##rdsadmin;`
	`SQL> grant alter database to C##rdsadmin;`
	`SQL> grant connect to C##rdsadmin with admin option;`
	`SQL> grant resource to C##rdsadmin with admin option;`
	`SQL> alter user C##rdsadmin account unlock identified by xxxxxxxxxxx;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`SQL> @?/rdbms/admin/userlock.sql` `SQL> @?/rdbms/admin/utlrp.sql`	

Erstellen Sie den Master-Benutzer.	Da die Startdatenbank gelöscht und die Zieldatenbank mithilfe von RMAN aus der Quelle wiederhergestellt wurde, müssen Sie den Masterbenutzer neu erstellen. In diesem Beispiel lautet der Master-Benutzername. `admin`
	
	Für Oracle 12.1.0.2:
	
	`SQL> create user admin identified by <password>;`
	`SQL> grant dba to admin`
	
	Für Oracle 19c:
	
	`SQL> alter session set container=VIS;`
	
	`Session altered.`
	
	`SQL> create user admin identified by <password>;`
	
	`User created.`
	
	`SQL> grant dba to admin;`
	
	`Grant succeeded.`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Ändern Sie die Superuser-Passwörter.	1. Ändern Sie die Systemkennwörter, indem Sie das Passwort verwenden, das Sie von Secrets Manager abgerufen haben.
	
	Für Oracle 12.1.0.2:
	
	`SQL> alter user sys identified by xxxxxxxxxxx;`
	`SQL> alter user system identified by xxxxxxxxxx;`
	
	Für Oracle 19c:
	
	`SQL> alter user sys identified by xxxxxxxxxxx container=all;`
	`SQL> alter user system identified by xxxxxxxxxx container=all;`
	
	1. Ändern Sie die `EBS_SYSTEM` Passwörter.
	
	Für Oracle 12.1.0.2:
	
	`SQL> alter user ebs_system identified by xxxxxxxxxx;`
	
	Für Oracle 19c:
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Für diese Version müssen Sie auch eine Verbindung zur Container-Datenbank herstelle n, um das `EBS_SYSTEM` Passwort dort zu aktualisieren.
	
	`SQL> alter session set container=vis;`
	`SQL> alter user ebs_system identified by xxxxxxxxxx;`
	
	`SQL> exit;`
	
	Wenn Sie diese Passwörter nicht ändern, zeigt Amazon RDS Custom die folgende Fehlermeldung an: Der Datenbanküberwachu ngsbenutzer oder die Benutzeranmeldedaten haben sich geändert.	

Erstellen Sie Verzeichnisse für Oracle E-Business Suite, installieren Sie ETCC und führen Sie Autoconfig aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die für Oracle E-Business Suite erforderlichen Verzeichnisse.	1. Führen Sie in der Amazon RDS Custom Oracle-Da tenbank das folgende Skript als Oracle-Heimanwende r aus, um das `9idata` Verzeichnis in zu erstellen `$ORACLE_HOME/nls/d`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`ata/9idata` . Dieses Verzeichnis ist für Oracle E-Business Suite erforderlich.
	
	`perl $ORACLE_HOME/nls/data/old/cr9idata.pl`
	
	Ignorieren Sie die `ORA_NLS10` Meldung, da Sie die kontextsensitive Umgebung in späteren Schritten erstellen werden.
	
	2. Kopieren Sie die `appsutil.tar` Datei, die Sie zuvor aus dem gemeinsam genutzten Amazon EFS-Dateisystem erstellt haben, und entpacken Sie sie im Amazon RDS Custom Oracle-Standardverzeichnis. Dadurch wird das `appsutil` Verzeichnis im `$ORACLE_HOME` Verzeichnis erstellt.
	
	`$ cd /RMAN/appsutil`
	`$ cp sourceappsutil.tar $ORACLE_HOME`
	`$ cd $ORACLE_HOME`
	`$ tar xvf sourceappsutil.tar appsutil`
	
	3. Kopieren Sie die `appsutil.zip` Datei, die Sie zuvor auf dem gemeinsam	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	genutzten Amazon EFS-Datei system gespeichert haben. Dies war die Datei, die Sie auf der Anwendungsebene erstellt haben.
	
	Als `rdsdb` Benutzer der Amazon RDS Custom DB-Instance:
	
	`$ cp /RMAN/appsutil/appsutil.zip $ORACLE_HOME`
	`$ cd $ORACLE_HOME`
	
	4. Entpacken Sie die `appsutil.zip` Datei, um das `appsutil` Verzeichnis und die Unterverzeichnisse im Oracle-Standardverzeichnis zu erstellen:
	
	`$ unzip -o appsutil.zip`
	
	Die `-o` Option bedeutet, dass einige Dateien überschrieben werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie die Dateien tsanames.ora und sqlnet.ora.	Sie müssen die `tnsnames.ora` Datei so konfigurieren, dass Sie mit dem Autoconfig-Tool eine Verbindung zur Datenbank herstellen können. Im folgenden Beispiel können Sie sehen, dass die `tnsnames.ora` Datei über einen Softlink verfügt, die Datei jedoch standardmäßig leer ist.
	
	`$ cd $ORACLE_HOME/network/admin`
	`$ ls -ltr`
	`-rw-r--r-- 1 rdsdb database 373 Oct 31 2013 shrept.lst`
	`lrwxrwxrwx 1 rdsdb database 30 Feb 9 17:17 listener.ora -> /rdsdbdata/config/listener.ora`
	`lrwxrwxrwx 1 rdsdb database 28 Feb 9 17:17 sqlnet.ora -> /rdsdbdata/config/sqlnet.ora`
	`lrwxrwxrwx 1 rdsdb database 30 Feb 9 17:17 tnsnames.ora -> /rdsdbdata/config/tnsnames.ora`
	
	1. Erstellen Sie den `tnsnames.ora` Eintrag. Aufgrund der Art und Weise, wie die Amazon RDS-
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Automatisierung die Dateien analysiert, müssen Sie sicherstellen, dass der Eintrag keine Leerzeichen, Kommentare oder zusätzlic hen Zeilen enthält. Andernfal ls könnten Probleme auftreten , wenn Sie einige von ihnen APIs wie create-db-instance -read -replica verwenden. Verwenden Sie das Folgende als Beispiel.
	
	2. Ersetzen Sie den Port, den Host und die SID entsprech end Ihren Anforderungen:
	
	`$ vi tnsnames.ora`
	`VIS=(DESCRIPTION=`
	`(ADDRESS_LIST=(ADD`
	`RESS=(PROTOCOL=TCP`
	`)(PORT=1521)(HOST=`
	`xx.xx.xx.xx)))(CON`
	`NECT_DATA=(SID=VIS)`
	`(SERVER=DEDICATED)))`
	
	Note
	Die Datei sollte keine zusätzlichen Zeilen enthalten. Wenn Sie die Zeilen nicht entfernen, können Probleme auftreten , wenn Sie in future eine Read Replica	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	erstellen. Die Erstellung einer Read Replica schlägt möglicherweise fehl und es wird folgende Fehlermeldung angezeigt: Die Aktivität hat eine Ausnahme ausgelöst HostManagerException: RestrictReplication kann auf keinem Host erfolgreich aufgerufen werden.
	
	3. Vergewissern Sie sich, dass auf die Datenbank zugegriffen werden kann:
	
	`$ tnsping vis`
	`OK (0 msec)`
	
	4. Nur für Oracle 19c aktualisieren Sie die `sqlnet.ora` Datei. Wenn Sie dies nicht tun, wird der Fehler ORA-01017: Ungültiger Benutzername/Passwort; Anmeldung verweigert angezeigt, wenn Sie versuchen, eine Verbindung zur Datenbank herzustellen. Bearbeiten Sie es so, dass es dem Folgenden entspricht: `sqlnet.ora $ORACLE_HOME/network/admin`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`NAMES.DIRECTORY_PATH=(TNSNAMES, ONAMES, HOSTNAME)`
	`SQLNET.EXPIRE_TIME= 10`
	`SQLNET.INBOUND_CONNECT_TIMEOUT =60`
	`SQLNET.ALLOWED_LOGON_VERSION_SERVER=10`
	`HTTPS_SSL_VERSION=undetermined`
	
	5. Konnektivität testen:
	
	`$ sqlplus apps/****@vis`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie die Datenbank.	Nachdem Sie die Konnektivität zur Datenbank getestet haben, können Sie die Datenbank mit dem Hilfsprogramm appsutil konfigurieren, um die kontextsensitive Umgebung zu erstellen.
	
	Für Oracle 12.1.0.2:
	
	1. Führen Sie die folgenden Befehle aus:
	
	`$ cd $ORACLE_HOME/appsutil/bin`
	`$ perl adbldxml.pl appsuser=apps`
	`Enter Hostname of Database server: oebs-db01`
	`Enter Port of Database server: 1521`
	`Enter SID of Database server: VIS`
	`Enter Database Service Name: VIS`
	`Enter the value for Display Variable: :1`
	`The context file has been created at: /rdsdbbin/oracle/appsutil/VIS_oebs-db01.xml`
	
	2. `oraInst.loc` Vom Root-Benutzer aus erstellen:
	
	`$ vi /etc/oraInst.loc`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`inventory_loc=/rdsdbbin/oracle.12.1.custom.r1.EE.1/oraInventory inst_group=database`	

	3. Klonen Sie die Kontextdatei, um den logischen Hostnamen festzulegen, indem Sie die Kontextdatei verwenden, die Sie im vorherigen Schritt erstellt haben. Führen Sie als `rdsdb` Benutzer Folgendes aus:
	`$ cd $ORACLE_HOME/appsutil/clone/bin`
	`$ perl adclonectx.pl \`
	`contextfile=[ORACLE_HOME]/appsutil/[current context file] \`
	`template=[ORACLE_HOME]/appsutil/template/adxdbctx.tmp`
	wo `oebs-db01log` sich auf den logischen Hostnamen bezieht. Zum Beispiel:
	`$ perl adclonectx.pl \`
	`contextfile=/rdsdbbin/oracle.12.1.custom.r1.EE.1/appsutil/VIS_oebs-db01.xml \`
	`template=/rdsdbbin/oracle/appsutil/template/adxdbctx.tmp`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Target System Hostname (virtual or normal) [oebs-db01] : oebs- db01log Target System Base Directory : /rdsdbbin/ oracle Target Instance is RAC (y/n) [n] : n Target System Database SID : VIS Oracle OS User [rdsdb] : Oracle OS Group [rdsdb] : database Role separation is supported y/n [n] ? : n Target System utl_file_ dir Directory List : / tmp Number of DATA_TOP's on the Target System [1] : Target System DATA_TOP Directory 1 [/rdsdbbi n/oracle/data] : / rdsdbdata/db/VIS_A/ datafile/ Target System RDBMS ORACLE_HOME Directory [/rdsdbbin/oracle/ 12.1.0] : /rdsdbbin/ oracle Do you want to preserve the Display [:1] (y/n) : y	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
Do you want the target
 system to have the
 same port values as
 the source system (y/n)
 [y] ? : y
The new database context
 file has been created :
   /rdsdbbin/oracle.1
2.1.custom.r1.EE.1/
appsutil/clone/bin/
VIS_oebs-db01log.xml
contextfile=/rdsdbbin/
oracle.12.1.custom
.r1.EE.1/appsutil/
clone/bin/VIS_oebs-
db01log.xml
```

Für Oracle 19c:

1. Führen Sie die folgenden Befehle aus:

```
$ cd $ORACLE_HOME/appsu
til/bin
$ perl adbldxml.pl
 appsuser=apps
Enter Hostname of
 Database server: oebs-
db01
Enter Port of Database
 server: 1521
Enter SID of Database
 server: VIS
Enter the database
 listener name:L_VI
SCDB_001
Enter the value for
 Display Variable: :1
The context file has
 been created at:
```

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`/rdsdbbin/oracle/appsutil/VIS_oebs-db01.xml`
	
	2. `oraInst.loc` Vom Root-Benutzer aus erstellen:
	
	`$ vi /etc/oraInst.loc`
	`inventory_loc=/rdsdbbin/oracle/oraInventory`
	`inst_group=database`
	
	3. Klonen Sie die Kontextdatei, um den logischen Hostnamen festzulegen, indem Sie die Kontextdatei verwenden, die Sie im vorherigen Schritt erstellt haben. Führen Sie als `rdsdb` Benutzer Folgendes aus:
	
	`$ cd $ORACLE_HOME/appsutil/clone/bin`
	`$ perl adclonectx.pl \`
	`contextfile=[ORACLE_HOME]/appsutil/[current context file] \`
	`template=[ORACLE_HOME]/appsutil/template/adxdbctx.tmp`
	
	wo `oebs-db01log` sich auf den logischen Hostnamen bezieht. Zum Beispiel:
	
	`$ perl adclonectx.pl \`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	contextfile=/rdsdbbin/oracle/appsutil/VIS_oebs-db01.xml \ template=/rdsdbbin/oracle/appsutil/template/adxdbctx.tmp Target System Hostname (virtual or normal) [oebs-db01] : oebs-db01log Target System Base Directory : /rdsdbbin/oracle Target Instance is RAC (y/n) [n] : n Target System CDB Name : VISCDB Target System PDB Name : VIS Oracle OS User [oracle] : rdsdb Oracle OS Group [dba] : database Role separation is supported y/n [n] ? : n Number of DATA_TOP's on the Target System [2] : Target System DATA_TOP Directory 1 [/d01/oracle/VISCDB] : /rdsdbdata/db/pdb/VISCDB_A Target System DATA_TOP Directory 2 [/d01/oracle/data] : /rdsdbdata/db/pdb/VISCDB_A/datafile Specify value for OSBACKUPDBA group [database] :	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Specify value for OSDGDBA group [database] : Specify value for OSKMDBA group [database] : Specify value for OSRACDBA group [database] : Target System RDBMS ORACLE_HOME Directory [/d01/oracle/19.0. 0] : /rdsdbbin/oracle Do you want to preserve the Display [:1] (y/n) : y Do you want the target system to have the same port values as the source system (y/n) [y] ? : y Validating if the source port numbers are available on the target system.. Complete port informati on available at / rdsdbbin/oracle/a ppsutil/clone/bin/ out/VIS_oebs-db01log/ portpool.lst New context path and file name [VIS_oebs -db01log.xml] : / rdsdbbin/oracle/a ppsutil/VIS_oebs-d b01log.xml Do you want to overwrite it (y/n) [n] ? : y Replacing /rdsdbbin /oracle/appsutil/V	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	IS_oebs-db01log.xml file. The new database context file has been created : contextfile=/rdsdbbin/oracle/appsutil/VIS_oebs-db01log.xml Check Clone Context logfile /rdsdbbin/oracle/appsutil/clone/bin/CloneContext_0609141428.log for details.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie ETCC und führen Sie Autoconfig aus.	1. Installieren Sie den Oracle E-Business Suite Technology Codelevel Checker (ETCC).
	
	Laden Sie Patch 17537119 von My Oracle Support herunter und folgen Sie den Anweisungen unter. `README.txt` Sie erstellen ein Verzeichnis namens `etcc` in dem `$ORACLE_HOME` Verzeichnis, entpacken den Patch, um ein Skript mit dem Namen zu erstellen `checkMTpatch.sh` , und führen dann das Skript aus, um die Patch-Versionen zu überprüfen.
	
	2. Führen Sie das Autoconfig-Hilfsprogramm aus und übergeben Sie die neue logische Hostnamen-Kontextdatei.
	
	Für Oracle 12.1.0.2:
	
	`cd $ORACLE_HOME/appsutil/bin`
	`$ ./adconfig.sh contextfile=/rdsdbbin/oracle.12.1.customstom.r1.EE.1/appsutil/clone/bin/VIS_oebs-db01log.xml`
	
	Für Oracle 19c:
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Autoconfig erwartet, dass der Listener-Name übereinst immt. CDBNAME Daher wird die gesicherte ursprüngliche Listener-Konfigurationsdate i vorübergehend verwendet. L_<CDBNAME>_001 `$ lsnrctl stop L_VISCDB_ 001 $ cp -rp /rdsdbdata/ config/listener.ora / rdsdbdata/config/ listener.ora_orig $ vi /rdsdbdata/ config/listener.ora :%s/L_VISCDB_001/ VISCDB/g $ lsnrctl start VISCDB $ cd /rdsdbbin/oracle/a ppsutil $ . ./txkSetCfgCDB.env dboraclehome=/rdsd bbin/oracle.19.cus tom.r1.EE-CDB.1 Oracle Home being passed: /rdsdbbin/ oracle $ echo $ORACLE_HOME /rdsdbbin/orac le.19.custom.r1.EE- CDB.1 $ export ORACLE_SI D=VISCDB $ cd $ORACLE_HOME/ appsutil/bin $ perl $ORACLE_H OME/appsutil/bin/t`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`xkPostPDBCreationTasks.pl -dboraclehome=$ORACLE_HOME -outdir=$ORACLE_HOME/appsutil/log -cdbsid=VISCDB -pdbsid=VIS -appsuser=apps -dbport=1521 -servicetype=onpremise`
	
	`Enter the APPS Password: <apps password>`
	
	`Enter the CDB SYSTEM Password:<password from secrets manager>`
	
	Note
	Wenn sich Ihre Datenbankverzeichnisse geändert haben, folgen Sie den Anweisungen in Oracle Support Note 2525754.1.	

Konfigurieren Sie die TNS-Einträge für Amazon RDS Custom und Oracle E-Business Suite

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die TNS-Einträge für Amazon RDS Custom und Oracle E-Business Suite.	Autoconfig generiert die TNS-Dateien an den Standardspeicherorten. Für Oracle 12.1.0.2 (das kein CDB ist)	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und für Oracle19c PDB ist der Standardspeicherort. `$ORACLE_HOME/network/admin/$<CONTEXT_NAME>` Die CDB für Oracle 19c verwendet den Standard`$ORACLE_HOME/network/admin/` , der in den Umgebungsdateien definiert ist, die generiert wurden, als Sie `$TNS_ADMIN` Autoconfig in den vorherigen Schritten ausgeführt haben. Für Oracle 12.1.0.2 und 19c CDB werden Sie diese nicht verwenden, da die von Autoconfig generierten `tnsnames.ora` und `listener.ora` Dateien nicht den Amazon RDS-Anforderungen entsprechen, z. B. keine Leerzeichen oder Kommentare. Stattdessen verwenden Sie die generischen Dateien, die mit der Amazon RDS-Custom-Datenbank bereitgestellt werden, um sicherzustellen, dass die vom System erwarteten Anforderungen eingehalten werden, und um die Fehlerquote zu verringern.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Amazon RDS Custom erwartet beispielsweise das folgende Benennungsformat:
	`L_<INSTANCE_NAME>_001`
	Für Oracle 12.1.0.2 wäre das:
	`L_VIS_001`
	Für Oracle 19c wäre das:
	`L_VISCDB_001`
	Hier ist ein Beispiel für die `listener.ora` Datei, die Sie verwenden werden. Dies wurde generiert, als Sie die benutzerdefinierte Amazon RDS-Datenbank erstellt haben. Zu diesem Zeitpunkt haben Sie noch keine Änderungen an dieser Datei vorgenommen und werden sie als Standard beibehalten.
	Für Oracle 12.1.0.2:
	`$ cd $ORACLE_HOME/network/admin`
	`$ cat listener.ora`
	`ADR_BASE_L_VIS_001=/rdsdbdata/log/`
	`SID_LIST_L_VIS_001=(SID_LIST =`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	(SID_DESC = (SID_NAME = VIS)(GLOBAL_DBNAME = VIS) (ORACLE_HOME = /rdsdbbin/oracle)))
	L_VIS_001=(DESCRIPTION_LIST = (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(PORT = 1521)(HOST = xx.xx.xx.xx))) (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(PORT = 1521)(HOST = 127.0.0.1))))
	SUBSCRIBE_FOR_NODE_DOWN_EVENT_L_VIS_001=OFF
	
	Für Oracle 19c: Stellen Sie die `listener.ora` Originaldatei mit dem Listener-Namen wieder her. `L_<INSTANCE_NAME>_001`
	
	`$ cd $ORACLE_HOME/network/admin`
	
	`$ cp -rp /rdsdbdata/config/listener.ora /rdsdbdata/config/listener.ora_autoconfig`
	`$ cp -rp /rdsdbdata/config/listener.ora_orig /rdsdbdata/config/listener.ora`
	
	`$ cat listener.ora`
	`SUBSCRIBE_FOR_NODE_DOWN_EVENT_L_VISCDB_001=OFF`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`ADR_BASE_L_VISCDB_001 =/rdsdbdata/log/ USE_SID_AS_SERVICE_ L_VISCDB_001=ON L_VISCDB_001=(DESCRI PTION_LIST = (DESCRIPT ION = (ADDRESS = (PROTOCOL = TCP)(PORT = 1521)(HOST = xx.xx.xx. xx))) (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(PORT = 1521)(HOST = 127.0.0.1)))) SID_LIST_L_VISCDB_001= (SID_LIST = (SID_DESC = (SID_NAME = VISCDB)(G LOBAL_DBNAME = VISCDB) (ORACLE_HOME = / rdsdbbin/oracle)))`  Starten Sie den Listener `L_<INSTANCE_NAME>_ 001` für Amazon RDS-Stand ardoperationen:  `$ lsnrctl stop $ lsnrctl start L_VISCDB_001`  Für Oracle 12.1.0.2:  Bearbeiten Sie die Oracle E-Business Suite-Umg ebungsdatei, um den `$TNS_ADMIN` Pfad zur Verwendung der generisch en Amazon RDS Custom TNS-ifiles zu ändern.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Die Umgebungsdatei wurde erstellt, als Sie Autoconfig zuvor ausgeführ t haben. Bearbeiten Sie die `TNS_ADMIN` Variable, indem Sie das `<CONTEXT_NAME>` Postfix entfernen.
	
	Note
	Sie sollten die Umgebungsdatei nur in Oracle 12.1.0.2 bearbeiten, da das Standard-Home für 19c lautet`$ORACLE_H OME/network/ admin`, was dem Standard für Amazon RDS Custom entsprich t.
	
	Bearbeiten Sie beispielsweise in Oracle 12.1.0.2 die Datei:
	
	`$ vi $ORACLE_HOME/VIS_o ebs-db01log.env`
	
	Ändern Sie den Pfad von:
	
	`TNS_ADMIN=”/rdsdbbin/ oracle/network/admin/ VIS_oebs-db01log” export TNS_ADMIN`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	auf:
	
	`TNS_ADMIN=”/rdsdbbin/oracle/network/admin”`
	`export TNS_ADMIN`
	
	Note
	Bei jeder Ausführung von Autoconfig müssen Sie diesen Schritt wiederholen, um sicherzustellen, dass die richtigen TNS-Dateien verwendet werden. (nur 12.1.0.2).
	
	Für Oracle 19c:
	
	1. Ändern Sie den Wert für die Kontextvariable `s_cdb_tnsadmin` auf Datenbankebene auf `<ORACLE_HOME>/network/admin` statt `<ORACLE_HOME>/network/admin/<CONTEXT_NAME>` auf.
	
	Note
	Aktualisieren Sie die `s_db_tnsadmin` Kontextvariable nicht. Belassen Sie es	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	so<ORACLE_HOME>/network/admin/<CONTEXT_NAME> .	
	`$ . $ORACLE_HOME/VIS_oebs-db01log.env` `$ vi $CONTEXT_FILE`	
	2. Speichern Sie die Änderungen, die Sie am Wert von vorgenommen habens_cdb_tnsadmin .	
	Die Werte für s_db_tnsadmin und s_cdb_tnsadmin sollten wie folgt aussehen, mit dem PDB-Namen als VIS und dem logischen Namen des Datenbankknotens alsoebs-db01log .	
	`$ grep -i tns_admin $CONTEXT_FILE` <TNS_ADMIN oa_var="s_db_tnsadmin">/rdsdbbin/oracle/network/admin/VIS_oebs-db01log</TNS_ADMIN> <CDB_TNS_ADMIN oa_var="s_cdb_tnsadmin">/rdsdbbin/oracle/network/admin</CDB_TNS_ADMIN>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	3. Führen Sie Autoconfig auf der Datenbankebene aus:
	
	`$ . $ORACLE_HOME/VISCDB_oebs-db01log.env`
	`$ export ORACLE_PDB_SID=VIS`
	`$ sqlplus "/ as sysdba" @$ORACLE_HOME/apps util/admin/adgrants.sql APPS`
	`$ sqlplus "/ as sysdba" @$ORACLE_HOME/rdbms/admin/utlrp.sql`
	
	`$ . $ORACLE_HOME/VIS_oebs-db01log.env`
	`$ echo $ORACLE_SID`
	`VIS`
	
	`$ cd $ORACLE_HOME/appsutil/scripts/$CONTEXT_NAME`
	`$ ./adautocfg.sh`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Legt die Umgebung für den rdsdb-Benutzer fest.	Überspringen Sie diesen Schritt für Oracle 19c.
	
	Für Oracle 12.1.0.2:
	
	Nachdem Sie die Autoconfig- und TNS-Einträge abgeschlossen haben, müssen Sie die Umgebungsdatei laden, indem Sie sie im `rdsdb` Benutzerprofil festlegen.
	
	Aktualisieren Sie `.bash_profile` , um die Datenbankdatei der Oracle E-Business Suite aufzurufen. `.env` Sie müssen das Profil aktualisieren, um sicherzustellen, dass die Umgebung geladen ist. Diese Umgebungsdatei wurde erstellt, als Sie Autoconfig zuvor ausgeführt haben.
	
	Die folgende Beispiel-Umgebungsdatei wird erstellt, wenn Sie Autoconfig ausführen:
	
	`. /rdsdbbin/oracle/VIS_oebs-db01log.env`
	
	Als `rdsdb` Benutzer:
	
	`cd $HOME`
	`vi .bash_profile`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`export LD_LIBRARY_PATH=${ORACLE_HOME}/lib:${ORACLE_HOME}/ctx/lib`
	`export SHLIB_PATH=${ORACLE_HOME}/lib`
	`export PATH=$PATH:${ORACLE_HOME}/bin`
	`alias sql='rlwrap -c sqlplus / as sysdba'`
	`. ${ORACLE_HOME}/VIS_oebs-db01log.env`
	
	Note
	Für Oracle 19c müssen Sie die CDB-Umgebung nicht laden. `.bash_profile` Dies liegt daran, dass der Standardpfad auf den Standardpfad festgelegt `ORACLE_HOME` ist`$ORACLE_HOME/network/admin`, der das Standardverzeichnis des Benutzers `rdsdb` (Oracle-Standardverzeichnis) ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Anwendung und Datenbank für Amazon RDS Custom.	Führen Sie die ersten beiden Schritte für Oracle 12.1.0.2 und 19c aus. Die nachfolgenden Schritte unterscheiden sich je nach Version. 1. Bearbeiten Sie auf der Anwendungsebene die IP-Adresse für die Datenbank `/etc/hosts` und ändern Sie sie in die benutzerdefinierte Amazon RDS-IP-Adresse: `xx.xx.xx.xx OEBS-db01.localdomain OEBS-db01 OEBS-db01log.localdomain OEBS-db01log` Da Sie logische Hostnamen verwenden, können Sie den Datenbankknoten fast problemlos ersetzen. 2. Fügen Sie auf der Amazon RDS Custom DB-Instance die Sicherheitsgruppe hinzu, die der EC2 Quell-Instance zugewiesen ist, oder ändern Sie sie, um die Amazon RDS Custom DB-Instance widerzuspiegeln, um sicherzustellen, dass die Anwendung auf den Knoten zugreifen kann. Für Oracle 12.1.0.2:	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	3. Führen Sie Autoconfig aus. Führen Sie als Besitzer der Anwendung (z. B.`applmgr`) Folgendes aus:
	`$ cd $INST_TOP/admin/scripts`
	`$ ./adautocfg.sh`
	`AutoConfig completed successfully.`
	4. Überprüfen Sie die `fnd_nodes` Einträge:
	`SQL> select node_name from apps.fnd_nodes`
	`NODE_NAME`
	`----------`
	`AUTHENTICATION`
	`OEBS-APP01LOG`
	`OEBS-DB01LOG`
	5. Vergewissern Sie sich, dass Sie sich anmelden können, und starten Sie die Anwendung:
	`$ ./adstrtal.sh`
	Für Oracle 19c:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	1. Prüfen Sie, ob die PDB geöffnet ist, und öffnen Sie sie bei Bedarf:
	
	`SQL> show pdbs`
	
	`CON_ID CON_NAME OPEN MODE RESTRICTED`
	`---------- --------- ---------- ---------- 2 PDB$SEED READ ONLY NO`
	`3 VIS MOUNTED`
	
	`SQL> alter session set container=vis;`
	
	`SQL> alter database open;`
	
	`SQL> alter database save state;`
	
	2. Testen Sie die Konnektivität als `apps`:
	
	`SQL> sqlplus apps/**** @vis`
	
	3. Führen Sie Autoconfig auf der Datenbankebene aus:
	
	`$ . $ORACLE_HOME/VIS_oebs-db01log.env`
	`$ echo $ORACLE_SID`
	`VIS`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>$ cd $ORACLE_HOME/appsutil/scripts/$CONTEXT_NAME
	$ ./adautocfg.sh</pre>
	4. Führen Sie Autoconfig auf der Anwendungsebene als Anwendungseigentümer aus (z. B.`applmgr`):
	<pre>$ cd $INST_TOP/admin/scripts
	$ ./adautocfg.sh
	AutoConfig completed successfully.</pre>
	5. Überprüfen Sie die `fnd_nodes` Einträge:
	<pre>SQL> select node_name from apps.fnd_nodes
	NODE_NAME
	-------------------- 	
	------------------ 	
	------------------ 	
	------------------ 	
	------ 	
	AUTHENTICATION
	OEBS-APP01LOG
	OEBS-DB01LOG</pre>
	6. Starten Sie die Anwendung:
	<pre>$ ./adstrtal.sh</pre>	

Führen Sie die Schritte nach der Migration durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Setzen Sie die Automatisierung fort, um zu bestätigen, dass sie funktioniert.	Setzen Sie die Automatisierung fort, indem Sie den folgenden AWS-CLI-Befehl verwenden:
	`aws rds modify-db-instance \ --db-instance-identifier vis \ --automation-mode full \`
	Die Datenbank wird jetzt von Amazon RDS Custom verwaltet. Wenn beispielsweise der Listener oder die Datenbank ausfällt, startet der Amazon RDS Custom Agent sie neu. Um dies zu testen, führen Sie Befehle wie die folgenden aus.
	Beispiel für einen Stop-Listener:
	`-bash-4.2$ lsnrctl stop vis`
	Beispiel für eine Shutdown-Datenbank:
	`SQL> shutdown immediate ;`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie Schema, Verbindungen und Wartungsaufgaben.	Um die Migration abzuschließen, müssen Sie mindestens die folgenden Aufgaben ausführen. • Führen Sie aus`FS_CLONE`, um das Patch-Dateisystem zu synchronisieren. • Erfassen Sie Schemastatistiken. • Stellen Sie sicher, dass externe Schnittstellen und Systeme eine Verbindung zur neuen Amazon RDS Custom-Datenbank herstellen können. • Richten Sie Ihre Backups und Wartungspläne ein. • Stellen Sie sicher, dass AD Online Patching (ADOP) erwartungsgemäß funktioniert, indem Sie eine Umstellung durchführen, um die Dateisysteme zu wechseln.	DBA

Fehlerbehebung

Problem	Lösung
Sie erhalten einen ORA-01624-Fehler, wenn Sie versuchen, die Protokolldateien zu löschen.	Wenn Sie beim Versuch, die Protokolldateien zu löschen, eine ORA-01624-Fehlermeldung erhalten, gehen Sie wie folgt vor.

Problem	Lösung

	Geben Sie den folgenden Befehl ein und warten Sie, bis der Status der Protokolldateien, die Sie löschen möchten, lautet. `INACTIVE` Weitere Informationen zu den Statuscodes in finden Sie in `V$log` der Oracle-Dokumentation. Hier ist ein Beispielbefehl und seine Ausgabe:
	
	`SQL> select group#, status from v$log;`
	
	`GROUP# STATUS`
	`---------- ----------------`
	`1 ACTIVE`
	`2 CURRENT`
	`3 UNUSED`
	`4 UNUSED`
	`5 UNUSED`
	`6 UNUSED`
	`6 rows selected.`
	
	In diesem Beispiel ist Protokolldatei 1`ACTIVE`, Sie müssen also dreimal einen Protokoll dateiwechsel erzwingen, um sicherzus tellen, dass die erste neue Protokolldatei, die Sie zuvor hinzugefügt haben, den Status hat`CURRENT`:
	
	`SQL>  alter system switch logfile;`
	`System altered.`
	`SQL>  alter system switch logfile;`
	`System altered.`
	`SQL>  alter system switch logfile;`
	`System altered.`
	
	Warten Sie, bis alle Protokolldateien, die Sie löschen möchten`INACTIVE`, wie im folgenden Beispiel, vorhanden sind, und führen Sie dann den `DROP LOGFILE` Befehl aus.

Problem	Lösung

	`SQL> select group#, status from v$log;`
	`GROUP# STATUS`
	`---------- ----------`
	`1 INACTIVE`
	`2 INACTIVE`
	`3 INACTIVE`
	`4 CURRENT`
	`5 UNUSED`
	`6 UNUSED`
	`6 rows selected.`

Sie erhalten einen ORA-00392-Fehler, wenn Sie die Datenbank mit öffnen. `resetlogs`	Wenn Sie den Fehler ORA-00392 erhalten: Protokoll xx von Thread 1 wird gelöscht, Vorgang nicht zulässig, führen Sie den folgenden Befehl aus (`xx`ersetzen Sie ihn durch die Protokolldateinummer), und führen Sie dann den Befehl open erneut aus: `resetlogs`
	
	`SQL> alter database clear logfile group xx;`
	`SQL> alter database open resetlogs;`

Problem	Lösung
Sie haben Probleme, mithilfe von Sysadmin oder Anwendungsbenutzer eine Verbindung zur Anwendung herzustellen.	Führen Sie die folgende SQL-Abfrage aus, um das Problem zu bestätigen: `SQL> select dbms_java.get_jdk_ version() from dual; select dbms_java.get_jdk_version() from dual ERROR at line 1: ORA-29548: Java system class reported: release of Java system classes in the database (19.0.0.0.220719 1.8) does not match that of the oracle executabl e (19.0.0.0.0 1.8)` Hauptursache: Die Quelldatenbank wurde mit mehreren Patches installiert, aber Amazon RDS Custom `DB_HOME` ist eine neue Installat ion, oder der CEV enthielt nicht alle Patches, weil Sie bei der Erstellung des CEV nicht die erforderlichen RSU-Patches wie OJVM verwendet haben. Um dies zu überprüfen, überprüfen Sie, ob die Quell-Patch-Detail s unter`$ORACLE_HOME/sqlpath` , und aufgeführt sind. `$ORACLE_HOME/.patc h_storage opatch – lsinventory` Referenz: datapatch -verbose schlägt mit folgender Fehlermeldung fehl: „Patch xxxxxx: Das archivierte Patch-Verzeichnis ist leer“ (Dokument-ID 2235541.1) Behebung: Kopieren Sie die fehlenden Patch-bezogenen Dateien von der Quelle (`$ORACLE_HOME/sqlpatch/`) nach Amazon RDS Custom (`$ORACLE_HOME/ sqlpatch/`) und führen Sie sie dann erneut aus. `./datapatch -verbose`

Problem	Lösung

	Zum Beispiel:
	`-bash-4.2$ cp -rp 18793246 20204035 20887355 22098146 22731026 $ORACLE_HOME/sqlpatch/`
	Alternativ können Sie das Problem umgehen, indem Sie den folgenden Befehl in der CDB und PDB ausführen:
	`@?/javavm/install/update_javavm_db.sql`
	Führen Sie dann den folgenden Befehl auf der PDB aus:
	`sql> alter session set container=vis; @?/javavm/install/update_javavm_db.sql`
	Führen Sie den Test nun erneut aus:
	`SQL> select dbms_java.get_jdk_version() from dual;`

Zugehörige Ressourcen

- Arbeiten mit Amazon RDS Custom (Amazon RDS-Dokumentation)
- Amazon RDS Custom for Oracle — Neue Kontrollfunktionen in der Datenbankumgebung (AWS-News-Blog)
- Integrieren Sie Amazon RDS Custom for Oracle mit Amazon EFS (AWS-Datenbank-Blog)
- Migration der Oracle E-Business Suite auf AWS (AWS-Whitepaper)
- Architektur der Oracle E-Business Suite auf AWS (AWS-Whitepaper)

- Richten Sie eine HA/DR-Architektur für Oracle E-Business Suite auf Amazon RDS Custom mit einer aktiven Standby-Datenbank ein (AWS Prescriptive Guidance)

Zusätzliche Informationen

Wartungsarbeiten

Patchen der Oracle E-Business Suite-Datenbank-Startseite mit neuen Patches

Da es sich bei dem Bin-Volume (`/rdsdbbin`) um ein out-of-place Upgrade handelt, wird der Inhalt des Bin-Volumes während des CEV-Upgrades gelöscht. Daher müssen Sie eine Kopie des `appsutil` Verzeichnisses erstellen, bevor Sie Upgrades mithilfe von CEV durchführen.

Erstellen Sie auf der benutzerdefinierten Amazon RDS-Quell-Instance vor dem Upgrade des CEV eine Sicherungskopie von`$ORACLE_HOME/appsutil`.

> **Note**
>
> In diesem Beispiel wird ein NFS-Volume verwendet. Sie können jedoch stattdessen eine Kopie für Amazon Simple Storage Service (Amazon S3) verwenden.

1. Erstellen Sie ein Verzeichnis zum Speichern von Appsutil auf der benutzerdefinierten Amazon RDS-Quell-Instance:

```
$ mkdir /RMAN/appsutil.preupgrade
```

2. Tar und auf das Amazon EFS-Volume kopieren:

```
$ tar cvf /RMAN/appsutil.preupgrade appsutil
```

3. Stellen Sie sicher, dass die TAR-Datei existiert:

```
$ bash-4.2$ ls -l /RMAN/appsutil.preupgrade
-rw-rw-r-- 1 rdsdb rdsdb 622981120 Feb  8 20:16 appsutil.tar
```

4. Führen Sie ein Upgrade auf das neueste CEV durch (Voraussetzung CEV ist bereits erstellt), indem Sie den Anweisungen unter Upgrade einer benutzerdefinierten RDS-Instance in der Amazon RDS-Dokumentation folgen.

Sie können Patches auch direkt mit OPATCH durchführen. Weitere Informationen finden Sie im Abschnitt Anforderungen und Überlegungen für Upgrades von RDS Custom for Oracle in der Amazon RDS-Dokumentation.

> **Note**
>
> Die IP-Adresse des Host-Computers ändert sich während des CEV-Patchvorgangs nicht. Bei diesem Vorgang wird ein out-of-place Upgrade durchgeführt, und beim Start wird ein neues Bin-Volume an dieselbe Instanz angehängt.

Migrieren Sie Oracle PeopleSoft zu Amazon RDS Custom

Erstellt von Gaurav Gupta (AWS)

Übersicht

Oracle PeopleSoft ist eine ERP-Lösung (Enterprise Resource Planning) für unternehmensweite Prozesse. PeopleSoft hat eine dreistufige Architektur: Client, Anwendung und Datenbank. PeopleSoft kann auf Amazon Relational Database Service (Amazon RDS) ausgeführt werden. Jetzt können Sie es auch PeopleSoft auf Amazon RDS Custom ausführen, das Zugriff auf das zugrunde liegende Betriebssystem bietet.

Amazon RDS Custom for Oracle ist ein verwalteter Datenbankservice für ältere, benutzerdefinierte und verpackte Anwendungen, die Zugriff auf das zugrunde liegende Betriebssystem und die Datenbankumgebung benötigen. Wenn Sie Ihre Oracle-Datenbank zu Amazon RDS Custom migrieren, kann Amazon Web Services (AWS) Backup-Aufgaben und Hochverfügbarkeit verwalten, während Sie sich auf die Wartung Ihrer PeopleSoft Anwendung und Funktionalität konzentrieren können. Wichtige Faktoren, die bei einer Migration zu berücksichtigen sind, finden Sie unter Strategien zur Migration von Oracle-Datenbanken in AWS Prescriptive Guidance.

Dieses Muster konzentriert sich auf die Schritte zur Migration einer PeopleSoft Datenbank auf Amazon Elastic Compute Cloud (Amazon EC2) zu Amazon RDS Custom mithilfe eines Oracle Recovery Manager (RMAN) -Backups. Es verwendet ein gemeinsam genutztes Amazon Elastic File System (Amazon EFS) -Dateisystem zwischen der EC2 Instance und Amazon RDS Custom, obwohl Sie auch Amazon FSx oder ein anderes gemeinsam genutztes Laufwerk verwenden können. Das Muster verwendet ein vollständiges RMAN-Backup (manchmal auch als Level-0-Backup bezeichnet).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Oracle-Quelldatenbank der Version 19C, die auf Amazon EC2 mit Oracle Linux 7, Oracle Linux 8, Red Hat Enterprise Linux (RHEL) 7 oder RHEL 8 ausgeführt wird. In den Beispielen für dieses Muster lautet der Name der Quelldatenbank`FSDM092`, aber das ist keine Voraussetzung.

> **Note**
>
> Sie können dieses Muster auch mit lokalen Oracle-Quelldatenbanken verwenden. Sie müssen über die entsprechende Netzwerkkonnektivität zwischen dem lokalen Netzwerk und einer Virtual Private Cloud (VPC) verfügen.

- Eine PeopleSoft 9.2-Demo-Instanz.
- Eine einzige PeopleSoft Anwendungsebene. Sie können dieses Muster jedoch so anpassen, dass es mit mehreren Anwendungsebenen funktioniert.
- Amazon RDS Custom ist mit mindestens 8 GB Swap-Speicherplatz konfiguriert.

Einschränkungen

Dieses Muster unterstützt die folgenden Konfigurationen nicht:

- Setzen des `ARCHIVE_LAG_TARGET` Datenbankparameters auf einen Wert außerhalb des Bereichs von 60—7200
- Deaktivierung des Protokollmodus der DB-Instance () `NOARCHIVELOG`
- Deaktivieren des für Amazon Elastic Block Store (Amazon EBS) optimierten Attributs der Instance EC2
- Ändern der ursprünglichen EBS-Volumes, die an die Instance angehängt sind EC2
- Hinzufügen neuer EBS-Volumes oder Ändern des Volumetyps von gp2 auf gp3
- Ändern des Erweiterungsformats für den `LOG_ARCHIVE_FORMAT` Parameter (erforderlich) `*.arc`
- Multiplexen oder Ändern des Speicherorts und Namens der Steuerdatei (das muss sein) `/rdsdbdata/db/*DBNAME*/controlfile/control-01.ctl`

Weitere Informationen zu diesen und anderen nicht unterstützten Konfigurationen finden Sie in der Amazon RDS-Dokumentation.

Produktversionen

Informationen zu Oracle-Datenbankversionen und Instance-Klassen, die von Amazon RDS Custom unterstützt werden, finden Sie unter Anforderungen und Einschränkungen für Amazon RDS Custom for Oracle.

Architektur

Zieltechnologie-Stack

- Application Load Balancer
- Amazon EFS
- Amazon RDS Custom für Oracle

- AWS Secrets Manager
- Amazon Simple Storage Service (Amazon-S3)

Zielarchitektur

Das folgende Architekturdiagramm stellt ein PeopleSoft System dar, das in einer einzigen Availability Zone auf AWS ausgeführt wird. Auf die Anwendungsebene wird über einen Application Load Balancer zugegriffen. Sowohl die Anwendung als auch die Datenbanken befinden sich in privaten Subnetzen, und die Amazon RDS Custom- und EC2 Amazon-Datenbank-Instance verwenden ein gemeinsam genutztes Amazon EFS-Dateisystem, um die RMAN-Backup-Dateien zu speichern und darauf zuzugreifen. Amazon S3 wird zur Erstellung der benutzerdefinierten RDS-Oracle-Engine und zum Speichern der Redo-Logs-Metadaten verwendet.

Tools

Tools

AWS-Services

- Amazon RDS Custom for Oracle ist ein verwalteter Datenbankservice für ältere, benutzerdefinierte und verpackte Anwendungen, die Zugriff auf das zugrunde liegende Betriebssystem und die Datenbankumgebung benötigen. Er automatisiert Datenbankverwaltungsaufgaben wie Backups und Hochverfügbarkeit.
- Amazon Elastic File System (Amazon EFS) unterstützt Sie bei der Erstellung und Konfiguration gemeinsam genutzter Dateisysteme in der AWS-Cloud. Dieses Muster verwendet ein gemeinsam genutztes Amazon EFS-Dateisystem, um die RMAN-Backup-Dateien zu speichern und darauf zuzugreifen.
- AWS Secrets Manager hilft Ihnen dabei, hartcodierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Geheimnis programmgesteuert abzurufen. In diesem Muster rufen Sie die Datenbankbenutzerkennwörter aus Secrets Manager ab, um die `ADMIN` Benutzer `RDSADMIN` und zu erstellen und die `system` Kennwörter `sys` und zu ändern.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Traffic auf Amazon Elastic Compute Cloud (Amazon

EC2) -Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen. Dieses Muster verwendet einen Application Load Balancer.

Andere Tools

- Oracle Recovery Manager (RMAN) bietet Backup- und Recovery-Unterstützung für Oracle-Datenbanken. Dieses Muster verwendet RMAN, um ein Hot-Backup der Oracle-Quelldatenbank auf Amazon durchzuführen EC2 , das auf Amazon RDS Custom wiederhergestellt wird.

Bewährte Methoden

- Passen Sie für Datenbankinitialisierungsparameter die Standard-P-Datei an, die von der Amazon RDS Custom DB-Instance bereitgestellt wird, PeopleSoft anstatt die SP-Datei aus der Oracle-Quelldatenbank zu verwenden. Dies liegt daran, dass Leerzeichen und Kommentare Probleme beim Erstellen von Read Replicas in Amazon RDS Custom verursachen. Weitere Informationen zu Datenbank-Initialisierungsparametern finden Sie in Oracle Support Note 1100831.1 (erfordert einen Oracle Support Account).
- Amazon RDS Custom verwendet standardmäßig die automatische Speicherverwaltung von Oracle. Wenn Sie den Hugemem-Kernel verwenden möchten, können Sie Amazon RDS Custom so konfigurieren, dass stattdessen die automatische Verwaltung gemeinsam genutzter Speicher verwendet wird.
- Lassen Sie den `memory_max_target` Parameter standardmäßig aktiviert. Das Framework verwendet dies im Hintergrund, um Read Replicas zu erstellen.
- Aktivieren Sie Oracle Flashback Database. Diese Funktion ist nützlich, wenn der Standbymodus in Failover-Testszenarien (nicht Switchover-Testszenarien) wiederhergestellt wird.

Epen

Richten Sie die DB-Instance und das Dateisystem ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die DB-Instance.	Erstellen Sie in der Amazon RDS-Konsole eine Amazon RDS Custom for Oracle DB-Instance mit einem DB-Namen	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	namens FSDMO92 (oder dem Namen Ihrer Quelldatenbank). Anweisungen finden Sie unter Arbeiten mit Amazon RDS Custom in der AWS-Dokumentation und im Blogbeitrag Amazon RDS Custom for Oracle — New Control Capabilities in Database Environment. Dadurch wird sichergestellt, dass der Datenbankname auf denselben Namen wie die Quelldatenbank gesetzt ist. (Wenn dieses Feld leer gelassen wird, werden der EC2 Instanz- und Datenbankname auf gesetzt`ORCL`.)	

Führen Sie eine vollständige RMAN-Backup der EC2 Amazon-Quelldatenbank durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Backup-Skript.	Erstellen Sie ein RMAN-Backup-Skript, um die Datenbank im Amazon EFS-Dateisystem zu sichern, das Sie bereitgestellt haben (`/efs`im folgenden Beispiel). Sie können den Beispielcode verwenden oder eines Ihrer vorhandenen RMAN-Skripts ausführen. `#!/bin/bash`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`Dt=`date +'%Y%m%d-%H%M'` `BACKUP_LOG="rman-${ORACLE_SID}-$Dt"` `export TAGDATE=`date +%Y%m%d%H%M`;` `LOGPATH=/u01/scripts/logs` `rman target / >>` ` $LOGPATH/rman-${ORACLE_SID}-$Dt << EOF` `SQL "ALTER SYSTEM SWITCH` ` LOGFILE";` `SQL "ALTER SESSION SET` ` NLS_DATE_FORMAT="DD.MM.YYYY HH24:MI:SS"";` `RUN` `{` ` ALLOCATE CHANNEL ch11` ` TYPE DISK MAXPIECESIZE` ` 5G;` ` ALLOCATE CHANNEL ch12` ` TYPE DISK MAXPIECESIZE` ` 5G;` ` BACKUP AS COMPRESSED` ` BACKUPSET FULL DATABASE` ` FORMAT '/efs/rman_backup/FSCM/%d_%T_%s_%p_FULL' ;` ` SQL "ALTER SYSTEM` ` ARCHIVE LOG CURRENT";` ` BACKUP FORMAT '/efs/rman_backup/FSCM/%d_%T_%s_%p_ARCHIVE'` ` ARCHIVELOG ALL DELETE` ` ALL INPUT ;` ` BACKUP CURRENT` ` CONTROLFILE FORMAT '/efs/rman_backup/FSCM/%d_%T_%s_%p_CONTROL';` `}`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`EXIT;` `EOF`	

Führen Sie das Backup-Skript aus.	Um das RMAN-Backup-Skript auszuführen, melden Sie sich als Oracle Home User an und führen Sie das Skript aus.
	`$  chmod a+x rman_backup.sh`
	`$ ./rman_backup.sh &`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Suchen Sie nach Fehlern und notieren Sie sich den Namen der Sicherungsdatei.	Überprüfen Sie die RMAN-Protokolldatei auf Fehler. Wenn alles in Ordnung aussieht, listen Sie die Sicherungskopie der Steuerdatei auf, indem Sie den folgenden Befehl ausführen.
	`RMAN> list backup of controlfile;`
	`using target database control file instead of recovery catalog`
	Notieren Sie sich den Namen der Ausgabedatei.
	`List of Backup Sets`
	`==========`
	`BS Key Type LV Size Device Type Elapsed Time Completion Time`
	`12 Full 21.58M DISK 00:00:01 13-JUL-22`
	`BP Key: 12 Status: AVAILABLE Compressed: NO Tag: TAG20220713T150155`
	`Piece Name: /efs/rman_backup/F`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`SCM/FSDMO92_202207 13_12_1_CONTROL Control File Included: Ckp SCN: 165591599 85898 Ckp time: 13- JUL-22` Sie verwenden die Backup-Kontrolldatei `/efs/rman _backup/FSCM/FSDMO 92_20220713_12_1_C ONTROL` , wenn Sie die Datenbank auf Amazon RDS Custom wiederherstellen.	

Fahren Sie die Ebene der Quellanwendung herunter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die Anwendung herunter.	Verwenden Sie das `psadmin` Hilfsprogramm oder das `psadmin` Befehlszeilenprogr amm, um die Ebene der Quellanwendung herunterz ufahren. 1. Führen Sie den folgenden Befehl aus, um den Webserver herunterz ufahren. `psadmin -w shutdown - d "webserver domain name"`	DBA, Administrator PeopleSoft

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	2. Führen Sie den folgenden Befehl aus, um den Anwendungsserver herunterzufahren.
	`psadmin -c shutdown -d "application server domain name"`
	3. Führen Sie den folgenden Befehl aus, um den Prozessplaner herunterz ufahren.
	`psadmin -p stop -d "process scheduler domain name"`	

Konfiguration der benutzerdefinierten Amazon RDS-Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie das nfs-utils-rpm-Paket.	Führen Sie den folgenden Befehl aus, um das `nfs-utils rpm` Paket zu installie ren. `$ yum install -y nfs-utils`	DBA
Mounten Sie den EFS-Speic her.	Rufen Sie den Amazon EFS-Mount-Befehl von der Amazon EFS-Konsolenseite ab. Mounten Sie das EFS-Dateisystem auf der Amazon	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	RDS-Instance mithilfe eines Network File System (NFS) - Clients. `sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport fs-xxxxxxxxxx.efs.eu-west-1.amazonaws.com:/ /efs` `sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport fs-xxxxxxxxxx.efs.eu-west-1.amazonaws.com:/ /efs`	

Löschen Sie die Startdatenbank und erstellen Sie die Verzeichnisse zum Speichern der Datenbankdateien

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Den Automatisierungsmodus unterbrechen.	Sie müssen den Automatisierungsmodus auf Ihrer Amazon RDS Custom DB-Instance anhalten, bevor Sie mit den nächsten Schritten fortfahren, um sicherzustellen, dass die Automatisierung die RMAN-Wiederherstellungsaktivität nicht beeinträchtigt.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie können die Automatisierung unterbrechen, indem Sie die AWS-Konsole oder den Befehl AWS Command Line Interface (AWS CLI) verwenden (stellen Sie sicher, dass Sie zuerst die AWS-CLI konfiguriert haben). `aws rds modify-db-instance \ --db-instance-id entifier peoplesoft-fscm-92 \ --automation-mode all-paused \ --resume-full-au tomation-mode-minute 360 \ --region eu-west-1` Wenn Sie die Dauer der Pause angeben, stellen Sie sicher, dass Sie genügend Zeit für die RMAN-Wiederherstellung einplanen. Dies hängt von der Größe der Quelldatenbank ab. Ändern Sie daher den 360-Wert entsprechend. Stellen Sie außerdem sicher, dass sich die Gesamtzeit der angehaltenen Automatisierung nicht mit dem Sicherungs-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	oder Wartungsfenster der Datenbank überschneidet.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen und ändern Sie die Parameterdatei für PeopleSoft	Um die Datei für zu erstellen und zu ändern PeopleSoft, verwenden Sie die Standardd atei, die mit der Amazon RDS Custom DB-Instance erstellt wurde. Fügen Sie die Parameter hinzu, die Sie für benötigen. PeopleSoft
	1. Wechseln Sie zu, `rds user rdsdb` indem Sie den folgenden Befehl ausführen.
	`$ sudo su - rdsdb`
	2. Melden Sie sich in der Startdatenbank bei SQL*Plus an und erstellen Sie die Datei, indem Sie den folgenden Befehl ausführen.
	`SQL> create pfile from spfile;`
	Dadurch wird die Datei in erstellt. `$ORACLE_HOME/dbs`
	3. Erstellen Sie eine Sicherungskopie dieser Datei.
	4. Bearbeiten Sie die Datei, um Parameter hinzuzufü
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	gen oder zu aktualisieren PeopleSoft.
	
	`*._gby_hash_aggregation_enabled=false`
	
	`*._unnest_subquery=false`
	
	`*.nls_language='AMERICAN'`
	
	`*.nls_length_semantics='CHAR'`
	
	`*.nls_territory='AMERICA'`
	
	`*.open_cursors=1000`
	
	`*.db_files=1200`
	
	`*.undo_tablespace='UNDOTBS1'`
	
	PeopleSoft Verwandte Parameter finden Sie in Oracle Support Note 1100831.1.
	5. Entfernen Sie die SPfile-Referenz aus der Pfile.
	
	`*.spfile='/rdsdbin/oracle/dbs/spfileFSDMO92.ora'`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Löschen Sie die Starter-Datenbank.	Verwenden Sie den folgenden Code, um die bestehende benutzerdefinierte Amazon RDS-Datenbank zu löschen.
	`$ sqlplus / as sysdba`
	`SQL> shutdown immediate ;`
	`SQL> startup mount exclusive restrict;`
	`SQL> drop database;`
	`SQL> exit`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die benutzerd efinierte Amazon RDS-Daten bank aus dem Backup wieder her.	Stellen Sie die Datenbank mithilfe des folgenden Skripts wieder her. Das Skript stellt zuerst die Steuerdatei wieder her und stellt dann die gesamte Datenbank aus den auf dem EFS-Mount gespeicherten Sicherung sdateien wieder her. `#!/bin/bash` `Dt=`date +'%Y%m%d-%H` `%M'` `BACKUP_LOG="rman-${O` `RACLE_SID}-$Dt"` `export TAGDATE=`date +` `%Y%m%d%H%M`;` `LOGPATH=/rdsdbdata/scr` `ipts/logs` `rman target / >>` ` $LOGPATH/rman-${OR` `ACLE_SID}-$Dt << EOF` `restore controlfi` `le from "/efs/rma` `n_backup/FSCM/FSDM` `O92_20220713_12_1_` `CONTROL";` `alter database mount;` `run` `{` `set newname for database` ` to '/rdsdbdata/db/FSD` `MO92_A/datafile/%f_` `%b';` `SET NEWNAME FOR TEMPFILE` ` 1 TO '/rdsdbdata/db/` `FSDMO92_A/datafile/%f` `_%b';` `RESTORE DATABASE;`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SWITCH DATAFILE ALL; SWITCH TEMPFILE ALL; RECOVER DATABASE; } EOF sqlplus / as sysdba >> $LOGPATH/rman-${OR ACLE_SID}-$Dt<<-EOF ALTER DATABASE RENAME FILE '/u01/psoft/db/ oradata/FSDMO92/redo0 1.log' TO '/rdsdbda ta/db/FSDMO92_A/on linelog/redo01.log'; ALTER DATABASE RENAME FILE '/u01/psoft/db/ oradata/FSDMO92/redo0 2.log' TO '/rdsdbda ta/db/FSDMO92_A/on linelog/redo02.log'; ALTER DATABASE RENAME FILE '/u01/psoft/db/ oradata/FSDMO92/redo0 3.log' TO '/rdsdbda ta/db/FSDMO92_A/on linelog/redo03.log'; alter database clear unarchived logfile group 1; alter database clear unarchived logfile group 2; alter database clear unarchived logfile group 3; alter database open resetlogs; EXIT EOF	

Passwörter aus Secrets Manager abrufen, Benutzer erstellen und Passwörter ändern

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie das Passwort von Secrets Manager ab.	Sie können diesen Schritt mithilfe der AWS-Konsole oder der AWS-CLI ausführen. Die folgenden Schritte zeigen Anweisungen für die Konsole. 1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon RDS-Konsole. 2. Wählen Sie im Navigationsbereich Datenbanken und dann die Amazon RDS-Datenbank aus. 3. Wählen Sie die Registerkarte Konfiguration und notieren Sie sich die Ressourcen-ID für die Instance. Sie wird das Format haben `db-<ID>` (zum Beispiel `db-73GJNHLGDNZNDOXNWXSECUW6LE`). 4. Öffnen Sie die Secrets Manager-Konsole. 5. Wählen Sie das Geheimnis aus, das denselben Namen hat wie `do-not-delete-custom-<resource_id>` , wobei es `resource-id` sich auf die Ressourcen-ID bezieht,	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Sie in Schritt 3 notiert haben. 6. Wählen Sie Retrieve secret value (Secret-Wert abrufen) aus. Dieses Passwort ist für die `admin` Benutzer`sys`, `systemrdsadmin`, und dasselbe.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den RDSADMIN-Benutzer.	`RDSADMIN`ist der Datenbankbenutzer für die Überwachung und Orchestrierung der Amazon RDS Custom DB-Instance. Da die Startdatenbank gelöscht und die Zieldatenbank mithilfe von RMAN aus der Quelle wiederhergestellt wurde, müssen Sie diesen Benutzer nach dem Wiederherstellungsvorgang neu erstellen, um sicherzustellen, dass die benutzerdefinierte Amazon RDS-Überwachung wie erwartet funktioniert. Sie müssen außerdem ein separates Profil und einen separaten Tablespace für den Benutzer erstellen. `RDSADMIN`
	
	1. Geben Sie an einer SQL-Eingabeaufforderung die folgenden Befehle ein.
	
	`SQL> set echo on feedback on serverout on`
	`SQL> @?/rdbms/admin/utlpwdmg.sql`
	`SQL> ALTER PROFILE DEFAULT LIMIT FAILED_LOGIN_ ATTEMPTS UNLIMITED PASSWORD_LIFE_TIME UNLIMITED`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	PASSWORD_VERIFY_F UNCTION NULL; 2. Erstellen Sie das ProfilRDSADMIN. SQL> set echo on feedback on serverout on SQL> alter session set "_oracle_script"=t rue; SQL> CREATE PROFILE RDSADMIN LIMIT COMPOSITE_LIMIT UNLIMITED SESSIONS_PER_USER UNLIMITED CPU_PER_SESSION UNLIMITED CPU_PER_CALL UNLIMITED LOGICAL_READS_PER _SESSION UNLIMITED LOGICAL_READS_PER _CALL UNLIMITED IDLE_TIME UNLIMITED CONNECT_TIME UNLIMITED PRIVATE_SGA UNLIMITED FAILED_LOGIN_ATTE MPTS 10 PASSWORD_LIFE_TIME UNLIMITED PASSWORD_REUSE_TIME UNLIMITED PASSWORD_REUSE_MAX UNLIMITED	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>PASSWORD_VERIFY_F
	UNCTION NULL
	PASSWORD_LOCK_TIME
	 86400/86400
	PASSWORD_GRACE_TIME
	 604800/86400;</pre>
	3. Erstellen Sie den RDSADMIN Tablespace.
	<pre>SQL> CREATE BIGFILE
	 TABLESPACE rdsadmin
	 '/rdsdbdata/db/FSD
	MO92_A/datafile/rd
	sadmin.dbf' DATAFILE
	 SIZE 7M
	AUTOEXTEND ON NEXT 1m
	LOGGING ONLINE
	 PERMANENT BLOCKSIZE
	 8192 EXTENT MANAGEMEN
	T LOCAL AUTOALLOCATE
	 DEFAULT NOCOMPRES
	S SEGMENT SPACE
	 MANAGEMENT AUTO;</pre>
	4. Erstellen Sie den RDSADMIN Benutzer. Ersetzen Sie das RDSADMIN Passwort durch das Passwort, das Sie zuvor von Secrets Manager erhalten haben.
	<pre>SQL> CREATE USER
	 rdsadmin IDENTIFIED
	 BY xxxxxxxxxx
	DEFAULT TABLESPACE
	 rdsadmin
	TEMPORARY TABLESPACE
	 TEMP</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	profile rdsadmin ; 5. Gewähren Sie RDSADMIN Rechte. SQL> GRANT "CONNECT" TO RDSADMIN WITH ADMIN OPTION; SQL> GRANT "RESOURCE" TO RDSADMIN WITH ADMIN OPTION; SQL> GRANT "DBA" TO RDSADMIN; SQL> GRANT "SELECT_CATALOG_ROLE" TO RDSADMIN WITH ADMIN OPTION; SQL> GRANT ALTER SYSTEM TO RDSADMIN; SQL> GRANT UNLIMITED TABLESPACE TO RDSADMIN; SQL> GRANT SELECT ANY TABLE TO RDSADMIN; SQL> GRANT ALTER DATABASE TO RDSADMIN; SQL> GRANT ADMINISTER DATABASE TRIGGER TO RDSADMIN; SQL> GRANT ANY OBJECT PRIVILEGE TO RDSADMIN WITH ADMIN OPTION; SQL> GRANT INHERIT ANY PRIVILEGES TO RDSADMIN; SQL> ALTER USER RDSADMIN DEFAULT ROLE ALL;	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	6. Set the SYS, SYSTEM, and DBSNMP user profiles to RDSADMIN.
	`SQL> set echo on feedback on serverout on`
	`SQL> alter user SYS profile RDSADMIN;`
	`SQL> alter user SYSTEM profile RDSADMIN;`
	`SQL> alter user DBSNMP profile RDSADMIN;`	

Erstellen Sie den Master-Benutzer.	Da die Startdatenbank gelöscht und die Zieldatenbank mithilfe von RMAN aus der Quelle wiederhergestellt wurde, müssen Sie den Masterbenutzer neu erstellen. In diesem Beispiel lautet der Masterbenutzername. `admin`
	`SQL> create user admin identified by <password>;`
	`SQL> grant dba to admin`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Ändern Sie die Systemken nwörter.	Ändern Sie die Systemken nwörter, indem Sie das Passwort verwenden, das Sie von Secrets Manager abgerufen haben.
	`SQL> alter user sys identified by xxxxxxxxxx;`
	`SQL> alter user system identified by xxxxxxxxxx;`
	Wenn Sie diese Passwörter nicht ändern, zeigt Amazon RDS Custom die Fehlermel dung „Der Benutzer oder die Benutzeranmeldedaten für die Datenbanküberwachung haben sich geändert“ an.
		DBA

Konfigurieren Sie die TNS-Einträge für Amazon RDS Custom und PeopleSoft

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Datei tnsnames.	Um von der Anwendung sebene aus eine Verbindung mit der Datenbank herzustel len, konfigurieren Sie die `tnsnames.ora` Datei so, dass Sie von der Anwendung sebene aus eine Verbindun g zur Datenbank herstelle n können. Im folgenden Beispiel können Sie sehen,	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	dass es einen Softlink zu der `tnsnames.ora` Datei gibt, die Datei jedoch standardmäßig leer ist.
	
	`$ cd /rdsdbbin/oracle/network/admin`
	`$ ls -ltr`
	`-rw-r--r-- 1 rdsdb database 1536 Feb 14 2018 shrept.lst`
	`lrwxrwxrwx 1 rdsdb database 30 Apr 5 13:19 listener.ora -> /rdsdbdata/config/listener.ora`
	`lrwxrwxrwx 1 rdsdb database 28 Apr 5 13:19 sqlnet.ora -> /rdsdbdata/config/sqlnet.ora`
	`lrwxrwxrwx 1 rdsdb database 30 Apr 5 13:19 tnsnames.ora -> /rdsdbdata/config/tnsnames.ora`
	
	1. Erstellen Sie den `tsnames.ora` Eintrag. Aufgrund der Art und Weise, wie die Amazon RDS-Automatisierung die Dateien analysiert, müssen Sie sicherstellen, dass der Eintrag keine Leerzeichen, Kommentare oder zusätzlichen Zeilen enthält. Andernfalls könnten	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Probleme auftreten, wenn Sie einige davon verwenden APIs, wie z. B. create-db-instance-read - replica.
	2. Ersetzen Sie den Port, den Host und die SID entsprechend Ihren PeopleSoft Datenbankanforderungen. Verwenden Sie den folgenden Code als Beispiel.
	`$ vi tnsnames.ora`
	`FSDMO92=(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = x.x.x.x)(PORT = 1521))) (CONNECT_DATA = (SERVER = DEDICATED) (SID = FSDMO92)))`
	3. Führen Sie den folgenden Befehl aus, um zu bestätigen, dass auf die PeopleSoft Datenbank zugegriffen werden kann.
	`$ tnsping FSDMO92`
	`TNS Ping Utility for Linux: Version 19.0.0.0.0 - Production on 14-JUL-2022 10:16:45`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>Copyright (c) 1997,
	 2021, Oracle. All
	 rights reserved.
	
	Used parameter files:
	/rdsdbbin/oracle/net
	work/admin/sqlnet.
	ora
	
	Used TNSNAMES adapter
	 to resolve the alias
	Attempting to
	 contact (DESCRIPT
	ION = (ADDRESS_
	LIST = (ADDRESS =
	 (PROTOCOL = TCP)(HOST
	 = x.x.x.x)(PORT =
	 1521))) (CONNECT_
	DATA = (SERVER =
	 DEDICATED) (SID =
	 FSDMO92)))
	OK (0 msec)</pre>	

Erstellen Sie den SPfile-Softlink

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den SPFile-Softlink.	1. Führen Sie den folgenden Befehl aus `/rdsdbdata/admin/FSDMO92/pfile` , um die Datei spfile an dem Speicherort zu erstellen.
	<pre>SQL> create spfile='/
	rdsdbdata/admin/FS
	DMO92/pfile/spfile</pre>
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`FSDMO92.ora' from pfile;`
	2. Navigieren Sie zu `$ORACLE_HOME/dbs` der SP-Datei und erstellen Sie einen Softlink für diese.
	`ln -s '/rdsdbdata/admin/FSDMO92/pfile/spfileFSDMO92.ora' spfileFSDMO92.ora`
	3. Nachdem diese Datei erstellt wurde, können Sie die Datenbank mithilfe der SP-Datei herunterfahren und starten.	

Führen Sie die Schritte nach der Migration durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie das Schema, die Verbindungen und die Wartungsaufgaben.	Führen Sie die folgenden Aufgaben aus, um die Migration abzuschließen. • Erfassen Sie Schemasta tistiken. • Stellen Sie sicher, dass die PeopleSoft Anwendung sebene eine Verbindung zur neuen Amazon RDS-Custom-Datenbank herstelle n kann.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Richten Sie Ihre Sicherung s- und Wartungspläne ein.	

Zugehörige Ressourcen

- Arbeiten mit Amazon RDS Custom
- Amazon RDS Custom for Oracle — Neue Kontrollfunktionen in der Datenbankumgebung (Blogbeitrag)
- Integrieren Sie Amazon RDS Custom for Oracle mit Amazon EFS (Blogbeitrag)
- Konfiguration von Amazon RDS als PeopleSoft Oracle-Datenbank (AWS-Whitepaper)

Migrieren Sie die Oracle ROWID-Funktionalität zu PostgreSQL auf AWS

Erstellt von Rakesh Raghav (AWS) und Ramesh Pathuri (AWS)

Übersicht

Dieses Muster beschreibt Optionen für die Migration der `ROWID` Pseudospaltenfunktionalität in Oracle Database zu einer PostgreSQL-Datenbank in Amazon Relational Database Service (Amazon RDS) for PostgreSQL, Amazon Aurora PostgreSQL-Compatible Edition oder Amazon Elastic Compute Cloud (Amazon). EC2

In einer Oracle-Datenbank ist die Pseudospalte eine physische Adresse einer Zeile in einer Tabelle`ROWID`. Diese Pseudospalte wird verwendet, um eine Zeile eindeutig zu identifizieren, auch wenn der Primärschlüssel in einer Tabelle nicht vorhanden ist. PostgreSQL hat eine ähnliche Pseudospalte namens`ctid`, aber sie kann nicht als verwendet werden. `ROWID` Wie in der PostgreSQL-Dokumentation erklärt, `ctid` kann es sich ändern, wenn es aktualisiert wird oder nach jedem `VACUUM` Prozess.

Es gibt drei Möglichkeiten, die `ROWID` Pseudospaltenfunktionalität in PostgreSQL zu erstellen:

- Verwenden Sie eine Primärschlüsselspalte, anstatt eine Zeile in einer Tabelle `ROWID` zu identifizieren.
- Verwenden Sie einen logischen Primär-/Einzelschlüssel (der ein zusammengesetzter Schlüssel sein kann) in der Tabelle.
- Fügen Sie eine Spalte mit automatisch generierten Werten hinzu und machen Sie sie zu einem primären/eindeutigen Schlüssel, der nachgeahmt werden soll. `ROWID`

Dieses Muster führt Sie durch alle drei Implementierungen und beschreibt die Vor- und Nachteile der einzelnen Optionen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Fachwissen in der prozeduralen Language/PostgreSQL (PL/pgSQL () Programmierung
- Quelle: Oracle-Datenbank
- Ein Amazon RDS for PostgreSQL- oder Aurora PostgreSQL-kompatibler Cluster oder eine EC2 Instance zum Hosten der PostgreSQL-Datenbank

Einschränkungen

- Dieses Muster bietet Behelfslösungen für die Funktionalität. `ROWID` PostgreSQL bietet kein Äquivalent zu `ROWID` in Oracle Database.

Produktversionen

- PostgreSQL 11.9 oder höher

Architektur

Quelltechnologie-Stack

- Oracle Database

Zieltechnologie-Stack

- Aurora PostgreSQL-kompatibel, Amazon RDS für PostgreSQL oder eine Instance mit einer PostgreSQL-Datenbank EC2

Implementierungsoptionen

Es gibt drei Optionen, um die mangelnde `ROWID` Unterstützung in PostgreSQL zu umgehen, je nachdem, ob Ihre Tabelle einen Primärschlüssel oder einen eindeutigen Index, einen logischen Primärschlüssel oder ein Identitätsattribut hat. Ihre Wahl hängt von Ihren Projektzeitplänen, Ihrer aktuellen Migrationsphase und den Abhängigkeiten von Anwendungs- und Datenbankcode ab.

Option	Beschreibung	Vorteile	Nachteile
Primärschlüssel oder eindeutiger Index	Wenn Ihre Oracle-Tabelle über einen Primärschlüssel verfügt, können Sie die Attribute dieses Schlüssels verwenden, um eine Zeile	• Keine Abhängigkeit von proprietären Datenbankfunktionen. • Minimale Auswirkungen auf die Leistung, da	• Erfordert Änderungen am Anwendungs- und Datenbankcode, der `ROWID` für den Wechsel zu

	eindeutig zu identifiz ieren.	Primärschlüsselfel der indexiert werden.	Primärschlüsselfel dern erforderlich ist.
Logischer Primär-/E inzelschlüssel	Wenn Ihre Oracle-Tabelle über einen logischen Primärsch lüssel verfügt, können Sie die Attribute dieses Schlüssels verwenden, um eine Zeile eindeutig zu identifizieren. Ein logischer Primärsch lüssel besteht aus einem Attribut oder einer Gruppe von Attributen, die eine Zeile eindeutig identifizieren können, aber dieser Wert wird in der Datenbank nicht durch eine Einschrän kung erzwungen.	• Keine Abhängigk eit von proprietären Datenbankfunktione n.	• Erfordert Änderungen am Anwendungs- und Datenbankcode, der `ROWID` für den Wechsel zu Primärschlüsselfel dern erforderlich ist. • Erhebliche Auswirkungen auf die Leistung, wenn die Attribute des logischen Primärschlüssels nicht indexiert werden. Sie können jedoch einen eindeutigen Index hinzufügen, um Leistungsprobleme zu vermeiden.

Identitätsattribut	Wenn Ihre Oracle-Tabelle keinen Primärschlüssel hat, können Sie ein zusätzliches Feld als erstellen `GENERATED ALWAYS AS IDENTITY`. Dieses Attribut generiert immer dann einen eindeutigen Wert, wenn Daten in die Tabelle eingefügt werden, sodass es verwendet werden kann, um eine Zeile für DML-Operationen (Data Manipulation Language) eindeutig zu identifizieren.	• Keine Abhängigkeit von proprietären Datenbankfunktionen. • Die PostgreSQL-Datenbank füllt das Attribut auf und behält seine Einzigartigkeit bei.	• Erfordert Änderungen am Anwendungs- und Datenbankcode, der für den Wechsel `ROWID` zum Identitätsattribut erforderlich ist. • Erhebliche Auswirkung auf die Leistung, wenn das zusätzliche Feld nicht indexiert wird. Sie können jedoch einen Index hinzufügen, um Leistungsprobleme zu vermeiden.

Tools

- Amazon Relational Database Service (Amazon RDS) für PostgreSQL unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen PostgreSQL-Datenbank in der AWS-Cloud.
- Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können. In diesem Muster können Sie die AWS-CLI verwenden, um SQL-Befehle über pgAdmin auszuführen.
- pgAdmin ist ein Open-Source-Verwaltungstool für PostgreSQL. Es bietet eine grafische Oberfläche, mit der Sie Datenbankobjekte erstellen, verwalten und verwenden können.

- Das AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist.

Epen

Identifizieren Sie die Quelltabellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Oracle-Tabellen, die das `ROWID` Attribut verwenden.	Verwenden Sie das AWS Schema Conversion Tool (AWS SCT), um Oracle-Tabellen zu identifizieren, die über `ROWID` Funktionen verfügen. Weitere Informationen finden Sie in der AWS SCT-Dokumentation. –oder– Verwenden Sie in Oracle die `DBA_TAB_COLUMNS` Ansicht, um Tabellen zu identifizieren, die ein `ROWID` Attribut haben. Diese Felder können zum Speichern von alphanumerischen 10-Byte-Zeichen verwendet werden. Ermitteln Sie die Verwendung und konvertieren Sie diese gegebenenfalls in ein `VARCHAR` Feld.	DBA oder Entwickler
Identifizieren Sie den Code, der auf diese Tabellen verweist.	Verwenden Sie AWS SCT, um einen Migrationsbewertungsbericht zu erstellen, um die Verfahren zu identifizieren,	DBA oder Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die betroffen sind von`ROWID`. Weitere Informationen finden Sie in der AWS SCT-Dokumentation. –oder– Verwenden Sie in der Oracle-Quelldatenbank das Textfeld der `dba_source` Tabelle, um Objekte zu identifizieren, die `ROWID` Funktionen verwenden.	

Ermitteln Sie die Verwendung von Primärschlüsseln

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Tabellen, die keine Primärschlüssel haben.	Verwenden Sie dies in der Oracle-Quelldatenbank, `DBA_CONSTRAINTS` um Tabellen zu identifizieren, die keine Primärschlüssel haben. Anhand dieser Informationen können Sie die Strategie für jede Tabelle festlegen. Zum Beispiel: `select dt.* from dba_tables dt where not exists (select 1 from all_constraints ct where ct.owner = Dt.owner`	DBA oder Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>and ct.table_name = Dt.table_name
	and ct.constraint_type = 'P'
	)
	and dt.owner = '{schema}'</pre>	

Identifizieren Sie die Lösung und wenden Sie sie an

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wenden Sie Änderungen für Tabellen an, die einen definierten oder logischen Primärschlüssel haben.	Nehmen Sie die im Abschnitt Zusätzliche Informationen aufgeführten Änderungen am Anwendungs- und Datenbankcode vor, um einen eindeutigen Primärschlüssel oder einen logischen Primärschlüssel zur Identifizierung einer Zeile in Ihrer Tabelle zu verwenden.	DBA oder Entwickler
Fügen Sie Tabellen, die keinen definierten oder logischen Primärschlüssel haben, ein zusätzliches Feld hinzu.	Fügen Sie ein Attribut des Typs hinzu`GENERATED ALWAYS AS IDENTITY`. Nehmen Sie die Änderungen an der Anwendung und dem Datenbankcode vor, die im Abschnitt Zusätzliche Informationen aufgeführt sind.	DBA oder Entwickler
Fügen Sie bei Bedarf einen Index hinzu.	Fügen Sie dem zusätzlichen Feld oder dem logischen Primärschlüssel einen Index	DBA oder Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	hinzu, um die SQL-Leistung zu verbessern.	

Zugehörige Ressourcen

- PostgreSQL CTID (PostgreSQL-Dokumentation)
- Generierte Spalten (PostgreSQL-Dokumentation)
- ROWID-Pseudospalte (Oracle-Dokumentation)

Zusätzliche Informationen

Die folgenden Abschnitte enthalten Oracle- und PostgreSQL-Codebeispiele, um die drei Ansätze zu veranschaulichen.

Szenario 1: Verwendung eines eindeutigen Primärschlüssels

In den folgenden Beispielen erstellen Sie die Tabelle `testrowid_s1` mit `emp_id` als Primärschlüssel.

Oracle-Code:

```
create table testrowid_s1 (emp_id integer, name varchar2(10), CONSTRAINT testrowid_pk
 PRIMARY KEY (emp_id));
INSERT INTO testrowid_s1(emp_id,name) values (1,'empname1');
INSERT INTO testrowid_s1(emp_id,name) values (2,'empname2');
INSERT INTO testrowid_s1(emp_id,name) values (3,'empname3');
INSERT INTO testrowid_s1(emp_id,name) values (4,'empname4');
commit;

SELECT rowid,emp_id,name FROM testrowid_s1;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3pAAAAAAAMOAAA          1 empname1
AAAF3pAAAAAAAMOAAB          2 empname2
AAAF3pAAAAAAAMOAAC          3 empname3
AAAF3pAAAAAAAMOAAD          4 empname4

UPDATE testrowid_s1 SET name = 'Ramesh' WHERE rowid = 'AAAF3pAAAAAAAMOAAB' ;
commit;
```

```
SELECT rowid,emp_id,name FROM testrowid_s1;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3pAAAAAAAMOAAA          1 empname1
AAAF3pAAAAAAAMOAAB          2 Ramesh
AAAF3pAAAAAAAMOAAC          3 empname3
AAAF3pAAAAAAAMOAAD          4 empname4
```

PostgreSQL-Code:

```
CREATE TABLE public.testrowid_s1
(
    emp_id integer,
    name character varying,
    primary key (emp_id)
);

insert into public.testrowid_s1 (emp_id,name) values
(1,'empname1'),(2,'empname2'),(3,'empname3'),(4,'empname4');

select emp_id,name from testrowid_s1;
 emp_id |   name
--------+----------
      1 | empname1
      2 | empname2
      3 | empname3
      4 | empname4

update testrowid_s1 set name = 'Ramesh' where emp_id = 2 ;

select emp_id,name from testrowid_s1;
 emp_id |   name
--------+----------
      1 | empname1
      3 | empname3
      4 | empname4
      2 | Ramesh
```

Szenario 2: Verwendung eines logischen Primärschlüssels

In den folgenden Beispielen erstellen Sie die Tabelle `testrowid_s2` mit `emp_id` dem logischen Primärschlüssel.

Oracle-Code:

```
create table testrowid_s2 (emp_id integer, name varchar2(10) );
INSERT INTO testrowid_s2(emp_id,name) values (1,'empname1');
INSERT INTO testrowid_s2(emp_id,name) values (2,'empname2');
INSERT INTO testrowid_s2(emp_id,name) values (3,'empname3');
INSERT INTO testrowid_s2(emp_id,name) values (4,'empname4');
commit;

SELECT rowid,emp_id,name FROM testrowid_s2;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3rAAAAAAAMeAAA          1 empname1
AAAF3rAAAAAAAMeAAB          2 empname2
AAAF3rAAAAAAAMeAAC          3 empname3
AAAF3rAAAAAAAMeAAD          4 empname4

UPDATE testrowid_s2 SET name = 'Ramesh' WHERE rowid = 'AAAF3rAAAAAAAMeAAB' ;
commit;

SELECT rowid,emp_id,name FROM testrowid_s2;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3rAAAAAAAMeAAA          1 empname1
AAAF3rAAAAAAAMeAAB          2 Ramesh
AAAF3rAAAAAAAMeAAC          3 empname3
AAAF3rAAAAAAAMeAAD          4 empname4
```

PostgreSQL-Code:

```
CREATE TABLE public.testrowid_s2
(
    emp_id integer,
    name character varying
);

insert into public.testrowid_s2 (emp_id,name) values
(1,'empname1'),(2,'empname2'),(3,'empname3'),(4,'empname4');

select emp_id,name from testrowid_s2;
 emp_id |   name
--------+----------
      1 | empname1
```

```
      2 | empname2
      3 | empname3
      4 | empname4

update testrowid_s2 set name = 'Ramesh' where emp_id = 2 ;

select emp_id,name from testrowid_s2;
 emp_id |   name
--------+----------
      1 | empname1
      3 | empname3
      4 | empname4
      2 | Ramesh
```

Szenario 3: Verwendung eines Identitätsattributs

In den folgenden Beispielen erstellen Sie die Tabelle `testrowid_s3` ohne Primärschlüssel und mithilfe eines Identitätsattributs.

Oracle-Code:

```
create table testrowid_s3 (name varchar2(10));
INSERT INTO testrowid_s3(name) values ('empname1');
INSERT INTO testrowid_s3(name) values ('empname2');
INSERT INTO testrowid_s3(name) values ('empname3');
INSERT INTO testrowid_s3(name) values ('empname4');
commit;

SELECT rowid,name FROM testrowid_s3;
ROWID              NAME
------------------ ----------
AAAF3sAAAAAAAMmAAA empname1
AAAF3sAAAAAAAMmAAB empname2
AAAF3sAAAAAAAMmAAC empname3
AAAF3sAAAAAAAMmAAD empname4

UPDATE testrowid_s3 SET name = 'Ramesh' WHERE rowid = 'AAAF3sAAAAAAAMmAAB' ;
commit;

SELECT rowid,name FROM testrowid_s3;
ROWID              NAME
------------------ ----------
AAAF3sAAAAAAAMmAAA empname1
```

```
AAAF3sAAAAAAAMmAAB Ramesh
AAAF3sAAAAAAAMmAAC empname3
AAAF3sAAAAAAAMmAAD empname4
```

PostgreSQL-Code:

```
CREATE TABLE public.testrowid_s3
(
    rowid_seq bigint generated always as identity,
    name character varying
);

insert into public.testrowid_s3 (name) values
('empname1'),('empname2'),('empname3'),('empname4');

select rowid_seq,name from testrowid_s3;
 rowid_seq |   name
-----------+----------
         1 | empname1
         2 | empname2
         3 | empname3
         4 | empname4

update testrowid_s3 set name = 'Ramesh' where rowid_seq = 2 ;

select rowid_seq,name from testrowid_s3;
 rowid_seq |   name
-----------+----------
         1 | empname1
         3 | empname3
         4 | empname4
         2 | Ramesh
```

Migrieren Sie Oracle-Datenbank-Fehlercodes in eine Amazon Aurora PostgreSQL-kompatible Datenbank

Erstellt von Sai Parthasaradhi (AWS) und Veeranjaneyulu Grandhi (AWS)

Übersicht

Dieses Muster zeigt, wie Oracle Database-Fehlercodes mithilfe einer vordefinierten Metadatentabelle in eine Amazon Aurora PostgreSQL-kompatible Edition-Datenbank migriert werden.

Oracle-Datenbankfehlercodes haben nicht immer einen entsprechenden PostgreSQL-Fehlercode. Dieser Unterschied in den Fehlercodes kann es schwierig machen, die Verarbeitungslogik der Prozeduren oder Funktionen in der PostgreSQL-Zielarchitektur zu konfigurieren.

Sie können den Vorgang vereinfachen, indem Sie die Fehlercodes der Quell- und Zieldatenbank, die für Ihr PL/pgSQL-Programm von Bedeutung sind, in einer Metadatentabelle speichern. Konfigurieren Sie dann die Tabelle so, dass gültige Oracle Database-Fehlercodes gekennzeichnet und sie ihren PostgreSQL-Entsprechungen zugeordnet werden, bevor Sie mit der verbleibenden Prozesslogik fortfahren. Wenn der Oracle-Datenbank-Fehlercode nicht in der Metadatentabelle enthalten ist, wird der Prozess mit der Ausnahme beendet. Anschließend können Sie die Fehlerdetails manuell überprüfen und den neuen Fehlercode zur Tabelle hinzufügen, falls Ihr Programm dies erfordert.

Mit dieser Konfiguration kann Ihre Amazon Aurora PostgreSQL-kompatible Datenbank Fehler genauso behandeln wie Ihre Oracle-Quelldatenbank.

> **Note**
>
> Die Konfiguration einer PostgreSQL-Datenbank für die korrekte Verarbeitung von Oracle-Datenbank-Fehlercodes erfordert normalerweise Änderungen an der Datenbank und dem Anwendungscode.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Oracle-Quelldatenbank mit laufenden Instance- und Listener-Services
- Ein Amazon Aurora PostgreSQL-kompatibler Cluster, der betriebsbereit ist

- Vertrautheit mit Oracle Database
- Vertrautheit mit PostgreSQL-Datenbanken

Architektur

Das folgende Diagramm zeigt ein Beispiel für einen Amazon Aurora PostgreSQL-kompatiblen Datenbank-Workflow für die Validierung und Behandlung von Datenfehlercodes:

Das Diagramm zeigt den folgenden Workflow:

1. Eine Tabelle enthält die Fehlercodes und Klassifizierungen von Oracle Database sowie die entsprechenden PostgreSQL-Fehlercodes und Klassifizierungen. Die Tabelle enthält eine valid_error-Spalte, die klassifiziert, ob bestimmte, vordefinierte Fehlercodes gültig sind oder nicht.
2. Wenn eine PL/pgSQL-Funktion (func_processdata) eine Ausnahme auslöst, ruft sie eine zweite PL/pgSQL-Funktion (error_validation) auf.
3. Die Funktion error_validation akzeptiert den Fehlercode der Oracle-Datenbank als Eingabeargument. Anschließend überprüft die Funktion den eingehenden Fehlercode anhand der Tabelle, um festzustellen, ob der Fehler in der Tabelle enthalten ist.
4. Wenn der Oracle Database-Fehlercode in der Tabelle enthalten ist, gibt die Funktion error_validation den Wert TRUE zurück und die Prozesslogik wird fortgesetzt. Wenn der Fehlercode nicht in der Tabelle enthalten ist, gibt die Funktion einen FALSE-Wert zurück und die Prozesslogik wird mit einer Ausnahme beendet.
5. Wenn die Funktion einen FALSE-Wert zurückgibt, werden die Fehlerdetails manuell vom Funktionsleiter der Anwendung überprüft, um festzustellen, ob sie gültig sind.
6. Der neue Fehlercode wird dann entweder manuell zur Tabelle hinzugefügt oder nicht. Wenn der Fehlercode gültig ist und der Tabelle hinzugefügt wurde, gibt die Funktion error_validation beim nächsten Auftreten der Ausnahme den Wert TRUE zurück. Wenn der Fehlercode nicht gültig ist und der Prozess beim Auftreten der Ausnahme fehlschlagen muss, wird der Fehlercode nicht zur Tabelle hinzugefügt.

Technologie-Stack

- Amazon Aurora PostgreSQL
- pgAdmin
- Oracle SQL Developer

Tools

- Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt.
- pgAdmin ist ein Open-Source-Verwaltungs- und Entwicklungstool für PostgreSQL. Es bietet eine grafische Oberfläche, die die Erstellung, Wartung und Verwendung von Datenbankobjekten vereinfacht.
- Oracle SQL Developer ist eine kostenlose, integrierte Entwicklungsumgebung, die die Entwicklung und Verwaltung von Oracle Database sowohl in herkömmlichen als auch in Cloud-Umgebungen vereinfacht.

Epen

Migrieren Sie Oracle-Datenbank-Fehlercodes in Ihre Amazon Aurora PostgreSQL-kompatible Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine Tabelle in der Amazon Aurora PostgreSQL-kompatiblen Datenbank.	Führen Sie den folgenden PostgreSQL-Befehl CREATE TABLE aus:
	`(`
	`source_error_code numeric NOT NULL,`
	`target_error_code character varying NOT NULL,`
	`valid_error character varying(1) NOT NULL`
	`);`
		PostgreSQL-Entwickler, Oracle, RDS/Aurora für PostgreSQL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie der Tabelle PostgreSQL-Fehlercodes und die entsprechenden Oracle-Datenbank-Fehlercodes hinzu.	Führen Sie den PostgreSQL-Befehl INSERT aus, um die erforderlichen Fehlercodewerte zur Tabelle error_codes hinzuzufügen.
	
	Die PostgreSQL-Fehlercodes müssen den zeichenvariablen Datentyp (SQLSTATE-Wert) verwenden. Die Oracle-Fehlercodes müssen den numerischen Datentyp (SQLCODE-Wert) verwenden.
	
	Beispiel für Insert-Anweisungen:
	
	`insert into error_codes values (-1817,'22007','Y');`
	`insert into error_codes values (-1816,'22007','Y');`
	`insert into error_codes values (-3114,'08006','N');`
	
	Note
	Wenn Sie Oracle-spezifische Java Database Connectivity (JDBC) -Ausnahmen abfangen, müssen Sie diese Ausnahmen entweder durch generische datenbank
		PostgreSQL-Entwickler, Oracle, RDS/Aurora für PostgreSQL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	übergreifende Ausnahmen ersetzen oder zu PostgreSQ L-spezifischen Ausnahmen wechseln.	
Erstellen Sie eine PL/pgSQL-Funktion zur Validierung von Fehlercodes.	Erstellen Sie eine PL/pgSQL-Funktion, indem Sie den PostgreSQL-Befehl CREATE FUNCTION ausführen. Stellen Sie sicher, dass die Funktion Folgendes tut: • Akzeptiert die von einem Programm ausgelösten Oracle-Fehlercodes. • Prüft, ob Fehlercodes in der Tabelle error_codes vorhanden sind. • Gibt den Wert TRUE oder FALSE zurück, je nachdem, ob der Fehlercode in der Metadatentabelle vorhanden ist oder nicht.	PostgreSQL-Entwickler, Oracle, RDS/Aurora für PostgreSQL

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie manuell neue Fehlercodes, während sie von der PL/pgSQL-Funktion aufgezeichnet werden.	Überprüfen Sie die neuen Fehlercodes manuell. Wenn ein neuer Fehlercode für Ihren Anwendungsfall gültig ist, fügen Sie ihn der Tabelle error_codes hinzu, indem Sie den PostgreSQL INSERT-Befehl ausführen. –oder– Wenn ein neuer Fehlercode für Ihren Anwendungsfall nicht gültig ist, fügen Sie ihn nicht der Tabelle hinzu. Die Prozesslogik schlägt weiterhin fehl und wird mit einer Ausnahme beendet, wenn der Fehler auftritt.	PostgreSQL-Entwickler, Oracle, RDS/Aurora für PostgreSQL

Zugehörige Ressourcen

Anhang A. PostgreSQL-Fehlercodes (PostgreSQL-Dokumentation)

Datenbank-Fehlermeldungen (Oracle Database-Dokumentation)

Migrieren Sie Redis-Workloads zu Redis Enterprise Cloud auf AWS

Erstellt von Antony Prasad Thevaraj (AWS) und Srinivas Pendyala (Redis)

Übersicht

In diesem Muster wird der allgemeine Prozess für die Migration von Redis-Workloads zu Redis Enterprise Cloud auf Amazon Web Services (AWS) beschrieben. Es beschreibt die Migrationsschritte, bietet Informationen zur Auswahl der verfügbaren Tools und erörtert die Vor- und Nachteile sowie die Schritte zur Verwendung der einzelnen Tools. Wenn Sie zusätzliche Hilfe bei der Migration von Workloads von Redis benötigen, können Sie optional Redis Professional Services in Anspruch nehmen.

Wenn Sie Redis OSS oder Redis Enterprise Software vor Ort ausführen, sind Sie mit dem erheblichen Verwaltungsaufwand und der betrieblichen Komplexität vertraut, die mit der Wartung Ihrer Redis-Datenbanken in Ihrem Rechenzentrum verbunden sind. Durch die Migration Ihrer Workloads in die Cloud können Sie diesen betrieblichen Aufwand erheblich reduzieren und die Vorteile von Redis Enterprise Cloud nutzen, einem vollständig gehosteten Database-as-a-Service (DBaaS) -Angebot von Redis. Diese Migration trägt dazu bei, Ihre geschäftliche Flexibilität zu erhöhen, die Anwendungszuverlässigkeit zu verbessern und die Gesamtkosten zu senken, während Sie gleichzeitig Zugriff auf die neuesten Funktionen von Redis Enterprise Cloud on AWS wie 99,999% Verfügbarkeit, einfache Architektur und Skalierbarkeit erhalten.

Es gibt potenzielle Anwendungen für Redis Enterprise Cloud in den Bereichen Finanzdienstleistungen, Einzelhandel, Gesundheitswesen und Glücksspiel sowie in Anwendungsfällen, die Lösungen für Betrugserkennung, Bestandsaufnahme in Echtzeit, Schadensbearbeitung und Sitzungsmanagement erfordern. Sie können Redis Enterprise Cloud verwenden, um eine Verbindung zu Ihren AWS-Ressourcen herzustellen, z. B. zu einem Anwendungsserver, der auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances ausgeführt wird, oder zu einem Microservice, der als AWS Lambda-Service bereitgestellt wird.

Voraussetzungen und Einschränkungen

Annahmen

- Sie betreiben derzeit ein lokales Datenbanksystem, das Sie in die Cloud migrieren möchten.
- Sie haben die Migrationsanforderungen für Ihre Workloads identifiziert, darunter:
  - Anforderungen an die Datenkonsistenz
  - Anforderungen an die Infrastruktur und die Systemumgebung

  - Anforderungen an Datenkartierung und Transformation
  - Anforderungen an Funktionstests
  - Anforderungen an Leistungstests
  - Anforderungen an die Validierung
  - Definierte Umstellungsstrategie
- Sie haben die für die Migration erforderlichen Zeitpläne und Kostenschätzungen bewertet.
- Ihre Anforderungen berücksichtigen den Umfang der Arbeit und die Systeme und Datenbanken, die Sie als Teil der Migration identifiziert haben.
- Sie haben die Beteiligten zusammen mit ihren Rollen und Verantwortlichkeiten in einer RACI-Matrix (verantwortungsbewusst, rechenschaftspflichtig, konsultiert, informiert) identifiziert.
- Sie haben die erforderlichen Zustimmungen und Genehmigungen von allen Beteiligten erhalten.

Kosten

Abhängig von den technischen Spezifikationen Ihrer vorhandenen Quelldatenbank (z. B. Speichergröße, Durchsatz und Gesamtdatengröße) kann ein Redis-Lösungsarchitekt die Größe des Zielsystems in Redis Enterprise Cloud dimensionieren. Allgemeine Preisinformationen finden Sie unter Redis Pricing auf der Redis-Website.

Menschen und Fähigkeiten

Der Migrationsprozess umfasst die folgenden Rollen und Verantwortlichkeiten.

Rolle	Beschreibung	Erforderliche Fähigkeiten
Architekt für Migration slösungen	Ein technischer Architekt, der Erfahrung in der Definitio n, Planung und Implement ierung von Migrationsstrategi en besitzt	Verständnis von Quell- und Zielsystemen auf technischer Ebene und auf Anwendung sebene; Erfahrung mit der Migration von Workloads in die Cloud
Datenarchitekt	Ein technischer Architekt mit umfassender Erfahrung in der Definition, Implement ierung und Bereitstellung	Datenmodellierung für strukturi erte und unstrukturierte Daten, tiefes Verständnis und Erfahrung in der Implement

	von Datenlösungen für eine Vielzahl von Datenbanken	ierung von Datenbanken für ein Unternehmen
Architekt für Redis-Lösungen	Ein technischer Architekt, der Ihnen helfen kann, einen optimal dimensionierten Redis-Cluster für den entsprech enden Anwendungsfall zu entwerfen	Expertise in der Architektur und Bereitstellung von Redis-Lösungen für eine Vielzahl von Anwendungsfällen
Architekt für Cloud-Lösungen	Ein technischer Architekt mit einem tieferen Verständn is von Cloud-Lösungen, insbesondere auf AWS	Expertise in der Entwicklung von Lösungen für die Cloud; Erfahrung in der Migration von Workloads und der Modernisi erung von Anwendungen
Unternehmensarchitekt	Ein technischer Architekt, der ein umfassendes Verständnis der technischen Landschaft in Ihrem Unternehmen hat, der eine gemeinsame Vision für die future Roadmap hat und der standardisierte architekt onische Best Practices für alle Teams in Ihrer Organisation praktiziert und festlegt	Zertifizierungen für Softwarea rchitektur wie TOGAF, grundlegende Kenntnisse in der Softwareentwicklun g sowie Fachwissen in den Bereichen Lösungsarchitektur und Unternehmensarchitektur
IT oder Ingenieur DevOps	Ein Ingenieur, der für die Erstellung und Wartung der Infrastruktur verantwor tlich ist, einschließlich der Überwachung der Infrastruktur auf Probleme, der Durchführ ung von Wartungsaufgaben und der Durchführung von Aktualisierungen bei Bedarf.	Fundiertes Verständnis verschiedener Technolog ien, darunter Betriebss ysteme, Netzwerke und Cloud Computing; Vertrautheit mit Programmiersprachen wie Python, Bash und Ruby sowie Tools wie Docker, Kubernetes und Ansible

Architektur

Optionen für die Migration

Das folgende Diagramm zeigt Optionen für die Migration Ihrer lokalen (Redis-basierten oder anderen) Datenquellen zu AWS. Es zeigt verschiedene Migrationstools, aus denen Sie wählen können, z. B. den Export von Redis-Datenbankdateien (RDB) nach Amazon Simple Storage Service (Amazon S3), die Verwendung der Redis-Replikationsfunktion oder die Verwendung von AWS DMS.

1. Lokale Datenquellen: Datenbanken, die nicht auf Redis basieren, wie MySQL, PostgreSQL, Oracle, SQL Server oder MariaDB.
2. Lokale Datenquellen: Auf dem Redis-Protokoll basierende Datenbanken wie Redis OSS und Redis Enterprise Software.
3. Die einfachste Methode, Daten aus Redis-basierten Datenbanken zu migrieren, besteht darin, RDB-Dateien zu exportieren und sie in die Ziel-Redis Enterprise Cloud auf AWS zu importieren.
4. Alternativ können Sie die Daten mithilfe der Replikationsfunktion () `ReplicaOf` in Redis von der Quelle zum Ziel migrieren.
5. Wenn Ihre Datenmigrationsanforderungen die Transformation von Daten beinhalten, können Sie die Redis Input/Output Tools (RIOT) verwenden, um die Daten zu migrieren.
6. Alternativ können Sie den AWS Data Migration Service (AWS DMS) verwenden, um die Daten aus SQL-basierten Datenbanken zu migrieren.
7. Sie müssen Virtual Private Cloud (VPC) -Peering für AWS DMS verwenden, um die Daten erfolgreich in die Ziel-Redis Enterprise Cloud auf AWS zu migrieren.

Zielarchitektur

Das folgende Diagramm zeigt eine typische Bereitstellungsarchitektur für Redis Enterprise Cloud auf AWS und veranschaulicht, wie sie mit wichtigen AWS-Services verwendet werden kann.

1. Sie können eine Verbindung zu den Geschäftsanwendungen herstellen, die von Redis Enterprise Cloud auf AWS unterstützt werden.
2. Sie können Geschäftsanwendungen in Ihrem eigenen AWS-Konto in einer VPC innerhalb dieses Kontos ausführen.
3. Sie können Redis Enterprise Cloud-Datenbank-Endpunkte verwenden, um eine Verbindung zu Ihren Anwendungen herzustellen. Beispiele hierfür sind ein Anwendungsserver, der auf EC2

Instances ausgeführt wird, ein als AWS Lambda Lambda-Service bereitgestellter Microservice, eine Amazon Elastic Container Service (Amazon ECS) -Anwendung oder eine Amazon Elastic Kubernetes Service (Amazon EKS) -Anwendung.

4. Geschäftsanwendungen, die in Ihrer VPC ausgeführt werden, benötigen eine VPC-Peer-Verbindung zur Redis Enterprise Cloud VPC. Dadurch können die Geschäftsanwendungen eine sichere Verbindung über private Endpunkte herstellen.
5. Redis Enterprise Cloud on AWS ist eine speicherinterne NoSQL-Datenbankplattform, die als DBaaS auf AWS bereitgestellt wird und vollständig von Redis verwaltet wird.
6. Redis Enterprise Cloud wird innerhalb einer VPC in einem Standard-AWS-Konto bereitgestellt, das von Redis erstellt wird.
7. Aus Sicherheitsgründen wird Redis Enterprise Cloud in einem privaten Subnetz bereitgestellt, auf das sowohl von privaten als auch von öffentlichen Endpunkten aus zugegriffen werden kann. Wir empfehlen, dass Sie Ihre Client-Anwendungen auf privaten Endpunkten mit Redis verbinden. Wenn Sie planen, einen öffentlichen Endpunkt zu verwenden, empfehlen wir dringend, TLS zu aktivieren, um die Daten zwischen Ihren Client-Anwendungen und Redis Enterprise Cloud zu verschlüsseln.

Die Redis-Migrationsmethodik entspricht der AWS-Migrationsmethodik, die unter Mobilize your organization to accelerate large migrations auf der AWS Prescriptive Guidance-Website veranschaulicht wird.

Automatisierung und Skalierung

Die Aufgaben zur Einrichtung der Umgebung für die Migration können über AWS Landing Zone und IaC-Vorlagen (Infrastructure as Code) für Automatisierung und Skalierung automatisiert werden. Diese werden im Abschnitt „Epics“ dieses Musters behandelt.

Tools

Basierend auf Ihren Datenmigrationsanforderungen können Sie aus einer Auswahl technologischer Optionen wählen, um Ihre Daten zu Redis Enterprise Cloud auf AWS zu migrieren. In der folgenden Tabelle werden diese Tools beschrieben und verglichen.

Werkzeug	Beschreibung	Vorteile	Nachteile
RDB-Export und -Import	Sie exportieren die Daten aus der	• Einfach.	• Erfüllt keine Anforderungen

	Quelldatenbank (z. B. Redis OSS oder Redis Enterprise Software) in Form von RDB-Dateien. Wenn Ihre Datenbank über einen Redis OSS-Cluster bereitgestellt wird, exportieren Sie jeden Master-Shard in eine RDB. Anschließend importieren Sie alle RDB-Dateien in einem Schritt. Wenn Ihre Quelldatenbank auf einem OSS-Cluster basiert, Ihre Zieldatenbank jedoch nicht die OSS-Cluster-API verwendet, müssen Sie den Quellcode Ihrer Anwendung ändern, um eine standardmäßige Redis-Clientbibliothek zu verwenden. Anforderungen an die Datentransformation oder logische Datenbank zusammenführungen erfordern einen komplexeren Prozess, der weiter unten in	• Funktioniert mit jeder Redis-basierten Lösung, die Daten im RDB-Format als Quelle exportieren kann (einschließlich Redis OSS und Redis Enterprise Software). • Erreicht Datenkonsistenz mit einem einfachen Prozess.	an die Datentransformation und unterstützt keine logischen Datenbank zusammenführungen. • Zeitaufwändig für größere Datensätze. • Keine Unterstützung für die Delta-Migration kann zu längeren Ausfallzeiten führen.

	dieser Tabelle unter Logische Datenbank zusammenführung erklärt wird.

Redis-Replikationsfunktion (aktiv/passiv)	Sie können kontinuierlich Daten aus einer Redis OSS-, Enterprise Software- oder Enterprise Cloud-Datenbank in eine Redis Enterprise Cloud-Datenbank replizieren. Nach der ersten Synchronisation führt die Redis-Replikationsfunktion (`ReplicaOf `) eine Delta-Migration durch, was bedeutet, dass praktisch keine Anwendungsausfälle beobachtet werden. Die Redis-Replikationsfunktion ist für die aktiv-passive Verwendung vorgesehen. Es wird davon ausgegangen, dass das Ziel passiv ist, und es wird vollständig neu synchronisiert (geleert und aus der Quelldatenbank synchronisiert). Daher ist das Umschalten zwischen der Quelle und dem Ziel etwas komplizierter.	• Unterstützt die kontinuierliche Replikation (anfängliches Laden von Daten, gefolgt von Deltas). • Fast keine Ausfallzeiten (abhängig von der Verzögerung bei der Replikation). • Erreicht Datenkonsistenz.	• Es ist vorgesehen, dass nur eine Site aktiv ist, sodass das Umschalten zwischen Sites komplizierter ist. • Unterstützt maximal 32 Master-Shards, wenn Sie von einem OSS-Cluster migrieren.

	Es ist möglich, von einem Redis OSS-Cluster auf eine standardmäßige geclusterte Redis Enterprise Cloud-Datenbank zu replizieren, indem alle Master-Shards des OSS-Clusters als Quellen angegeben werden. Die Redis-Replikationsfunktion ermöglicht jedoch maximal 32 Quelldatenbanken.		
AWS DMS	Sie können AWS DMS verwenden, um Daten von jeder unterstützten Quelldatenbank zu einem Redis-Zieldatenspeicher mit minimaler Ausfallzeit zu migrieren. Weitere Informationen finden Sie unter Verwenden von Redis als Ziel für AWS DMS in der AWS DMS-Dokumentation.	• Unterstützt die Migration von NoSQL- und SQL-Datenquellen. • Funktioniert gut mit anderen AWS-Services. • Unterstützt Anwendungsfälle für Live-Migration und Change Data Capture (CDC).	• Redis-Schlüsselwerte dürfen keine Sonderzeichen wie % enthalten. • Unterstützt nicht die Migration von Daten, die Sonderzeichen in Zeilen oder Feldnamen enthalten. • Unterstützt den vollständigen LOB-Modus (Large Binary Object) nicht.

Logische Datenbank zusammenführung	Für spezielle Anforderungen an die Datenbank zusammenführung ist möglicherweise eine benutzerd efinierte Datenmigr ationslösung erforderl ich. Sie könnten beispielsweise vier logische Datenbank en (`SELECT 0..3`) in Redis OSS haben, aber Sie möchten vielleicht einen einzigen Datenbank endpunkt verwenden , anstatt die Daten in mehrere Redis Enterprise Cloud-Datenbanken zu verschieben. Redis Enterprise unterstützt keine auswählbaren logischen Datenbank en, sodass Sie das physische Datenmode ll der Quelldate nbank transformieren müssten. Sie könnten beispielsweise jeden Datenbankindex einem Präfix zuordnen (`0`to `usrcmp`, 1 to usw.) und dann ein Migrationsskript oder	• Präzise Kontrolle über die Gestaltung der Daten während der Migration zum Zielsystem mithilfe benutzerdefinierter Skripts.	• Wenn Sie sich entscheiden, die Migration nicht abzuschli eßen, kann ein Rollback eine große Herausforderung sein, insbesondere wenn neuere Daten auf die Quellsyst eme zurückgesetzt werden müssen. • Die Erstellun gskosten können hoch sein, wenn das Ziel darin besteht, eine Einmallösung für eine einmalige Migration zu entwickeln. • Die Wartungsk osten für Code, Infrastruktur, Entwicklungszeit und andere Bereiche können hoch sein, wenn sich die Migration sanforderungen häufig ändern.

	ein ETL-Tool (Extrahie ren, Transform ieren und Laden) verwenden, um eine RDB-Datei auszugebe n, die Sie dann in die Zieldatenbank importieren können.

Darüber hinaus können Sie die folgenden Tools und Services von AWS verwenden.

Tools zur Bewertung und Entdeckung:

- AWS Application Discovery Service
- Evaluator für Migration

Tools für die Anwendungs- und Servermigration:

- AWS Application Migration Service

Tools für die Datenbankmigration:

- AWS-Schemakonvertierungstool (AWS SCT)
- AWS Database Migration Service (AWS DMS)

Tools zur Datenmigration:

- AWS Storage Gateway
- AWS DataSync
- AWS Direct Connect
- AWS Snowball
- Amazon Data Firehose

Verwaltung der Migration:

- AWS Migration Hub

AWS-Partnerlösungen:

- AWS-Kompetenzpartner für Migration

Epen

Erledigen Sie Ermittlungs- und Bewertungsaufgaben

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Workloads.	Identifizieren Sie die geeignete n Kandidaten-Workloads, die Sie migrieren möchten. Beachten Sie Folgendes, bevor Sie einen Workload für die Migration auswählen: • Welchen geschäftlichen Nutzen hat es, diesen Workload zu migrieren oder nicht zu migrieren? • Gibt es einen Notfallplan für den Fall, dass dieser Workload nicht erfolgreich auf das Zielsystem migriert wird? Wählen Sie idealerweise einen Workload, der maximale Auswirkungen auf das Geschäft mit minimalen Risiken hat. Halten Sie den Gesamtprozess iterativ und	Datenarchitekt, Vorreiter in der Wirtschaft, Sponsoren von Migrationsprojekten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	migrieren Sie in kleinen Schritten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Datenquellen und Anforderungen; entwerfen Sie ein Datenmodell.	Redis veranstaltet einen Workshop, um die Entdeckung zu beschleunigen und die Migrationsplanung für das Projekt zu definieren. Im Rahmen dieses Workshops identifizieren die Redis-Teams die Datenquellen und die Anforderungen an das Quelldatenmodell und analysieren, wie diese in Redis Enterprise Cloud umgestaltet werden können. Das Redis-Migrationsteam (Professional Services) führt mit Ihrer Organisation eine detaillierte Übung zum Entwurf eines Datenmodells durch. Im Rahmen dieser Übung führt das Redis-Team folgende Schritte durch: • Identifiziert die Redis-Zieldatenstrukturen. • Definiert die Strategie zur Datenzuweisung. • Dokumentiert den Migrationsansatz und die Empfehlungen. • Überprüft und finalisiert das Datenmodell zusammen mit den Stakeholdern.	Der Lösungsarchitekt von Redis

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Eigenschaften der Quelldatenbank.	Identifizieren Sie das Redis-Produkt, das in der Quell- und Zielumgebung verwendet wird. Zum Beispiel: • Ist die Quelldatenbank eine OSS-Cluster-Datenbank, eine eigenständige Redis-Datenbank oder eine Redis Enterprise-Datenbank? • Wird die Zieldatenbank eine Redis Enterprise-Standarddatenbank oder eine OSS-Cluster-kompatible Datenbank sein? • Was sind die Auswirkungen auf den Quellcode der Anwendung?	Datenarchitekt
Erfassen Sie die aktuelle System-SLA und andere Größenkennzahlen.	Ermitteln Sie die aktuellen Service Level Agreements (SLAs), ausgedrückt als Durchsatz (Operationen pro Sekunde), Latenz, Gesamtspeichergröße pro Datenbank und Anforderungen an die Hochverfügbarkeit (HA).	Datenarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Eigenschaften des Zielsystems.	Ermitteln Sie die Antworten auf diese Fragen: • Wie viele Daten müssen migriert werden? • Wie lange dauert es, die angegebene Datenmenge zu migrieren? • Was sind die Ausfallzeitanforderungen für die Migration? Ist es akzeptabel, dass Ihr Service oder Ihre Anwendung für einen bestimmten Zeitraum nicht verfügbar ist? Falls ja, für wie lange? • Wie konsistent sollten die migrierten Daten sein? Kann sich die Zieldatenbank in einem leicht inkonsistenten (veralteten) Zustand befinden? • Müssen Daten transformiert werden, bevor sie in die Zieldatenbank geladen werden? (Beispielsweise möchten Sie möglicherweise auswählbare DB-Indizes vor der Migration in Präfixe konvertieren.) • Ist die Quelldatenbank vom Host der Zieldatenbank aus erreichbar (z. B. von einer Peer-VPC oder von	Datenarchitekt, Redis-Lösungsarchitekt (optional)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	einem öffentlichen Endpunkt aus, der Verschlüsselung verwendet)? • Führen Sie mit einem technischen Redis-Arc hitekten eine Übung zur Datendimensionierung und zur Redis-Clusterdimen sionierung durch. • Identifizieren Sie die Netzwerkanforderun gen, Infrastrukturanfor derungen, Softwarev ersionen und Softwarel izenzen und beschaffen Sie alle Komponenten vor der Migration. • Gibt es Sicherheitsbedenke n im Zusammenhang mit der Übertragung dieser Daten?	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Abhängigkeiten.	Identifizieren Sie die Upstream- und Downstream-Abhängigkeiten des aktuellen Systems, das migriert werden soll. Stellen Sie sicher, dass die Migrationsarbeiten mit anderen abhängigen Systemmigrationen übereinstimmen. Wenn Sie beispielsweise planen, andere Geschäftsanwendungen von lokalen Standorten in die AWS-Cloud zu migrieren, identifizieren Sie diese Anwendungen und richten Sie sie auf der Grundlage von Projektzielen, Zeitplänen und Stakeholdern aus.	Datenarchitekt, Unternehmensarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Migration stools.	Abhängig von Ihren Anforderungen an die Datenmigration (z. B. Quelldaten oder Ausfallzeiten) können Sie jedes der zuvor im Abschnitt Tools beschriebenen Tools verwenden. Darüber hinaus können Sie Folgendes verwenden: • Bidirektionale (aktiv-aktive) Replikation mithilfe der CRDB-Bereitstellung. • Benutzerdefinierte Export-/Import-Skripts (z. B. mithilfe von Befehlen). `DUMP/RESTORE` • Zusätzliche Export-/Import-Tools und Hilfstools wie RIOT - oder ETL-Tools. ECstats2 • IaC-Tools wie Terraform - oder AWS-Vorlagen. CloudFormation	Architekt für Migrationslösungen, Architekt für Redis-Lösungen
Erstellen Sie einen Notfallplan.	Erstellen Sie einen Notfallplan für den Fall, dass Sie während der Migration auf Probleme stoßen, ein Rollback durchführen können.	Projektmanagement, technische Teams, einschließlich Architekt

Erledigen Sie Sicherheits- und Compliance-Aufgaben

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sichern Sie die Redis-Verwaltungskonsole.	Folgen Sie den Anweisungen in der Redis-Dokumentation, um die Verwaltungskonsole zu sichern.	Administrator der IT-Infrastruktur
Sichern Sie die Redis-Datenbank.	Auf den folgenden Seiten in der Redis-Dokumentation finden Sie Informationen zu: • Definieren Sie die rollenbasierte Zugriffskontrolle. • Definieren Sie Netzwerksicherheit. • Aktivieren Sie TLS.	
Sichere Redis Cloud APIs.	Wenn Sie die API aktivieren, können Sie die API-Schlüssel für alle Besitzer Ihres Redis Cloud-Kontos verwalten. Einen Überblick über die Sicherheitsfunktionen der API finden Sie in der API-Authentifizierungsdokumentation auf der Redis-Website.	Administrator der IT-Infrastruktur

Richten Sie die neue Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine neue Umgebung auf AWS ein.	Diese Aufgabe beinhaltet:	DevOps IT oder Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	• Aktivitäten zur Einrichtung der AWS-Landing Zone. Die landing zone unterstützt:
	  • Bereitstellungen mit mehreren Konten
	  • Mindestsicherheits standard
	  • Automatisierte Methode zur Bereitstellung neuer Konten mit einer Sicherheitsbasis und ISV-Voraussetzunge n (Netzwerk, Sicherhei tskonfiguration usw.)
	  • Benachrichtigungen, zentrale Protokollierung und Überwachung
	• Aktivitäten zur ISV-Softwarekonfiguration. Dazu gehören Konfigura tionen, die in die Migration einbezogen werden müssen, z. B. Produkt- und Workload-Einstellungen und Änderungen.
	• IaC-Aktivitäten wie die Konfiguration oder Anpassung von AWS-CloudFormation oder Terraform-Vorlagen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Migration sarchitektur bereit.	1. Richten Sie Redis Enterpris e Cloud auf AWS ein. 2. Installieren Sie Migration stools wie RIOT oder AWS DMS. Im Abschnitt Tools finden Sie eine Liste der verfügbaren Tools. 3. Stellen Sie die Konnektivität zwischen der Anwendungs-, Migrations- und Datenbank ebene her. 4. Erstellen Sie einen Beispiel-Workload, der jede Ebene durchläuft, und migrieren Sie einen kleinen Satz von Beispieldaten. Sie sind jetzt bereit, die eigentlichen Datenmigr ationspipelines auszuführen und zu testen.	IT oder Ingenieur DevOps

Richten Sie das Netzwerk ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konnektivität herstellen.	Stellen Sie Konnektivität zwischen der lokalen Infrastru ktur und den AWS-Cloud-Ressourcen her. Verwenden Sie Sicherheitsgruppen, AWS Direct Connect und andere Ressourcen, um diese	IT oder DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Funktionalität zu erreichen. Weitere Informationen finden Sie unter Connect Your Data Center to AWS auf der AWS-Website.	
Richten Sie VPC-Peering ein.	Richten Sie VPC-Peering zwischen den VPCs Geschäfts anwendungen (oder den EC2 Instances, die Migrationstools ausführen, oder dem AWS DMS-Replikationsserver) und der VPC ein, auf der Redis Enterprise Cloud ausgeführ t wird. Anweisungen finden Sie unter Erste Schritte mit Amazon VPC in der Amazon VPC-Dokumentation und unter Aktivieren von VPC-Peering in der Redis-Dokumentation.	IT oder Ingenieur DevOps

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie ein Datenmigr ationstool.	In der Tabelle im Abschnitt Tools finden Sie Beschreib ungen, Vor- und Nachteile dieser Tools: • RDS-Export und -Import • Redis-Replikationsfunktion () `ReplicaOf` • AWS DMS	Architekt für Migration slösungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Logische Datenbank zusammenführung In den folgenden Zeilen werden die Datenmigr ationsaufgaben beschrieben, die mit den einzelnen Tools verknüpft sind.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 1: Verwenden Sie RDB-Export und -Import.	1. Trennen Sie die Verbindung zur Quelle: Stoppen Sie den Datenverkehr in der Quelldatenbank (z. B. indem Sie die Verbindung zu Geschäftsanwendungen trennen). 2. Export: Exportieren Sie die Daten der Quelldatenbank als RDB-Datei. 3. Phase: Laden Sie die Daten an einen Ort hoch, auf den die Redis Enterprise Cloud-Instanzen auf AWS zugreifen können (Sie können sie beispielsweise auf einen S3-Bucket oder einen FTP-Server hochladen). 4. Import: Importieren Sie die RDB-Dateien (indem Sie sie alle in einem Importschritt auflisten) in Ihre Redis Enterprise Cloud-Zieldatenbank. 5. Cut over: Wechseln Sie zur Zieldatenbank (indem Sie beispielsweise Ihre Anwendung mit ihr verbinden).	Architekt für Migrationslösungen, Redis-Lösungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie in der Redis-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 2: Verwenden Sie die Redis-Replikationsfunktion (aktiv/passiv).	1. Datenbank Connect: Stellen Sie eine `ReplicaOf` Verbindung zwischen der Quell- und der Zieldaten bank her. 2. Führen Sie eine erste Synchronisierung durch: Warten Sie, bis die erste Synchronisation zwischen der Quell- und der Zieldaten bank abgeschlossen ist. 3. Trennen Sie die Verbindung zur Quelle: Stoppen Sie den Verkehr in der Quelldate nbank (z. B. indem Sie die Verbindung zur Anwendung trennen). 4. Deltareplikation ausführen: Warten Sie, bis das Delta in der Zieldatenbank repliziert ist. 5. Cut over: Wechseln Sie zur Zieldatenbank (indem Sie beispielsweise Ihre Anwendung mit ihr verbinden). 6. Löschen: Entfernen Sie die `ReplicaOf` Verknüpfung zwischen der Quell- und der Zieldatenbank.	Architekt für Migration slösungen, Redis-Lös ungsarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie in der Redis-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 3: Verwenden Sie AWS DMS.	1. Richten Sie eine AWS DMS-Replikationsinstanz ein: Diese Instanz führt alle Migrationsprozesse durch. Anweisungen finden Sie unter Arbeiten mit einer AWS DMS-Replikationsinstanz in der AWS DMS-Dokumentation. 2. Definieren Sie die Quelldatenbank: Definieren Sie den Quellendpunkt. Testen Sie die Konnektivität zwischen dem Quellendpunkt und dem AWS DMS-Replikationsserver. Anweisungen finden Sie unter Quell- und Zielendpunkte in der AWS DMS-Dokumentation erstellen. 3. Richten Sie die Zieldatenbank ein: Richten Sie Redis Enterprise Cloud auf AWS ein und richten Sie die Datenbank ein, zu der migriert werden soll. 4. Definieren Sie die Zieldatenbank: Definieren Sie den Zielendpunkt. Stellen Sie sicher, dass VPC-Peering zwischen der VPC, auf der AWS DMS ausgeführt wird, und der VPC, die Redis Enterprise Cloud auf AWS	Architekt für Migrationslösungen, Architekt für Redis-Lösungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	hostet, eingerichtet ist. Testen Sie die Konnektivität zwischen dem AWS DMS-Replikationsserver und der Zieldatenbank. 5. Erstellen Sie eine AWS DMS-Aufgabe: Erstellen Sie eine Aufgabe oder eine Reihe von Aufgaben, um die Tabellen und Replikationsprozesse zu definieren, die Sie für die Migration der Daten verwenden möchten. Anweisungen finden Sie unter Arbeiten mit AWS DMS-Aufgaben in der AWS DMS-Dokumentation. 6. Migrieren: Migrieren Sie die Daten, indem Sie die AWS DMS-Aufgabe ausführen. 7. Cut over: Wechseln Sie zur Zieldatenbank (indem Sie beispielsweise Ihre Anwendung damit verbinden).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 4: Verwenden Sie die logische Datenbank zusammenführung.	Diese Option beinhaltet die Verwendung eines Migration sskripts oder eines ETL-Tools, das das physische Datenmodell der Quelldate nbank transformieren kann, und das Generieren einer RDB-Datei. Redis Professional Services kann bei Bedarf bei diesem Schritt helfen.	Architekt für Migration slösungen, Architekt für Redis-Lösungen

Migrieren Sie Ihre Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Zeitpläne und Ziele des Projektma nagements ab.	Stimmen Sie die Ziele, Meilensteine und Zeitpläne des Migrationsprojekts auf der Anwendungsebene mit denen des Redis-Datenmigrati onsprojekts ab.	Projektmanagement
Passen Sie die Testaktivitäten an.	Nachdem die Anwendung sschicht in der AWS-Cloud migriert und modernisiert wurde, verweisen Sie die Anwendungsschicht zum Testen auf die neu migrierte Redis Enterprise Cloud auf AWS.	Testen

Test

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Implementieren Sie Testpläne.	Führen Sie die Datenmigr ationsroutinen und die Skripts, die während der Implement ierungsphase entwickelt wurden, in einer Testumgeb ung gemäß den Testanfor derungen an Ihrem Standort aus.	Testen
Testen Sie die Datenqualität.	Testen Sie die Datenqual ität, nachdem Sie die Daten migriert haben.	Testen
Testen Sie die Funktionalität.	Testen Sie Datenabfragen und die Anwendungsebene, um sicherzustellen, dass die Anwendung auf derselben Ebene wie im Quellsystem ausgeführt wird.	Testen

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Treffen Sie die Entscheidung über die Umstellung.	Nachdem alle Tests auf Anwendungs- und Datenbank ebene abgeschlossen sind, treffen das Führungsteam und die Stakeholder auf der Grundlage der von den Testteams bestätigten Endergebnisse die endgültige Entscheidung, ob auf die neue	Projektmanagement, Vorreiter in der Wirtschaft

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Umgebung auf AWS umgestellt werden soll.	
Wechseln Sie zur AWS-Cloud.	Wenn Sie bestätigt haben, dass alles vorhanden ist, verweisen Sie die Anwendungsschicht auf die neu migrierten Daten und verweisen Sie die Clients auf die neue Anwendungsebene, die auf dem neuen Redis Enterprise Cloud-System auf AWS basiert.	IT oder DevOps Ingenieur, Datenarchitekt, Architekt für Migrationslösungen, Redis-Lösungsarchitekt

Zugehörige Ressourcen

Redis-Ressourcen

- Dokumentation zu Redis Enterprise Cloud
- RIOT-Tool (Repository) GitHub
- Terraform Provider (herunterladen)

AWS-Ressourcen

- Demo-Migrationen
- AWS-Partnerlösungen
- Dokumentation
- Blog-Posts
- Weiße Papiere
- Tutorials und Videos
- AWS-Cloud-Migration
- AWS Prescriptive Guidance

Zusätzliche Informationen

Standardsicherheitsanforderungen für die Migration von Redis-Workloads in die AWS-Cloud finden Sie in den Best Practices for Security, Identity, and Compliance auf der AWS-Website und im Redis Trust Center auf der Redis-Website.

Migrieren Sie SAP ASE auf Amazon EC2 zu Amazon Aurora PostgreSQL-kompatibel mit AWS SCT und AWS DMS

Erstellt von Amit Kumar (AWS) und Ankit Gupta (AWS)

Übersicht

Dieses Muster beschreibt, wie eine SAP Adaptive Server Enterprise (SAP ASE) -Datenbank, die auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance gehostet wird, mithilfe des AWS Schema Conversion Tool (AWS SCT) und des AWS Database Migration Service (AWS DMS) zur Amazon Aurora PostgreSQL-kompatiblen Edition migriert wird. Das Muster konzentriert sich sowohl auf DDL-Konvertierungen (Data Definition Language) für gespeicherte Objekte als auch auf Datenmigration.

Aurora PostgreSQL-kompatibel unterstützt OLTP-Workloads (Online Transaction Processing). Dieser verwaltete Service bietet Konfigurationen, die bei Bedarf automatisch skaliert werden. Er kann Ihre Datenbank je nach den Anforderungen Ihrer Anwendung automatisch starten, herunterfahren, hoch- oder herunterskalieren. Sie können Ihre Datenbank in der Cloud ausführen, ohne Datenbankinstanzen zu verwalten. Aurora PostgreSQL-kompatibel bietet eine kostengünstige Option für seltene, intermittierende oder unvorhersehbare Workloads.

Der Migrationsprozess besteht aus zwei Hauptphasen:

- Konvertieren des Datenbankschemas mithilfe von AWS SCT
- Migrieren der Daten mithilfe von AWS DMS

Detaillierte Anweisungen für beide Phasen finden Sie im Abschnitt Epics. Informationen zur Behebung von Problemen, die spezifisch für die Verwendung von AWS DMS mit SAP ASE-Datenbanken sind, finden Sie unter Problembehandlung mit SAP ASE in der AWS DMS-Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine SAP ASE-Quelldatenbank auf einer EC2 Instance, in der Server-, Datenbank- und Listener-Services aktiv sind
- Eine Aurora PostgreSQL-kompatible Zieldatenbank

Einschränkungen

- Die Portnummer für Verbindungen muss 5432 sein.
- Die Funktion huge_pages ist standardmäßig aktiviert, kann aber geändert werden.
- Point-in-time Die Granularität der Wiederherstellung (PITR) beträgt 5 Minuten.
- Eine regionsübergreifende Replikation ist derzeit nicht verfügbar.
- Die maximale Speichergröße für eine Aurora-Datenbank beträgt 128 TiB.
- Sie können bis zu 15 Read Replicas erstellen.
- Die Tabellengrößenbeschränkung wird nur durch die Größe des Aurora-Cluster-Volumes eingeschränkt, sodass die maximale Tabellengröße für einen Aurora PostgreSQL-kompatiblen DB-Cluster 32 TiB beträgt. Wir empfehlen, dass Sie sich an bewährte Methoden für das Tabellendesign halten, z. B. das Partitionieren großer Tabellen.

Produktversionen

- Quelldatenbank: AWS DMS unterstützt derzeit SAP ASE 15, 15.5, 15.7 und 16.x. Aktuelle Informationen zur Unterstützung der SAP ASE-Version finden Sie im AWS DMS-Benutzerhandbuch.
- Zieldatenbank: PostgreSQL 9.4 und höher (für Version 9.x), 10.x, 11.x, 12.x, 13.x und 14.x. Die neuesten unterstützten PostgreSQL-Versionen finden Sie im AWS DMS-Benutzerhandbuch.
- Amazon Aurora 1.x oder höher. Die neuesten Informationen finden Sie in der Aurora-Dokumentation unter Aurora PostgreSQL-kompatible Releases und Engine-Versionen.

Architektur

Quelltechnologie-Stack

- SAP ASE-Datenbank läuft auf Amazon EC2

Zieltechnologie-Stack

- Aurora PostgreSQL-kompatible Datenbank

Migrationsarchitektur

Tools

- Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt.
- Das AWS Schema Conversion Tool (AWS SCT) unterstützt heterogene Datenbankmigrationen, indem das Quelldatenbankschema und der Großteil des benutzerdefinierten Codes automatisch in ein Format konvertiert werden, das mit der Zieldatenbank kompatibel ist.
- AWS DMS unterstützt mehrere verschiedene Quell- und Zieldatenbanken. Weitere Informationen finden Sie unter Quellen für Datenmigration und Ziele für die Datenmigration in der AWS DMS-Dokumentation. Für die umfassendste Versions- und Funktionsunterstützung empfehlen wir Ihnen, die neueste Version von AWS DMS zu verwenden.

Epen

Richte die Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Netzwerkzugriff in der EC2 Quellinstanz.	Richten Sie Sicherheitsgruppen in der EC2 Instanz ein, die Ihre SAP ASE-Quelldatenbank hostet. Anweisungen finden Sie in der EC2 Amazon-Dokumentation unter EC2 Amazon-Sicherheitsgruppen für Linux-Instances.	Systemadministrator
Erstellen Sie Ihren Aurora PostgreSQL-kompatiblen Ziel-DB-Cluster.	Installieren, konfigurieren und starten Sie einen Aurora PostgreSQL-kompatiblen Cluster für Ihre Zieldatenbank. Weitere Informationen finden Sie unter Erstellen eines Amazon Aurora Aurora-DB	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	-Clusters in der Aurora-Do kumentation.	
Richten Sie die Autorisierung für den Ziel-DB-Cluster ein.	Richten Sie Sicherhei tsgruppen und Firewalls für die Zieldatenbank ein. Anweisungen finden Sie in der Aurora-Dokumentation unter Erstellen eines Amazon Aurora Aurora-DB-Clusters.	DBA, Systemadministrator

Konvertieren Sie Ihr Datenbankschema mit AWS SCT

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie AWS SCT.	Starten Sie AWS SCT, indem Sie den Anweisungen in der AWS SCT-Dokumentation folgen. AWS SCT bietet eine projektbasierte Benutzero berfläche zur automatischen Konvertierung des Datenbank schemas Ihrer SAP ASE-Quell datenbank in ein Format, das mit Ihrer Aurora PostgreSQL-kompatiblen Ziel-DB-Instance kompatibel ist.	DBA
Erstellen Sie AWS SCT-Endpo ints.	Erstellen Sie Endpunkte für die Quell-SAP-ASE- und Ziel-PostgreSQL-Datenbanken.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anweisungen finden Sie in der AWS SCT-Dokumentation.	
Erstellen Sie einen Bewertungsbericht.	Erstellen Sie einen Bewertungsbericht zur Datenbankmigration, um die Migration zu bewerten und alle inkompatiblen Objekte und Funktionen zu erkennen. Anweisungen finden Sie in der AWS SCT-Dokumentation.	DBA
Konvertiert das Schema.	Konvertieren Sie das Datenbankschema, indem Sie den Anweisungen in der AWS SCT-Dokumentation folgen.	DBA
Datenbankobjekte validieren.	Wenn AWS SCT ein Datenbankobjekt nicht konvertieren kann, identifiziert es seinen Namen und andere Details. Sie müssen diese Objekte manuell konvertieren. Um diese Diskrepanzen zu identifizieren, folgen Sie den Anweisungen im AWS-Blogbeitrag Datenbankobjekte nach der Migration von SAP ASE zu Amazon RDS for PostgreSQL oder Amazon Aurora PostgreSQL validieren.	DBA

Analysieren Sie die AWS DMS-Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversionen.	Überprüfen Sie die SAP ASE-Datenbankversionen auf Kompatibilität mit AWS DMS. Weitere Informationen finden Sie unter Quellen für AWS DMS und Ziele für AWS DMS in der AWS DMS-Dokum entation.	DBA
Identifizieren Sie die Anforderu ngen für den Speichertyp und die Kapazität.	Wählen Sie die geeignete Speicherkapazität für die Zieldatenbank auf der Grundlage der Größe Ihrer Quelldatenbank aus.	DBA, Systemadministrator
Wählen Sie den Instanzty p, die Kapazität und andere Funktionen der Replikati onsinstanz aus.	Wählen Sie den Instanztyp, die Kapazität, die Speicherf unktionen und die Netzwerkf unktionen, die Ihren Anforderu ngen entsprechen. Weitere Informationen finden Sie in der AWS DMS-Dokum entation unter Auswahl der richtigen AWS DMS-Replikationsinstanz für Ihre Migration.	DBA, Systemadministrator
Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerkzugriff.	Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.	DBA, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Folgen Sie den Anweisungen unter Einrichten eines Netzwerks für eine Replikationsinstanz in der AWS DMS-Dokumentation.	

Migrieren Sie die Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie die Daten, indem Sie eine Migrationsaufgabe in AWS DMS erstellen.	Um Daten zu migrieren, erstellen Sie eine Aufgabe und folgen Sie den Anweisungen in der AWS DMS-Dokumentation. Wir empfehlen Ihnen, die neueste Version von AWS DMS zu verwenden, um die umfassendste Version von Versionen und Funktionen zu erhalten.	DBA
Validieren Sie die Daten.	Um zu überprüfen, ob Ihre Daten korrekt von der Quelldatenbank zur Zieldatenbank migriert wurden, befolgen Sie die Datenvalidierungsrichtlinien in der AWS DMS-Dokumentation.	DBA

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Strategie zur Anwendungsmigration.	Wählen Sie eine der sieben Strategien (7Rs) für die Migration von Anwendungen in die Cloud.	DBA, App-Besitzer, Systemadministrator
Folgen Sie der Strategie zur Anwendungsmigration.	Führen Sie die vom Anwendungsteam identifizierten Datenbankaufgaben aus, einschließlich der Aktualisierung der DNS-Verbindungsdetails für die Zieldatenbank und der Aktualisierung dynamischer Abfragen.	DBA, App-Besitzer, Systemadministrator

Wechseln Sie zur Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendungsclients auf die neue Infrastruktur um.	Wechseln Sie die Verbindung von der Quelldatenbank zur Zieldatenbank. Weitere Informationen finden Sie im Abschnitt Cutover der Migrationsstrategie für relationale Datenbanken.	DBA, App-Besitzer, Systemadministrator

Schließen Sie das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die temporären AWS-Ressourcen herunter.	Beenden Sie alle Migration saufgaben, Replikationsinstan zen, Endpunkte und andere AWS SCT- und AWS DMS-Ressourcen. Weitere Informationen finden Sie in der AWS DMS-Dokum entation.	DBA, Systemadministrator
Überprüfen und validieren Sie die Projektdokumente.	Überprüfen Sie alle Schritte in der Projektdokumentati on, um sicherzustellen, dass alle Aufgaben erfolgreich abgeschlossen wurden.	DBA, App-Besitzer, Systemadministrator
Schließt das Projekt.	Schließen Sie das Migration sprojekt und geben Sie Feedback.	DBA, App-Besitzer, Systemadministrator

Zugehörige Ressourcen

Referenzen

- Verschlüsselte Verbindungen für PostgreSQL-DB-Instances in Amazon RDS aktivieren (AWS Prescriptive Guidance)
- Transport von PostgreSQL-Datenbanken zwischen zwei Amazon RDS-DB-Instances mithilfe von pg_transport (AWS Prescriptive Guidance)
- Amazon-Aurora-Preise
- Bewährte Methoden mit Amazon Aurora PostgreSQL-Compatible Edition (Amazon Aurora Aurora-Dokumentation)
- AWS SCT-Dokumentation
- AWS DMS-Dokumentation

- Verwenden einer SAP ASE-Datenbank als Quelle für AWS DMS

Tutorials und Videos

- Erste Schritte mit dem AWS Database Migration Service
- AWS Database Migration Service (Video)

Migrieren Sie Windows-SSL-Zertifikate mithilfe von ACM zu einem Application Load Balancer

Erstellt von Chandra Sekhar Yaratha (AWS) und Igor Kovalchuk (AWS)

Übersicht

Das Muster enthält Anleitungen zur Verwendung von AWS Certificate Manager (ACM) zur Migration vorhandener Secure Sockets Layer (SSL) -Zertifikate von Websites, die auf lokalen Servern oder Amazon Elastic Compute Cloud (Amazon EC2) -Instances auf Microsoft Internet Information Services (IIS) gehostet werden. Die SSL-Zertifikate können dann mit Elastic Load Balancing auf AWS verwendet werden.

SSL schützt Ihre Daten, bestätigt Ihre Identität, sorgt für bessere Platzierungen in Suchmaschinen, trägt zur Erfüllung der Anforderungen des Payment Card Industry Data Security Standard (PCI DSS) bei und stärkt das Kundenvertrauen. Entwickler und IT-Teams, die diese Workloads verwalten, möchten, dass ihre Webanwendungen und ihre Infrastruktur, einschließlich des IIS-Servers und des Windows-Servers, ihren grundlegenden Richtlinien entsprechen.

Dieses Muster umfasst den manuellen Export vorhandener SSL-Zertifikate aus Microsoft IIS, deren Konvertierung vom PFX-Format (Personal Information Exchange) in das von ACM unterstützte PEM-Format (Private Enhanced Mail) und das anschließende Importieren in ACM in Ihrem AWS-Konto. Außerdem wird beschrieben, wie Sie einen Application Load Balancer für Ihre Anwendung erstellen und den Application Load Balancer so konfigurieren, dass er Ihre importierten Zertifikate verwendet. HTTPS-Verbindungen werden dann auf dem Application Load Balancer beendet, und Sie benötigen keinen weiteren Konfigurationsaufwand auf dem Webserver. Weitere Informationen finden Sie unter Einen HTTPS-Listener für Ihren Application Load Balancer erstellen.

Windows-Server verwenden PFX- oder .P12-Dateien, um die öffentliche Schlüsseldatei (SSL-Zertifikat) und ihre eindeutige private Schlüsseldatei zu speichern. Die Zertifizierungsstelle (CA) stellt Ihnen Ihre öffentliche Schlüsseldatei zur Verfügung. Sie verwenden Ihren Server, um die zugehörige private Schlüsseldatei zu generieren, in der die Certificate Signing Request (CSR) erstellt wurde.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine virtuelle private Cloud (VPC) auf AWS mit mindestens einem privaten und einem öffentlichen Subnetz in jeder Availability Zone, die von Ihren Zielen verwendet wird

- IIS-Version 8.0 oder höher, läuft auf Windows Server 2012 oder höher
- Eine Webanwendung, die auf IIS ausgeführt wird
- Administratorzugriff auf den IIS-Server

Architektur

Quelltechnologie-Stack

- IIS-Webserver-Implementierung mit SSL, um sicherzustellen, dass Daten sicher in einer verschlüsselten Verbindung (HTTPS) übertragen werden

Quellarchitektur

Zieltechnologie-Stack

- ACM-Zertifikate in Ihrem AWS-Konto
- Ein Application Load Balancer, der für die Verwendung importierter Zertifikate konfiguriert ist
- Windows Server-Instanzen in den privaten Subnetzen

Zielarchitektur

Tools

- AWS Certificate Manager (ACM) unterstützt Sie bei der Erstellung, Speicherung und Erneuerung von öffentlichen und privaten SSL/TLS X.509-Zertifikaten und Schlüsseln, die Ihre AWS-Websites und -Anwendungen schützen.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Datenverkehr auf EC2 Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen.

Bewährte Methoden

- Erzwingen Sie Verkehrsumleitungen von HTTP zu HTTPS.

- Konfigurieren Sie Sicherheitsgruppen für Ihren Application Load Balancer ordnungsgemäß, um eingehenden Datenverkehr nur zu bestimmten Ports zuzulassen.
- Starten Sie Ihre EC2 Instances in verschiedenen Availability Zones, um eine hohe Verfügbarkeit sicherzustellen.
- Konfigurieren Sie die Domain Ihrer Anwendung so, dass sie auf den DNS-Namen des Application Load Balancers statt auf dessen IP-Adresse verweist.
- Stellen Sie sicher, dass für den Application Load Balancer Integritätsprüfungen auf Anwendungsebene konfiguriert sind.
- Konfigurieren Sie den Schwellenwert für Integritätsprüfungen.
- Verwenden Sie Amazon CloudWatch, um den Application Load Balancer zu überwachen.

Epen

Exportieren Sie eine PFX-Datei

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Exportieren Sie die PFX-Datei von Windows Server.	So exportieren Sie das SSL-Zertifikat als PFX-Datei aus dem lokalen IIS-Manager in Windows Server: 1. Wählen Sie Start, Verwaltung und Internetinformationsdienste-Manager (IIS). 2. Wählen Sie den Servernamen aus, und doppelklicken Sie unter Sicherheit auf Serverzertifikate. 3. Wählen Sie das Zertifikat aus, das Sie exportieren möchten, und klicken Sie dann auf Exportieren. 4. Wählen Sie im Feld Zertifikat exportieren einen	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Speicherort, einen Pfad und einen Namen für Ihre PFX-Datei aus. 5. Geben Sie ein Passwort für Ihre PFX-Datei ein und bestätigen Sie es. **Note** Sie benötigen dieses Passwort, wenn Sie die PFX-Datei installieren. 6. Wählen Sie OK aus. Ihre PFX-Datei sollte jetzt an dem von Ihnen angegeben en Speicherort und Pfad gespeichert werden.	

Konvertieren Sie das PFX-kodierte Zertifikat in das PEM-Format

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das OpenSSL-T oolkit herunter und installieren Sie es.	1. Laden Sie Win32/Win64 OpenSSL von der Shining Light Productions-Website herunter und installieren Sie es. 2. Fügen Sie den Speichero rt der OpenSSL-Binärdatei en zu Ihrer `PATH` Systemvar iablen hinzu, sodass	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Binärdateien für die Befehlszeilenverwendung verfügbar sind.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konvertieren Sie das PFX-kodierte Zertifikat in das PEM-Format.	Mit den folgenden Schritten wird die PFX-kodierte, signierte Zertifikatsdatei in drei Dateien im PEM-Format konvertiert: • `cert-file.pem` enthält das SSL/TLS-Zertifikat für die Ressource. • `privatekey.pem` enthält den privaten Schlüssel des Zertifikats ohne Passworts chutz. • `ca-chain.pem` enthält das Stammzertifikat der CA. Um das PFX-kodierte Zertifika t zu konvertieren: 1. Führen Sie Windows aus. PowerShell 2. Verwenden Sie den folgenden Befehl, um den privaten Schlüssel des Zertifikats aus der PFX-Datei zu extrahieren. Geben Sie das Passwort für das Zertifikat ein, wenn Sie dazu aufgefordert werden. `openssl pkcs12 -in <filename>.pfx -nocerts -out withpw-privatekey.pem`	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Der Befehl generiert eine PEM-kodierte private Schlüsseldatei mit dem Namen. `privateke y.pem` Geben Sie eine Passphrase ein, um die private Schlüsseldatei zu schützen, wenn Sie dazu aufgefordert werden.
	3. Führen Sie den folgenden Befehl aus, um die Passphrase zu entfernen. Wenn Sie dazu aufgeford ert werden, geben Sie die Passphrase ein, die Sie in Schritt 2 erstellt haben.
	`openssl rsa -in withpw-privatekey. pem -out privateke y.pem`
	Wenn der Befehl erfolgrei ch ist, wird die Meldung „RSA-Schlüssel schreiben“ angezeigt.
	4. Verwenden Sie den folgenden Befehl, um das Zertifikat von der PFX-Datei in eine PEM-Datei zu übertragen.
	`openssl pkcs12 -in <file_name>.pfx -`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`clcerts -nokeys -out cert-file.pem`
	
	Dadurch wird eine PEM-kodierte Zertifikatsdatei mit dem Namen erstellt. `cert-file.pem` Wenn der Befehl erfolgreich ist, wird die Meldung „MAC verified OK“ angezeigt.
	5. Erstellen Sie eine CA-Kettendatei aus der PFX-Datei. Der folgende Befehl erstellt eine CA-Kettendatei mit dem Name `ca-chain.pem` .
	
	`openssl pkcs12 -in <file_name>.pfx -cacerts -nokeys -chain -out ca-chain.pem`
	
	Wenn der Befehl erfolgreich ist, wird die Meldung „MAC verified OK“ angezeigt.	

Importieren Sie ein Zertifikat in ACM

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie den Import des Zertifikats vor.	Wählen Sie in der ACM-Konsole die Option Zertifikat importieren aus.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie die Zertifizierungsstelle an.	Fügen Sie in das Feld Zertifikatshauptteil das PEM-kodierte Zertifikat ein, das Sie importieren möchten. Weitere Informationen zu den Befehlen und Schritten, die in diesem und anderen Aufgaben in diesem Epos beschrieben werden, finden Sie in der ACM-Dokumentation unter Importieren eines Zertifikats.	Cloud-Administrator
Geben Sie den privaten Schlüssel des Zertifikats an.	Fügen Sie für Certificate private key den PEM-kodierten, unverschlüsselten privaten Schlüssel ein, der mit dem öffentlichen Schlüssel des Zertifikats übereinstimmt.	Cloud-Administrator
Geben Sie die Zertifikatskette an.	Fügen Sie für Certificate chain die PEM-kodierte Zertifikatskette ein, die in der Datei gespeichert ist. `CertificateChain.pem`	Cloud-Administrator
Importieren Sie das Zertifikat.	Wählen Sie Review and import. Vergewissern Sie sich, dass die Informationen zu Ihrem Zertifikat korrekt sind, und wählen Sie dann Import aus.	Cloud-Administrator

Erstellen eines Application Load Balancers

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und konfigurieren Sie den Load Balancer und die Listener.	Folgen Sie den Anweisungen in der Elastic Load Balancing Balancing-Dokumentation, um eine Zielgruppe zu konfiguri eren, Ziele zu registrieren und einen Application Load Balancer und Listener zu erstellen. Fügen Sie einen zweiten Listener (HTTPS) für Port 443 hinzu.	Cloud-Administrator

Fehlerbehebung

Problem	Lösung
Windows PowerShell erkennt den OpenSSL-B efehl nicht, auch wenn Sie ihn dem Systempfad hinzugefügt haben.	Stellen Sie `$env:path` sicher, dass es den Speicherort der OpenSSL-Binärdateien enthält. Ist dies nicht der Fall, führen Sie den folgenden Befehl in aus: PowerShell `$env:path = $env:path + ";C:\OpenSSL-Win64\bin"`

Zugehörige Ressourcen

Ein Zertifikat in ACM importieren

- ACM-Konsole
- Zertifikat und Schlüsselformat für den Import
- Ein Zertifikat importieren
- AWS Certificate Manager Manager-Benutzerhandbuch

Einen Application Load Balancer erstellen

- Erstellen Sie einen Application Load Balancer
- Application Load Balancer Balancer-Benutzerhandbuch

Migrieren Sie eine Messaging-Warteschlange von Microsoft Azure Service Bus zu Amazon SQS

Erstellt von Nisha Gambhir (AWS)

Übersicht

Dieses Muster beschreibt, wie Sie eine.NET Framework- oder .NET Core-Web- oder Konsolenanwendung von der Microsoft Azure Service Bus-Queue-Messaging-Plattform zu Amazon Simple Queue Service (Amazon SQS) migrieren.

Anwendungen verwenden Messaging-Dienste, um Daten an andere Anwendungen zu senden und Daten von anderen Anwendungen zu empfangen. Diese Dienste helfen beim Aufbau entkoppelter, hoch skalierbarer Microservices, verteilter Systeme und serverloser Anwendungen in der Cloud.

Azure Service Bus-Warteschlangen sind Teil einer umfassenderen Azure-Messaging-Infrastruktur, die das Einstellen von Warteschlangen und das Veröffentlichen und Abonnieren von Nachrichten unterstützt.

Amazon SQS ist ein vollständig verwalteter Message Queuing-Service, mit dem Sie Microservices, verteilte Systeme und serverlose Anwendungen entkoppeln und skalieren können. Amazon SQS beseitigt die Komplexität und den Aufwand, die mit der Verwaltung und dem Betrieb nachrichtenorientierter Middleware verbunden sind, und ermöglicht es Entwicklern, sich auf differenzierte Aufgaben zu konzentrieren. Mit Amazon SQS können Sie Nachrichten zwischen Softwarekomponenten in beliebiger Menge senden, speichern und empfangen, ohne dass Nachrichten verloren gehen oder andere Dienste verfügbar sein müssen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine.NET Framework- oder .NET Core-Web- oder Konsolenanwendung, die Azure Service Bus-Warteschlangen verwendet (Beispielcode im Anhang)

Produktversionen

- .NET Framework 3.5 oder höher oder.NET Core 1.0.1, 2.0.0 oder höher

Architektur

Quelltechnologie-Stack

- Eine.NET-Web- oder Konsolenanwendung (Core oder Framework), die eine Azure Service Bus-Warteschlange zum Senden von Nachrichten verwendet

Zieltechnologie-Stack

- Amazon SQS

Tools

Tools

- Microsoft Visual Studio

Code

So erstellen Sie eine AWS Identity and Access Management (IAM) -Richtlinie für Amazon SQS:

1. Melden Sie sich in der AWS-Managementkonsole an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.

2. Wählen Sie im Navigationsbereich auf der linken Seite Policies (Richtlinien) und dann Create Policy (Richtlinie erstellen) aus.

3. Wählen Sie die Registerkarte JSON und fügen Sie den folgenden Code ein:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "sqs:DeleteMessage",
            "sqs:GetQueueUrl",
            "sqs:ChangeMessageVisibility",
            "sqs:SendMessageBatch",
            "sqs:ReceiveMessage",
```

```
            "sqs:SendMessage",
            "sqs:GetQueueAttributes",
            "sqs:ListQueueTags",
            "sqs:ListDeadLetterSourceQueues",
            "sqs:DeleteMessageBatch",
            "sqs:PurgeQueue",
            "sqs:DeleteQueue",
            "sqs:CreateQueue",
            "sqs:ChangeMessageVisibilityBatch",
            "sqs:SetQueueAttributes"
         ],
         "Resource": "arn:aws:sqs:*:<AccountId>:*"
      },
      {
         "Sid": "VisualEditor1",
         "Effect": "Allow",
         "Action": "sqs:ListQueues",
         "Resource": "*"
      }
   ]
}
```

4. Wählen Sie Richtlinie überprüfen, geben Sie einen Namen ein und wählen Sie dann Richtlinie erstellen aus.

5. Fügen Sie die neu erstellte Richtlinie Ihrer vorhandenen IAM-Rolle hinzu oder erstellen Sie eine neue Rolle.

Epen

Amazon SQS in AWS einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Richt linie für Amazon SQS.	Erstellen Sie die IAM-Richt linie, die den Zugriff auf Amazon SQS ermöglicht. Eine Beispielrichtlinie finden Sie im Abschnitt Code.	Systemingenieur
Erstellen Sie ein AWS-Profil.	Erstellen Sie ein neues Profil, indem Sie die AWS-Tools für	Systemingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den PowerShell Befehl Set-ausführenAWSCredential. Dieser Befehl speichert Ihren Zugriffsschlüssel und Ihren geheimen Schlüssel in Ihrer Standardanmeldedatei unter dem von Ihnen angegeben en Profilnamen. Verknüpfen Sie die Amazon SQS SQS-Richtlinie, die Sie zuvor erstellt haben, mit diesem Konto. Bewahren Sie die AWS-Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel auf. Diese werden in den nächsten Schritten benötigt.	
Erstellen Sie eine SQS-Warte schlange.	Sie können eine Standardw arteschlange oder eine FIFO-Warteschlange (First In, First Out) erstellen. Anweisungen finden Sie unter dem Link im Abschnitt Referenzen.	Systemingenieur

Überarbeiten Sie Ihren .NET-Anwendungscode

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie AWS Toolkit for Visual Studio.	Dieses Toolkit ist eine Erweiterung für Microsoft Visual Studio und erleichte rt Ihnen das Erstellen und Bereitstellen von.NET-Anwendungen in AWS. Anweisungen zur Installation	Entwickler der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und Verwendung finden Sie unter dem Link im Abschnitt Referenzen.	
Installieren Sie das AWSSDK .SQS-Paket. NuGet	Sie AWSSDK können.SQS installieren, indem Sie in Visual Studio „ NuGet Package verwalten“ wählen oder den Befehl „ AWSSDKInstall-Package .SQS“ ausführen.	Entwickler der Anwendung
Erstellen Sie ein AWSCredentials Objekt in Ihrer .NET-Anwendung.	Die Beispielanwendung im Anhang zeigt, wie Sie ein AWSCredentials Basic-Objekt erstellen, das von AWSCredentials erbt. Sie können die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel von früher verwenden oder das Objekt diese zur Laufzeit als Teil des Benutzerprofils aus dem Ordner „.aws“ auswählen lassen.	Entwickler der Anwendung
Erstellen Sie ein SQS-Client-Objekt.	Erstellen Sie ein SQS-Client-Objekt (AmazonSQSClient) für.NET Framework. Dies ist Teil des Amazon.SQS-Namespace. Dieses Objekt ist anstelle von IQueue Client erforderlich, der Teil von Microsoft.Azure ist. ServiceBus Namespace.	Entwickler von Anwendungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie die SendMessageAsync Methode auf, um Nachrichten an die SQS-Warteschlange zu senden.	Ändern Sie den Code, der die Nachricht an die Warteschlange sendet, um die zu verwenden. amazonSqsClient SendMessageAsync Methode. Einzelheiten finden Sie im beigefügten Codebeispiel.	Entwickler der Anwendung
Rufen Sie die ReceiveMessageAsync Methode auf, um Nachrichten aus der SQS-Warteschlange zu empfangen.	Ändern Sie den Code, der die Nachricht empfängt, um den zu verwenden. amazonSqs Client ReceiveMessageAsync Methode. Einzelheiten finden Sie im beigefügten Codebeispiel.	Entwickler der Anwendung
Rufen Sie die DeleteMessageAsync Methode auf, um Nachrichten aus der SQS-Warteschlange zu löschen.	Um Nachrichten zu löschen, ändern Sie den Code im QueueClient. CompleteAsync Methode zum. amazonSqs Client DeleteMessageAsync Methode. Einzelheiten finden Sie im beigefügten Codebeispiel.	Entwickler der Anwendung

Zugehörige Ressourcen

- AWS SDK for .NET Entwicklerhandbuch
- Nachrichtenübermittlung mit Amazon SQS
- Erstellen und Verwenden einer Amazon SQS SQS-Warteschlange mit dem AWS SDK for .NET
- Eine Amazon SQS SQS-Nachricht senden
- Empfangen einer Nachricht aus einer Amazon SQS SQS-Warteschlange
- Eine Nachricht aus einer Amazon SQS SQS-Warteschlange löschen

- AWS Toolkit for Visual Studio

Zusätzliche Informationen

Dieses Muster umfasst zwei Beispielanwendungen (siehe Abschnitt Anlagen):

- AzureSbTestAppenthält Code, der die Azure Service Bus-Warteschlange verwendet.
- AmazonSqsTestAppverwendet Amazon SQS. Dies ist eine Konsolenanwendung, die .NET Core 2.2 verwendet und Beispiele für das Senden und Empfangen von Nachrichten enthält.

Hinweise:

- QueueClient ist ein Objekt von IQueue Client, das Teil von Microsoft.Azure ist. ServiceBus Namespace (in Microsoft.Azure enthalten). ServiceBus NuGet Paket).
- amazonSqsClient ist ein Objekt von AmazonSQSClient, das Teil des Amazon.SQS-Namespace ist (im .SQS-Paket enthalten). AWSSDK NuGet
- Je nachdem, wo der Code ausgeführt wird, z. B. ob er ausgeführt wird, benötigt die Rolle die Berechtigung EC2, in die SQS-Warteschlange zu schreiben.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Migrieren Sie eine relationale Datenbank zu MongoDB Atlas am AWS

Erstellt von Battulga Purevragchaa (AWS), Babu Srinivasan (MongoDB) und Igor Alekseev (AWS)

Übersicht

Dieses Muster beschreibt die Schritte für die Migration von einer relationalen Datenbank wie SQL Server, MySQL oder PostgreSQL zu MongoDB Atlas in der. AWS Cloud Es verwendet MongoDB Relational Migrator, um die Datenmigration von relationalen Datenbanken zu MongoDB Atlas zu beschleunigen.

Das Muster ist Teil des Leitfadens Migration zu MongoDB Atlas AWS auf der AWS Prescriptive Guidance-Website. Es enthält die Implementierungsschritte für eines der Migrationsszenarien, die in diesem Leitfaden erörtert werden. Weitere Migrationsszenarien finden Sie in den folgenden Mustern auf der AWS Prescriptive Guidance-Website:

- Migrieren Sie eine selbst gehostete MongoDB-Umgebung zu MongoDB Atlas am AWS
- Streamen Sie Daten von IBM Db2, SAP, Sybase und anderen Datenbanken nach MongoDB Atlas auf AWS

Das Muster ist für Partner und AWS Benutzer von AWS System Integrator (SI) vorgesehen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine relationale Quelldatenbank (Oracle Database, SQL Server, PostgreSQL, MySQL, SAP/Sybase ASE und andere) für die Migration zu MongoDB Atlas.
- Vertrautheit mit relationalen Datenbanken, MongoDB Atlas und. AWS-Services Dieses Muster erklärt einige der Migrationsschritte auf allgemeiner Ebene. Zusätzliche Details werden in future Versionen hinzugefügt.

Produktversionen

- MongoDB Version 5.0 oder höher

Architektur

Das folgende Diagramm zeigt die Migration von einer Datenbank mit einem relationalen Datenbankmanagementsystem (RDBMS) zu MongoDB Atlas am. AWS

Informationen zu MongoDB Atlas-Referenzarchitekturen, die verschiedene Nutzungsszenarien unterstützen, finden Sie unter Migration zu MongoDB Atlas AWS auf der AWS Prescriptive Guidance-Website.

Tools

- MongoDB Atlas ist ein vollständig verwalteter Database-as-a-Service (DBaaS) für die Bereitstellung und Verwaltung von MongoDB-Datenbanken in der Cloud.
- MongoDB Relational Migrator bietet einen reibungslosen Übergang von Daten von herkömmlichen relationalen Datenbanken zu MongoDB. Es hilft bei der Automatisierung des Konvertierungsprozesses und wandelt das strukturierte Datenmodell relationaler Datenbanken in das von MongoDB bereitgestellte flexible Dokumentformat um. Der Relational Migrator bewahrt die Datenintegrität und die Beziehungen, um die Migration zu vereinfachen. Organizations können die Vorteile der Skalierbarkeit, Leistung und Vielseitigkeit, die MongoDB bietet, nutzen und gleichzeitig die Vertrautheit mit ihren vorhandenen Daten beibehalten.

Bewährte Methoden

Bewährte Methoden für die Verwendung von MongoDB auf AWS finden Sie in den Beiträgen im AWS Partner Network-Blog.

Epen

Entdeckung und Bewertung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie die Parameter und die Größe der relationalen Datenbank.	Schätzen Sie die Größe des Arbeitssets, indem Sie die Empfehlungen von Relationa l Migrator und die Informati onen aus dem gesamten `db.stats()` Indexraum	App-Besitzer, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	verwenden. Gehen Sie davon aus, dass auf einen Prozentsatz Ihres Datenspeichers häufig zugegriffen wird. Diese Aufgabe sollte ungefähr eine Woche dauern. Weitere Informationen und Beispiele für diese und die anderen Geschichten in diesem Epos finden Sie im Abschnitt Verwandte Ressourcen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schätzen Sie die Anforderungen an die Netzwerkbandbreite.	Um Ihre Netzwerkbandbreitenanforderungen zu schätzen, multiplizieren Sie die durchschnittliche Dokumentengröße mit der Anzahl der pro Sekunde bereitgestellten Dokumente. Berücksichtigen Sie den maximalen Datenverkehr, den jeder Knoten in Ihrem Cluster als Grundlage tragen kann. Um die Downstream-Datenübertragungsraten von Ihrem Cluster zu den Client-Anwendungen zu berechnen, verwenden Sie die Summe aller Dokumente, die über einen bestimmten Zeitraum zurückgegeben wurden. Wenn Ihre Anwendungen von sekundären Knoten lesen, dividieren Sie diese Gesamtzahl der Dokumente durch die Anzahl der Knoten, die Lesevorgänge ausführen können. Verwenden Sie den `db.stats().avgObjSize` Befehl, um die durchschnittliche Dokumentgröße für eine Datenbank zu ermitteln. Diese Aufgabe dauert in der Regel einen Tag.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie die Atlas-Stufe aus.	Folgen Sie den Anweisungen in der MongoDB-Dokumentation, um die richtige Atlas-Clusterstufe auszuwählen.	DBA
Plan für die Umstellung.	Plan für die Umstellung der Anwendung.	DBA, Besitzer der App

Richten Sie eine neue MongoDB Atlas-Umgebung ein auf AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen neuen MongoDB Atlas-Cluster auf AWS.	Wählen Sie in MongoDB Atlas Build a Cluster aus. Wählen AWS Sie im Dialogfeld „Neuen Cluster erstellen“ den Cloud-Anbieter aus.	DBA
Wählen Sie AWS-Regionen eine globale Clusterkonfiguration aus.	Wählen Sie aus der Liste der AWS-Regionen für Ihren Atlas-Cluster verfügbaren aus. Konfigurieren Sie bei Bedarf globale Cluster.	DBA
Wählen Sie die Clusterebene aus.	Wählen Sie Ihre bevorzugte Clusterstufe aus. Ihre Tierauswahl bestimmt Faktoren wie Arbeitsspeicher, Speicher und IOPS-Spezifikation.	DBA
Konfigurieren Sie zusätzliche Cluster-Einstellungen.	Konfigurieren Sie zusätzliche Clustereinstellungen wie MongoDB-Version, Sicherungs- und Verschlüsselungsop	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	tionen. Weitere Informationen zu diesen Optionen finden Sie im Abschnitt Verwandte Ressourcen.	

Konfigurieren Sie Sicherheit und Compliance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Zugriffsliste.	Um eine Verbindung zum Atlas-Cluster herzustellen, müssen Sie der Zugriffsliste des Projekts einen Eintrag hinzufügen. Atlas verwendet TLS/SSL, um die Verbindungen zur Virtual Private Cloud (VPC) für Ihre Datenbank zu verschlüsseln. Informationen zur Einrichtung der Zugriffsliste für das Projekt und weitere Informationen zu den Geschichten in diesem Epos finden Sie im Abschnitt Verwandte Ressourcen.	DBA
Authentifizieren und autorisieren Sie Benutzer.	Sie müssen die Datenbankbenutzer, die auf die MongoDB Atlas-Cluster zugreifen, erstellen und authentifizieren. Um auf Cluster in einem Projekt zugreifen zu können, müssen Benutzer zu diesem Projekt gehören, und sie	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	können mehreren Projekten angehören.	
Erstellen Sie benutzerdefinierte Rollen.	(Optional) Atlas unterstützt die Erstellung benutzerdefinierter Rollen in Fällen, in denen die integrierten Benutzerberechtigungen für die Atlas-Datenbank nicht den gewünschten Berechtigungssatz abdecken.	DBA
Richten Sie VPC-Peering ein.	(Optional) Atlas unterstützt VPC-Peering mit anderen VPCs . AWS	AWS-Administrator
Richten Sie einen AWS PrivateLink Endpunkt ein.	(Optional) Sie können private Endpunkte einrichten, AWS indem Sie AWS PrivateLink Weitere Informationen finden Sie in der Amazon VPC-Dokumentation.	AWS-Administrator
Aktivieren Sie die Zwei-Faktor-Authentifizierung.	(Optional) Atlas unterstützt die Zwei-Faktor-Authentifizierung (2FA), damit Benutzer den Zugriff auf ihre Atlas-Konten kontrollieren können.	AWS-Administrator
Richten Sie die Benutzerauthentifizierung und -autorisierung mit LDAP ein.	(Optional) Atlas unterstützt die Benutzerauthentifizierung und -autorisierung mit dem Lightweight Directory Access Protocol (LDAP).	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Unified AWS Access ein.	(Optional) Einige Atlas-Funktionen, darunter Atlas Data Lake und Verschlüsselung im Ruhezustand mithilfe der Kundenschlüsselverwaltung, verwenden AWS Identity and Access Management (IAM-) Rollen für die Authentifizierung.	AWS-Administrator
Richten Sie die Verschlüsselung im Ruhezustand ein mit AWS KMS.	(Optional) Atlas unterstützt die Verwendung von AWS Key Management Service (AWS KMS) zur Verschlüsselung von Speicher-Engines und Backups von Cloud-Anbietern.	AWS-Administrator
Richten Sie eine clientseitige Verschlüsselung auf Feldebene ein.	(Optional) Atlas unterstützt die clientseitige Verschlüsselung auf Feldebene, einschließlich der automatischen Verschlüsselung von Feldern.	AWS-Administrator

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie MongoDB Relational Migrator zur Zugriffsliste hinzu.	Fügen Sie den Relational Migrator der Zugriffsliste für Ihre Quelldatenbank hinzu. Dies hilft dabei, die Quellumgebung auf die Verbindung mit dem Atlas-Zielcluster vorzubereiten.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beurteilen Sie die relationalen Datenbankobjekte.	Starten Sie MongoDB Relational Migrator und stellen Sie eine Verbindung zu Ihrer relationalen Datenbank her. Starten Sie die Bewertung.	DBA
Akzeptieren Sie die Migration smuster oder entscheiden Sie sich dafür, sie je nach Ihren Geschäftsanforderungen zu ändern.	Akzeptieren Sie entweder die vom Relational Migrator auf der Grundlage der anfänglichen Bewertung und der Leistungsparameter empfohlenen Datenbank muster, oder ändern Sie sie entsprechend Ihren Geschäfts anforderungen.	DBA
Starten Sie Ihren Zielrepli katsatz in MongoDB Atlas.	Starten Sie Ihren Zielrepli katsatz in MongoDB Atlas. Wählen Sie in Relational Migrator die Option Ich bin bereit zur Migration aus.	DBA

Betriebsintegration konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Connect zum MongoDB Atlas-Cluster her.	Stellen Sie sicher, dass die MongoDB Atlas-Cluster-Konn ektivität wie erwartet funktioni ert.	Besitzer der App
Interagieren Sie mit Clusterda ten.	Überprüfen Sie die Clusterda ten.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überwachen Sie Ihre Cluster.	Stellen Sie sicher, dass Ihre Cluster korrekt eingerichtet sind.	DBA
Clusterdaten sichern und wiederherstellen.	Planen Sie Backups für Clusterdaten in regelmäßigen Abständen.	DBA

Zugehörige Ressourcen

Alle folgenden Links führen, sofern nicht anders angegeben, zu Webseiten in der MongoDB-Dokumentation.

Leitfaden zur Migration

- Migration zu MongoDB Atlas on AWS (AWS Prescriptive Guidance)

Entdeckung und Bewertung

- Arbeitsspeicher
- Beispiel zur Größenbestimmung mit Atlas-Beispieldatensätzen
- Beispiel zur Größenbestimmung für mobile Anwendungen
- Netzwerkverkehr
- Automatische Cluster-Skalierung
- Vorlage für die Größenbestimmung von Atlas

Konfiguration von Sicherheit und Compliance

- Einträge in der IP-Zugriffsliste konfigurieren
- Datenbankbenutzer konfigurieren
- Konfigurieren Sie den Zugriff auf die Atlas-Benutzeroberfläche
- Konfigurieren Sie benutzerdefinierte Datenbankrollen
- Datenbankbenutzer konfigurieren

- Richten Sie eine Netzwerk-Peering-Verbindung ein
- Erfahren Sie mehr über private Endpunkte in Atlas
- Verwalten Sie Ihre Multi-Faktor-Authentifizierungsoptionen
- Richten Sie die Benutzerauthentifizierung und -autorisierung mit LDAP ein
- Atlas Data Lake
- Verschlüsselung im Ruhezustand mithilfe von Customer Key Management
- Methoden zur Übernahme einer Rolle (IAM-Dokumentation)
- Clientseitige Verschlüsselung auf Feldebene
- Automatische Verschlüsselung
- MongoDB Atlas Sicherheitskontrollen
- MongoDB-Vertrauenszentrum
- Konfigurieren Sie Sicherheitsfunktionen für Cluster

Einrichtung einer neuen MongoDB Atlas-Umgebung auf AWS

- Cloud-Anbieter und Regionen
- Globale Cluster verwalten
- Wählen Sie die Clusterebene
- Konfigurieren Sie zusätzliche Einstellungen
- Fangen Sie mit Atlas an
- Konfigurieren Sie den Zugriff auf die Atlas-Benutzeroberfläche
- Cluster verwalten

Daten migrieren

- Daten migrieren oder importieren

Cluster überwachen

- Überwachen Sie Ihre Cluster

Integrieren von Abläufen

- Mit einem Cluster verbinden
- Interagieren Sie mit Ihren Daten
- Überwachen Sie Ihre Cluster
- Daten sichern, wiederherstellen und archivieren

Blog-Posts

- Modernisierung von RDBMS-Schemas mit einem MongoDB-Dokumentenmodell

Migrieren Sie eine selbst gehostete MongoDB-Umgebung zu MongoDB Atlas am AWS

Erstellt von Battulga Purevragchaa (AWS), Babu Srinivasan (MongoDB) und Igor Alekseev (AWS)

Übersicht

Dieses Muster beschreibt die Schritte für die Migration von einer selbstverwalteten MongoDB-Umgebung (einschließlich MongoDB Community Server, Enterprise Server, Enterprise Advanced, mLab oder einem beliebigen verwalteten MongoDB-Cluster) zu MongoDB Atlas in der. AWS Cloud Es verwendet den Atlas Live Migration Service, um die Datenmigration von MongoDB zu MongoDB Atlas zu beschleunigen.

Das Muster ist Teil des Leitfadens Migration zu MongoDB Atlas AWS auf der AWS Prescriptive Guidance-Website. Es enthält die Implementierungsschritte für eines der Migrationsszenarien, die in diesem Leitfaden erörtert werden. Weitere Migrationsszenarien finden Sie in den folgenden Mustern auf der AWS Prescriptive Guidance-Website:

- Migrieren Sie eine relationale Datenbank zu MongoDB Atlas am AWS
- Streamen Sie Daten von IBM Db2, SAP, Sybase und anderen Datenbanken nach MongoDB Atlas auf AWS

Das Muster ist für Partner und Benutzer von AWS Systems Integrator (SI) vorgesehen. AWS

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine MongoDB Enterprise Advanced-, Community Server- oder andere selbstverwaltete MongoDB-Umgebung für die Migration zu MongoDB Atlas.
- Vertrautheit mit MongoDB, MongoDB Atlas und. AWS-Services Dieses Muster erklärt einige der Migrationsschritte auf allgemeiner Ebene. Zusätzliche Details werden in future Versionen hinzugefügt.

Produktversionen

- MongoDB Version 6.0.13 oder höher

Architektur

Das folgende Diagramm zeigt den Atlas Live Migration Service, der verwendet wird, um Daten aus einer MongoDB Enterprise Advanced-Datenbank und einer MongoDB Community-Datenbank zu MongoDB Atlas on zu migrieren. AWS Verwenden Sie diesen Service, wenn Sie große, komplexe Datenbanken mit minimalen Ausfallzeiten und kontinuierlicher Datensynchronisierung auf MongoDB Atlas migrieren müssen. Dieses Muster verwendet den Atlas Live Migration Service.

Das folgende Diagramm zeigt den MongoDB-Spiegeldienst (`mongomirror`), mit dem Sie auch Daten aus einer MongoDB Enterprise Advanced-Datenbank und einer MongoDB-Community-Datenbank AWS über eine sichere Verbindung zu MongoDB Atlas migrieren können. AWS PrivateLink Wird `mongomirror` für die laufende Datenreplikation zwischen MongoDB vor Ort und MongoDB Atlas verwendet. Dieses Tool ist ideal für Disaster Recovery oder phasenweise Migrationen, fällt aber nicht in den Anwendungsbereich dieses Musters.

Weitere MongoDB Atlas-Referenzarchitekturen, die verschiedene Nutzungsszenarien unterstützen, finden Sie unter Migration zu MongoDB Atlas AWS auf der AWS Prescriptive Guidance-Website.

Tools

- MongoDB Atlas ist ein vollständig verwalteter Database-as-a-Service (DBaaS) für die Bereitstellung und Verwaltung von MongoDB-Datenbanken in der Cloud.
- Atlas Live Migration Service ist ein kostenloses MongoDB-Hilfsprogramm, das bei der Migration von Datenbanken zu Atlas hilft. Dieser Dienst hält die Quelldatenbank bis zur Übernahme mit der Zieldatenbank synchron. Wenn Sie bereit sind, die Übertragung vorzunehmen, beenden Sie Ihre Anwendungsinstanzen, verweisen sie auf den Atlas-Ziel-Cluster und starten sie neu. Um auf diesen Service zuzugreifen, wählen Sie Datenbankoptionen aus Ihrem MongoDB Atlas-Cluster.
- mongomirror ist ein Tool zur manuellen Migration von Daten aus einem vorhandenen MongoDB-Replikatsatz zu einem MongoDB-Atlas-Replikatsatz. `mongomirror`erfordert nicht, dass Sie Ihren vorhandenen Replikatsatz oder Ihre Anwendungen herunterfahren, importiert keine Benutzer- oder Rollendaten und kopiert auch nicht die Konfigurationsdatenbank. Sie können es `mongomirror` von der MongoDB-Dokumentation herunterladen.

Bewährte Methoden

Bewährte Methoden für die Verwendung von MongoDB auf AWS finden Sie in den Beiträgen im AWS Partner Network-Blog.

Epen

Entdeckung und Bewertung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie die Clustergröße.	Schätzen Sie die Größe des Arbeitssets, indem Sie die Informationen `db.stats()` für den gesamten Indexraum verwenden. Gehen Sie davon aus, dass auf einen Prozentsatz Ihres Datenspeichers häufig zugegriffen wird. Oder Sie können Ihren Speicherbedarf auf der Grundlage Ihrer eigenen Annahmen abschätzen. Diese Aufgabe sollte ungefähr eine Woche dauern. Weitere Informationen und Beispiele für diese und die anderen Geschichten in diesem Epos finden Sie im Abschnitt Verwandte Ressourcen.	DBA, App-Besitzer
Schätzen Sie die Anforderungen an die Netzwerkbandbreite.	Um Ihre Netzwerkbandbreitenanforderungen zu schätzen, multiplizieren Sie die durchschnittliche Dokumentengröße mit der Anzahl der pro Sekunde bereitgestellten Dokumente. Berücksichtigen	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie den maximalen Datenverkehr, den jeder Knoten in Ihrem Cluster als Grundlage tragen kann. Um die Downstream-Datenübertragungsraten von Ihrem Cluster zu den Client-Anwendungen zu berechnen, verwenden Sie die Summe der gesamten Dokumente, die über einen bestimmten Zeitraum zurückgegeben wurden. Wenn Ihre Anwendungen von sekundären Knoten lesen, dividieren Sie diese Gesamtzahl der Dokumente durch die Anzahl der Knoten, die Lesevorgänge ausführen können. Verwenden Sie den `db.stats().avgObjSize` Befehl, um die durchschnittliche Dokumentgröße für eine Datenbank zu ermitteln. Diese Aufgabe dauert in der Regel einen Tag.	
Wählen Sie die Atlas-Stufe aus.	Folgen Sie den Anweisungen in der MongoDB-Dokumentation, um die richtige Atlas-Clusterstufe auszuwählen.	DBA
Plan für die Umstellung.	Plan für die Umstellung der Anwendung.	DBA, Besitzer der App

Richten Sie eine neue MongoDB Atlas-Umgebung auf AWS ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen neuen MongoDB Atlas-Cluster auf AWS.	Melden Sie sich bei Atlas an und öffnen Sie die Übersicht sseite für Ihr Projekt. Wählen Sie die Schaltfläche Erstellen , um einen Cluster zu erstellen . Weitere Informationen finden Sie in der MongoDB-D okumentation.	DBA
Wählen Sie AWS-Regionen eine globale Clusterkonfigurati on aus.	Wählen Sie aus der Liste der AWS-Regionen für Ihren Atlas-Cluster verfügbaren aus. Konfigurieren Sie bei Bedarf globale Cluster. Weitere Informationen finden Sie in der MongoDB-Dokumentation.	DBA
Wählen Sie die Clusterebene aus.	Wählen Sie Ihre bevorzugt e Clusterstufe aus. Ihre Tierauswahl bestimmt Faktoren wie Arbeitsspeicher, Speicher und IOPS-Spez ifikation.	DBA
Konfigurieren Sie zusätzliche Cluster-Einstellungen.	Konfigurieren Sie zusätzlic he Clustereinstellungen wie MongoDB-Version, Sicherung s- und Verschlüsselungsop tionen. Weitere Informationen zu diesen Optionen finden Sie im Abschnitt Verwandte Ressourcen.	DBA

Konfigurieren Sie Sicherheit und Compliance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Authentifizieren und autorisieren Sie Benutzer.	Sie müssen die Datenbankbenutzer, die auf die MongoDB Atlas-Cluster zugreifen, erstellen und authentifizieren. Um auf Cluster in einem Projekt zugreifen zu können, müssen Benutzer zu diesem Projekt gehören, und sie können mehreren Projekten angehören. Atlas unterstützt auch die Authentifizierung auf Basis von AWS Identity and Access Management (IAM). Weitere Informationen finden Sie in der MongoDB-Dokumentation.	DBA
Erstellen Sie benutzerdefinierte Rollen.	(Optional) Atlas unterstützt die Erstellung benutzerdefinierter Rollen in Fällen, in denen die integrierten Benutzerberechtigungen für die Atlas-Datenbank nicht den gewünschten Berechtigungssatz abdecken.	DBA
Richten Sie VPC-Peering ein.	(Optional) Atlas unterstützt Virtual Private Cloud (VPC) - Peering mit anderen VPCs . AWS	AWS-Administrator
Richten Sie einen AWS PrivateLink Endpunkt ein.	(Optional) Sie können private Endpunkte einrichten, AWS	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	indem Sie AWS PrivateLink Weitere Informationen finden Sie in der Amazon VPC-Dokumentation.	
Aktivieren Sie die Zwei-Faktor-Authentifizierung.	(Optional) Atlas unterstützt die Zwei-Faktor-Authentifizierung (2FA), damit Benutzer den Zugriff auf ihre Atlas-Konten kontrollieren können.	AWS-Administrator
Richten Sie die Benutzerauthentifizierung und -autorisierung mit LDAP ein.	(Optional) Atlas unterstützt die Benutzerauthentifizierung und -autorisierung mit dem Lightweight Directory Access Protocol (LDAP).	AWS-Administrator
Richten Sie AWS einen einheitlichen Zugriff ein.	(Optional) Einige Atlas-Funktionen, darunter Atlas Data Lake und Verschlüsselung im Ruhezustand mithilfe der Kundenschlüsselverwaltung, verwenden IAM-Rollen für die Authentifizierung.	AWS-Administrator
Richten Sie die Verschlüsselung im Ruhezustand ein mit AWS KMS.	(Optional) Atlas unterstützt die Verwendung von AWS Key Management Service (AWS KMS) zur Verschlüsselung von Speicher-Engines und Backups von Cloud-Anbietern.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine clientsei tige Verschlüsselung auf Feldebene ein.	(Optional) Atlas unterstützt die clientseitige Verschlüsselung auf Feldebene, einschließlich der automatischen Verschlüs selung von Feldern.	AWS-Administrator

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie Ihren Zielrepli katsatz in MongoDB Atlas aus.	Navigieren Sie zum Atlas-Ziel-Cluster und klicken Sie auf die Schaltfläche mit den Auslassungspunkten (...). In der Clusterliste wird diese Schaltfläche unter dem Clusternamen angezeigt. In den Clusterdetails wird die Schaltfläche rechts neben den Schaltflächen Connect und Konfiguration angezeigt . Weitere Informationen finden Sie in der MongoDB-D okumentation.	DBA
Fügen Sie den Atlas Live Migration Service zur Zugriffsl iste hinzu.	Fügen Sie den Atlas Live Migration Service zur Zugriffsl iste in Ihrem AWS Quellclus ter hinzu. Dies hilft dabei, die Quellumgebung auf die Verbindung mit dem Atlas-Zie l-Cluster vorzubereiten.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Migration mit dem Atlas Live Migration Service durch.	Wählen Sie Migration starten. Wenn die Schaltfläche „Für die Übernahme vorbereiten“ grün wird, führen Sie die Übernahme durch. Überprüfen Sie die Leistungskennzahlen des Atlas-Clusters. Erwägen Sie, die Datenbankverbindung in allen Anwendungsebenen so zu aktualisieren, dass sie auf die neue Datenbank verweist.	DBA

Betriebsintegration konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Connect zum MongoDB Atlas-Cluster her.	Stellen Sie sicher, dass die MongoDB Atlas-Clusterkonnektivität wie erwartet funktioniert.	Besitzer der App
Interagieren Sie mit Clusterdaten.	Testen Sie die Clusterdaten.	DBA
Überwachen Sie Ihre Cluster.	Stellen Sie sicher, dass Ihre Cluster korrekt eingerichtet sind.	DBA
Clusterdaten sichern und wiederherstellen.	Planen Sie Backups für Clusterdaten in regelmäßigen Abständen.	DBA

Fehlerbehebung

Problem	Lösung

Fehler: Die angegebene Quelle konnte nicht erreicht werden	• Stellen Sie sicher, dass Sie der IP-Zugrif fsliste auf dem Quellcluster die richtigen Subnetzbereiche hinzugefügt haben. Sie finden die vier erforderlichen Subnetzbe reiche im modalen Fenster der Live-Migr ation.
	• Vergewissern Sie sich, dass der von Ihnen angegebene Hostname in eine öffentliche IP-Adresse aufgelöst wird. Verwenden Sie in einer Befehlszeile einen der folgenden Befehle:
	`nslookup <hostname>`
	`ping <hostname>`
	• Stellen Sie sicher, dass Sie keine VPC-Peeri ng-Verbindung verwenden, die nicht mit der Pull-Live-Migration kompatibel ist. Wenn eine VPC-Peering-Verbindung Ihre einzige Option ist, verwenden Sie `mongomirror` stattdess en.

Fehler: Hostname konnte nicht aufgelöst werden	Für den angegebenen Hostnamen wurde keine IP-Adresse gefunden. Bestätigen Sie, dass der angegebene Hostname korrekt und öffentlich zugänglich ist.
Irgendein anderer Fehler	Wenn Sie auf andere Fehler stoßen, finden Sie weitere Informationen unter Problembe handlung bei Live-Migration (Pull) in der MongoDB-Dokumentation.

Zugehörige Ressourcen

Alle folgenden Links führen, sofern nicht anders angegeben, zu Webseiten in der MongoDB-Dokumentation.

Leitfaden zur Migration

- Migration zu MongoDB Atlas on AWS (AWS Prescriptive Guidance)

Migration älterer Versionen

- Migration älterer Versionen von MongoDB

Entdeckung und Bewertung

- Arbeitsspeicher
- Beispiel zur Größenbestimmung mit Atlas-Beispieldatensätzen
- Beispiel zur Größenbestimmung für mobile Anwendungen
- Netzwerkverkehr
- Automatische Cluster-Skalierung
- Vorlage für die Größenbestimmung von Atlas

Konfiguration von Sicherheit und Compliance

- Einträge in der IP-Zugriffsliste konfigurieren
- Datenbankbenutzer konfigurieren
- Konfigurieren Sie den Zugriff auf die Atlas-Benutzeroberfläche
- Konfigurieren Sie benutzerdefinierte Datenbankrollen
- Datenbankbenutzer konfigurieren
- Richten Sie eine Netzwerk-Peering-Verbindung ein
- Erfahren Sie mehr über private Endpunkte in Atlas
- Verwalten Sie Ihre Multi-Faktor-Authentifizierungsoptionen
- Richten Sie die Benutzerauthentifizierung und -autorisierung mit LDAP ein
- Atlas Data Lake
- Verschlüsselung im Ruhezustand mithilfe von Customer Key Management

- Methoden zur Übernahme einer Rolle (IAM-Dokumentation)
- Clientseitige Verschlüsselung auf Feldebene
- Automatische Verschlüsselung
- MongoDB Atlas Sicherheitskontrollen
- MongoDB-Vertrauenszentrum
- Konfigurieren Sie Sicherheitsfunktionen für Cluster

Einrichtung einer neuen MongoDB Atlas-Umgebung auf AWS

- Cloud-Anbieter und Regionen
- Globale Cluster verwalten
- Wählen Sie die Clusterebene
- Konfigurieren Sie zusätzliche Einstellungen
- Fangen Sie mit Atlas an
- Konfigurieren Sie den Zugriff auf die Atlas-Benutzeroberfläche
- Cluster verwalten

Daten migrieren

- Daten migrieren oder importieren

Cluster überwachen

- Überwachen Sie Ihre Cluster

Integrieren von Abläufen

- Mit einem Cluster verbinden
- Interagieren Sie mit Ihren Daten
- Überwachen Sie Ihre Cluster
- Daten sichern, wiederherstellen und archivieren

Training

- Live-Migration mit MongoDB Atlas

Zusätzliche Informationen

Weitere Informationen finden Sie in den folgenden Themen in der MongoDB-Dokumentation:

- Um Daten auf eine serverlose Instanz zu verschieben, verwenden Sie Compass, um Daten zu exportieren und zu importieren, oder migrieren Sie Daten mit selbstverwalteten Tools. Weitere Informationen finden Sie unter Einschränkungen für serverlose Instances.
- Informationen zum Laden von Daten in einen neuen Cluster in Atlas finden Sie unter Daten in Atlas laden.
- Informationen zum Erstellen einer Kopie Ihres Clusters zu Testzwecken finden Sie unter Sicherungsmethoden für eine selbstverwaltete Bereitstellung.
- Wenn die Anwendung, die Sie migrieren möchten, eine nahezu ununterbrochene Verfügbarkeit benötigt, wenden Sie sich an den MongoDB-Support und teilen Sie uns Ihre Verfügbarkeitsanforderungen und die Clusterkonfiguration mit.
- Weitere Informationen finden Sie unter Daten migrieren oder importieren.

Migrieren Sie eine Oracle JD EnterpriseOne Edwards-Datenbank mithilfe von Oracle Data Pump und AWS DMS zu AWS

Erstellt von Thanigaivel Thirumalai (AWS)

Übersicht

Sie können Ihre JD EnterpriseOne Edwards-Datenbank auf Amazon Relational Database Service (Amazon RDS) migrieren und ausführen. Wenn Sie Ihre Datenbank zu Amazon RDS migrieren, kann AWS sich um Backup-Aufgaben und die Einrichtung von Hochverfügbarkeit kümmern, sodass Sie sich auf die Wartung Ihrer EnterpriseOne Anwendung und ihrer Funktionalität konzentrieren können. Eine umfassende Liste der wichtigsten Faktoren, die während des Migrationsprozesses zu berücksichtigen sind, finden Sie unter Strategien zur Oracle-Datenbankmigration in AWS Prescriptive Guidance.

Es gibt mehrere Möglichkeiten, eine EnterpriseOne Datenbank zu migrieren, darunter:

- Verwenden von Oracle Universal Batch Engine (UBE) R98403 für die Schema- und Tabellenerstellung und Verwendung von AWS Database Migration Service (AWS DMS) für die Migration
- Verwendung nativer DB-Tools für die Schema- und Tabellenerstellung und Verwendung von AWS DMS für die Migration
- Verwendung von nativen DB-Tools für die Migration vorhandener Daten (Volllast) und Verwendung von AWS DMS für Change Data Capture-Aufgaben (CDC)

Dieses Muster deckt die dritte Option ab. Es wird erklärt, wie Sie Ihre lokalen EnterpriseOne Datenbanken mithilfe von Oracle Data Pump mit AWS DMS und seiner CDC-Funktion zu Amazon RDS for Oracle migrieren.

Oracle JD Edwards EnterpriseOne ist eine ERP-Lösung (Enterprise Resource Planning) für Unternehmen, die Produkte oder Sachanlagen herstellen, konstruieren, vertreiben, warten oder verwalten. JD Edwards EnterpriseOne unterstützt verschiedene Hardware, Betriebssysteme und Datenbankplattformen.

Bei der Migration kritischer ERP-Anwendungen wie JD Edwards EnterpriseOne ist die Minimierung von Ausfallzeiten von entscheidender Bedeutung. AWS DMS minimiert Ausfallzeiten, indem es sowohl Volllast als auch kontinuierliche Replikation von der Quelldatenbank zur Zieldatenbank unterstützt. AWS DMS bietet außerdem Echtzeitüberwachung und Protokollierung der Migration, sodass Sie Probleme, die zu Ausfallzeiten führen könnten, identifizieren und lösen können.

Wenn Sie Änderungen mit AWS DMS replizieren, müssen Sie eine Zeit- oder Systemänderungsnummer (SCN) als Ausgangspunkt für das Lesen von Änderungen aus den Datenbankprotokollen angeben. Es ist wichtig, diese Protokolle für einen bestimmten Zeitraum (wir empfehlen 15 Tage) auf dem Server zugänglich zu halten, um sicherzustellen, dass AWS DMS Zugriff auf diese Änderungen hat.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Amazon RDS for Oracle Oracle-Datenbank, die in Ihrer AWS-Cloud-Umgebung als Zieldatenbank bereitgestellt wird. Anweisungen finden Sie in der Amazon RDS-Dokumentation.
- Eine EnterpriseOne Datenbank, die lokal oder auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance auf AWS läuft.

> **Note**
>
> Dieses Muster ist für die Migration von lokal zu AWS konzipiert, wurde jedoch mithilfe einer EnterpriseOne Datenbank auf einer EC2 Instance getestet. Wenn Sie eine Migration von Ihrer lokalen Umgebung planen, müssen Sie die entsprechende Netzwerkkonnektivität konfigurieren.

- Schemadetails. Identifizieren Sie, für welches Oracle-Datenbankschema (z. B. DV92 0) Sie migrieren möchten EnterpriseOne. Bevor Sie mit dem Migrationsprozess beginnen, sollten Sie die folgenden Informationen über das Schema sammeln:
  - Größe des Schemas
  - Die Anzahl der Objekte pro Objekttyp
  - Die Anzahl der ungültigen Objekte

Einschränkungen

- Sie müssen alle gewünschten Schemas auf der Amazon RDS for Oracle Oracle-Zieldatenbank erstellen — AWS DMS erstellt diese nicht für Sie. (Im Abschnitt Epics wird beschrieben, wie Data Pump zum Exportieren und Importieren von Schemas verwendet wird.) Der Schemaname muss für die Oracle-Zieldatenbank bereits existieren. Tabellen aus dem Quellschema werden in den Benutzer oder das Schema importiert, und AWS DMS verwendet das Administrator- oder Systemkonto, um eine Verbindung mit der Ziel-Instance herzustellen. Um mehrere

Schemata zu migrieren, können Sie mehrere Replikationsaufgaben erstellen. Sie können Daten auch in verschiedene Schemas auf einer Zielinstanz migrieren. Verwenden Sie dazu Schematransformationsregeln für die AWS DMS-Tabellenzuordnungen.

- Dieses Muster wurde mit einem Demo-Datensatz getestet. Wir empfehlen Ihnen, die Kompatibilität Ihres Datensatzes und die Anpassung zu überprüfen.
- Dieses Muster verwendet eine EnterpriseOne Datenbank, die unter Microsoft Windows läuft. Sie können dasselbe Verfahren jedoch mit anderen Betriebssystemen verwenden, die von AWS DMS unterstützt werden.

Architektur

Das folgende Diagramm zeigt ein System, das EnterpriseOne auf einer Oracle-Datenbank als Quelldatenbank und einer Amazon RDS for Oracle Oracle-Datenbank als Zieldatenbank läuft. Die Daten werden aus der Oracle-Quelldatenbank exportiert und mithilfe von Oracle Data Pump in die Zieldatenbank Amazon RDS for Oracle importiert und für CDC-Updates mithilfe von AWS DMS repliziert.

1. Oracle Data Pump extrahiert Daten aus der Quelldatenbank und die Daten werden an das Datenbankziel Amazon RDS for Oracle gesendet.
2. CDC-Daten werden von der Quelldatenbank an einen Quellendpunkt in AWS DMS gesendet.
3. Vom Quellendpunkt werden die Daten an die AWS DMS-Replikationsinstanz gesendet, wo die Replikationsaufgabe ausgeführt wird.
4. Nach Abschluss der Replikationsaufgabe werden die Daten an den Zielendpunkt in AWS DMS gesendet.
5. Vom Zielendpunkt werden die Daten an die Amazon RDS for Oracle Oracle-Datenbank-Instance gesendet.

Tools

AWS-Services

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS-Cloud oder zwischen Kombinationen von Cloud- und lokalen Setups.
- Amazon Relational Database Service (Amazon RDS) für Oracle unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Oracle-Datenbank in der AWS-Cloud.

Andere Dienste

- Mit Oracle Data Pump können Sie Daten und Metadaten mit hoher Geschwindigkeit von einer Datenbank in eine andere verschieben.

Bewährte Methoden

Migrating LOBs

Wenn Ihre Quelldatenbank große binäre Objekte (LOBs) enthält, die in die Zieldatenbank migriert werden müssen, bietet AWS DMS die folgenden Optionen:

- Vollständiger LOB-Modus — AWS DMS migriert alle Daten LOBs von der Quell- zur Zieldatenbank, unabhängig von ihrer Größe. Die Migration ist zwar langsamer als die anderen Modi, hat aber den Vorteil, dass die Daten nicht gekürzt werden. Um die Leistung zu verbessern, können Sie für die neue Replikationsinstanz eine separate Aufgabe erstellen, um die Tabellen zu migrieren, LOBs die größer als ein paar Megabyte sind.
- Eingeschränkter LOB-Modus — Sie geben die maximale Größe der LOB-Spaltendaten an, sodass AWS DMS Ressourcen vorab zuweisen und diese in großen Mengen anwenden kann. LOBs Wenn die Größe der LOB-Spalten die in der Aufgabe angegebene Größe überschreitet, kürzt AWS DMS die Daten und sendet Warnungen an die AWS DMS-Protokolldatei. Sie können die Leistung verbessern, indem Sie den eingeschränkten LOB-Modus verwenden, wenn Ihre LOB-Datengröße innerhalb der begrenzten LOB-Größe liegt.
- Inline-LOB-Modus — Sie können migrieren, LOBs ohne die Daten zu kürzen oder die Leistung Ihrer Aufgabe zu beeinträchtigen, indem Sie sowohl kleine als auch große Daten replizieren. LOBs Geben Sie zunächst einen Wert für den `InlineLobMaxSize` Parameter an, der nur verfügbar ist, wenn der vollständige LOB-Modus auf eingestellt ist. `true` Die AWS DMS-Aufgabe überträgt die kleine LOBs Inline, was effizienter ist. Anschließend migriert AWS DMS die große Datei, LOBs indem es eine Suche aus der Quelltabelle durchführt. Der Inline-LOB-Modus funktioniert jedoch nur während der Volllastphase.

Generieren von Sequenzwerten

Während des AWS DMS-CDC-Prozesses werden inkrementelle Sequenznummern nicht aus der Quelldatenbank repliziert. Um Diskrepanzen bei den Sequenzwerten zu vermeiden, müssen Sie für alle Sequenzen den neuesten Sequenzwert aus der Quelle generieren und ihn auf die Amazon RDS for Oracle Oracle-Zieldatenbank anwenden.

AWS Secrets Manager

Um Ihnen bei der Verwaltung Ihrer Anmeldeinformationen zu helfen, empfehlen wir Ihnen, die Anweisungen im Blogbeitrag Manage your AWS DMS-Endpoint Credentials with AWS Secrets Manager zu befolgen.

Leistung

- Replikationsinstanzen – Anleitungen zur Auswahl der besten Instance-Größe finden Sie unter Auswahl der besten Größe für eine Replikationsinstanz in der AWS DMS-Dokumentation.
- Konnektivitätsoptionen – Um Latenzprobleme zu vermeiden, empfehlen wir Ihnen, die richtige Verbindungsoption zu wählen. AWS Direct Connect bietet den kürzesten Weg zu AWS-Ressourcen, da es sich um eine dedizierte Verbindung zwischen Ihren Unternehmensrechenzentren und AWS handelt. Während der Übertragung verbleibt Ihr Netzwerkverkehr im globalen AWS-Netzwerk und wird niemals über das Internet übertragen. Dies reduziert die Wahrscheinlichkeit von Engpässen oder unerwarteten Erhöhungen der Latenz im Vergleich zur Verwendung von VPN oder dem öffentlichen Internet.
- Netzwerkbandbreite – Um die Leistung zu optimieren, stellen Sie sicher, dass Ihr Netzwerkdurchsatz schnell ist. Wenn Sie einen VPN-Tunnel zwischen Ihrer lokalen Quelldatenbank und AWS DMS verwenden, stellen Sie sicher, dass die Bandbreite für Ihre Arbeitslast ausreicht.
- Aufgabenparallelität – Sie können die Datenreplikation beschleunigen, indem Sie bei Volllast mehrere Tabellen parallel laden. Dieses Muster verwendet RDBMS-Endpunkte, sodass diese Option nur für den Vollladevorgang gilt. Die Aufgabenparallelität wird durch den `MaxFullLoadSubTasks` Parameter gesteuert, der bestimmt, wie viele Volllast-Unteraufgaben parallel ausgeführt werden. Standardmäßig ist dieser Parameter auf 8 gesetzt, was bedeutet, dass acht Tabellen (sofern in der Tabellenzuordnung ausgewählt) im Vollmodus zusammen geladen werden. Sie können diesen Parameter im Abschnitt mit den Einstellungen für Vollladeaufgaben des JSON-Skripts für die Aufgabe anpassen.
- Tabellenparallelität – Mit AWS DMS können Sie auch eine einzelne große Tabelle laden, indem Sie mehrere parallel Threads verwenden. Dies ist besonders nützlich für Oracle-Quelltabellen mit Milliarden von Datensätzen sowie mehreren Partitionen und Unterpartitionen. Wenn die Quelltabelle nicht partitioniert ist, können Sie Spaltengrenzen für parallel Ladevorgänge verwenden.
- Lasten aufteilen – Wenn Sie Lasten auf mehrere Aufgaben oder AWS DMS-Instanzen aufteilen, sollten Sie bei der Erfassung von Änderungen die Transaktionsgrenzen berücksichtigen.

Epen

Verwenden Sie Oracle Data Pump, um das EnterpriseOne Schema zu exportieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Generieren Sie das SCN.	Wenn die Quelldatenbank aktiv ist und von der Enterpris eOne Anwendung verwendet wird, initiieren Sie den Datenexport mit Oracle Data Pump. Sie müssen zunächst eine System Change Number (SCN) aus der Quelldate nbank generieren, um sowohl die Datenkonsistenz beim Export mit Oracle Data Pump als auch als Ausgangspunkt für CDC in AWS DMS zu gewährleisten.
	
	Verwenden Sie die folgende SQL-Anweisung, um die aktuelle SCN aus Ihrer Quelldatenbank zu generieren:
	
	`SQL> select current_scn from v$database;`
	
	`CURRENT_SCN`
	`-----------`
	`30009727`
	
	Speichern Sie die generiert e SCN. Sie verwenden das SCN, wenn Sie die Daten exportieren und die AWS
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	DMS-Replikationsaufgabe erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Parameterdatei.	Um eine Parameterdatei für den Export des Schemas zu erstellen, können Sie den folgenden Code verwenden.
	`directory=DMS_DATA_PUMP_DIR logfile=export_dms.log dumpfile=export_dms_data.dmp schemas=<schema name> flashback_scn=<SCN from previous command>`
	Note
	Sie können auch Ihren eigenen definieren, `DATA_PUMP_DIR` indem Sie die folgenden Befehle verwenden, die Ihren Anforderungen entsprechen.
	`SQL> CREATE OR REPLACE DIRECTORY DMS_DATA_PUMP_DIR AS '<Directory for dump>'; Directory created.`
	`SQL> GRANT READ, WRITE ON DIRECTORY DMS_DATA_PUMP_DIR TO SYSTEM; Grant succeeded.`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Exportieren Sie das Schema.	Verwenden Sie das `expdp` Hilfsprogramm wie folgt, um den Export durchzuführen:
	
	`C:\Users\Administrator>expdp system/********@<DB Name> PARFILE='<Path to PAR file create above>'`
	
	`Export: Release 19.0.0.0.0 - Production on *** *** ** **:**:** **** Version 19.3.0.0.0`
	
	`Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved.`
	
	`Connected to: Oracle Database 19c Standard Edition 2 Release 19.0.0.0.0 - Production Starting "SYSTEM"."SYS_EXPORT_SCHEMA_02": system/******@<DB Name>PARFILE='E:\exp_dms_datapump.par' Processing object type SCHEMA_EXPORT/TABLE/TABLE_DATA Processing object type SCHEMA_EXPORT/TABLE/INDEX/STATISTICS/INDEX_STATISTICS Processing object type SCHEMA_EXPORT/TABL`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	E/STATISTICS/TABLE _STATISTICS Processing object type SCHEMA_EXPORT/STAT ISTICS/MARKER Processing object type SCHEMA_EXPORT/USER Processing object type SCHEMA_EXPORT/ROLE _GRANT Processing object type SCHEMA_EXPORT/DEFA ULT_ROLE Processing object type SCHEMA_EXPORT/TABL ESPACE_QUOTA Processing object type SCHEMA_EXPORT/PRE_ SCHEMA/PROCACT_SCHEMA Processing object type SCHEMA_EXPORT/TABLE/ TABLE Processing object type SCHEMA_EXPORT/TABL E/GRANT/OWNER_GRANT/ OBJECT_GRANT Processing object type SCHEMA_EXPORT/TABLE/ INDEX/INDEX Processing object type SCHEMA_EXPORT/TABLE/ CONSTRAINT/CONSTRAINT . . exported "<Schema Name>"."<Table Name>" 228.9 MB 496397 rows Master table "SYSTEM". "SYS_EXPORT_SCHEMA _02" successfully loaded/unloaded	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	``` ********** ********** ********** ********** **** Dump file set for SYSTEM.SYS_EXPORT_ SCHEMA_02 is: E:\DMSDUMP\EXPORT_ DMS_DATA.DMP Job "SYSTEM"."SYS_EXPO RT_SCHEMA_02" successfully completed at *** *** ** **:**:** **** elapsed 0 00:01:57 ```	

Verwenden Sie Oracle Data Pump, um das EnterpriseOne Schema zu importieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Übertragen Sie die Dump-Datei auf die Zielinstanz.	Um Ihre Dateien mithilfe des `DBMS_FILE_TRANSFER` Dienstprogramms zu übertragen, müssen Sie einen Datenbank-Link von der Quelldatenbank zur Amazon RDS for Oracle Oracle-In stance erstellen. Nachdem die Verbindung hergestellt wurde, können Sie das Hilfsprog ramm verwenden, um die Data Pump-Dateien direkt auf die Amazon RDS-Instance zu übertragen. Alternativ können Sie die Data Pump-Dateien an Amazon	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Simple Storage Service (Amazon S3) übertragen und sie dann in die Amazon RDS for Oracle Oracle-Instance importieren. Weitere Informationen zu dieser Option finden Sie im Abschnitt Zusätzliche Informationen.
	
	Um einen Datenbank-Link zu erstellen`ORARDSDB`, der eine Verbindung zum Amazon RDS-Master-Benutzer auf der Ziel-DB-Instance herstellt, führen Sie die folgenden Befehle in der Quelldatenbank aus:
	
	`sqlplus / as sysdba`
	
	`SQL*Plus: Release 19.0.0.0.0 on *** *** ** **:**:** **** Version 19.3.0.0.0`
	
	`Copyright (c) 1982, 2019, Oracle. All rights reserved.`
	
	`Connected to: Oracle Database 19c Standard Edition 2 Release 19.0.0.0.0 Version 19.3.0.0.0`
	
	`SQL> create database link orardsdb connect to admin identifie d by "******" using`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`'(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = orcl.******.us-east-1.rds.amazonaws.com)(PORT = 1521))(CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = orcl)))';`
	
	`Database link created.`
	
	`SQL>`	

Testen Sie den Datenbank-Link.	Testen Sie den Datenbank-Link, um sicherzustellen, dass Sie mit der Amazon RDS for Oracle Oracle-Zieldatenbank eine Verbindung herstellen können`sqlplus`.
	
	`SQL> select name from v$database@orardsdb;`
	
	`NAME`
	`---------`
	`ORCL`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Übertragen Sie die Dump-Datei in die Zieldatenbank.	Um die Dump-Datei in die Amazon RDS for Oracle Oracle-Datenbank zu kopieren, können Sie entweder das `DATA_PUMP_DIR` Standardverzeichnis verwenden oder Sie können Ihr eigenes Verzeichnis erstellen, indem Sie den folgenden Code verwenden, der auf der Amazon RDS-Zielinstanz ausgeführt werden muss:
	`exec rdsadmin.rdsadmin_util.create_directory(p_directory_name => 'DMS_TARGET_PUMP_DIR');`
	`PL/SQL procedure successfully completed.`
	Das folgende Skript kopiert eine `EXPORT_DMS_DATA.DMP` aus der Quell-Instance benannte Dump-Datei mithilfe des angegebenen Datenbank-Links in eine Amazon RDS for Oracle Oracle-Zieldatenbank. `orardsdb` Sie müssen das Skript auf der Quelldatenbank-Instance ausführen.
	`BEGIN`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`DBMS_FILE_TRANSFER.PUT_FILE( source_directory_object => 'DMS_DATA_PUMP_DIR', source_file_name => 'EXPORT_DMS_DATA.DMP', destination_directory_object => 'DMS_TARGET_PUMP_DIR', destination_file_name => 'EXPORT_DMS_DATA.DMP', destination_database => 'orardsdb'); END;`
	
	`PL/SQL procedure successfully completed.`	

Listet die Dump-Datei in der Zieldatenbank auf.	Nachdem das PL/SQL-Verfahren abgeschlossen ist, können Sie die Datendump-Datei in der Amazon RDS for Oracle Oracle-Datenbank auflisten, indem Sie den folgenden Code verwenden: `select * from table (rdsadmin.rds_file_util.listdir(p_directory => 'DMS_TARGET_PUMP_DIR'));`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie JDE-spezifische Benutzer in der Zielinstanz.	Erstellen Sie ein JD Edwards-Profil und eine Rolle, indem Sie die folgenden Befehle in der Zielinstanz verwenden:
	`SQL> CREATE PROFILE "JDEPROFILE" LIMIT IDLE_TIME 15;`
	`Profile created.`
	
	`SQL> CREATE ROLE "JDE_ROLE";`
	`Role created.`
	
	`SQL> CREATE ROLE "JDEADMIN";`
	`CREATE ROLE "JDEUSER";`
	`Role created.`
	`Role created.`
	
	Erteilen Sie der Rolle die erforderlichen Berechtigungen:
	`SQL> GRANT CREATE ANY SEQUENCE TO JDE_ROLE;`
	`GRANT DROP ANY SEQUENCE TO JDE_ROLE;`
	`GRANT CREATE ANY TRIGGER TO JDE_ROLE;`
	`GRANT DROP ANY TRIGGER TO JDE_ROLE;`
		DBA, JDE CNC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie Tablespaces in der Zielinstanz.	Erstellen Sie die erforderlichen Tablespaces in der Zielinstanz, indem Sie die folgenden Befehle für die Schemas verwenden, die an dieser Migration beteiligt sind:
	`SQL> CREATE TABLESPACE <Tablespace Name for Tables>;`
	`Tablespace created.`
	
	`SQL> CREATE TABLESPACE <Tablespace Name for Indexes>;`
	`Tablespace created.`
		DBA, JDE CNC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initiieren Sie den Import in der Zieldatenbank.	Bevor Sie den Importvorgang starten, richten Sie die Rollen, Schemas und Tablespaces in der Amazon RDS for Oracle Oracle-Zieldatenbank mithilfe der Datendumpdatei ein. Um den Import durchzuführen, greifen Sie mit dem primären Amazon RDS-Benutzerkonto auf die Zieldatenbank zu und verwenden Sie den Namen der Verbindungszeichen folge in der `tnsnames.ora` Datei, die die Amazon RDS for Oracle Database enthält`tns-entry` . Bei Bedarf können Sie eine Remap-Option hinzufügen, um die Datendumpdatei in einen anderen Tablespace oder unter einem anderen Schemanamen zu importieren. Verwenden Sie den folgenden Code, um den Import zu starten: `impdp admin@orardsdb directory=DMS_TARGET_PUMP_DIR logfile=import.log dumpfile=EXPORT_DMS_DATA.DMP` Um einen erfolgreichen Import sicherzustellen, überprüfen	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie die Import-Protokolldatei auf Fehler und überprüfen Sie Details wie Objektanzahl, Zeilenanzahl und ungültige Objekte. Wenn ungültige Objekte vorhanden sind, kompilieren Sie sie erneut. Vergleichen Sie außerdem die Quell- und Zieldatenbankobjekte, um sicherzustellen, dass sie übereinstimmen.	

Stellen Sie eine AWS-DMS-Replikationsinstanz mit den Quell- und Zielendpunkten bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Vorlage für herunter.	Laden Sie die AWS-Vorlage CloudFormation DMS_Instance.yaml herunter, um die AWS DMS-Replikationsinstanz und ihre Quell- und Zielendpunkte bereitzustellen.	Cloud-Administrator, DBA
Starten Sie die Stack-Erstellung.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudFormation AWS-Konsole unter https://console.aws.amazon.com/cloudformation. 2. Wählen Sie Stack erstellen aus. 3. Wählen Sie unter Vorlage angeben die Option	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Vorlagendatei hochladen aus. 4. Wählen Sie Datei auswählen. 5. Wählen Sie die `DMS_instance.yaml` Datei aus. 6. Wählen Sie Weiter aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie die Parameter an.	1. Geben Sie unter Stack-Name Ihren Stack-Namen ein. 2. Geben Sie für AWS DMS-Instanzparameter die folgenden Parameter ein: • DMSInstanceTyp — Wählen Sie die erforderliche Instanz für die AWS DMS-Replikationsinstanz, basierend auf Ihren Geschäftsanforderungen. • DMSStorageGröße — Geben Sie die Speichergröße für die AWS DMS-Instance ein, basierend auf der Größe Ihrer Migration. 3. Geben Sie für Source Oracle Database Configuration die folgenden Parameter ein: • SourceOracleEndpointID — Der Name des Oracle-Quelldatenbankservers • SourceOracleDatabaseName— Der Dienstname oder die Sitzungs-ID (SID) der Quelldatenbank, sofern zutreffend • SourceOracleUserName— Der Benutzername der Quelldatenbank	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(die Standardeinstellung ist`system`) • SourceOracleDBPassword— Das Passwort des Benutzernamens der Quelldatenbank • SourceOracleDBPort— Der Port der Quelldatenbank 4. Geben Sie für Target RDS for Oracle Database Configuration die folgenden Parameter ein: • Target RDSOracle EndpointID — Der Ziel-RDS-Datenbank-Endpunkt • Ziel RDSOracle DatabaseName — Der Name der RDS-Zieldatenbank • Ziel RSOracle UserName — Der RDS-Zielbenutzername • Ziel RDSOracle DBPassword — Das Ziel-RDS-Passwort • TargetOracleDBPort— Der Ziel-RDS-Datenbankport 5. Geben Sie für die Konfiguration von VPC, Subnetz	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und Sicherheitsgruppe die folgenden Parameter ein: • VPCID — Die VPC für die Replikationsinstanz • VPCSecurityGroupId— Die VPC-Sicherheitsgruppe für die Replikationsinstanz • DMSSubnet1— Das Subnetz für Availability Zone 1 • DMSSubnet2— Das Subnetz für Availability Zone 2 6. Wählen Sie Weiter aus.	
Erstellen Sie den Stack.	1. Geben Sie auf der Seite „Stack-Optionen konfigurieren“ für Tags beliebige optionale Werte ein. 2. Wählen Sie Weiter aus. 3. Überprüfen Sie auf der Seite „Überprüfen“ die Details und wählen Sie dann Senden aus. Die Bereitstellung sollte in etwa 5—10 Minuten abgeschlossen sein. Es ist abgeschlossen, wenn auf der Seite AWS CloudFormation Stacks CREATE_COMPLETE angezeigt wird.	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Endpunkte ein.	1. Öffnen Sie die AWS DMS-Konsole in https://console.aws.amazon.com/dms/v2/. 2. Wählen Sie für Ressourcenmanagement die Option Replication Instances aus und überprüfen Sie dann die Replikations-Instances. 3. Wählen Sie für Ressourcenmanagement die Option Endpoints aus, und überprüfen Sie dann die Endpoints.	Cloud-Administrator, DBA
Testen Sie die Konnektivität.	Nachdem der Quell- und der Zielendpunkt den Status Aktiv angezeigt haben, testen Sie die Konnektivität. Wählen Sie für jeden Endpunkt (Quell- und Zielpunkt) die Option Test ausführen aus, um sicherzustellen, dass der Status als erfolgreich angezeigt wird.	Cloud-Administrator, DBA

Erstellen Sie eine AWS DMS-Replikationsaufgabe für die Live-Replikation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Replikationsaufgabe.	Erstellen Sie die AWS DMS-Replikationsaufgabe mithilfe der folgenden Schritte:	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Öffnen Sie die AWS DMS-Konsole in https://console.aws.amazon.com/dms/v2/. 2. Wählen Sie im Navigationsbereich unter Daten migrieren die Option Datenbankmigrationsaufgabe aus. 3. Geben Sie im Feld Aufgabenkonfiguration für Task-ID Ihre Task-ID ein. 4. Wählen Sie für Replikationsinstanz die DMS-Replikationsinstanz aus, die Sie erstellt haben. 5. Wählen Sie für Quelldatenbank-Endpunkt Ihren Quellendpunkt aus. 6. Wählen Sie als Zieldatenbank-Endpunkt Ihre Amazon RDS for Oracle Oracle-Zieldatenbank aus. 7. Wählen Sie als Migrationstyp die Option Nur Datenänderungen replizieren aus. Wenn Sie eine Meldung erhalten, dass die zusätzliche Protokollierung aktiviert werden muss, folgen Sie den Anweisungen im Abschnitt Problembehandlung.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Wählen Sie im Feld Aufgabeneinstellungen die Option Protokollsequenznummer angeben aus. 9. Geben Sie als Systemänderungsnummer die Oracle-Datenbank-SCN ein, die Sie aus der Oracle-Quelldatenbank generiert haben. 10. Wählen Sie Validierung aktivieren. 11. Wählen Sie „ CloudWatch Protokolle aktivieren“. Wenn Sie diese Funktion aktivieren, können Sie die Daten und CloudWatchAmazon-Protokolle validieren, um die Protokolle der AWS DMS-Replikationsinstanz zu überprüfen. 12. Gehen Sie unter Auswahlregeln wie folgt vor: • Wählen Sie unter Schema die Option Schema eingeben aus. • Geben Sie als Schemaname den Namen des JDE-Schemas ein (zum Beispiel: DV920). • Geben Sie als Tabellenname% ein.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wählen Sie für Aktion die Option Include aus. 13. Wählen Sie Create task aus. Nachdem Sie die Aufgabe erstellt haben, migriert AWS DMS laufende Änderungen zur Amazon RDS for Oracle Oracle-Datenbank-Instance aus der SCN, die Sie im CDC-Startmodus bereitgestellt haben. Sie können die Migration auch überprüfen, indem Sie die Protokolle überprüfen. CloudWatch	
Wiederholen Sie die Replizierungsaufgabe.	Wiederholen Sie die vorherigen Schritte, um Replikationsaufgaben für andere JD Edwards-Schemas zu erstellen, die Teil der Migration sind.	Cloud-Administrator, DBA, JDE-CNC-Administrator

Überprüfen Sie das Datenbankschema auf der Amazon RDS for Oracle Oracle-Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie die Datenübertragung.	Nachdem die AWS DMS-Aufgabe gestartet wurde, können Sie auf der Seite Aufgaben auf der Registerkarte Tabellenstatistiken nachsehen, welche	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Änderungen an den Daten vorgenommen wurden. Sie können den Status der laufenden Replikation in der Konsole auf der Seite mit den Aufgaben zur Datenbank migration überwachen. Weitere Informationen finden Sie unter AWS DMS-Daten validierung.	

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beenden Sie die Replikation.	Brechen Sie den Replikati onsvorgang ab und beenden Sie die Quellanwendungsdie nste.	Cloud-Administrator, DBA
Starten Sie die JD Edwards-A nwendung.	Starten Sie die Präsentations- und Logik-Tier-Zielanwendung von JD Edwards auf AWS und leiten Sie sie an die Amazon RDS for Oracle Oracle-Da tenbank weiter. Wenn Sie auf die Anwendung zugreifen, sollten Sie feststell en, dass jetzt alle Verbindun gen mit der Amazon RDS for Oracle Oracle-Datenbank hergestellt sind.	DBA, JDE-CNC-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schalten Sie die Quelldatenbank aus.	Nachdem Sie bestätigt haben, dass keine Verbindungen mehr bestehen, können Sie die Quelldatenbank ausschalten.	DBA

Fehlerbehebung

Problem	Lösung

Sie erhalten eine Warnmeldung, um die zusätzliche Protokollierung in der Quelldatenbank für die laufende Replikation zu aktivieren	Geben Sie die folgenden Befehle ein, um die zusätzliche Protokollierung zu aktivieren:
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (ALL) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (FOREIGN KEY) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;`

In AWS DMS ist die zusätzliche Protokollierung deaktiviert.	Die zusätzliche Protokollierung ist in AWS DMS standardmäßig deaktiviert. Gehen Sie wie folgt vor, um es für einen Oracle-Quellendpunkt zu aktivieren: 1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS DMS-Konsole in Version 2/ https://console.aws.amazon.com/dms/. 2. Wählen Sie Endpunkte aus.

Problem	Lösung
	3. Wählen Sie den Oracle-Quellendpunkt, dem Sie die zusätzliche Protokollierung hinzufüge n möchten. 4. Wählen Sie Ändern aus. 5. Wählen Sie Erweitert aus und fügen Sie dann den folgenden Code im Textfeld Extra Verbindungsattribute hinzu: `addSupplementalLogging=Y` 6. Wählen Sie Ändern aus.

Die zusätzliche Protokollierung ist auf CDB-Ebene nicht aktiviert.	1. Geben Sie diesen Befehl ein:
	`SQL> alter session set container = CDB$ROOT;`
	`Session altered.`
	2. Wiederholen Sie die Schritte, um die zusätzliche Protokollierung zu aktivieren.

Sie erhalten die folgende Fehlermeldung: „Der Testendpunkt ist fehlgeschlagen: Anwendung sstatus: 1020912, Anwendungsnachricht: LogMiner wird in der Oracle PDB-Umgebung nicht unterstützt. Die Endpunktinitialisierung ist fehlgeschlagen.“	Wenn Sie auf diese Fehlermeldung stoßen, können Sie stattdessen Binary Reader verwenden. LogMiner Fügen Sie unter Endpunkteinstellungen diese Zeile zu den zusätzlichen Verbindungsattribu ten für Ihre Quelldatenbank hinzu: `useLogMinerReader=N;useBfile=Y;`

Zugehörige Ressourcen

- Erste Schritte mit AWS Database Migration Service
- Bewährte Methoden für den AWS Database Migration Service

- Migration von Oracle-Datenbanken in die AWS-Cloud
- Referenz zum Ressourcentyp des AWS Database Migration Service für AWS CloudFormation
- Verwalten Sie Ihre AWS-DMS-Endpunkt-Anmeldeinformationen mit AWS Secrets Manager
- Fehlerbehebung bei Migrationsaufgaben im AWS Database Migration Service
- Bewährte Methoden für den AWS Database Migration Service

Zusätzliche Informationen

Dateien mit Amazon S3 übertragen

Um die Dateien auf Amazon S3 zu übertragen, können Sie die AWS-CLI oder die Amazon S3 S3-Konsole verwenden. Nachdem Sie die Dateien zu Amazon S3 übertragen haben, können Sie die Amazon RDS for Oracle Oracle-Instance verwenden, um die Data Pump-Dateien aus Amazon S3 zu importieren.

Wenn Sie die Dump-Datei mithilfe der Amazon S3 S3-Integration als alternative Methode übertragen möchten, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen S3-Bucket.
2. Exportieren Sie die Daten mit Oracle Data Pump aus der Quelldatenbank.
3. Laden Sie die Data Pump-Dateien in den S3-Bucket hoch.
4. Laden Sie die Data Pump-Dateien aus dem S3-Bucket in die Amazon RDS for Oracle Oracle-Zieldatenbank herunter.
5. Führen Sie den Import mithilfe der Data Pump-Dateien durch.

> **Note**
>
> Um große Datendateien zwischen S3- und RDS-Instances zu übertragen, empfehlen wir Ihnen, die Amazon S3 Transfer Acceleration Acceleration-Funktion zu verwenden.

Migrieren Sie eine PeopleSoft Oracle-Datenbank mithilfe von AWS DMS zu AWS

Erstellt von sampath kathirvel (AWS)

Übersicht

Oracle PeopleSoft ist eine ERP-Lösung (Enterprise Resource Planning) für unternehmensweite Prozesse. PeopleSoft hat eine dreistufige Architektur: Client, Anwendung und Datenbank. PeopleSoft kann auf Amazon Relational Database Service (Amazon RDS) ausgeführt werden.

Wenn Sie Ihre Oracle-Datenbank zu Amazon RDS migrieren, kann Amazon Web Services (AWS) Backup-Aufgaben und Hochverfügbarkeit übernehmen, sodass Sie sich auf die Wartung Ihrer PeopleSoft Anwendung und ihrer Funktionalität konzentrieren können. Eine umfassende Liste der wichtigsten Faktoren, die während des Migrationsprozesses zu berücksichtigen sind, finden Sie unter Strategien zur Oracle-Datenbankmigration in AWS Prescriptive Guidance.

Dieses Muster bietet eine Lösung für die Migration Ihrer lokalen Oracle-Datenbanken zu Amazon RDS for Oracle mithilfe von Oracle Data Pump mit AWS Database Migration Service (AWS DMS) und seiner Change Data Capture (CDC) -Funktion.

Bei der Migration kritischer ERP-Anwendungen wie Oracle PeopleSoft ist die Minimierung der Ausfallzeiten von entscheidender Bedeutung. AWS DMS minimiert Ausfallzeiten, indem es sowohl Volllast- als auch kontinuierliche Replikation von der Quelldatenbank zur Zieldatenbank unterstützt. AWS DMS bietet außerdem eine Überwachung und Protokollierung der Migration in Echtzeit, sodass Sie Probleme, die zu Ausfallzeiten führen könnten, identifizieren und lösen können.

Wenn Sie Änderungen mit AWS DMS replizieren, müssen Sie eine Uhrzeit oder eine Systemänderungsnummer (SCN) als Ausgangspunkt angeben, damit AWS DMS Änderungen aus den Datenbankprotokollen lesen kann. Es ist wichtig, diese Protokolle für einen bestimmten Zeitraum auf dem Server zugänglich zu halten, um sicherzustellen, dass AWS DMS Zugriff auf diese Änderungen hat.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Bereitgestellte Amazon RDS for Oracle Oracle-Datenbank in Ihrer AWS-Cloud-Umgebung als Zieldatenbank.
- Eine PeopleSoft Oracle-Datenbank, die lokal oder auf Amazon Elastic Compute Cloud (Amazon EC2) in der AWS-Cloud ausgeführt wird.

> **Note**
>
> Dieses Muster ist für die Migration von lokalen Systemen zu AWS konzipiert, wurde jedoch mithilfe von Oracle Database auf einer EC2 Amazon-Instance getestet. Für die Migration von einer lokalen Infrastruktur müssen Sie die entsprechende Netzwerkkonnektivität konfigurieren.

- Schemadetails. Bei der Migration einer PeopleSoft Oracle-Anwendung zu Amazon RDS for Oracle muss angegeben werden, welches Oracle-Datenbankschema (z. B.`SYSADM`) migriert werden soll. Bevor Sie mit dem Migrationsprozess beginnen, sollten Sie die folgenden Informationen über das Schema sammeln:
  - Größe
  - Die Anzahl der Objekte pro Objekttyp
  - Die Anzahl der ungültigen Objekte.

  Diese Informationen helfen beim Migrationsprozess.

Einschränkungen

- Dieses Szenario wurde nur mit der PeopleSoft DEMO-Datenbank getestet. Es wurde nicht mit einem großen Datensatz getestet.

Architektur

Das folgende Diagramm zeigt eine Instance, auf der eine Oracle-Datenbank als Quelldatenbank und eine Amazon RDS for Oracle Oracle-Datenbank als Zieldatenbank ausgeführt wird. Die Daten werden mit Oracle Data Pump aus der Oracle-Quelldatenbank in die Amazon RDS for Oracle Oracle-Zieldatenbank exportiert und importiert und für CDC-Änderungen mit AWS DMS repliziert.

1. Im ersten Schritt werden Daten mithilfe von Oracle Data Pump aus der Quelldatenbank extrahiert und anschließend an das Datenbankziel Amazon RDS for Oracle gesendet.
2. Daten werden von der Quelldatenbank an einen Quellendpunkt in AWS DMS gesendet.
3. Vom Quellendpunkt werden die Daten an die AWS DMS-Replikationsinstanz gesendet, wo die Replikationsaufgabe ausgeführt wird.

4. Nach Abschluss der Replikationsaufgabe werden die Daten an den Zielendpunkt in AWS DMS gesendet.
5. Vom Zielendpunkt werden die Daten an die Amazon RDS for Oracle Oracle-Datenbank-Instance gesendet.

Tools

AWS-Services

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS-Cloud oder zwischen Kombinationen von Cloud- und lokalen Setups.
- Amazon Relational Database Service (Amazon RDS) für Oracle unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Oracle-Datenbank in der AWS-Cloud.

Andere Dienste

- Mit Oracle Data Pump können Sie Daten und Metadaten mit hoher Geschwindigkeit von einer Datenbank in eine andere verschieben.

Bewährte Methoden

Migrating LOBs

Wenn Ihre Quelldatenbank große binäre Objekte (LOBs) enthält, die in die Zieldatenbank migriert werden müssen, bietet AWS DMS die folgenden Optionen:

- Vollständiger LOB-Modus — AWS DMS migriert alle Daten LOBs von der Quell- zur Zieldatenbank, unabhängig von ihrer Größe. Die Migration ist zwar langsamer, hat aber den Vorteil, dass die Daten nicht gekürzt werden. Um die Leistung zu verbessern, können Sie für die neue Replikationsinstanz eine separate Aufgabe erstellen, um die Tabellen zu migrieren, die mehr LOBs als ein paar Megabyte haben.
- Eingeschränkter LOB-Modus — Sie geben die maximale Größe der LOB-Spaltendaten an, sodass AWS DMS Ressourcen vorab zuweisen und diese in großen Mengen anwenden kann. LOBs Wenn die Größe der LOB-Spalten die in der Aufgabe angegebene Größe überschreitet, kürzt AWS DMS die Daten und sendet Warnungen an die AWS DMS-Protokolldatei. Sie können die Leistung verbessern, indem Sie den eingeschränkten LOB-Modus verwenden, wenn Ihre LOB-Datengröße innerhalb der begrenzten LOB-Größe liegt.

- Inline-LOB-Modus — Sie können migrieren, LOBs ohne die Daten zu kürzen oder die Leistung Ihrer Aufgabe zu beeinträchtigen, indem Sie sowohl kleine als auch große Daten replizieren. LOBs Geben Sie zunächst einen Wert für den InlineLobMaxSize Parameter an, der nur verfügbar ist, wenn der Full-LOB-Modus auf true gesetzt ist. Die AWS-DMS-Aufgabe überträgt die kleine LOBs Inline, was effizienter ist. Anschließend migriert AWS DMS die große Datei, LOBs indem es eine Suche aus der Quelltabelle durchführt. Der Inline-LOB-Modus funktioniert jedoch nur während der Volllastphase.

Generieren von Sequenzwerten

Beachten Sie, dass während der Erfassung von Änderungsdaten mit AWS DMS inkrementelle Sequenznummern nicht aus der Quelldatenbank repliziert werden. Um Diskrepanzen bei den Sequenzwerten zu vermeiden, müssen Sie für alle Sequenzen den neuesten Sequenzwert aus der Quelle generieren und ihn auf die Amazon RDS for Oracle Oracle-Zieldatenbank anwenden.

Verwaltung von Anmeldedaten

Um Ihre AWS-Ressourcen zu schützen, empfehlen wir, die Best Practices für AWS Identity and Access Management (IAM) zu befolgen.

Epen

Stellen Sie eine AWS-DMS-Replikationsinstanz mit den Quell- und Zielendpunkten bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Vorlage für herunter.	Laden Sie die CloudFormation AWS-Vorlage DMS_Instance.yaml herunter, um die AWS DMS-Replikationsinstanz und ihre Quell- und Zielendpunkte bereitzustellen.	Cloud-Administrator, DBA
Starten Sie die Stack-Erstellung.	1. Wählen Sie in der AWS-Managementkonsole CloudFormation. 2. Wählen Sie Stack erstellen aus.	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie unter Vorlage angeben die Option Vorlagendatei hochladen aus. 4. Wählen Sie Datei auswählen. 5. Wählen Sie die `DMS_instance.yaml` Datei aus. 6. Wählen Sie Weiter aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie die Parameter an.	1. Geben Sie unter Stack-Name Ihren Stack-Namen ein. 2. Geben Sie unter AWS DMS-Instanzparameter die folgenden Parameter ein: • DMSInstanceTyp — Wählen Sie die erforderliche Instanz für die AWS DMS-Replikationsinstanz, basierend auf Ihren Geschäftsanforderungen. • DMSStorageGröße — Geben Sie die Speichergröße für die AWS DMS-Instance ein, basierend auf der Größe Ihrer Migration. 3. Geben Sie unter Konfiguration der Oracle-Quelldatenbank die folgenden Parameter ein: • SourceOracleEndpointID — Der Name des Oracle-Quelldatenbankservers • SourceOracleDatabaseName— Der Dienstname oder die Sitzungs-ID (SID) der Quelldatenbank, sofern zutreffend • SourceOracleUserName— Der Benutzername der Quelldatenbank (die	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Standardeinstellung ist System) • SourceOracleDBPassword— Das Passwort des Benutzernamens der Quelldatenbank • SourceOracleDBPort— Der Port der Quelldatenbank 4. Geben Sie unter Target RDS for Oracle Database Configuration die folgenden Parameter ein: • Target RDSOracle EndpointID — Der Ziel-RDS-Datenbank-Endpunkt • Ziel RDSOracle DatabaseName — Der Name der RDS-Zieldatenbank • Ziel RSOracle UserName — Der Ziel-RDS-Benutzername • Ziel RDSOracle DBPassword — Das Ziel-RDS-Passwort • TargetOracleDBPort— Der Ziel-RDS-Datenbankport 5. Geben Sie unter VPC-, Subnetz- und Sicherhei	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	tsgruppenkonfiguration die folgenden Parameter ein: • VPCID — Die VPC für die Replikationsinstanz • VPCSecurityGroupId— Die VPC-Sicherheitsgru ppe für die Replikati onsinstanz • DMSSubnet1— Das Subnetz für Availability Zone 1 • DMSSubnet2— Das Subnetz für Availability Zone 2 6. Wählen Sie Weiter aus.	
Erstellen Sie den Stack.	1. Geben Sie auf der Seite „Stack-Optionen konfiguri eren“ für Tags beliebige optionale Werte ein. 2. Wählen Sie Weiter aus. 3. Überprüfen Sie auf der Seite „Überprüfen“ die Details und wählen Sie dann Senden aus. Die Bereitstellung sollte in etwa 5—10 Minuten abgeschlossen sein. Es ist abgeschlossen, wenn auf der Seite AWS CloudFormation Stacks CREATE_COMPLETE angezeigt wird.	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Endpunkte ein.	1. Wählen Sie in der AWS-Managementkonsole Database Migration Services aus. 2. Wählen Sie unter Ressourcenmanagement die Option Replication instances aus. 3. Wählen Sie unter Ressourcenverwaltung die Option Endpoints aus.	Cloud-Administrator, DBA
Testen Sie die Konnektivität.	Nachdem der Quell- und der Zielendpunkt den Status Aktiv angezeigt haben, testen Sie die Konnektivität. Wählen Sie für jeden Endpunkt (Quell- und Zielpunkt) die Option Test ausführen aus, um sicherzustellen, dass der Status als erfolgreich angezeigt wird.	Cloud-Administrator, DBA

Exportieren Sie das PeopleSoft Schema mithilfe von Oracle Data Pump aus der lokalen Oracle-Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie das SCN.	Wenn die Quelldatenbank aktiv ist und von der Anwendung verwendet wird, initiieren Sie den Datenexport mit Oracle Data Pump. Sie müssen zunächst eine System Change Number	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	(SCN) aus der Quelldate nbank generieren, um sowohl die Datenkonsistenz beim Export mit Oracle Data Pump als auch als Ausgangsp unkt für die Erfassung von Änderungsdaten in AWS DMS zu gewährleisten.
	
	Um die aktuelle SCN aus Ihrer Quelldatenbank zu generieren, geben Sie die folgende SQL-Anweisung ein.
	
	`SQL> select name from v $database;`
	`SQL> select name from v $database;`
	`NAME`
	`---------`
	`PSFTDMO`
	`SQL> SELECT current_s cn FROM v$database;`
	`CURRENT_SCN`
	`-----------`
	`23792008`
	
	Speichern Sie die generierte SCN, um sie beim Exportieren der Daten und zur Erstellung der AWS DMS-Replikationsau fgabe zu verwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Parameterdatei.	Um eine Parameterdatei für den Export des Schemas zu erstellen, können Sie den folgenden Code verwenden.
	`$ cat exp_datapmp.par`
	`userid=system/*******`
	`directory=DATA_P`
	`UMP_DIR`
	`logfile=export_dms_`
	`sample_user.log`
	`dumpfile=export_dms_`
	`sample_data_%U.dmp`
	`schemas=SYSADM`
	`flashback_scn=237920`
	`08`
	Note
	Sie können auch Ihren eigenen definiere n, `DATA_PUMP _DIR` indem Sie die folgenden Befehle verwenden, die Ihren Anforderungen entsprechen.
	`SQL> CREATE OR REPLACE`
	`DIRECTORY DATA_PUMP`
	`_DIR AS '/opt/oracle/`
	`product/19c/dbhome_1/`
	`dmsdump/';`
	`Directory created.`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SQL> GRANT READ, WRITE ON DIRECTORY DATA_PUMP _DIR TO system; Grant succeeded. SQL> SQL> SELECT owner, directory_name, directory_path FROM dba_directories WHERE directory_name='DA TA_PUMP_DIR'; OWNER DIRECTORY_NAME DIRECTORY_PATH ---------- ---------- ---------- ---------- ---------- ---------- SYS DATA_PUMP_DIR /opt/ oracle/product/19c/dbh ome_1/dmsdump/	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Exportieren Sie das Schema.	Verwenden Sie das `expdp` Hilfsprogramm, um den Export durchzuführen. `$ expdp parfile=e xp_datapmp.par .... Transferring the dump file with DBMS_FILE _TRANSFER to Target: . . exported "SYSADM". "PS_XML_TEMPLT_LNG" 6.320 KB 0 rows . . exported "SYSADM". "PS_XML_TEMPLT_LNK" 6.328 KB 0 rows . . exported "SYSADM". "PS_XML_XLATDEF_LNG" 6.320 KB 0 rows . . exported "SYSADM". "PS_XML_XLATITM_LNG" 7.171 KB 0 rows . . exported "SYSADM". "PS_XPQRYRUNCNTL" 7.601 KB 0 rows . . exported "SYSADM". "PS_XPQRYRUNPARM" 7.210 KB 0 rows . . exported "SYSADM". "PS_YE_AMOUNTS" 9.351 KB 0 rows . . exported "SYSADM". "PS_YE_DATA" 16.58 KB 0 rows . . exported "SYSADM". "PS_YE_EE" 6.75 KB 0 rows . . exported "SYSADM". "PS_YE_W2CP_AMOUNTS" 9.414 KB 0 rows`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	. . exported "SYSADM". "PS_YE_W2CP_DATA" 20.94 KB 0 rows . . exported "SYSADM". "PS_YE_W2C_AMOUNTS" 10.27 KB 0 rows . . exported "SYSADM". "PS_YE_W2C_DATA" 20.95 KB 0 rows . . exported "SYSADM". "PS_ZBD_JOBCODE_TBL" 14.60 KB 0 rows . . exported "SYSADM". "PTGRANTTBL" 5.468 KB 0 rows Master table "SYSTEM". "SYS_EXPORT_SCHEMA _01" successfully loaded/unloaded ** Dump file set for SYSTEM.SYS_EXPORT_ SCHEMA_01 is: /opt/oracle/pr oduct/19c/dbhome_1 /dmsdump/export_dm s_sample_data_01.dmp Job "SYSTEM"."SYS_EXPO RT_SCHEMA_01" successfully completed at Mon Dec 19 20:13:57 2022 elapsed 0 00:38:22	

Importieren Sie das PeopleSoft Schema mithilfe von Oracle Data Pump in die Amazon RDS for Oracle-Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Übertragen Sie die Dump-Datei auf die Zielinstanz.	Um Ihre Dateien mit zu übertragen`DBMS_FILE_TRANSFER`, müssen Sie einen Datenbank-Link von der Quelldatenbank zur Amazon RDS for Oracle Oracle-Instance erstellen. Nachdem die Verbindung hergestellt wurde, können Sie das Hilfsprogramm verwenden, um die Data Pump-Dateien direkt auf die RDS-Instance zu übertragen. Alternativ können Sie die Data Pump-Dateien an Amazon Simple Storage Service (Amazon S3) übertragen und sie dann in die Amazon RDS for Oracle Oracle-Instance importieren. Weitere Informationen zu dieser Option finden Sie im Abschnitt Zusätzliche Informationen. Um einen Datenbank-Link zu erstellen`ORARDSDB`, der eine Verbindung zum Amazon RDS-Master-Benutzer auf der Ziel-DB-Instance herstellt, führen Sie die folgenden Befehle in der Quelldatenbank aus.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`$sqlplus / as sysdba`
	`$ SQL> create database link orardsdb connect to admin identified by "*****" using '(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = testpsft.*******.us-west-2.rds.amazonaws.com)(PORT = 1521))(CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = orcl)))';`
	`Database link created.`	

Testen Sie den Datenbank-Link.	Testen Sie den Datenbank-Link, um sicherzustellen, dass Sie mit sqlplus eine Verbindung zur Amazon RDS for Oracle Oracle-Zieldatenbank herstellen können.
	`SQL>`
	`SQL> select name from v$database@orardsdb;`
	`NAME`
	`---------`
	`ORCL`
	`SQL>`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Übertragen Sie die Dump-Datei in die Zieldatenbank.	Um die Dump-Datei in die Amazon RDS for Oracle Oracle-Datenbank zu kopieren, können Sie entweder das `DATA_PUMP_DIR` Standardverzeichnis verwenden oder mit dem folgenden Code Ihr eigenes Verzeichnis erstellen.
	`exec rdsadmin.rdsadmin_util.create_directory(p_directory_name => 'TARGET_PUMP_DIR');`
	Das folgende Skript kopiert eine `export_dms_sample_data_01.dmp` aus der Quell-Instance benannte Dump-Datei mithilfe des angegebenen Datenbank-Links in eine Amazon RDS for Oracle Oracle-Zieldatenbank. `orardsdb`
	`$ sqlplus / as sysdba`
	`SQL>`
	`BEGIN`
	`DBMS_FILE_TRANSFER.PUT_FILE(`
	`source_directory_object => 'DATA_PUMP_DIR',`
	`source_file_name => 'export_dms_sample_data_01.dmp',`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`destination_directory _object => 'TARGET_P UMP_DIR'', destination_file_name => 'export_dms_sample _data_01.dmp', destination_database => 'orardsdb' ); END; / PL/SQL procedure successfully completed .`	
Listet die Dump-Datei in der Zieldatenbank auf.	Nachdem das PL/SQL-Ve rfahren abgeschlossen ist, können Sie die Datendump -Datei in der Amazon RDS for Oracle Oracle-Datenbank auflisten, indem Sie den folgenden Code verwenden. `SQL> select * from table (rdsadmin.rds_file _util.listdir(p_di rectory => 'TARGET_P UMP_DIR'));`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initiieren Sie den Import in der Zieldatenbank.	Bevor Sie den Importvorgang starten, richten Sie die Rollen, Schemas und Tablespaces in der Amazon RDS for Oracle Oracle-Zieldatenbank mithilfe der Datendumpdatei ein. Um den Import durchzuführen, greifen Sie mit dem Amazon RDS-Master-Benutzerkonto auf die Zieldatenbank zu und verwenden Sie den Namen der Verbindungszeichen folge in der `tnsnames.ora` Datei, die die Amazon RDS for Oracle Database enthält`tns-entry` . Bei Bedarf können Sie eine Remap-Option hinzufügen, um die Datendumpdatei in einen anderen Tablespace oder unter einem anderen Schemanamen zu importieren. Verwenden Sie den folgenden Code, um den Import zu starten. `impdp admin@orardsdb directory=TARGET_PUMP_DIR logfile=import.log dumpfile=export_dms_sample_data_01.dmp`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Um einen erfolgreichen Import sicherzustellen, überprüfen Sie die Import-Protokolldatei auf Fehler und überprüfen Sie Details wie Objektanzahl, Zeilenanzahl und ungültige Objekte. Wenn ungültige Objekte vorhanden sind, kompilieren Sie sie erneut. Vergleichen Sie außerdem die Quell- und Zieldatenbankobjekte, um sicherzustellen, dass sie übereinstimmen.	

Erstellen Sie eine AWS DMS-Replikationsaufgabe mithilfe von CDC, um die Live-Replikation durchzuführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Replikationsaufgabe.	Erstellen Sie die AWS DMS-Replikationsaufgabe mithilfe der folgenden Schritte: 1. Wählen Sie in der AWS DMS-Konsole unter Konvertierung und Migration die Option Datenbankmigrationsaufgabe aus. 2. Geben Sie unter Aufgabenkonfiguration für Aufgaben-ID Ihre Aufgaben-ID ein. 3. Wählen Sie für Replikationsinstanz die DMS-Repli	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	kationsinstanz aus, die Sie erstellt haben. 4. Wählen Sie für Quelldatenbank-Endpunkt Ihren Quellendpunkt aus. 5. Wählen Sie als Zieldatenbank-Endpunkt Ihre Amazon RDS for Oracle Oracle-Zieldatenbank aus. 6. Wählen Sie als Migrationstyp die Option Nur Datenänderungen replizieren aus. Wenn Sie eine Meldung erhalten, dass die zusätzliche Protokollierung aktiviert werden muss, folgen Sie den Anweisungen im Abschnitt Zusätzliche Informationen. 7. Wählen Sie unter Taskeinstellungen die Option Protokollsequenznummer angeben aus. 8. Geben Sie als Systemänderungsnummer die Oracle-Datenbank-SCN ein, die Sie aus der Oracle-Quelldatenbank generiert haben. 9. Wählen Sie Validierung aktivieren. 10. Wählen Sie „ CloudWatch Protokolle aktivieren“.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wenn Sie diese Funktion aktivieren, können Sie die Daten und CloudWatchAmazon-Protokolle validieren, um die Protokolle der AWS DMS-Replikationsinstanz zu überprüfen. 11. Gehen Sie unter Auswahlregeln wie folgt vor: • Wählen Sie unter Schema die Option Schema eingeben aus. • Geben Sie als Schemaname SYSADM ein. • Geben Sie als Tabellenname% ein. • Wählen Sie für Aktion die Option Include aus. 12. Gehen Sie unter Transformationsregeln wie folgt vor: • Wählen Sie für Target die Option Tabelle aus. • Wählen Sie unter Schemaname die Option Schema eingeben aus. • Geben Sie als Schemaname SYSADM ein. • Wählen Sie für Aktion die Option Umbenennen in.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	13. Wählen Sie Create task aus. Nachdem Sie die Aufgabe erstellt haben, migriert sie das CDC von der SCN, die Sie im CDC-Startmodus bereitgestellt haben, zur Amazon RDS for Oracle Oracle-Datenbank-Instance. Sie können dies auch überprüfen, indem Sie die Protokolle überprüfen. CloudWatch	

Überprüfen Sie das Datenbankschema auf der Amazon RDS for Oracle Oracle-Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie die Datenübertragung.	Nachdem die AWS DMS-Aufgabe gestartet wurde, können Sie auf der Seite Aufgaben auf der Registerkarte Tabellenstatistiken nachsehen, welche Änderungen an den Daten vorgenommen wurden. Sie können den Status der laufenden Replikation in der Konsole auf der Seite mit den Aufgaben zur Datenbankmigration überwachen.	Cloud-Administrator, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter AWS DMS-Daten validierung.	

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beenden Sie die Replikation.	Brechen Sie den Replikationsvorgang ab und halten Sie die Dienste der Quellanwendung an.	Cloud-Administrator, DBA
Starten Sie die PeopleSoft mittlere Stufe.	Starten Sie die PeopleSoft Middle-Tier-Zielanwendung in AWS und leiten Sie sie an die kürzlich migrierte Amazon RDS for Oracle Oracle-Datenbank weiter. Wenn Sie auf die Anwendung zugreifen, sollten Sie feststellen, dass jetzt alle App-Verbindungen mit der Amazon RDS for Oracle Oracle-Datenbank hergestellt sind.	DBA, Administrator PeopleSoft
Schalten Sie die Quelldatenbank aus.	Nachdem Sie bestätigt haben, dass keine Verbindungen mehr zur Quelldatenbank bestehen, kann sie ausgeschaltet werden.	DBA

Zugehörige Ressourcen

- Erste Schritte mit AWS Database Migration Service
- Bewährte Methoden für den AWS Database Migration Service
- Migration von Oracle-Datenbanken in die AWS-Cloud

Zusätzliche Informationen

Dateien mit Amazon S3 übertragen

Um die Dateien auf Amazon S3 zu übertragen, können Sie die AWS-CLI oder die Amazon S3 S3-Konsole verwenden. Nachdem Sie die Dateien zu Amazon S3 übertragen haben, können Sie die Amazon RDS for Oracle Oracle-Instance verwenden, um die Data Pump-Dateien aus Amazon S3 zu importieren.

Wenn Sie die Dump-Datei mithilfe der Amazon S3 S3-Integration als alternative Methode übertragen möchten, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen S3-Bucket.
2. Exportieren Sie die Daten mit Oracle Data Pump aus der Quelldatenbank.
3. Laden Sie die Data Pump-Dateien in den S3-Bucket hoch.
4. Laden Sie die Data Pump-Dateien aus dem S3-Bucket in die Amazon RDS for Oracle Oracle-Zieldatenbank herunter.
5. Führen Sie den Import mithilfe der Data Pump-Dateien durch.

> **Note**
>
> Um große Datendateien zwischen S3- und RDS-Instances zu übertragen, wird empfohlen, die Amazon S3 Transfer Acceleration Acceleration-Funktion zu verwenden.

Aktivieren Sie die zusätzliche Protokollierung

Wenn Sie eine Warnmeldung erhalten, um die zusätzliche Protokollierung in der Quelldatenbank für die laufende Replikation zu aktivieren, gehen Sie wie folgt vor.

```
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (ALL) COLUMNS;
```

```
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (FOREIGN KEY) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;
```

Migrieren Sie eine lokale MySQL-Datenbank zu Amazon RDS for MySQL

Erstellt von Lorenzo Mota (AWS)

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer lokalen MySQL-Datenbank zu Amazon Relational Database Service (Amazon RDS) for MySQL. Das Muster beschreibt die Verwendung von AWS Database Migration Service (AWS DMS) oder nativen MySQL-Tools wie mysqldump für eine vollständige Datenbankmigration. Dieses Muster richtet sich in erster Linie an DBAs Lösungsarchitekten. Es kann in kleinen oder großen Projekten als Testverfahren (wir empfehlen mindestens einen Testzyklus) oder als abschließendes Migrationsverfahren verwendet werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS Konto
- Eine MySQL-Quelldatenbank in einem lokalen Rechenzentrum

Einschränkungen

- Größenbeschränkung der Datenbank: 64 TB

Produktversionen

- MySQL-Versionen 5.5, 5.6, 5.7, 8.0. Die aktuelle Liste der unterstützten Versionen finden Sie in der AWS Dokumentation unter MySQL on Amazon RDS. Wenn Sie verwenden AWS DMS, siehe auch Verwenden einer MySQL-kompatiblen Datenbank als Ziel AWS DMS für MySQL-Versionen, die derzeit von unterstützt werden. AWS DMS

Architektur

Quelltechnologie-Stack

- Eine lokale MySQL-Datenbank

Zieltechnologie-Stack

- Eine Amazon RDS-DB-Instance, auf der MySQL ausgeführt wird

Zielarchitektur

Das folgende Diagramm zeigt die Zielimplementierung von Amazon RDS for MySQL nach der Migration.

AWS Architektur der Datenmigration

Verwenden von AWS DMS:

Das folgende Diagramm zeigt die Datenmigrationsarchitektur, wenn Sie bis AWS DMS zur Übernahme vollständige und inkrementelle Änderungen senden. Die Netzwerkverbindung von lokal zu AWS hängt von Ihren Anforderungen ab und ist für dieses Muster nicht geeignet.

Verwendung nativer MySQL-Tools:

Das folgende Diagramm zeigt die Datenmigrationsarchitektur, wenn Sie native MySQL-Tools verwenden. Die Export-Dumpdateien werden in Amazon Simple Storage Service (Amazon S3) kopiert und AWS vor der Übernahme in die Amazon RDS for MySQL MySQL-Datenbank importiert. Die Netzwerkverbindung von lokal zu AWS hängt von Ihren Anforderungen ab und fällt nicht in den Anwendungsbereich dieses Musters.

Hinweise:

- Abhängig von den Anforderungen an Ausfallzeiten und der Größe der Datenbank minimiert die Verwendung AWS DMS oder ein CDC-Tool (Change Data Capture) die Umstellungszeit. AWS DMS kann dazu beitragen, die Umstellungszeit auf das neue Ziel auf ein Minimum zu reduzieren (in der Regel Minuten). Eine Offline-Strategie mit mysqldump kann ausreichen, wenn die Größe der Datenbank und die Netzwerklatenz ein kurzes Zeitfenster zulassen. (Wir empfehlen, zu testen, um eine ungefähre Zeit zu erhalten.)
- In der Regel AWS DMS erfordert eine CDC-Strategie mehr Überwachung und Komplexität als Offline-Optionen.

Tools

- AWS services:AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern auf die AWS Cloud Festplatte oder zwischen Kombinationen von Cloud- und lokalen Konfigurationen. Hinweise zu MySQL-Quell- und Zieldatenbanken, die von unterstützt werden AWS DMS, finden Sie unter MySQL-kompatible Datenbanken migrieren zu. AWS Wenn Ihre Quelldatenbank von nicht unterstützt wird AWS DMS, müssen Sie eine andere Methode für die Migration Ihrer Daten wählen.
- Systemeigene MySQL-Tools: mysqldump
- Tools von Drittanbietern: Percona XtraBackup

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Datenbankversionen.	Validieren Sie die Quell- und Zieldatenbankversionen.	DBA
Identifizieren Sie die Hardwareanforderungen.	Identifizieren Sie die Hardwareanforderungen für den Zielserver.	DBA, Systemadministrator
Identifizieren Sie die Speicheranforderungen.	Identifizieren Sie die Speicheranforderungen (wie Speichertyp und Kapazität) für die Zieldatenbank.	DBA, Systemadministrator
Wählen Sie den Instance-Typ aus.	Wählen Sie den Zielinstanztyp auf der Grundlage von Kapazität, Speicher- und Netzwerkfunktionen aus.	DBA, Systemadministrator
Identifizieren Sie die Anforderungen für den Netzwerkzugriff.	Identifizieren Sie die Sicherheitsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.	DBA, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie nicht unterstützte Objekte.	Identifizieren Sie nicht unterstützte Objekte (falls vorhanden) und ermitteln Sie den Migrationsaufwand.	DBA
Identifizieren Sie Abhängigkeiten.	Identifizieren Sie alle Abhängigkeiten von entfernten Datenbanken.	DBA
Ermitteln Sie die Strategie für die Anwendungsmigration.	Ermitteln Sie die Strategie für die Migration von Client-Anwendungen.	DBA, App-Besitzer, Systemadministrator

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC).	Konfigurieren Sie Routentabellen, Internet-Gateways, NAT-Gateways und Subnetze. Weitere Informationen finden Sie unter VPCs und Amazon RDS in der Amazon RDS-Dokumentation.	Systemadministrator
Erstellen Sie Sicherheitsgruppen.	Konfigurieren Sie IPs je nach Ihren Anforderungen Ports und CIDR-Bereiche oder spezifische. Der Standardport für MySQL ist 3306. Weitere Informationen finden Sie unter Steuern des Zugriffs mit Sicherheitsgruppen in der Amazon RDS-Dokumentation.	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren und starten Sie eine Amazon RDS for MySQL MySQL-DB-Instance.	Anweisungen finden Sie in der Amazon RDS-Dokumentation unter Erstellen einer Amazon RDS-DB-Instance. Suchen Sie nach unterstützten Versionen.	Systemadministrator

Daten migrieren – Option 1 (mit systemeigenen Tools)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie native MySQL-Tools oder Tools von Drittanbietern, um Datenbankobjekte und Daten zu migrieren.	Anweisungen finden Sie in der Dokumentation für MySQL-Tools wie mysqldump und Percona XtraBackup (für physische Migration). Weitere Informationen zu Optionen finden Sie im Blogbeitrag Migrationsoptionen für MySQL zu Amazon RDS for MySQL oder Amazon Aurora MySQL.	DBA

Daten migrieren – Option 2 (verwenden AWS DMS)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie Daten mit AWS DMS.	Anweisungen finden Sie in der AWS DMS Dokumentation.	DBA

Führen Sie vor der Umstellung vorläufige Aufgaben durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Korrigieren Sie Diskrepanzen bei der Anzahl der Objekte.	Sammelt Objektzahlen aus der Quelldatenbank und der neuen Zieldatenbank. Korrigier en Sie Diskrepanzen in der Zieldatenbank.	DBA
Überprüfen Sie die Abhängigk eiten.	Prüfen Sie, ob Abhängigkeiten (Links) zu und von anderen Datenbanken gültig sind und wie erwartet funktionieren.	DBA
Tests durchführen.	Wenn es sich um einen Testzyklus handelt, führen Sie Abfragetests durch, sammeln Sie Metriken und beheben Sie Probleme.	DBA

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wechseln Sie zur Zieldaten bank.	Stellen Sie die Client-An wendungen auf die neue Infrastruktur um.	DBA, App-Besitzer, Systemadministrator
Bieten Sie Unterstützung beim Testen an.	Bieten Sie Unterstützung für funktionale Anwendungstests.	DBA

Schließt das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ressourcen herunterfahren.	Fahren Sie die temporären AWS Ressourcen herunter, die Sie für die Migration erstellt haben.	DBA, Systemadministrator
Validieren Sie Projektdokumente.	Überprüfen und validieren Sie die Projektdokumente.	DBA, App-Besitzer, Systemadministrator
Sammeln Sie Metriken.	Erfassen Sie Kennzahlen wie die Zeit für die Migration, den Prozentsatz des manuellen Aufwands im Vergleich zum automatisierten Aufwand, Kosteneinsparungen usw.	DBA, App-Besitzer, Systemadministrator
Schließt das Projekt ab.	Schließen Sie das Projekt ab und geben Sie Feedback.	DBA, App-Besitzer, Systemadministrator
Nehmen Sie die Quelldatenbank außer Betrieb.	Wenn alle Migrations- und Umstellungsaufgaben abgeschlossen sind, nehmen Sie die lokale Datenbank außer Betrieb.	DBA, Systemadministrator

Zugehörige Ressourcen

Referenzen

- Migrationsstrategie für relationale Datenbanken
- AWS DMS website
- AWS DMS Dokumentation
- Dokumentation zu Amazon RDS
- Amazon-RDS-Preise

- Amazon VPC und Amazon RDS
- Amazon RDS Multi-AZ-Bereitstellungen
- Migrieren Sie lokale MySQL-Datenbanken mit Percona XtraBackup, Amazon EFS und Amazon S3 zu Aurora MySQL
- Amazon RDS-DB-Instance-Speicher

Tutorials

- Erste Schritte mit AWS DMS
- Erste Schritte mit Amazon RDS

Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Amazon RDS for SQL Server

Erstellt von Henrique Lobao (AWS), Jonathan Pereira Cruz (AWS) und Vishal Singh (AWS)

Übersicht

Dieses Muster bietet Anleitungen für die Migration von einer lokalen Microsoft SQL Server-Datenbank zu Amazon Relational Database Service (Amazon RDS) für SQL Server. Es beschreibt zwei Optionen für die Migration: die Verwendung von AWS Data Migration Service (AWS DMS) oder die Verwendung systemeigener Microsoft SQL Server-Tools wie Copy Database Wizard.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Microsoft SQL Server-Quelldatenbank in einem lokalen Rechenzentrum

Einschränkungen

- Größenbeschränkung für Datenbanken: 16 TB

Produktversionen

- SQL Server 2014-2019, Enterprise, Standard, Workgroup und Developer. Die aktuelle Liste der unterstützten Versionen und Funktionen finden Sie in der AWS-Dokumentation unter Microsoft SQL Server on Amazon RDS. Wenn Sie AWS DMS verwenden, finden Sie weitere Informationen unter Verwenden einer Microsoft SQL Server-Datenbank als Ziel für AWS DMS für SQL Server-Versionen, die von AWS DMS unterstützt werden.

Architektur

Quelltechnologie-Stack

- Eine lokale Microsoft SQL Server-Datenbank

Zieltechnologie-Stack

- Eine Amazon RDS for SQL Server Server-DB-Instance

Quell- und Zielarchitektur

Verwenden von AWS DMS:

Verwendung nativer SQL Server-Tools:

Tools

- AWS DMS unterstützt verschiedene Arten von Quell- und Zieldatenbanken. Einzelheiten finden Sie unter AWS DMS Step-by-Step Walkthroughs. Wenn AWS DMS die Quelldatenbank nicht unterstützt, wählen Sie eine andere Methode für die Migration der Daten.
- Zu den systemeigenen Microsoft SQL Server-Tools gehören Sicherung und Wiederherstellung, der Assistent zum Kopieren von Datenbanken sowie das Kopieren und Anfügen von Datenbanken.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversion und die Engine.		DBA
Identifizieren Sie die Hardwareanforderungen für die Zielserverinstanz.		DBA, Systemadministrator
Identifizieren Sie die Speicheranforderungen (Speichertyp und Kapazität).		DBA, Systemadministrator
Wählen Sie den richtigen Instanztyp auf der Grundlage		DBA, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
von Kapazität, Speicherf unktionen und Netzwerkf unktionen aus.		
Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerkzugriff für Quell- und Zieldatenbanken.		DBA, Systemadministrator
Identifizieren Sie die Strategie zur Anwendungsmigration.		DBA, Systemadministrator

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC).		Systemadministrator
Erstellen Sie Sicherhei tsgruppen.		Systemadministrator
Konfigurieren und starten Sie eine Amazon RDS-DB-In stance.		DBA, Systemadministrator

Daten migrieren — Option 1

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie native SQL Server-Tools oder Tools von Drittanbietern, um Datenbankobjekte und Daten zu migrieren.		DBA

Daten migrieren — Option 2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie Daten mit AWS DMS.		DBA

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Anwendungsmigration.		DBA, App-Besitzer, Systemadministrator

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung sclients auf die neue Infrastru ktur um.		DBA, Besitzer der App, Systemadministrator

Schließen Sie das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die temporären AWS-Ressourcen herunter.		DBA, Systemadministrator
Überprüfen und validieren Sie die Projektdokumente.		DBA, App-Besitzer, Systemadministrator
Erfassen Sie Kennzahlen wie die Zeit bis zur Migration , den Prozentsatz manueller		DBA, App-Besitzer, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aufgaben im Vergleich zu automatisierten Aufgaben und Kosteneinsparungen.		
Schließen Sie das Projekt ab und geben Sie Feedback.		DBA, App-Besitzer, Systemadministrator

Zugehörige Ressourcen

Referenzen

- Bereitstellung von Microsoft SQL Server auf Amazon Web Services
- AWS DMS-Webseite
- Amazon RDS-Preise
- Microsoft-Produkte auf AWS
- Microsoft-Lizenzierung auf AWS
- Microsoft SQL Server auf AWS
- Verwenden der Windows-Authentifizierung mit einer Microsoft SQL Server-DB-Instance
- Amazon RDS Multi-AZ-Bereitstellungen

Tutorials und Videos

- Erste Schritte mit AWS DMS
- Erste Schritte mit Amazon RDS
- AWS DMS (Video)
- Amazon RDS (Video)

Migrieren Sie Daten mithilfe von Rclone von Microsoft Azure Blob zu Amazon S3

Erstellt von Suhas Basavaraj (AWS), Aidan Keane (AWS) und Corey Lane (AWS)

Übersicht

Dieses Muster beschreibt, wie Rclone verwendet wird, um Daten vom Microsoft Azure Blob-Objektspeicher in einen Amazon Simple Storage Service (Amazon S3) -Bucket zu migrieren. Sie können dieses Muster verwenden, um eine einmalige Migration oder eine fortlaufende Synchronisation der Daten durchzuführen. Rclone ist ein in Go geschriebenes Befehlszeilenprogramm, das zum Verschieben von Daten zwischen verschiedenen Speichertechnologien von Cloud-Anbietern verwendet wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Daten, die im Azure Blob Container Service gespeichert sind

Architektur

Quelltechnologie-Stack

- Azure Blob-Speichercontainer

Zieltechnologie-Stack

- Amazon-S3-Bucket
- Linux-Instanz von Amazon Elastic Compute Cloud (Amazon EC2)

Architektur

Tools

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

- Rclone ist ein Open-Source-Befehlszeilenprogramm, das von rsync inspiriert wurde. Es wird zur Verwaltung von Dateien auf vielen Cloud-Speicherplattformen verwendet.

Bewährte Methoden

Beachten Sie bei der Migration von Daten von Azure zu Amazon S3 die folgenden Überlegungen, um unnötige Kosten oder langsame Übertragungsgeschwindigkeiten zu vermeiden:

- Erstellen Sie Ihre AWS-Infrastruktur in derselben geografischen Region wie das Azure-Speicherkonto und der Blob-Container, z. B. in der AWS-Region `us-east-1` (Nord-Virginia) und der Azure-Region. `East US`
- Vermeiden Sie nach Möglichkeit die Verwendung von NAT Gateway, da dadurch Datenübertragungsgebühren sowohl für die eingehende als auch für die ausgehende Bandbreite anfallen.
- Verwenden Sie einen VPC-Gateway-Endpunkt für Amazon S3, um die Leistung zu steigern.
- Erwägen Sie die Verwendung einer EC2 Instance auf Basis des AWS Graviton2 (ARM) -Prozessors, um im Vergleich zu Intel x86-Instances kostengünstiger und leistungsfähiger zu sein. Rclone ist stark querkompiliert und bietet eine vorkompilierte ARM-Binärdatei.

Epen

Bereiten Sie AWS- und Azure-Cloud-Ressourcen vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie einen S3-Ziel-Bucket vor.	Erstellen Sie einen neuen S3-Bucket in der entsprechenden AWS-Region oder wählen Sie einen vorhandenen Bucket als Ziel für die Daten, die Sie migrieren möchten.	AWS-Administrator
Erstellen Sie eine IAM-Instance-Rolle für Amazon EC2.	Erstellen Sie eine neue AWS Identity and Access Management (IAM) -Rolle für Amazon EC2. Diese Rolle gewährt Ihrer EC2 Instance	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Schreibzugriff auf den Ziel-S3-Bucket.	
Fügen Sie der IAM-Instanzrolle eine Richtlinie hinzu.	Verwenden Sie die IAM-Konsole oder die AWS-Befehlszeilenschnittstelle (AWS CLI), um eine Inline-Richtlinie für die EC2 Instance-Rolle zu erstellen, die Schreibzugriffsberechtigungen für den S3-Ziel-Bucket gewährt. Eine Beispielrichtlinie finden Sie im Abschnitt Zusätzliche Informationen.	AWS-Administrator
Starten Sie eine EC2 Instanz.	Starten Sie eine Amazon EC2 Linux-Instance, die für die Verwendung der neu erstellten IAM-Servicerolle konfiguriert ist. Diese Instanz benötigt außerdem Zugriff auf öffentliche Azure-API-Endpunkte über das Internet. **Note** Erwägen Sie die Verwendung von AWS Graviton-basierten EC2 Instances, um die Kosten zu senken. Rclone stellt ARM-kompilierte Binärdateien bereit.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Azure AD-Dienstprinzipal.	Verwenden Sie die Azure-CLI, um einen Azure Active Directory-Dienstprinzipal (Azure AD) zu erstellen , der schreibgeschützten Zugriff auf den Azure Blob-Quellspeichercontainer hat. Anweisungen finden Sie im Abschnitt Zusätzliche Informationen. Speichern Sie diese Anmeldeinformation en auf Ihrer EC2 Instance am Standort`~/azure-p rincipal.json` .	Cloud-Administrator, Azure

Installieren und konfigurieren Sie Rclone

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Downloaden und installieren Sie Rclone.	Laden Sie das Befehlsze ilenprogramm Rclone herunter und installieren Sie es. Installationsanweisungen finden Sie in der Rclone-In stallationsdokumentation.	Allgemein AWS, Cloud-Adm inistrator
Rclone konfigurieren.	Kopieren Sie die folgende `rclone.conf` Beispield atei. `AZStorage Account` Ersetzen Sie es durch Ihren Azure Storage-K ontonamen und `us-east-1` durch die AWS-Region, in der sich Ihr S3-Bucket befindet.	Allgemein AWS, Cloud-Adm inistrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Speichern Sie diese Datei an dem Speicherort `~/.config/rclone/rclone.conf` auf Ihrer EC2 Instance.
	
	`[AZStorageAccount]`
	`type = azureblob`
	`account = AZStorageAccount`
	`service_principal_file = azure-principal.json`
	
	`[s3]`
	`type = s3`
	`provider = AWS`
	`env_auth = true`
	`region = us-east-1`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Rclone-Konfiguration.	Um sicherzustellen, dass Rclone konfiguriert ist und die Berechtigungen ordnungsgemäß funktionieren, stellen Sie sicher, dass Rclone Ihre Konfigurationsdatei analysieren kann und dass auf Objekte in Ihrem Azure Blob-Container und S3-Bucket zugegriffen werden kann. Im Folgenden finden Sie beispielsweise Validierungsbefehle.
	• Listet die konfigurierten Fernbedienungen in der Konfigurationsdatei auf. Dadurch wird sichergestellt, dass Ihre Konfigurationsdatei korrekt analysiert wird. Überprüfen Sie die Ausgabe, um sicherzustellen, dass sie mit Ihrer `rclone.conf` Datei übereinstimmt.
	`rclone listremotes`
	`AZStorageAccount:`
	`s3:`
	• Listet die Azure Blob-Container im konfigurierten Konto auf. `AZStorageAccount` Ersetzen Sie es durch den Namen des Speicherkontos, den Sie in
		Allgemein AWS, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	der `rclone.conf` Datei verwendet haben.
	
	`rclone lsd AZStorage Account:`
	`2020-04-29 08:29:26 docs`
	
	• Listet die Dateien im Azure Blob-Container auf. Ersetzen Sie die Dokumente in diesem Befehl durch einen tatsächlichen Blob-Container-Namen in Ihrem Azure-Speicherkonto.
	
	`rclone ls AZStorage Account:docs`
	`824884 administrator-en.a4.pdf`
	
	• Listen Sie die Buckets in Ihrem AWS-Konto auf.
	
	`[root@ip-10-0-20-157 ~]# rclone lsd s3:`
	`2022-03-07 01:44:40 amzn-s3-demo-bucket1`
	`2022-03-07 01:45:16 amzn-s3-demo-bucket2`
	`2022-03-07 02:12:07 amzn-s3-demo-bucket3`
	
	• Listet die Dateien im S3-Bucket auf.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`[root@ip-10-0-20-157 ~]# rclone ls s3:amzn-s3-demo-bucket1`
	`template0.yaml`
	`template1.yaml`	

Migrieren Sie Daten mit Rclone

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Migrieren Sie Daten aus Ihren Containern.	Führen Sie den Befehl Rclone copy oder sync aus.
	
	Beispiel: Kopieren
	
	Dieser Befehl kopiert Daten aus dem Azure-Blob-Quellcontainer in den S3-Ziel-Bucket.
	
	`rclone copy AZStorageAccount:blob-container s3:amzn-s3-demo-bucket1`
	
	Beispiel: Sync
	
	Dieser Befehl synchronisiert Daten zwischen dem Azure-Blob-Quellcontainer und dem Ziel-S3-Bucket.
	
	`rclone sync AZStorageAccount:blob-conta`
		Allgemein AWS, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`iner s3:amzn-s3-demo-bucket1` **Important** Wenn Sie den Befehl sync verwenden, werden Daten, die nicht im Quellcontainer vorhanden sind, aus dem Ziel-S3-Bucket gelöscht.	
Synchronisieren Sie Ihre Container.	Führen Sie nach Abschluss der ersten Kopie den Befehl Rclone sync für die laufende Migration aus, sodass nur neue Dateien kopiert werden, die im S3-Ziel-Bucket fehlen.	Allgemein AWS, Cloud-Administrator
Stellen Sie sicher, dass die Daten erfolgreich migriert wurden.	Führen Sie die Befehle Rclone lsd und ls aus, um zu überprüfen, ob die Daten erfolgreich in den Ziel-S3-Bucket kopiert wurden.	Allgemein AWS, Cloud-Administrator

Zugehörige Ressourcen

- Amazon S3 S3-Benutzerhandbuch (AWS-Dokumentation)
- IAM-Rollen für Amazon EC2 (AWS-Dokumentation)
- Einen Microsoft Azure Blob-Container erstellen (Microsoft Azure-Dokumentation)
- Rclone-Befehle (Rclone-Dokumentation)

Zusätzliche Informationen

Beispiel für eine Rollenrichtlinie für Instanzen EC2

Diese Richtlinie gewährt Ihrer EC2 Instance Lese- und Schreibzugriff auf einen bestimmten Bucket in Ihrem Konto. Wenn Ihr Bucket einen vom Kunden verwalteten Schlüssel für die serverseitige Verschlüsselung verwendet, benötigt die Richtlinie möglicherweise zusätzlichen Zugriff auf AWS Key Management Service (AWS KMS).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
              "arn:aws:s3:::amzn-s3-demo-bucket/*",
              "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Einen schreibgeschützten Azure AD-Dienstprinzipal erstellen

Ein Azure-Dienstprinzipal ist eine Sicherheitsidentität, die von Kundenanwendungen, Diensten und Automatisierungstools für den Zugriff auf bestimmte Azure-Ressourcen verwendet wird. Stellen Sie sich das als Benutzeridentität (Login und Passwort oder Zertifikat) mit einer bestimmten Rolle und streng kontrollierten Zugriffsberechtigungen für Ihre Ressourcen vor. Gehen Sie wie folgt vor, um einen schreibgeschützten Dienstprinzipal zu erstellen, der die geringsten Rechte einhält und Daten in Azure vor versehentlichem Löschen schützt:

1. Melden Sie sich bei Ihrem Microsoft Azure-Cloud-Kontoportal an und starten Sie Cloud Shell in PowerShell oder verwenden Sie die Azure-Befehlszeilenschnittstelle (CLI) auf Ihrer Workstation.
2. Erstellen Sie einen Dienstprinzipal und konfigurieren Sie ihn mit schreibgeschütztem Zugriff auf Ihr Azure BLOB-Speicherkonto. Speichern Sie die JSON-Ausgabe dieses Befehls in einer lokalen Datei namens. `azure-principal.json` Die Datei wird auf Ihre EC2 Instanz hochgeladen. Ersetzen Sie die Platzhaltervariablen, die in geschweiften Klammern ({und}) angezeigt werden, durch Ihre Azure-Abonnement-ID, den Namen der Ressourcengruppe und den Namen des Speicherkontos.

```
az ad sp create-for-rbac `
--name AWS-Rclone-Reader `
--role "Storage Blob Data Reader" `
--scopes /subscriptions/{Subscription ID}/resourceGroups/{Resource Group Name}/
providers/Microsoft.Storage/storageAccounts/{Storage Account Name}
```

Migrieren Sie von Couchbase Server zu Couchbase Capella auf AWS

Erstellt von Battulga Purevragchaa (AWS), Mark Gamble und Saurabh Shanbhag (AWS)

Übersicht

Couchbase Capella ist eine vollständig verwaltete NoSQL-Datenbank als Service (DBaaS) für unternehmenskritische Anwendungen (z. B. Benutzerprofile oder Online-Kataloge und Inventarverwaltung). Couchbase Capella verwaltet Ihren DBaa S-Workload in einem von Couchbase verwalteten Amazon Web Services (AWS) -Konto. Capella macht es einfach, die Replikation mit mehreren Clustern, mehreren AWS-Regionen, Multicloud und Hybrid-Clouds über eine einzige Oberfläche auszuführen und zu verwalten.

Couchbase Capella hilft Ihnen dabei, Ihre Couchbase Server-Anwendungen sofort zu skalieren, sodass Sie innerhalb von Minuten Cluster mit mehreren Knoten erstellen können. Couchbase Capella unterstützt alle Couchbase Server-Funktionen, einschließlich SQL++, Volltextsuche, Eventing Service und Analytics Service. Außerdem entfällt die Notwendigkeit, Installationen, Upgrades, Backups und die allgemeine Datenbankwartung zu verwalten.

Dieses Muster beschreibt die Schritte und bewährten Methoden für die Migration einer selbstverwalteten Couchbase Server-Umgebung in die AWS-Cloud. Das Muster bietet einen wiederholbaren Prozess für die Migration von Daten und Indizes von Couchbase Serverclustern, die entweder vor Ort oder in der Cloud ausgeführt werden, zu Couchbase Capella. Mithilfe dieser Schritte können Sie Probleme bei der Migration vermeiden und den gesamten Migrationsprozess beschleunigen.

Dieses Muster bietet die folgenden zwei Migrationsoptionen:

- Option 1 ist geeignet, wenn Sie weniger als 50 Indizes migrieren müssen.
- Option 2 ist geeignet, wenn Sie mehr als 50 Indizes migrieren müssen.

Sie können auch Beispieldaten auf Ihrem selbst verwalteten Couchbase-Server einrichten, um sie zusammen mit dem Migrationsleitfaden zu befolgen.

Wenn Sie die Migrationsoption 2 wählen oder Bereiche oder Sammlungen verwenden, die nicht dem Standardwert entsprechen, müssen Sie die Beispielkonfigurationsdatei verwenden, die sich im Abschnitt Zusätzliche Informationen befindet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein vorhandenes kostenpflichtiges Couchbase Capella-Konto. Sie können auch ein Couchbase Capella-Konto auf AWS erstellen und die kostenlose Testversion von Couchbase Capella nutzen und dann auf ein kostenpflichtiges Konto upgraden, um Ihren Cluster für die Migration zu konfigurieren. Folgen Sie den Anweisungen unter Erste Schritte mit Couchbase Capella, um mit der Testversion zu beginnen.
- Eine bestehende, selbstverwaltete Couchbase Server-Umgebung, entweder vor Ort oder bei einem Cloud-Dienstanbieter bereitgestellt.
- Für Migrationsoption 2 Couchbase Shell und eine Konfigurationsdatei. Um die Konfigurationsdatei zu erstellen, können Sie die Beispieldatei verwenden, die sich im Abschnitt Zusätzliche Informationen befindet.
- Vertrautheit mit der Verwaltung von Couchbase Server und Couchbase Capella.
- Vertrautheit mit dem Öffnen von TCP-Ports und dem Ausführen von Befehlen in einer Befehlszeilenschnittstelle (CLI).

Für den Migrationsprozess sind außerdem die in der folgenden Tabelle beschriebenen Rollen und Fachkenntnisse erforderlich.

Rolle	Fachwissen	Verantwortlichkeiten
Couchbase-Administrator	• Vertrautheit mit Couchbase Server und Couchbase Capella • Grundkenntnisse in der Befehlszeile sind hilfreich, aber nicht erforderlich	• Couchbase Server- und Capella-spezifische Aufgaben
Systemadministrator, IT-Administrator	• Vertrautheit mit der selbstverwalteten Couchbase Server-Sy stemumgebung und Verwaltung	• Öffnen von Ports und Ermitteln von IP-Adress en auf selbstverwalteten Couchbase Server-Cl usterknoten

Einschränkungen

- Dieses Muster wird verwendet, um Daten, Indizes und Couchbase-Volltextsuchindizes von Couchbase Server zu Couchbase Capella auf AWS zu migrieren. Das Muster gilt nicht für die Migration von Couchbase Eventing Service oder Couchbase Analytics.
- Couchbase Capella ist in mehreren AWS-Regionen verfügbar. up-to-dateInformationen zu den Regionen, die Capella unterstützt, finden Sie unter Amazon Web Services in der Couchbase-Dokumentation.

Produktversionen

- Couchbase Server (Community oder Enterprise) Edition Version 5.x oder höher

Architektur

Quelltechnologie-Stack

- Couchbase-Server

Zieltechnologie-Stack

- Couchbase Capella

Zielarchitektur

1. Sie greifen über die Capella Control Plane auf Couchbase Capella zu. Sie können die Capella Control Plane verwenden, um Folgendes zu tun:
   - Kontrollieren und überwachen Sie Ihr Konto.
   - Verwalten Sie Cluster und Daten, Indizes, Benutzer und Gruppen, Zugriffsberechtigungen, Überwachung und Ereignisse.
2. Cluster werden erstellt.
3. Die Capella-Datenebene befindet sich im von Couchbase verwalteten AWS-Konto. Nachdem Sie einen neuen Cluster erstellt haben, stellt Couchbase Capella ihn in mehreren Availability Zones in der ausgewählten AWS-Region bereit.

4. Sie können Couchbase-Anwendungen in einer VPC in Ihrem AWS-Konto entwickeln und bereitstellen. In der Regel greift diese VPC über VPC-Peering auf die Capella-Datenebene zu.

Tools

- Couchbase Cross Data Center Replication (XDCR) hilft bei der Replikation von Daten über Cluster hinweg, die sich bei verschiedenen Cloud-Anbietern und verschiedenen Rechenzentren befinden. Es wird verwendet, um Daten aus selbstverwalteten Couchbase Server-Clustern nach Couchbase Capella zu migrieren.

> **Note**
>
> XDCR kann nicht mit Couchbase Server Community Edition für die Migration zu Couchbase Capella verwendet werden. Stattdessen können Sie cbexport verwenden. Weitere Informationen finden Sie im Abschnitt Daten aus der Community Edition migrieren.

- Couchbase Shell ist eine Befehlszeilen-Shell für Couchbase Server und Couchbase Capella für den Zugriff auf lokale und entfernte Couchbase-Cluster. In diesem Muster wird Couchbase Shell zur Migration von Indizes verwendet.
- cbexport ist ein Couchbase-Hilfsprogramm zum Exportieren von Daten aus einem Couchbase-Cluster. In den Couchbase Server CLI-Tools enthalten.

Epen

Bereiten Sie die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bewerten Sie die Größe des selbstverwalteten Couchbase Server-Clusters.	Melden Sie sich bei der Couchbase-Webkonsole für Couchbase Server an und überprüfen Sie die Knoten und Buckets Ihres selbstverwalteten Clusters. 1. Um eine Liste der Clusterknoten anzuzeigen, wählen	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie in der Navigationsleiste die Registerkarte Server. 2. Notieren Sie sich die Anzahl der Knoten und wählen Sie dann jeden Knoten in der Liste aus, um seine Eigenschaften anzuzeigen. 3. Notieren Sie den Arbeitsspeicher und den Speicherplatz für jeden einzelnen Knoten. 4. Wählen Sie in der Navigationsleiste die Registerkarte Buckets und wählen Sie dann jeden Bucket in der Liste aus, um dessen Eigenschaften anzuzeigen. Notieren Sie sich das RAM-Kontingent und die Einstellung zur Konfliktlösung für jeden Bucket. Sie verwenden Ihre selbst verwalteten Couchbase Server-Clusterkonfigurationen als allgemeinen Leitfaden für die Dimensionierung und Konfiguration des Zielclusters auf Couchbase Capella. Wenn Sie Hilfe bei einer detaillierteren Anleitung zur Dimensionierung von Couchbase Capella benötigen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	, wenden Sie sich an Couchbase.	
Zeichnen Sie die Couchbase -Dienstverteilung auf dem selbstverwalteten Couchbase Server-Cluster auf.	1. Wählen Sie in der Couchbase-Webkonsole die Registerkarte Server, um die Liste der Clusterknoten anzuzeigen. 2. Wählen Sie jeden Knoten aus, um seine Eigenschaften anzuzeigen, und zeichnen Sie dann die Couchbase Service-Verteilung für jeden Knoten auf (Data Service, Query Service, Index Service, Search Service, Analytics Serviceund Eventing Service).	Couchbase-Administrator
Notieren Sie sich die IP-Adressen der selbstverwalteten Couchbase Server-Clusterknoten.	(Ignorieren Sie diesen Schritt, wenn Sie die Community Edition verwenden.) Notieren Sie sich die IP-Adresse für jeden Knoten in Ihrem Cluster. Sie werden später zur Zulassungsliste auf Ihrem Couchbase Capella-Cluster hinzugefügt.	Couchbase-Administrator, Systemadministrator

Stellen Sie Ressourcen auf Couchbase Capella bereit und konfigurieren Sie sie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Auswahl einer Vorlage.	1. Melden Sie sich bei Ihrer Couchbase Capella Control Plane an, wählen Sie in der Hauptnavigation die Registerkarte Dashboard oder die Registerkarte Cluster und wählen Sie dann Create Cluster aus. 2. Wählen Sie anhand der Informationen, die Sie bei der Evaluierung Ihres selbstverwalteten Couchbase Server-Clusters aufgezeichnet haben, die Clustervorlage aus, die den Anforderungen der Konfiguration entspricht. Wenn Sie keine geeignete Vorlage finden, wählen Sie im Editor für die Clustergröße die Option Benutzerdefinierte Vorlage aus.	Couchbase-Administrator
Wählen und konfigurieren Sie die Knoten.	Wählen und konfigurieren Sie die Knoten so, dass sie zu Ihrer selbstverwalteten Couchbase Server-Cluster-Umgebung passen, einschließlich der Anzahl der Knoten, der Dienstverteilung, der Rechenleistung oder des Arbeitsspeichers und des Speichers.	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Couchbase Capella verwendet bewährte Methoden zur multidimensionalen Skalierung. Dienste und Knoten können nur gemäß den bewährten Bereitstellungsmethoden ausgewählt werden. Dies kann bedeuten, dass Sie die Konfigurationen Ihres selbstverwalteten Couchbase Server-Clusters nicht genau anpassen können.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Cluster bereit.	Wählen Sie eine Supportzone und ein Supportpaket aus und stellen Sie dann den Cluster bereit. Ausführliche Schritte und Anweisungen finden Sie in der Couchbase-Dokumentation unter Cluster erstellen. **Important** Wenn Sie die kostenlose Testversion von Couchbase Capella verwenden, müssen Sie sie in ein kostenpflichtiges Konto umwandeln, bevor Sie mit der Migration beginnen. Um Ihr Konto zu konvertieren, öffnen Sie in der Couchbase Capella Control Plane den Bereich Abrechnung und wählen Sie dann Aktivierungs-ID hinzufügen. Die Aktivierungs-ID wird an Ihre Rechnungskontakt-E-Mail-Adresse gesendet, nachdem Sie einen Kaufvertrag mit Couchbase Sales	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	abgeschlossen haben oder nachdem Sie einen Kauf über AWS Marketplace getätigt haben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Benutzer mit Datenbankanmeldedaten.	Ein Benutzer mit Datenbank anmeldedaten ist clustersp ezifisch und besteht aus einem Benutzernamen, einem Passwort und einer Reihe von Bucket-Rechten. Dieser Benutzer ist erforderlich, um Buckets zu erstellen und auf Bucket-Daten zuzugreifen. Erstellen Sie in der Couchbase Capella Control Plane Datenbankanmeldeda ten für den neuen Cluster, indem Sie den Anweisungen unter Datenbankanmeldeda ten konfigurieren in der Couchbase Capella-D okumentation folgen. **Note** Einem Organisat ionsbenutzer müssen Anmeldeinformation en für die Organisat ionsrolle zugewiese n werden, wenn er entweder remote oder über die Couchbase Capella-Benutzerob erfläche auf Bucket-Daten in einem bestimmten Cluster zugreifen möchte.	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dies ist unabhängig von Datenbankanmeldedaten, die normalerweise von Apps und Integrationen verwendet werden. Wenn Sie den Organisationsbenutzer erstellen, können Sie die Ziel-Buckets auf Ihrem Couchbase Capella-Cluster erstellen und verwalten.	
Wenn Sie die Migrationsoption 2 verwenden, installieren Sie Couchbase Shell.	Sie können Couchbase Shell auf jedem System installieren, das Netzwerkzugriff sowohl auf Ihren selbst verwalteten Couchbase-Server als auch auf die Couchbase Capella-Cluster hat. Weitere Informationen finden Sie unter Installieren von Couchbase Shell Version 1.0.0-beta.5 in der Couchbase Shell-Dokumentation. Stellen Sie sicher, dass Couchbase Shell installiert ist, indem Sie eine Verbindung zu Ihrem selbstverwalteten Cluster in einem Befehlszeilenterminal testen.	Couchbase-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
IP-Adressen zulassen.	1. Wählen Sie in der Couchbase Capella Control Plane Clusters und dann Ihren Zielcluster aus. 2. Wählen Sie die Registerk arte Connect für den Cluster und notieren Sie den Verbindungsendpunkt für Ihren Cluster, der unter Zulässige IP verwalten aufgeführt ist. 3. Gehen Sie wie folgt vor, um die IP-Adresse für das System, auf dem Sie Couchbase Shell installiert haben, und die IP-Adress e Ihrer selbstverwalteten Couchbase Server-Cluster-Instanzen als zulässige IP-Adressen hinzuzufügen: a. Wählen Sie unter Wide Area Network die Option Zulässige IP verwalten aus. b. Wählen Sie Add Allowed IP, geben Sie die IP-Adresse für das System ein, auf dem Sie Couchbase Shell installie rt haben, und wählen Sie dann Add IP. c. Wiederholen Sie den vorherigen Schritt,	Couchbase-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	um die IP-Adresse Ihrer selbstverwalteten Couchbase Server-Cl usterinstanz hinzuzufü gen. Weitere Informationen zu zulässigen IP-Adressen finden Sie unter Zulässige IP-Adressen konfigurieren in der Couchbase-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Zertifikate konfigurieren.	1. Um das Stammzertifikat für Ihren Cluster herunterzuladen, wählen Sie unter Stammzertifikat die Option Herunterladen aus. 2. Speichern Sie das Stammzertifikat mit der Dateierweiterung.pem in einem Ordner auf dem System, auf dem Couchbase Shell ausgeführt werden soll. 3. Melden Sie sich als Nächstes bei Ihrer selbst verwalteten Couchbase Server-Webkonsole an, wählen Sie in der linken Navigationsleiste Sicherheit und dann die Registerkarte Zertifikate. 4. Kopieren Sie das Stammzertifikat für Ihren selbstverwalteten Couchbase Server-Cluster und speichern Sie es als.pem-Datei in demselben Ordner, in dem Sie die Stammzertifikatsdatei für Ihren Couchbase Capella-Cluster gespeichert haben. Weitere Informationen zum Stammzertifikat finden Sie unter Root-Zertifikat in der	Couchbase-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Couchbase Server-Dokumentation.	
Erstellen Sie die Konfigurationsdatei für Couchbase Shell.	Erstellen Sie eine Konfigurations-Punktdatei im Home-Verzeichnis der Couchbase Shell-Installation (z. B.). `/<HOME_DIRECTORY>/.cbsh/config` Weitere Informationen finden Sie unter Config Dotfiles in der Couchbase-Dokumentation. Fügen Sie der Konfigurationsdatei Verbindungseigenschaften für die Quell- und Zielcluster hinzu. Sie können die Beispielkonfigurationsdatei im Abschnitt Zusätzliche Informationen verwenden und die Einstellungen für Ihre Cluster bearbeiten. Speichern Sie die Konfigurationsdatei mit den aktualisierten Einstellungen in dem `.cbsh` Ordner (z. B.`/<HOME_DIRECTORY>/.cbsh/config`).	Couchbase-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ziel-Buckets erstellen.	Erstellen Sie für jeden Quell-Bucket einen Ziel-Bucket in Ihrem Couchbase Capella-Cluster, indem Sie den Anweisungen unter Bucket erstellen in der Couchbase-Dokumentation folgen. Ihre Ziel-Bucket-Konfigurationen müssen mit den Bucket-Namen, Speichereinstellungen und Konfliktlösungseinstellungen der Buckets in Ihrem selbstverwalteten Couchbase Server-Cluster übereinstimmen.	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiche und Sammlungen erstellen.	Jeder Bucket enthält einen Standardbereich und eine Standardsammlung mit dem `_default._default` Schlüsselraum. Wenn Sie andere Schlüsselräume für Ihren Bereich und Ihre Sammlung verwenden , müssen Sie identische Schlüsselräume im Capella-Zielcluster erstellen. 1. Öffnen Sie das Befehlszeilenterminal auf dem System, auf dem Sie Couchbase Shell installiert haben. 2. Führen Sie den folgenden Befehl aus, um Couchbase Shell zu starten. `./cbsh` 3. Erstellen Sie für jeden Bucket, den Sie migrieren möchten, Bereiche und Sammlungen im Capella-Cluster, indem Sie die folgenden Befehle ausführen. Stellen Sie sicher, dass Sie es <BUCKET_NAME>durch den Namen des Buckets ersetzen, den Sie migrieren möchten.	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`scopes --clusters "On-Prem-Cluster" --bucket <BUCKET_NAME> | select scope | where scope != "_default" | each { |it| scopes create $it.scope --clusters "Capella-Cluster" } collections --clusters "On-Prem-Cluster" --bucket <BUCKET_NAME> | select scope collection | where $it.scope != "_default" | where $it.collection != "_default" | each { |it| collections create $it.collection --clusters "Capella-Cluster" --bucket <BUCKET_NAME> --scope $it.scope }`	

Migrieren Sie die Daten aus der Enterprise Edition

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Öffnen Sie TCP-Ports auf den selbstverwalteten Couchbase Server-Clusterknoten.	Stellen Sie sicher, dass die entsprechenden Ports für die XDCR-Kommunikation auf den Knoten des selbstverwalteten Couchbase Server-Clusters geöffnet sind. Weitere Informationen finden Sie in der Dokumentation zu den Couchbase Server-Ports.	Couchbase-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wenn Sie Couchbase Server Enterprise Edition verwenden, richten Sie Couchbase XDCR ein.	1. Wählen Sie in der Hauptnavigation der Couchbase Capella Control Plane die Option Clusters und dann den Zielcluster für die Migration aus. 2. Wählen Sie unter Root Certificate die Option Copy aus. 3. Melden Sie sich bei Ihrer selbst verwalteten Couchbase Server-We bkonsole an und wählen Sie in der Hauptnavigation XDCR aus. Wählen Sie dann „Fernbedienung hinzufügen“. 4. Geben Sie die folgenden Einstellungen ein: • Clustername — Ein Name für die Capella-C luster-Verbindung • IP/Hostname — Der Verbindungsendpunk t für Ihren Couchbase Capella-Cluster • Benutzername für Remote Cluster — Der Datenbankbenutzer für Ihren Couchbase Capella-Cluster • Passwort — Das Datenbankbenutzerp	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	asswort für Ihren Couchbase Capella-C luster • Sichere Verbindung aktivieren — Ausgewählt • Vollständig (TLS-Verschlüsselung von Passwort und Daten) — Ausgewählt 5. Fügen Sie das Capella-Cluster-Root-Zertifikat ein, das Sie zuvor kopiert haben, und wählen Sie dann Speichern.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie Couchbase XDCR.	1. Wählen Sie in Ihrer selbst verwalteten Couchbase Server-Webkonsole in der Hauptnavigation XDCR und dann Add Replication aus. 2. Geben Sie die folgenden Einstellungen ein: • Aus Bucket replizieren — Wählen Sie den Quell-Bucket für die Migration aus. • Remote-Bucket — Geben Sie den Namen des Ziel-Buckets ein. • Remote-Cluster — Wählen Sie den Zielcluster aus, den Sie zuvor erstellt haben. 3. Wählen Sie „Replizierung speichern“. Der Replikationsvorgang sollte innerhalb weniger Sekunden beginnen.	Couchbase-Administrator

Migrieren Sie die Indizes mithilfe von Option 1

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie selbstverwaltete Cluster-Indizes zu Couchbase Capella.	⚠ Important Wir empfehlen diesen Vorgang, wenn Sie weniger als 50	Couchbase-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Indizes migrieren müssen. Wenn Sie mehr als 50 Indizes migrieren müssen, empfehlen wir Ihnen, die Migrationsoption 2 zu verwenden. 1. Wählen Sie auf der Couchbase-Webkonsole Indizes aus. 2. Wählen Sie in der Liste der Indizes den ersten Index aus, den Sie migrieren möchten. Die Indexdefinition wird dann angezeigt. 3. Kopieren Sie die Indexdefinition mithilfe der `CREATE` Anweisung, aber kopieren Sie sie nicht`WITH { "defer_build":true }` . Aus der folgenden Beispielindexdefinition würden Sie beispielsweise nur kopieren`CREATE INDEX` `` `cityindex` `` `ON` `` `travel-sample`(`city`) `` . `CREATE INDEX `cityindex` ON `travel-sample`(`city`)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>WITH { "defer_bu
	ild":true }</pre>
	4. Wählen Sie in der Couchbase Capella Control Plane Clusters und dann den Zielcluster aus.
	5. Wählen Sie in der Dropdownliste Tools die Option Query Workbench aus. Fügen Sie die **CREATE** Anweisung, die Sie zuvor kopiert haben, in den Abfrage-Editor ein, und wählen Sie dann Ausführen . Dadurch wird der Index erstellt und erstellt.
	6. Um zu bestätigen, dass der Index erstellt wurde, wählen Sie Indizes aus der Dropdownliste Tools aus. Die Liste zeigt, dass der Index erstellt und erstellt wurde.
	7. Wiederholen Sie diesen Vorgang für jeden Index, der migriert werden muss.	

Migrieren Sie die Indizes mithilfe von Option 2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Migrieren Sie die Indexdefinitionen.	**⚠ Important**
	Wir empfehlen diesen Vorgang, wenn Sie mehr als 50 Indizes migrieren müssen. Wenn Sie weniger als 50 Indizes migrieren müssen, empfehlen wir Ihnen, die Migrationsoption 1 zu verwenden.
	
	1. Öffnen Sie das Befehlszeilenterminal auf dem System, auf dem Sie Couchbase Shell installiert haben.
	2. Führen Sie den folgenden Befehl aus, um Couchbase Shell zu starten.
	`./cbsh`
	3. Führen Sie den folgenden Befehl aus, um eine Verbindung zum selbstverwalteten Couchbase Server-Cluster herzustellen.
	`cb-env cluster On-Prem-Cluster`
		Couchbase-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Um Indexdefinitionen vom selbstverwalteten Couchbase Server-Cluster zum Couchbase Capella-Cluster zu migrieren, führen Sie den folgenden Befehl für jeden Bucket aus, den Sie migrieren möchten. Stellen Sie sicher, dass Sie es durch den Bucket-Namen <BUCKET_NAME> ersetzen, der den Indizes entspricht, die Sie migrieren möchten. Diese Migrationsoption setzt voraus, dass Ihre Ziel-Bucket-Namen mit den Quell-Bucket-Namen identisch sind. `query indexes --definitions | where bucket =~ <BUCKET_NAME>| get definition | each { |it| query $it --clusters Capella-Cluster }`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Indexdefinitionen.	1. Führen Sie den folgenden Befehl aus, um den Kontext zum Couchbase Capella-Cluster zu wechseln:
	`cb-env cluster Capella-Cluster`
	2. Um die Indexdefinitionen zu erstellen, die auf den Couchbase Capella-Cluster migriert wurden, führen Sie den folgenden Befehl aus und <BUCKET_NAME> ersetzen Sie ihn durch den Bucket-Namen, der den Indizes entspricht, die Sie erstellen möchten.
	`query 'SELECT RAW CONCAT("BUILD INDEX ON ", k , "(['", CONCAT2 ("','", inames), "']);") FROM system:indexes AS s LET bid = CONCAT("` ",s.bucket_id, "`"), sid = CONCAT("`", s.scope_id, "`"), kid = CONCAT("` ", s.keyspace_id, "`"), k = NVL2(bid, CONCAT2(".", bid, sid, kid), kid) WHERE s.namespa ce_id = "default" AND s.bucket_id = "" GROUP BY k LETTING`
		Couchbase-Administrator, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`inames = ARRAY_AGG (s.name) FILTER (WHERE s.state = 'deferred') HAVING ARRAY_LENGTH(inames) > 0;' | each { | it| query $it }` 3. Wiederholen Sie den Vorgang für jeden Bucket.	

Migrieren Sie Volltext-Suchindexe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie selbstverwaltete Cluster-Volltextsuchindizes zu Couchbase Capella.	1. Wählen Sie in der Couchbase-Webkonsole Suchen aus. 2. Wählen Sie in der Liste der Indizes für die Volltextsuche (FTS) den ersten FTS-Index aus, den Sie migrieren möchten, wählen Sie Indexdefinition anzeigen aus und wählen Sie In die Zwischenablage kopieren aus. Notieren Sie sich den Indexnamen und den Bucket, zu dem er gehört. 3. Wählen Sie in der Couchbase Capella Control Plane Clusters und dann den Zielcluster aus.	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie in der Dropdownliste Tools die Option Volltextsuche aus. 5. Wählen Sie Index importieren und fügen Sie die FTS-Indexdefinition ein. 6. Geben Sie den Indexnamen ein, wählen Sie den richtigen Bucket aus, wie auf dem selbstverwalteten Cluster angegeben, und wählen Sie dann Create aus. 7. Wiederholen Sie diesen Vorgang für jeden FTS-Index, der migriert werden muss.	

Migrieren Sie Daten aus der Couchbase Community Edition

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Exportieren Sie Daten aus der selbstverwalteten Couchbase Server Community Edition.	Verschlüsseltes XDCR ist in der Couchbase Community Edition nicht verfügbar. Sie können Daten aus der Couchbase Community Edition exportieren und die Daten dann manuell in Couchbase Capella importieren. Verwenden `cbexport` Sie die Befehlszeile, um Daten aus	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dem Quell-Bucket zu exportieren. Der folgende Befehl dient als Beispiel. `cbexport json \ --cluster localhost \ --bucket <SOURCE BUCKET NAME> \ --format lines \ --username <USERNAME> \ --password <PASSWORD> \ --include-key cbkey \ --scope-field cbscope \ --collection-field cbcoll \ --output cbexported_data.json` Beachten Sie`cbkey`, dass `cbscope`und `cbcoll` beliebige Bezeichnungen `cbexported_data.json` sind. Sie werden später im Prozess referenziert. Wenn Sie sie also anders benennen möchten, notieren Sie sich das.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Daten in Couchbase Capella importieren.	1. Wählen Sie in der Couchbase Capella Control Plane Clusters und dann den Zielcluster aus. 2. Wählen Sie in der Dropdownliste Tools die Option Import aus. Dadurch wird ein Assistent mit den folgenden sechs Schritten geöffnet: a. Bucket — Wählen Sie den Ziel-Bucket aus. b. Datei — Wählen Sie JSON, dann Lines und anschließend Using your web browser aus. Wenn Sie über eine große Datenmenge verfügen, können Sie die Option Manuell ausprobieren. Wählen Sie die Datei aus, die von erstellt wurde`cbexport`. c. Sammlungen — Wählen Sie „Benutzerdefiniertes Sammlungs-Mapping“. Wenn Ihre Community Edition-Datenbank keine Bereiche oder Sammlungen oder nur _default verwendet, können Sie stattdess en die Option Einzelne	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sammlung auswählen wählen. Geben Sie als Ausdruck für die Zuordnung von Sammlungen den Wert ein. `%cbscope %.%cbcoll%` Um zu überprüfen, ob dieser Ausdruck korrekt funktioniert, können Sie Beispieldaten einfügen, z. B. die folgenden. `{ "cbscope" :"inventory", "cbcoll":"landmark", "cbkey":" landmark_3991" }` d. Schlüssel — Wählen Sie Customer Generation. (Wenn Sie nicht daran interessiert sind, die Schlüssel der zu importierenden Daten beizubehalten, können Sie stattdessen Automatisch generierte UUID auswählen und mit Schritt 5 fortfahren.) Geben Sie für Key Name Generator Expression %cbkey% ein. Um zu überprüfen, ob dieser Ausdruck korrekt	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	funktioniert, fügen Sie einige Beispieldaten ein. e. Konfigurationen — Wählen Sie Felder ignorieren und geben Sie cbscope, cbcoll, cbkey ein. Diese Felder enthalten vorüberge hende Informationen, die sich nach einem Import nicht im Ziel-Buck et befinden müssen. Übernehmen Sie für die anderen Einstellungen die Standardwerte. f. Import — Überprüfen Sie den Vorgang und wählen Sie Import, wenn Sie bereit sind. Warten Sie auf den Upload und den Datenimport. Für große Dateien unterstüt zt Couchbase Capella den Befehlszeilenimport mit cURL. Weitere Informationen zu den Importoptionen finden Sie unter Daten importieren in der Couchbase Capella-D okumentation.	

Testen und verifizieren Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Datenmigration.	1. Wählen Sie in der Couchbase Capella Control Plane Clusters und dann den Zielcluster in Ihrer Cluster-Liste aus. 2. Wählen Sie die Registerkarte Buckets für Ihren Zielcluster. Stellen Sie sicher, dass die Anzahl der Elemente (Dokumente) im Ziel-Bucket mit der Anzahl der Elemente im Quell-Bucket übereinstimmt. 3. Wählen Sie im Zielcluster in der Dropdownliste Tools die Option Dokumente aus. Stellen Sie sicher, dass alle Dokumente migriert wurden. 4. (Optional) Nachdem alle Daten migriert wurden, können Sie die Replikation beenden, indem Sie sie löschen. Weitere Informationen finden Sie in der Couchbase-Dokumentation unter Löschen einer Replikation.	Couchbase-Administrator
Überprüfen Sie die Indexmigration.	Wählen Sie in der Couchbase Capella Control Plane in der Dropdownliste Tools für Ihren	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Zielcluster die Option Indizes aus. Stellen Sie sicher, dass die Indizes migriert und erstellt wurden.	
Überprüfen Sie die Abfrageergebnisse.	1. Wählen Sie in der Couchbase Capella Control Plane in der Dropdownliste Tools für Ihren Zielcluster die Option Query Workbench aus. 2. Führen Sie eine N1QL-Beispielabfrage oder eine in Ihrer Anwendung verwendete Abfrage aus. Stellen Sie sicher, dass Sie dieselben Ergebnisse erhalten wie bei der Ausführung der Abfrage in Ihrem selbstverwalteten Couchbase Server-Cluster.	Couchbase-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Ergebnisse der Volltextsuche (gilt, wenn Sie FTS-Indizes migriert haben).	1. Wählen Sie in der Couchbase Capella Control Plane in der Dropdownliste Tools für Ihren Zielcluster die Option Volltextsuche aus. 2. Wählen Sie einen FTS-Index aus, indem Sie seinen Namen wählen. 3. Wählen Sie Search (Suchen) aus. 4. Geben Sie eine Beispielsuchabfrage ein und wählen Sie Suchen aus. 5. Stellen Sie sicher, dass die Ergebnisse dieselben sind wie bei der Ausführung der Suche auf Ihrem selbstverwalteten Cluster.	Couchbase-Administrator

Zugehörige Ressourcen

Bereiten Sie die Migration vor

- Beginnen Sie mit der kostenlosen Testversion von Couchbase Capella
- Anforderungen des Cloud-Anbieters für Couchbase Capella
- Größenrichtlinien für Couchbase Capella

Migrieren Sie die Daten und Indizes

- Couchbase XDCR
- Couchbase Shell-Dokumentation

Couchbase Capella und Support SLAs

- Couchbase Capella-Serviceverträge () SLAs
- Support-Richtlinie für den Couchbase Capella Service

Zusätzliche Informationen

Der folgende Code ist eine Beispielkonfigurationsdatei für Couchbase Shell.

```
Version = 1

[[clusters]]
identifier = "On-Prem-Cluster"
hostnames = ["<SELF_MANAGED_COUCHBASE_CLUSTER>"]
default-bucket = "travel-sample"
username = "<SELF_MANAGED_ADMIN>"
password = "<SELF_MANAGED_ADMIN_PWD>"
tls-cert-path = "/<ABSOLUTE_PATH_TO_SELF_MANAGED_ROOT_CERT>"
data-timeout = "2500ms"
connect-timeout = "7500ms"
query-timeout = "75s"

[[clusters]]
identifier = "Capella-Cluster"
hostnames = ["<COUCHBASE_CAPELLA_ENDPOINT>"]
default-bucket = "travel-sample"
username = "<CAPELLA_DATABASE_USER>"
password = "<CAPELLA_DATABASE_USER_PWD>"
tls-cert-path = "/<ABSOLUTE_PATH_TO_COUCHBASE_CAPELLA_ROOT_CERT>"
data-timeout = "2500ms"
connect-timeout = "7500ms"
query-timeout = "75s"
```

Bevor Sie die Konfigurationsdatei speichern, stellen Sie anhand der folgenden Tabelle sicher, dass Sie Ihre eigenen Quell- und Zielclusterinformationen hinzugefügt haben.

<SELF_MANAGED_COUCHBASE_CLUSTER>	Verwenden Sie die IP-Adresse für Ihren selbstverwalteten Couchbase Server-Cluster.

<SELF_MANAGED_ADMIN>	Verwenden Sie den Administratorbenutzer für Ihren selbstverwalteten Couchbase Server-Cluster.
<ABSOLUTE_PATH_TO_SELF_MANAGED_ROOT_CERT>	Verwenden Sie den absoluten Pfad zur gespeicherten Root-Zertifikatsdatei für Ihren selbstverwalteten Couchbase Server-Cluster.
<COUCHBASE_CAPELLA_ENDPOINT>	Verwenden Sie den Verbindungsendpunkt für Ihren Couchbase Capella-Cluster.
<CAPELLA_DATABASE_USER>	Verwenden Sie den Datenbankbenutzer für Ihren Couchbase Capella-Cluster.
<CAPELLA_DATABASE_USER_PWD>	Verwenden Sie das Datenbank-Benutzerpasswort für Ihren Couchbase Capella-Cluster.
<ABSOLUTE_PATH_TO_COUCHBASE_CAPELLA_ROOT_CERT>	Verwenden Sie den absoluten Pfad zur gespeicherten Root-Zertifikatsdatei für Ihren Couchbase Capella-Cluster.

Migrieren Sie von IBM WebSphere Application Server zu Apache Tomcat auf Amazon EC2

Erstellt von Neal Ardeljan (AWS) und Afroz Khan (AWS)

Übersicht

Dieses Muster führt Sie durch die Schritte für die Migration von einem lokalen System mit Red Hat Enterprise Linux (RHEL) 6.9 oder höher, auf dem IBM WebSphere Application Server (WAS) ausgeführt wird, zu RHEL 8 mit Apache Tomcat auf einer Amazon Elastic Compute Cloud (Amazon) - Instance. EC2

Das Muster kann auf die folgenden Quell- und Zielversionen angewendet werden:

- WebSphere Application Server 7.x auf Apache Tomcat 8 (mit Java 7 oder höher)
- WebSphere Anwendungsserver 8.x auf Apache Tomcat 8 (mit Java 7 oder höher)
- WebSphere Anwendungsserver 8.5.5.x auf Apache Tomcat 9 (mit Java 8 oder höher)
- WebSphere Anwendungsserver 8.5.5.x auf Apache Tomcat 10 (mit Java 8 oder höher)

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Java-Quellcode mit den folgenden Annahmen:
  - Verwendet die Java Development Kit (JDK) -Version von Java 7 oder höher
  - Verwendet das Spring- oder Apache Struts-Framework
  - Verwendet weder das Enterprise Java Beans (EJB) -Framework noch andere WebSphere Serverfunktionen, die für Tomcat nicht ohne weiteres verfügbar sind
  - Verwendet hauptsächlich Servlets oder Java Server Pages () JSPs
  - Verwendet JDBC-Konnektoren (Java Database Connectivity), um eine Verbindung zu Datenbanken herzustellen
- Quelle: IBM WebSphere Application Server Version 7.x oder höher
- Zielversion von Apache Tomcat 8.5 oder höher

Architektur

Quelltechnologie-Stack

- Eine Webanwendung, die mit dem Apache Struts Model-View-Controller (MVC) -Framework erstellt wurde
- Eine Webanwendung, die auf IBM WebSphere Application Server Version 7.x oder 8.x ausgeführt wird
- Eine Webanwendung, die einen LDAP-Connector (Lightweight Directory Access Protocol) verwendet, um eine Verbindung zu einem LDAP-Verzeichnis (iPlanet/eTrust) herzustellen
- Eine Anwendung, die IBM Tivoli Access Manager (TAM) -Konnektivität verwendet, um das TAM-Benutzerkennwort zu aktualisieren (in der aktuellen Implementierung verwenden Anwendungen PD.jar)

Lokale Datenbanken

- Oracle Database 21c (21.0.0.0)
- Oracle Database 19c (19.0.0.0)
- Oracle Database 12c Release 2 (12.2.0.1)
- Oracle Database 12c Release 1 (12.1.0.2)

Zieltechnologie-Stack

- Apache Tomcat Version 8 (oder höher) wird auf RHEL auf einer Instanz ausgeführt EC2
- Amazon Relational Database Service (Amazon RDS) für Oracle

Weitere Informationen zu den von Amazon RDS unterstützten Oracle-Versionen finden Sie auf der Website Amazon RDS for Oracle.

Zielarchitektur

Tools

- Anwendungsebene: Neuaufbau der Java-Anwendung in eine WAR-Datei.
- Datenbankebene: systemeigenes Backup und Wiederherstellung von Oracle.

- Apache Tomcat-Migrationstool für Jakarta EE. Dieses Tool konvertiert eine für Java EE 8 geschriebene Webanwendung, die auf Apache Tomcat 9 läuft, automatisch in die Ausführung auf Apache Tomcat 10, das Jakarta EE 9 implementiert.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vervollständigen Sie die Anwendungserkennung, den aktuellen Status und die Leistungsbasis.		BA, Leiter der Migration
Validieren Sie die Quell- und Zieldatenbankversionen.		DBA
Identifizieren Sie die Hardwareanforderungen für die EC2 Zielserverinstanz.		DBA, SysAdmin
Identifizieren Sie die Speicheranforderungen (Speichertyp und Kapazität).		DBA, SysAdmin
Wählen Sie den richtigen EC2 Instanztyp auf der Grundlage von Kapazität, Speicherf unktionen und Netzwerkf unktionen aus.		DBA, SysAdmin
Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Strategie und die Tools für die Anwendungsmigration.		DBA, Leiter der Migration
Füllen Sie das Migration sdesign und den Migration sleitfaden für die Anwendung aus.		Leitung aufbauen, Leitung Migration
Vervollständigen Sie das Runbook zur Anwendung smigration.		Leiter Aufbau, Leiter der Umstellung, Leiter des Tests, Leiter der Migration

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC).		SysAdmin
Erstellen Sie die Sicherhei tsgruppen.		SysAdmin
Konfigurieren und starten Sie Amazon RDS for Oracle.		DBA, SysAdmin

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Endpoints oder verschaffen Sie sich Zugriff auf diese, um die		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Datenbank-Backupdateien abzurufen.		
Verwenden Sie die native Datenbank-Engine oder ein Drittanbieter-Tool, um Datenbankobjekte und Daten zu migrieren.	Einzelheiten finden Sie unter „Migrieren von Datenbank objekten und Daten“ im Abschnitt Zusätzliche Informati onen.	DBA

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Reichen Sie den Änderungs antrag (CR) für die Migration ein.		Übernahme (Leitung)
Besorgen Sie sich die CR-Genehmigung für die Migration.		Übernahme (Leitung)
Folgen Sie der Strategie zur Anwendungsmigration gemäß dem Runbook zur Anwendung smigration.	Einzelheiten finden Sie unter „Einrichtung der Anwendung sebene“ im Abschnitt Zusätzlic he Informationen.	DBA, Migrationsingenieur, App-Besitzer
Aktualisieren Sie die Anwendung (falls erforderlich).		DBA, Migrationsingenieur, App-Besitzer
Führen Sie die Funktions- und Nichtfunktionstests sowie die Datenvalidierungs-, SLA- und Leistungstests durch.		Testleiter, App-Besitzer, App-Nutzer

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Lassen Sie sich vom Inhaber der Anwendung oder dem Geschäftsinhaber genehmigen.		Übernahme (Leitung)
Stellen Sie die Anwendungsclients auf die neue Infrastruktur um.		DBA, Migrationsingenieur, App-Besitzer

Schließen Sie das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre AWS-Ressourcen herunter.		DBA, Migrationsingenieur, SysAdmin
Überprüfen und validieren Sie die Projektdokumente.		Leiter der Migration
Erfassen Sie Kennzahlen wie die Zeit bis zur Migration, den Prozentsatz manueller Aufgaben im Vergleich zu automatisierten Aufgaben und Kosteneinsparungen.		Leiter der Migration
Schließen Sie das Projekt ab und geben Sie Feedback.		Leiter der Migration, Inhaber der App

Zugehörige Ressourcen

Referenzen

- Dokumentation zu Apache Tomcat 10.0
- Apache Tomcat 9.0-Dokumentation
- Apache Tomcat 8.0-Dokumentation
- Installationsanleitung für Apache Tomcat 8.0
- Apache Tomcat JNDI-Dokumentation
- Amazon RDS for Oracle Oracle-Website
- Amazon-RDS-Preise
- Oracle und Amazon Web Services
- Oracle auf Amazon RDS
- Amazon RDS Multi-AZ-Bereitstellungen

Tutorials und Videos

- Erste Schritte mit Amazon RDS

Zusätzliche Informationen

Migrieren von Datenbankobjekten und Daten

Wenn Sie beispielsweise native Oracle-Dienstprogramme für Backup/Restore verwenden:

1. Erstellen Sie das Amazon Simple Storage Service (Amazon S3) -Backup für Datenbank-Backup-Dateien (optional).
2. Sichern Sie die Oracle-DB-Daten im gemeinsam genutzten Netzwerkordner.
3. Melden Sie sich beim Migration-Staging-Server an, um den Netzwerkfreigabeordner zuzuordnen.
4. Kopieren Sie Daten aus dem Netzwerkfreigabeordner in den S3-Bucket.
5. Fordern Sie eine Amazon RDS Multi-AZ-Bereitstellung für Oracle an.
6. Stellen Sie das lokale Datenbank-Backup auf Amazon RDS for Oracle wieder her.

Einrichtung der Anwendungsebene

1. Installieren Sie Tomcat 8 (oder 9/10) von der Apache Tomcat-Website.
2. Package Sie die Anwendung und die gemeinsam genutzten Bibliotheken in eine WAR-Datei.
3. Stellen Sie die WAR-Datei in Tomcat bereit.

4. Überwachen Sie das Startprotokoll `Linux cat` aller fehlenden gemeinsam genutzten Bibliotheken von WebSphere.
5. Sehen Sie sich den Startdatensatz `Linux cat` aller WebSphere -spezifischen Deployment-Deskriptor-Erweiterungen an.
6. Sammeln Sie alle fehlenden abhängigen Java-Bibliotheken vom WebSphere Server.
7. Ändern Sie WebSphere spezifische Deployment-Deskriptorelemente durch Tomcat-kompatible Äquivalente.
8. Erstellen Sie die WAR-Datei mit den abhängigen Java-Bibliotheken und den aktualisierten Deployment-Deskriptoren neu.
9. Aktualisieren Sie die LDAP-Konfiguration, die Datenbankkonfiguration und testen Sie die Verbindungen (siehe Realm Configuration HOW-TO und JNDI Datasource HOW-TO in der Apache Tomcat-Dokumentation).
10. Testen Sie die installierte Anwendung anhand der wiederhergestellten Amazon RDS for Oracle Oracle-Datenbank.
11. Erstellen Sie aus der EC2 Instance ein Amazon Machine Image (AMI) für Linux.
12. Starten Sie die fertige Architektur mit der Application Load Balancer- und Auto Scaling Scaling-Gruppe.
13. Aktualisieren Sie den URLs (mithilfe der WebSeal-Verbindung) so, dass er auf den Application Load Balancer verweist.
14. Aktualisieren Sie die Configuration Management Database (CMDB).

Migrieren Sie EC2 mit Auto Scaling von IBM WebSphere Application Server zu Apache Tomcat auf Amazon

Erstellt von Kevin Yung (AWS) und Afroz Khan (AWS)

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer Java-Anwendung von IBM WebSphere Application Server zu Apache Tomcat auf einer Amazon Elastic Compute Cloud (Amazon EC2) - Instance mit aktiviertem Amazon EC2 Auto Scaling.

Mit diesem Muster können Sie Folgendes erreichen:

- Eine Senkung der IBM-Lizenzkosten
- Hohe Verfügbarkeit durch Multi-AZ-Bereitstellung
- Verbesserte Anwendungsausfallsicherheit mit Amazon EC2 Auto Scaling

Voraussetzungen und Einschränkungen

Voraussetzungen

- Java-Anwendungen (Version 7). x oder 8. x) sollte in LAMP-Stacks entwickelt werden.
- Der Zielstatus besteht darin, Java-Anwendungen auf Linux-Hosts zu hosten. Dieses Muster wurde erfolgreich in einer Red Hat Enterprise Linux (RHEL) 7-Umgebung implementiert. Andere Linux-Distributionen können diesem Muster folgen, es sollte jedoch auf die Konfiguration der Apache Tomcat-Distribution verwiesen werden.
- Sie sollten die Abhängigkeiten der Java-Anwendung verstehen.
- Sie müssen Zugriff auf den Quellcode der Java-Anwendung haben, um Änderungen vornehmen zu können.

Einschränkungen und Änderungen an der Platformierung

- Sie sollten die Komponenten des Unternehmensarchivs (EAR) verstehen und sicherstellen, dass alle Bibliotheken in den WAR-Dateien der Webkomponente enthalten sind. Sie müssen das Apache Maven WAR-Plugin konfigurieren und WAR-Dateiartefakte erzeugen.
- Bei der Verwendung von Apache Tomcat 8 besteht ein bekannter Konflikt zwischen servlet-api.jar und den in das Anwendungspaket integrierten JAR-Dateien. Um dieses Problem zu beheben, löschen Sie servlet-api.jar aus dem Anwendungspaket.

- Sie müssen WEB-INF/Resources konfigurieren, das sich im Klassenpfad der Apache Tomcat-Konfiguration befindet. Standardmäßig werden die JAR-Bibliotheken nicht in das Verzeichnis geladen. Alternativ können Sie alle Ressourcen unter bereitstellen src/main/resources.
- Suchen Sie in der Java-Anwendung nach fest codierten Kontextwurzeln und aktualisieren Sie das neue Kontextstammverzeichnis von Apache Tomcat.
- Um die JVM-Laufzeitoptionen festzulegen, können Sie die Konfigurationsdatei setenv.sh im bin-Ordner von Apache Tomcat erstellen, z. B. JAVA_OPTS, JAVA_HOME usw.
- Die Authentifizierung wird auf Containerebene konfiguriert und in Apache Tomcat-Konfigurationen als Realm eingerichtet. Die Authentifizierung wird für einen der folgenden drei Bereiche eingerichtet:
  - JDBC Database Realm sucht nach Benutzern in einer relationalen Datenbank, auf die der JDBC-Treiber zugreift.
  - DataSource Database Realm sucht nach Benutzern in einer Datenbank, auf die JNDI zugreift.
  - JNDI Directory Realm sucht nach Benutzern im LDAP-Verzeichnis (Lightweight Directory Access Protocol), auf das der JNDI-Anbieter zugreift. Für die Suchvorgänge ist Folgendes erforderlich:
    - LDAP-Verbindungsdetails: Benutzersuchbasis, Suchfilter, Rollenbasis, Rollenfilter
    - Der wichtige JNDI-Verzeichnisbereich: Stellt eine Verbindung zu LDAP her, authentifiziert Benutzer und ruft alle Gruppen ab, in denen ein Benutzer Mitglied ist
- Autorisierung: Im Fall eines Containers mit einer rollenbasierten Autorisierung, die die Autorisierungseinschränkungen in web.xml überprüft, müssen Webressourcen definiert und mit den in den Einschränkungen definierten Rollen verglichen werden. Wenn LDAP nicht über eine Gruppenrollen-Zuordnung verfügt, müssen Sie das Attribut < security-role-ref > in web.xml festlegen, um eine Gruppenrollen-Zuordnung zu erreichen. Ein Beispiel für ein Konfigurationsdokument finden Sie in der Oracle-Dokumentation.
- Datenbankverbindung: Erstellen Sie eine Ressourcendefinition in Apache Tomcat mit einer Amazon Relational Database Service (Amazon RDS) -Endpunkt-URL und Verbindungsdetails. Aktualisieren Sie den Anwendungscode mithilfe der JNDI-Suche so, dass er auf a DataSource verweist. Eine in definierte bestehende DB-Verbindung WebSphere würde nicht funktionieren, da sie die WebSphere JNDI-Namen verwendet. Sie können <resource-ref>in web.xml einen Eintrag mit dem JNDI-Namen und der DataSource Typdefinition hinzufügen. Ein Beispiel für ein Konfigurationsdokument finden Sie in der Apache Tomcat-Dokumentation.
- Protokollierung: Standardmäßig protokolliert Apache Tomcat in der Konsole oder in einer Protokolldatei. Sie können die Ablaufverfolgung auf Realmebene aktivieren, indem Sie logging.properties aktualisieren (siehe Logging in Tomcat). Wenn Sie Apache Log4j verwenden,

um Logs an eine Datei anzuhängen, müssen Sie tomcat-juli herunterladen und dem Klassenpfad hinzufügen.

- Sitzungsmanagement: Wenn Sie IBM WebSEAL für den Lastenausgleich von Anwendungen und das Sitzungsmanagement beibehalten, sind keine Änderungen erforderlich. Wenn Sie einen Application Load Balancer oder Network Load Balancer auf AWS verwenden, um die IBM WebSeal-Komponente zu ersetzen, müssen Sie das Sitzungsmanagement mithilfe einer ElastiCache Amazon-Instance mit einem Memcache-Cluster einrichten und Apache Tomcat für die Verwendung von Open-Source-Sitzungsmanagement einrichten.
- Wenn Sie den IBM WebSeal Forward Proxy verwenden, müssen Sie einen neuen Network Load Balancer auf AWS einrichten. Verwenden Sie die vom Network Load Balancer für WebSeal-Verbindungskonfigurationen IPs bereitgestellten.
- SSL-Konfiguration: Wir empfehlen, Secure Sockets Layer (SSL) für end-to-end die Kommunikation zu verwenden. Folgen Sie den Anweisungen in der Apache Tomcat-Dokumentation, um eine SSL-Serverkonfiguration in Apache Tomcat einzurichten.

Architektur

Quelltechnologie-Stack

- IBM WebSphere Anwendungsserver

Zieltechnologie-Stack

- Die Architektur verwendet Elastic Load Balancing (Version 2). Wenn Sie IBM WebSeal für Identify Management und Load Balancing verwenden, können Sie einen Network Load Balancer auf AWS auswählen, der in den IBM WebSeal Reverse-Proxy integriert werden soll.
- Java-Anwendungen werden auf einem Apache Tomcat-Anwendungsserver bereitgestellt, der auf einer EC2 Instance in einer Amazon EC2 Auto Scaling Scaling-Gruppe ausgeführt wird. Sie können eine Skalierungsrichtlinie einrichten, die auf CloudWatch Amazon-Metriken wie der CPU-Auslastung basiert.
- Wenn Sie die Verwendung von IBM WebSeal für den Lastenausgleich einstellen, können Sie Amazon ElastiCache for Memcached für die Sitzungsverwaltung verwenden.
- Für die Back-End-Datenbank können Sie High Availability (Multi-AZ) für Amazon RDS bereitstellen und einen Datenbank-Engine-Typ auswählen.

Zielarchitektur

Tools

- AWS CloudFormation
- AWS-Befehlszeilenschnittstelle (AWS CLI)
- Apache Tomcat (Version 7). x oder 8. x)
- RHEL 7 oder Centos 7
- Bereitstellung von Amazon RDS Multi-AZ
- Amazon ElastiCache für Memcached (optional)

Epen

VPC einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC).		
Erstellen Sie Subnetze.		
Erstellen Sie bei Bedarf Routing-Tabellen.		
Erstellen Sie Listen zur Netzwerkzugriffskontrolle (ACLs).		
Richten Sie AWS Direct Connect oder eine Unternehm ens-VPN-Verbindung ein.		

Führen Sie die Anwendung auf eine neue Plattform

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Refaktorieren Sie die Maven-Konfiguration des Anwendungsbuilds, um die WAR-Artefakte zu generieren.		
Refaktorieren Sie die Datenquellen für Anwendungsabhängigkeiten in Apache Tomcat.		
Refaktorieren Sie die Anwendungsquellcodes so, dass sie JNDI-Namen in Apache Tomcat verwenden.		
Stellen Sie die WAR-Artefakte in Apache Tomcat bereit.		
Vollständige Anwendungsvalidierungen und Tests.		

Konfigurieren Sie das Netzwerk

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Unternehmensfirewall so, dass die Verbindung zu den Abhängigkeitsdiensten hergestellt werden kann.		
Konfigurieren Sie die Unternehmensfirewall so, dass Endbenutzer auf Elastic Load		

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Balancing auf AWS zugreifen können.		

Erstellen Sie die Anwendungsinfrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Anwendung und stellen Sie sie auf einer EC2 Instanz bereit.		
Erstellen Sie einen Amazon ElastiCache for Memcached -Cluster für die Sitzungsv erwaltung.		
Erstellen Sie eine Amazon RDS Multi-AZ-Instance für die Backend-Datenbank.		
Erstellen Sie SSL-Zertifikate und importieren Sie sie in AWS Certificate Manager (ACM).		
Installieren Sie SSL-Zertifikate auf Load Balancern.		
Installieren Sie SSL-Zertifikate für Apache Tomcat-Server.		
Führen Sie die Validierungen und Tests der Anwendungen durch.		

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die bestehende Infrastruktur herunter.		
Stellen Sie die Datenbank aus der Produktion in Amazon RDS wieder her.		
Überarbeiten Sie die Anwendung, indem Sie DNS-Änderungen vornehmen.		

Zugehörige Ressourcen

Referenzen

- Dokumentation zu Apache Tomcat 7.0
- Installationsanleitung für Apache Tomcat 7.0
- Apache Tomcat JNDI-Dokumentation
- Amazon RDS Multi-AZ-Bereitstellungen
- Amazon ElastiCache für Memcached

Tutorials und Videos

- Erste Schritte mit Amazon RDS

Migrieren Sie eine.NET-Anwendung von Microsoft Azure App Service zu AWS Elastic Beanstalk

Erstellt von Raghavender Madamshitti (AWS)

Übersicht

Dieses Muster beschreibt, wie eine auf Microsoft Azure App Service gehostete .NET-Webanwendung zu AWS Elastic Beanstalk migriert wird. Es gibt zwei Möglichkeiten, Anwendungen zu Elastic Beanstalk zu migrieren:

- Verwenden Sie AWS Toolkit for Visual Studio — Dieses Plugin für die Microsoft Visual Studio IDE bietet die einfachste und unkomplizierteste Möglichkeit, benutzerdefinierte.NET-Anwendungen in AWS bereitzustellen. Sie können diesen Ansatz verwenden, um .NET-Code direkt in AWS bereitzustellen und unterstützende Ressourcen wie Amazon Relational Database Service (Amazon RDS) für SQL Server-Datenbanken direkt aus Visual Studio zu erstellen.
- Upload und Bereitstellung auf Elastic Beanstalk — Jeder Azure App Service umfasst einen Hintergrunddienst namens Kudu, der für die Erfassung von Speicherabbildern und Bereitstellungsprotokollen, die Anzeige von Konfigurationsparametern und den Zugriff auf Bereitstellungspakete nützlich ist. Sie können die Kudu-Konsole verwenden, um auf Azure App Service-Inhalte zuzugreifen, das Bereitstellungspaket zu extrahieren und das Paket dann mithilfe der Upload- und Bereitstellungsoption in der Elastic Beanstalk-Konsole auf Elastic Beanstalk hochzuladen.

Dieses Muster beschreibt den zweiten Ansatz (Hochladen Ihrer Anwendung auf Elastic Beanstalk über Kudu). Das Muster verwendet auch die folgenden AWS-Services: AWS Elastic Beanstalk, Amazon Virtual Private Cloud (Amazon VPC), Amazon CloudWatch, Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling, Amazon Simple Storage Service (Amazon S3) und Amazon Route 53

Die.NET-Webanwendung wird auf AWS Elastic Beanstalk bereitgestellt, das in einer Amazon EC2 Auto Scaling Scaling-Gruppe ausgeführt wird. Sie können eine Skalierungsrichtlinie einrichten, die auf CloudWatch Amazon-Metriken wie der CPU-Auslastung basiert. Für eine Datenbank können Sie je nach Anwendung und Geschäftsanforderungen Amazon RDS in einer Multi-AZ-Umgebung oder Amazon DynamoDB verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine .NET-Webanwendung, die in Azure App Service ausgeführt wird
- Erlaubnis zur Verwendung der Azure App Service Kudu-Konsole

Produktversionen

- .NET Core (x64) 1.0.1, 2.0.0 oder höher oder.NET Framework 4.x, 3.5 (siehe Plattformhistorie von.NET auf Windows Server)
- Internetinformationsdienste (IIS) Version 8.0 oder höher, ausgeführt auf Windows Server 2012 oder höher
- .NET 2.0 oder 4.0 Runtime.

Architektur

Quelltechnologie-Stack

- Anwendung, die mit.NET Framework 3.5 oder höher oder .NET Core 1.0.1, 2.0.0 oder höher entwickelt und auf Azure App Service (Web-App oder API-App) gehostet wird

Zieltechnologie-Stack

- AWS Elastic Beanstalk wird in einer Amazon EC2 Auto Scaling Scaling-Gruppe ausgeführt

Migrationsarchitektur

Arbeitsablauf bei der Bereitstellung

Tools

Tools

- .NET Core oder.NET Framework
- C#
- IIS

- Kudu-Konsole

AWS-Services und -Funktionen

- AWS Elastic Beanstalk — Elastic Beanstalk ist ein easy-to-use Service für die Bereitstellung und Skalierung von.NET-Webanwendungen. Elastic Beanstalk verwaltet automatisch die Kapazitätsbereitstellung, den Lastenausgleich und die auto Skalierung.
- Amazon EC2 Auto Scaling Scaling-Gruppe — Elastic Beanstalk umfasst eine Auto Scaling Scaling-Gruppe, die die EC2 Amazon-Instances in der Umgebung verwaltet. In einer Umgebung mit nur einer Instance stellt die Auto Scaling-Gruppe sicher, dass immer eine Instance ausgeführt wird. In einer Umgebung mit Lastenausgleich können Sie die Gruppe mit einer Reihe von Instances konfigurieren, die ausgeführt werden sollen, und Amazon EC2 Auto Scaling fügt Instances je nach Bedarf hinzu oder entfernt sie, je nach Auslastung.
- Elastic Load Balancing — Wenn Sie Load Balancing in AWS Elastic Beanstalk aktivieren, wird ein Load Balancer erstellt, der den Traffic auf die EC2 Instances in der Umgebung verteilt.
- Amazon CloudWatch — Elastic Beanstalk verwendet Amazon automatisch CloudWatch , um Informationen über Ihre Anwendungs- und Umgebungsressourcen bereitzustellen. Amazon CloudWatch unterstützt Standardmetriken, benutzerdefinierte Metriken und Alarme.
- Amazon Route 53 — Amazon Route 53 ist ein hochverfügbarer und skalierbarer Cloud-Webservice für das Domain Name System (DNS). Sie können Route 53-Aliaseinträge verwenden, um benutzerdefinierte Domainnamen AWS Elastic Beanstalk-Umgebungen zuzuordnen.

Epen

Richten Sie eine VPC ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine virtuelle private Cloud (VPC) ein.	Erstellen Sie in Ihrem AWS-Konto eine VPC mit den erforderlichen Informationen.	Systemadministrator
Erstellen Sie Subnetze.	Erstellen Sie zwei oder mehr Subnetze in Ihrer VPC.	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Routing-Tabelle.	Erstellen Sie eine Routentabelle, die Ihren Anforderungen entspricht.	Systemadministrator

Elastic Beanstalk einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Greifen Sie auf die Azure App Service Kudu-Konsole zu.	Greifen Sie über das Azure-Portal auf Kudu zu, indem Sie zum App Service-Dashboard navigieren und dann Advanced Tools, Go auswählen. Oder Sie können die Azure App Service-URL wie folgt ändern:. `https://<appservicename>.scm.azurewebsites.net`	App-Entwickler, Systemadministrator
Laden Sie das Bereitstellungspaket von Kudu herunter.	Navigieren Sie zu Windows, PowerShell indem Sie die DebugConsoleOption auswählen. Dadurch wird die Kudo-Konsole geöffnet. Gehe zum `wwwroot` Ordner und lade ihn herunter. Dadurch wird das Azure App Service-Bereitstellungspaket als ZIP-Datei heruntergeladen. Ein Beispiel finden Sie im Anhang.	App-Entwickler, Systemadministrator
Erstellen Sie ein Paket für Elastic Beanstalk.	Entpacken Sie das Bereitstellungspaket, das Sie von Azure App Service herunterg	App-Entwickler, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eladen haben. Erstellen Sie eine JSON-Datei mit dem Namen `aws-windows-deployment-manifest.json` (diese Datei ist nur für.NET Core-Anwendungen erforderlich). Erstellen Sie eine ZIP-Datei, die die Azure App Service-Bereitstellungspaketdatei enthält`aws-windows-deployment-manifest.json`. Ein Beispiel finden Sie im Anhang.	
Erstellen Sie eine neue Elastic Beanstalk Beanstalk-Anwendung.	In der Elastic-Beanstalk-Konsole öffnen. Wählen Sie eine bestehende Anwendung oder erstellen Sie eine neue Anwendung.	App-Entwickler, Systemadministrator
Erstellen Sie die Umgebung.	Wählen Sie im Aktionsmenü der Elastic Beanstalk Beanstalk-Konsole die Option Umgebung erstellen aus. Wählen Sie die Webserver-Umgebung und die .NET/IIS-Plattform aus. Wählen Sie für Anwendungscode Upload aus. Laden Sie die ZIP-Datei hoch, die Sie für Elastic Beanstalk vorbereitet haben, und wählen Sie dann Create Environment.	App-Entwickler, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Amazon CloudWatch.	Standardmäßig ist die grundlegende CloudWatch Überwachung aktiviert. Wenn Sie die Konfiguration ändern möchten, wählen Sie im Elastic Beanstalk-Assistenten die veröffentlichte Anwendung und dann Monitoring aus.	Systemadministrator
Stellen Sie sicher, dass sich das Bereitstellungspaket in Amazon S3 befindet.	Wenn die Anwendung sumgebung erstellt wurde, finden Sie das Bereitste llungspaket im S3-Bucket.	App-Entwickler, Systemadm inistrator
Testen Sie die Anwendung.	Wenn die Umgebung erstellt wurde, verwenden Sie die in der Elastic Beanstalk Beanstalk-Konsole angegeben e URL, um die Anwendung zu testen.	Systemadministrator

Zugehörige Ressourcen

- Konzepte von AWS Elastic Beanstack (Elastic Beanstalk Beanstalk-Dokumentation)
- Erste Schritte mit.NET auf Elastic Beanstalk (Elastic Beanstalk Beanstalk-Dokumentation)
- Kudu-Konsole () GitHub
- Verwendung von „Kudu“ zur Verwaltung von Azure Web Apps (GS Lab-Artikel)
- Benutzerdefinierte ASP.NET Core Elastic Beanstalk Beanstalk-Bereitstellungen (AWS Toolkit for Visual Studio Studio-Benutzerhandbuch)
- Dokumentation zu Elastic Load Balancing
- Von AWS Elastic Beanstalk unterstützte Plattformen (Elastic Beanstalk Beanstalk-Dokumentation)
- Bereitstellen einer Webanwendung in AWS (C# Corner-Artikel)
- Skalierung der Größe Ihrer Auto Scaling Scaling-Gruppe (EC2 Amazon-Dokumentation)

- Hochverfügbarkeit (Multi-AZ) für Amazon RDS (Amazon RDS-Dokumentation)

Zusätzliche Informationen

Hinweise

- Wenn Sie eine lokale Datenbank oder eine Azure SQL Server-Datenbank zu Amazon RDS migrieren, müssen Sie auch die Datenbankverbindungsdetails aktualisieren.
- Zu Testzwecken ist eine Beispiel-Demoanwendung beigefügt.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Migrieren Sie von Oracle WebLogic zu Apache Tomcat (ToMEE) auf Amazon ECS

Erstellt von Anya Epishcheva (AWS) und Harshad Gohil (AWS)

Übersicht

In diesem Muster werden die Schritte für die Migration eines lokalen Oracle Solaris SPARC-Systems, auf dem Oracle ausgeführt wird, WebLogic zu einer Docker-Container-basierten Installation beschrieben, auf der Apache TomEE (Apache Tomcat mit zusätzlicher Container-Unterstützung) mit Amazon Elastic Container Service (Amazon ECS) ausgeführt wird.

Informationen zur Migration von Datenbanken, die mit den Anwendungen verknüpft sind, die Sie von Oracle WebLogic zu Tomcat migrieren, finden Sie in den Datenbankmigrationsmustern in diesem Katalog.

Bewährte Methoden

Die Schritte für die Migration von Java- und Java Enterprise Edition (Java EE) -Webanwendungen variieren je nach der Anzahl der containerspezifischen Ressourcen, die von der Anwendung verwendet werden. Spring-basierte Anwendungen sind in der Regel einfacher zu migrieren, da sie eine geringe Anzahl von Abhängigkeiten vom Bereitstellungscontainer aufweisen. Im Gegensatz dazu erfordern Java EE-Anwendungen, die Enterprise JavaBeans (EJBs) und verwaltete Container-Ressourcen wie Thread-Pools, Java Authentication and Authorization Service (JAAS) und Container-Managed Persistence (CMP) verwenden, mehr Aufwand.

Anwendungen, die für Oracle Application Server entwickelt wurden, verwenden häufig die Oracle Identity Management Suite. Kunden, die auf Open-Source-Anwendungsserver migrieren, entscheiden sich häufig dafür, Identitäts- und Zugriffsmanagement mithilfe eines SAML-basierten Verbunds neu zu implementieren. Andere verwenden Oracle HTTP Server Webgate für Fälle, in denen eine Migration von der Oracle Identity Management Suite keine Option ist.

Java- und Java EE-Webanwendungen eignen sich hervorragend für die Bereitstellung auf Docker-basierten AWS-Services wie AWS Fargate und Amazon ECS. Kunden entscheiden sich häufig für ein Docker-Image, auf dem die neueste Version des Zielanwendungsservers (z. B. TomEE) und das Java Development Kit (JDK) vorinstalliert sind. Sie installieren ihre Anwendungen auf dem Basis-Decker-Image, veröffentlichen es in ihrer Amazon Elastic Container Registry (Amazon ECR) -Registrierung und verwenden es für die skalierbare Bereitstellung ihrer Anwendungen auf AWS Fargate oder Amazon ECS.

Im Idealfall ist die Anwendungsbereitstellung elastisch, d. h. die Anzahl der Anwendungsinstanzen skaliert je nach Traffic oder Arbeitslast nach oben oder unten. Das bedeutet, dass

Anwendungsinstanzen online gehen oder beendet werden müssen, um die Kapazität an den Bedarf anzupassen.

Wenn Sie eine Java-Anwendung nach AWS verschieben, sollten Sie erwägen, sie zustandslos zu machen. Dies ist ein zentrales Architekturprinzip des AWS Well-Architected Framework, das eine horizontale Skalierung mithilfe von Containerisierung ermöglicht. Beispielsweise speichern die meisten Java-basierten Webanwendungen Benutzersitzungsinformationen lokal. Um die Beendigung der Anwendungsinstanz aufgrund der automatischen Skalierung in Amazon Elastic Compute Cloud (Amazon EC2) oder aus anderen Gründen zu überstehen, sollten Benutzersitzungsinformationen global gespeichert werden, sodass Benutzer von Webanwendungen weiterhin nahtlos und transparent arbeiten können, ohne sich erneut mit einer Webanwendung verbinden oder erneut anmelden zu müssen. Für diesen Ansatz gibt es mehrere Architekturoptionen, darunter Amazon ElastiCache for Redis oder das Speichern des Sitzungsstatus in einer globalen Datenbank. Anwendungsserver wie TomEE verfügen über Plug-ins, die die Speicherung und Verwaltung von Sitzungen über Redis, Datenbanken und andere globale Datenspeicher ermöglichen.

Verwenden Sie ein gemeinsames, zentralisiertes Protokollierungs- und Debugging-Tool, das sich leicht in Amazon CloudWatch und AWS X-Ray integrieren lässt. Die Migration bietet die Möglichkeit, die Funktionen des Anwendungslebenszyklus zu verbessern. Möglicherweise möchten Sie den Erstellungsprozess automatisieren, sodass Änderungen mithilfe einer CI/CD-Pipeline (Continuous Integration and Continuous Delivery) problemlos vorgenommen werden können. Dies kann Änderungen an der Anwendung erfordern, sodass sie ohne Ausfallzeiten bereitgestellt werden kann.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Java-Quellcode und JDK
- Mit Oracle erstellte Quellanwendung WebLogic
- Definierte Lösung für Identitäts- und Zugriffsmanagement (SAML oder Oracle Webgate)
- Definierte Lösung für die Verwaltung von Anwendungssitzungen (Umzug like-for-like oder mit Amazon oder Zustandslosigkeit der Anwendung ElastiCache, falls erforderlich)
- Erläuterung, ob das Team J2EE-spezifische Bibliotheken umgestalten muss, um die Portabilität auf Apache ToMEE zu gewährleisten (siehe Status der Implementierung von Java EE 7 auf der Apache-Website)
- Gehärtetes ToMEE-Image auf der Grundlage Ihrer Sicherheitsanforderungen

- Container-Image mit vorinstalliertem Ziel-TomEE
- Vereinbarte und bei Bedarf durchgeführte Anwendungskorrektur (z. B. Protokollierung, Debug-Erstellung, Authentifizierung)

Versionen der Produkte

- Oracle WebLogic OC4 J, 9i, 10 g
- Tomcat 7 (mit Java 1.6 oder höher)

Architektur

Quelltechnologie-Stack

- Mit Oracle erstellte Webanwendung WebLogic
- Webanwendung, die Oracle Webgate oder SAML-Authentifizierung verwendet
- Webanwendungen, die mit Oracle Database Version 10g und höher verbunden sind

Zieltechnologie-Stack

- ToMee (Apache Tomcat mit zusätzlicher Container-Unterstützung) läuft auf Amazon ECS (siehe auch Bereitstellen von Java-Webanwendungen und Java-Microservices auf Amazon ECS)
- Amazon Relational Database Service (Amazon RDS) für Oracle; Informationen zu Oracle-Versionen, die von Amazon RDS unterstützt werden, finden Sie unter Amazon RDS for Oracle

Zielarchitektur

Tools

Um mit TomEE arbeiten zu können, muss eine Java-Anwendung in eine WAR-Datei neu erstellt werden. In einigen Fällen können Änderungen an der Anwendung erforderlich sein, um die Anwendung auf ToMEE ausführen zu können. Sie sollten überprüfen, ob die erforderlichen Konfigurationsoptionen und Umgebungseigenschaften korrekt definiert sind.

Außerdem sollten JNDI-Lookups (Java Naming and Directory Interface) und JSP-Namespaces (JavaServer Pages) korrekt definiert sein. Erwägen Sie, die von der Anwendung verwendeten

Dateinamen zu überprüfen, um Namenskonflikte mit integrierten T-Bibliotheken zu vermeiden. Zum Beispiel ist persistence.xml ein Dateiname, der vom Apache OpenJPA-Framework (das mit OpenEJB in TomEE gebündelt ist) für Konfigurationszwecke verwendet wird. Die Datei persistence.xml in PUI enthält Bean-Deklarationen für das Spring Framework.

ToMee Version 7.0.3 und höher (Tomcat 8.5.7 und höher) gibt eine HTTP 400-Antwort (schlechte Anfrage) für uncodierte Rohdaten mit Sonderzeichen zurück. URLs Die Serverantwort wird dem Endbenutzer als leere Seite angezeigt. Frühere Versionen von ToMee und Tomcat erlaubten die Verwendung bestimmter unverschlüsselter Sonderzeichen in URLs; dies gilt jedoch als unsicher, wie auf der CVE-2016-6816-Website angegeben. Um das Problem mit der URL-Kodierung zu lösen, JavaScript müssen die direkt URLs an den Browser übergebenen Daten mit der Methode encodeURI () codiert werden, anstatt als unformatierte Zeichenketten verwendet zu werden.

Nachdem Sie die .war-Datei in ToMEE bereitgestellt haben, überprüfen Sie das Startprotokoll von Linux Cat auf fehlende gemeinsam genutzte Bibliotheken und Oracle-spezifische Erweiterungen, um fehlende Komponenten aus Tomcat-Bibliotheken hinzuzufügen.

Allgemeines Verfahren

- Konfigurieren Sie die Anwendung auf TomEE.
- Identifizieren und rekonfigurieren Sie anwendungsserverspezifische Konfigurationsdateien und Ressourcen vom Quell- bis zum Zielformat.
- Identifizieren und rekonfigurieren Sie JNDI-Ressourcen.
- Passen Sie den EJB-Namespace und die Lookups an das vom Zielanwendungsserver benötigte Format an (falls zutreffend).
- Konfigurieren Sie containerspezifische Sicherheitsrollen und Prinzipalzuordnungen für JAAS-Anwendungen neu (falls zutreffend).
- Package Sie die Anwendung und die gemeinsam genutzten Bibliotheken in eine WAR-Datei.
- Stellen Sie die .war-Datei in TomEE mithilfe des bereitgestellten Docker-Containers bereit.
- Überwachen Sie das Startprotokoll, um alle fehlenden Erweiterungen für gemeinsam genutzte Bibliotheken und Bereitstellungsdeskriptoren zu identifizieren. Wenn welche gefunden wurden, kehren Sie zur ersten Aufgabe zurück.
- Testen Sie die installierte Anwendung anhand der wiederhergestellten Amazon RDS-Datenbank.
- Starten Sie die komplette Architektur mit einem Load Balancer und einem Amazon ECS-Cluster, indem Sie den Anweisungen unter Deploy Docker Containers folgen.

- Aktualisieren Sie die URLs , um auf den Load Balancer zu verweisen.
- Aktualisieren Sie die Configuration Management Database (CMDB).

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie eine Anwendung serkennung durch (aktueller Status und Leistungsbasis).		BA, Leiter der Migration
Validieren Sie die Versionen und Engines der Quell- und Zieldatenbank.		DBA
Validieren Sie das Design der Quell- und Zielanwendung (Identitäts- und Sitzungsm anagement).		DBA, Migrationsingenieur, App-Besitzer
Identifizieren Sie die Hardware- und Speichera nforderungen für die Zielserve rinstanz.		DBA, SysAdmin
Wählen Sie den richtigen Instanztyp auf der Grundlage von Kapazität, Speicherf unktionen und Netzwerkf unktionen aus.		DBA, SysAdmin
Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.		DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Strategie und die Tools für die Anwendungsmigration.		DBA, Leiter der Migration
Füllen Sie das Migration sdesign und den Migration sleitfaden für die Anwendung aus.		Leitung aufbauen, Leitung Migration
Füllen Sie das Runbook zur Anwendungsmigration aus.		Leiter Aufbau, Leiter der Umstellung, Leiter des Tests, Leiter der Migration

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC).		SysAdmin
Erstellen Sie Sicherhei tsgruppen.		SysAdmin
Konfigurieren und starten Sie die Amazon RDS-DB-In stance.		DBA, SysAdmin
Konfigurieren Sie die Amazon ECS-Bereitstellung.		SysAdmin
Package Sie Ihre Anwendung als Docker-Image.		SysAdmin
Übertragen Sie das Image in die Amazon ECR-Regis trierung (oder übersprin		SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
gen Sie diesen Schritt und übertragen Sie es in den Amazon ECS-Cluster).		
Konfigurieren Sie die Aufgabendefinition für die Anwendung und die Amazon ECS-Serviceoptionen.		SysAdmin
Konfigurieren Sie Ihren Cluster, überprüfen Sie die Sicherheitseinstellungen und legen Sie AWS Identity and Access Management (IAM) - Rollen fest.		SysAdmin
Starten Sie Ihr Setup und führen Sie Tests gemäß Ihrem Runbook für die Anwendung smigration aus.		SysAdmin

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Holen Sie sich die Erlaubnis Ihres Sicherheitsteams, Produktionsdaten nach AWS zu verschieben.		DBA, Migrationsingenieur, App-Besitzer
Erstellen Sie Endpunkte und erhalten Sie Zugriff auf diese, um Datenbank-Backupdateien abzurufen.		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie die native Datenbank-Engine oder Tools von Drittanbietern, um Datenbankobjekte und Daten zu migrieren.		DBA
Führen Sie die erforderlichen Tests im Runbook für die Anwendungsmigration aus, um die erfolgreiche Datenmigration zu bestätigen.		DBA, Migrationsingenieur, App-Besitzer

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Änderungsantrag (CR) für die Migration.		Leitung der Umstellung
Besorgen Sie sich die CR-Genehmigung für die Migration.		Übernahme (Leitung)
Folgen Sie der Strategie zur Anwendungsmigration aus dem Runbook zur Anwendungsmigration.		DBA, Migrationsingenieur, App-Besitzer
Aktualisieren Sie die Anwendung (falls erforderlich).		DBA, Migrationsingenieur, App-Besitzer
Führen Sie funktionale und nichtfunktionale Tests sowie Datenvalidierungs-, SLA- und Leistungstests durch.		Testleiter, App-Besitzer, App-Nutzer

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Lassen Sie sich vom Antrag oder Geschäftsinhaber unterschreiben.		Übernahme (Leitung)
Führen Sie eine Übung mit einem Tabellenthema durch, in der Sie alle Schritte des Cutover-Runbooks durchgehe n.		DBA, Migrationsingenieur, App-Besitzer
Wechseln Sie zu den Anwendungsclients auf die neue Infrastruktur.		DBA, Migrationsingenieur, App-Besitzer

Schließen Sie das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie temporäre AWS-Ressourcen herunter.		DBA, Migrationsingenieur, SysAdmin
Überprüfen und validieren Sie die Projektdokumente.		Leiter der Migration
Erfassen Sie Kennzahlen zum Zeitpunkt der Migration, zum prozentualen Anteil manueller Änderungen im Vergleich zu Tools, zu Kosteneinsparungen usw.		Leiter der Migration
Schließen Sie das Projekt ab und geben Sie Feedback.		Leiter der Migration, Inhaber der App

Zugehörige Ressourcen

Referenzen

- Dokumentation zu Apache Tomcat 7.0
- Installationsanleitung für Apache Tomcat 7.0
- Apache Tomcat JNDI-Dokumentation
- Apache TomEE-Dokumentation
- Amazon RDS für Oracle
- Amazon-RDS-Preise
- Oracle und AWS
- Dokumentation zu Oracle auf Amazon RDS
- Amazon RDS Multi-AZ-Bereitstellungen
- Erste Schritte mit Amazon ECS
- Erste Schritte mit Amazon RDS

Tutorials und Videos

- Bewährte Methoden für den Betrieb von Oracle-Datenbanken auf Amazon RDS (Präsentation re:Invent 2018)

Migrieren Sie mithilfe von AWS DMS eine Oracle-Datenbank von Amazon EC2 zu Amazon RDS for Oracle

Erstellt von Chethan Gangadharaiah (AWS) und Brian Motzer (AWS)

Übersicht

Dieses Muster beschreibt die Schritte zur Migration einer Oracle-Datenbank auf Amazon Elastic Compute Cloud (Amazon EC2) zu Amazon Relational Database Service (Amazon RDS) für Oracle mithilfe von AWS Database Migration Service (AWS DMS). Das Muster verwendet auch Oracle SQL Developer oder SQL *Plus, um eine Verbindung zu Ihrer Oracle-DB-Instance herzustellen, und beinhaltet eine CloudFormation AWS-Vorlage, die einige der Aufgaben automatisiert.

Durch die Migration zu Amazon RDS for Oracle können Sie sich auf Ihr Geschäft und Ihre Anwendungen konzentrieren, während Amazon RDS sich um Datenbankverwaltungsaufgaben wie die Bereitstellung von Datenbanken, Sicherung und Wiederherstellung, Sicherheitspatches, Versions-Upgrades und Speichermanagement kümmert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Amazon Machine Image (AMI) für Oracle Database auf Amazon EC2

Produktversionen

- AWS DMS unterstützt die Oracle-Versionen 11g (Version 11.2.0.3.v1 und höher), 12c und 18c für Amazon RDS-Instance-Datenbanken für die Editionen Enterprise, Standard, Standard One und Standard Two. Aktuelle Informationen zu unterstützten Versionen finden Sie in der AWS-Dokumentation unter Using an Oracle Database as a Target for AWS DMS. (Die angehängten CloudFormation AWS-Vorlagen verwenden Oracle Version 12c als Quelldatenbank.)
- Oracle SQL Developer 4.0.3

Architektur

Quellarchitektur

- Oracle-Datenbank auf Amazon EC2

Zielarchitektur

- Amazon RDS für Oracle

Migrationsarchitektur

Tools

- AWS DMS — Mit dem AWS Database Migration Service (AWS DMS) können Sie Datenbanken schnell und sicher zu AWS migrieren. Es unterstützt sowohl homogene als auch heterogene Migrationen. Informationen zu den unterstützten Oracle-Datenbankversionen und -Editionen finden Sie in der AWS-Dokumentation unter Verwenden einer Oracle-Datenbank als Quelle für AWS DMS und Verwenden einer Oracle-Datenbank als Ziel für AWS DMS.
- Oracle SQL Developer oder SQL *Plus — Mit diesen Tools können Sie eine Verbindung zur Amazon RDS for Oracle Oracle-DB-Instance herstellen.

Epen

Richten Sie Ihre Zieldatenbank ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon RDS for Oracle Oracle-DB-Instance.	Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon RDS-Konsole unter https://console.aws.amazon.com/rds/. Erstellen Sie eine Oracle-DB-Instance, indem Sie die entsprechende Engine, Vorlage, Einstellung für Datenbankanmeldedaten, Instance-Typ, Speicher, Multi-AZ-Einstellungen, Virtual Private Cloud (VPC) und Konfiguration, Anmeldein	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	formationen und zusätzlic he Einstellungen für die Oracle-Datenbank auswählen . Anweisungen finden Sie unter den Links im Abschnitt „Verwandte Ressourcen“. Oder verwenden Sie die CloudFormation AWS-Vorla ge (create_rds.YAML) im Anhang, um die Amazon RDS for Oracle Oracle-DB-Instance zu erstellen.	
Connect zu Amazon RDS her und gewähren Sie dem Oracle-Benutzer Rechte.	Ändern Sie die Sicherhei tsgruppe, um die entsprech enden Ports für die Verbindun g vom lokalen Computer und der AWS DMS-Replikationsin stanz aus zu öffnen. Stellen Sie bei der Konfiguration der Konnektivität sicher, dass die Option „Öffentlich zugänglic h“ ausgewählt ist, damit Sie von außerhalb der VPC eine Verbindung zur Datenbank herstellen können. Stellen Sie mit Oracle SQL Developer oder SQL *Plus mithilfe der Anmeldeinformationen eine Connect zu Amazon RDS her, erstellen Sie einen AWS DMS-Benutzer und gewähren Sie dem AWS DMS-Benutzer die erforderlichen Rechte, um die Datenbank zu ändern.	Developer

Konfigurieren Sie die Sicherheitsgruppe der Quell-Instance EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Prüfen Sie, ob die Oracle-Datenbank läuft.	Verwenden Sie Secure Shell (SSH), um eine Verbindung zur EC2 Instance herzustellen, und versuchen Sie, mithilfe von SQL *Plus eine Verbindung zur Oracle-Datenbank herzustellen.	Developer
Ändern Sie die Sicherheitsgruppe.	Ändern Sie die Sicherheitsgruppe der EC2 Instance, um die entsprechenden Ports zu öffnen, sodass Sie von Ihrem lokalen Computer und der AWS DMS-Replikationsinstanz aus eine Verbindung herstellen können.	Developer

AWS DMS einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS DMS-Replikations-Instance.	Erstellen Sie in AWS DMS eine Replikationsinstanz in derselben VPC wie Ihre Amazon RDS for Oracle DB-Instance. Geben Sie den Namen und die Beschreibung für die Replikationsinstanz an, wählen Sie die Instance-Klasse und die Version der Replication Engine (verwenden Sie die Standardversion),	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wählen Sie die VPC aus, in der Sie die Amazon RDS-DB-Instance erstellt haben, legen Sie bei Bedarf Multi-AZ-Einstellungen fest, weisen Sie Speicher zu, geben Sie die Availability Zone an und konfigurieren Sie zusätzliche Einstellungen. Alternativ können Sie die CloudFormation AWS-Vorlage (dms.YAML) im Anhang verwenden, um diesen Schritt zu implementieren.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Connect zu den Quell- und Zieldatenbank-Endpunkten her.	Erstellen Sie die Quell- und Zieldatenbankendpunkte, indem Sie die Endpunkt-ID, die Engine, den Server, den Port, die Anmeldeinformationen und zusätzliche Verbindungsattribute angeben. Verwenden Sie für den Quellserver den öffentlichen DNS der EC2 Instanz, die die Oracle-Datenbank hostet. Verwenden Sie für den Zielserver den Endpunkt von Amazon RDS for Oracle. Führen Sie einen Test durch, um zu überprüfen, ob die Quell- und Zielverbindungen funktionieren. Alternativ können Sie die CloudFormation AWS-Vorlage (dms.YAML) im Anhang verwenden, um diesen Schritt zu implementieren.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS DMS-Aufgabe.	Erstellen Sie eine AWS DMS-Aufgabe, um Daten vom Quellendpunkt zum Zielendpunkt zu migrieren, um die Replikation zwischen dem Quell- und Zielendpunkt oder beiden einzurichten. Geben Sie bei der Erstellung der AWS DMS-Aufgabe die Replikationsinstanz, den Quellendpunkt, den Zielendpunkt, den Migrationstyp (nur Daten, nur Replikation oder beides), die Tabellenzuordnung und den Filter an. Führen Sie die AWS DMS-Aufgabe aus, überwachen Sie die Aufgabe, überprüfen Sie die Tabellenstatistiken und überprüfen Sie die Protokolle in Amazon CloudWatch. Alternativ können Sie die CloudFormation AWS-Vorlage (dms.YAML) im Anhang verwenden, um diesen Schritt zu implementieren.	DBA

Zugehörige Ressourcen

- Eine Amazon RDS-DB-Instance erstellen
- Eine Verbindung zu einer DB-Instance aufbauen, die mit der Oracle-Datenbank-Engine ausgeführt wird
- AWS DMS-Dokumentation

- Exemplarische Vorgehensweisen zu AWS DMS Step-by-Step
- Migration von Oracle-Datenbanken in die AWS-Cloud

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Migrieren Sie eine lokale Oracle-Datenbank mit Logstash zu Amazon OpenSearch Service

Erstellt von Aditya Goteti (AWS)

Übersicht

Dieses Muster beschreibt, wie Daten mithilfe von Logstash aus einer lokalen Oracle-Datenbank zu Amazon OpenSearch Service verschoben werden. Es beinhaltet architektonische Überlegungen sowie einige erforderliche Fähigkeiten und Empfehlungen. Die Daten können aus einer einzelnen Tabelle oder aus mehreren Tabellen stammen, in denen eine Volltextsuche durchgeführt werden muss.

OpenSearch Der Dienst kann in einer Virtual Private Cloud (VPC) konfiguriert oder mit IP-basierten Einschränkungen öffentlich platziert werden. Dieses Muster beschreibt ein Szenario, in dem der OpenSearch Dienst in einer VPC konfiguriert ist. Logstash wird verwendet, um die Daten aus der Oracle-Datenbank zu sammeln, sie im JSON-Format zu parsen und die Daten dann in Service einzuspeisen. OpenSearch

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Java 8 (für Logstash 6.4.3 erforderlich)
- Konnektivität zwischen den lokalen Datenbankservern und Amazon Elastic Compute Cloud (Amazon EC2) -Instances in einer VPC, eingerichtet mit AWS Virtual Private Network (AWS VPN)
- Eine Abfrage zum Abrufen der erforderlichen Daten, die an den OpenSearch Service übertragen werden sollen, aus der Datenbank
- Treiber für Oracle Java Database Connectivity (JDBC)

Einschränkungen

- Logstash kann keine Datensätze identifizieren, die dauerhaft aus der Datenbank gelöscht wurden

Versionen der Produkte

- Oracle Datenbank 12c

- OpenSearch Service 6.3
- Logstash 6.4.3

Architektur

Quelltechnologie-Stack

- Lokale Oracle-Datenbank
- Lokales AWS-VPN

Zieltechnologie-Stack

- VPC
- EC2 Instanz
- OpenSearch Dienst
- Logstash
- NAT Gateway (für Betriebssystem-Updates auf EC2 Instanzen und zur Installation von Java 8, Logstash und Plugins)

Architektur der Datenmigration

Tools

- Logstash 6.4.3
- JDBC-Eingabe-Plugin (Download und weitere Informationen)
- Logstash-Ausgabe-Plugin (_es) logstash-output-amazon
- Oracle JDBC-Treiber

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Größe der Quelldaten.	Die Größe der Quelldaten ist einer der Parameter, mit denen Sie die Anzahl der Shards bestimmen, die in einem Index konfiguriert werden sollen.	DBA, Datenbankentwickler
Analysieren Sie die Datentypen jeder Spalte und die entsprechenden Daten.	OpenSearch Service ordnet den Datentyp dynamisch zu, wenn ein zuvor unsichtbares Feld im Dokument gefunden wird. Wenn bestimmte Datentypen oder Formate (z. B. Datumsfelder) explizit deklariert werden müssen, identifizieren Sie die Felder und definieren Sie die Zuordnung für diese Felder bei der Indexerstellung.	App-Besitzer, Entwickler, Datenbankentwickler
Ermitteln Sie, ob Spalten mit Primärschlüsseln oder eindeutigen Schlüsseln vorhanden sind.	Um bei Aktualisierungen oder Einfügungen doppelte Datensätze in Amazon OpenSearch Service zu vermeiden, müssen Sie die `document_id` Einstellung im Ausgabebereich des `amazon_es` Plug-ins konfigurieren (z. B. `document_id => "%{customer_id}"`	Besitzer der App, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wo `customer_id` ist ein Primärschlüssel).	
Analysieren Sie die Anzahl und Häufigkeit neu hinzugefügter Datensätze und überprüfen Sie, wie oft die Datensätze gelöscht werden.	Diese Aufgabe ist erforderlich, um die Wachstumsrate von Quelldaten zu verstehen. Wenn Daten intensiv gelesen werden und Einfügungen selten sind, können Sie einen einzigen Index verwenden. Wenn häufig neue Datensätze eingefügt werden und keine Löschungen vorgenommen werden, kann die Shard-Größe leicht die empfohlene Maximalgröße von 50 GB überschreiten. In diesem Fall können Sie einen Index dynamisch erstellen, indem Sie Indexmuster in Logstash und im Code konfigurieren, über den Sie mithilfe eines Alias darauf zugreifen können.	Besitzer der App, Entwickler
Ermitteln Sie, wie viele Replikate erforderlich sind.		Besitzer der App, Entwickler
Ermitteln Sie die Anzahl der Shards, die für den Index konfiguriert werden sollen.		Besitzer der App, Entwickler
Identifizieren Sie die Instanztypen für dedizierte Master-Knoten, Datenknoten und die EC2 Instanz.	Weitere Informationen finden Sie im Abschnitt Verwandte Ressourcen.	Besitzer der App, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie die Anzahl der erforderlichen dedizierten Master- und Datenknoten.	Weitere Informationen finden Sie im Abschnitt Verwandte Ressourcen.	

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie eine EC2 Instanz.	Starten Sie eine EC2 Instance innerhalb der VPC, mit der AWS VPN verbunden ist.	Amazon VPC-Konstrukte, AWS-VPN
Installieren Sie Logstash auf der Instance. EC2		Developer
Installieren Sie die Logstash-Plugins.	Installieren Sie die erforderl ichen Logstash-Plugins und. `jdbc-input logstash-output-amazon_es`	Developer
Konfigurieren Sie Logstash.	Erstellen Sie den Logstash-Keystore, um vertrauliche Informationen wie AWS Secrets Manager Manager-Schlüssel und Datenbank anmeldedaten zu speichern , und platzieren Sie die Verweise dann in einer Logstash-Konfigurationsdatei.	Developer
Konfigurieren Sie die Warteschlange für unzulässi ge Nachrichten und die permanente Warteschlange.	Wenn Logstash auf ein Ereignis trifft, das nicht verarbeitet werden kann, weil die Daten einen Zuordnung sfehler oder ein anderes	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Problem enthalten, hängt die Logstash-Pipeline standardmäßig entweder oder löscht das erfolglose Ereignis. Um in dieser Situation vor Datenverlust zu schützen, können Sie Logstash so konfigurieren, dass erfolglose Ereignisse in eine Warteschlange mit unbestätigten Nachrichten geschrieben werden, anstatt sie zu löschen. Zum Schutz vor Datenverlust bei abnormalem Abbruch verfügt Logstash über eine persistente Warteschlangenfunktion, die die Nachrichtenwarteschlange auf der Festplatte speichert. Persistente Warteschlangen sorgen für die Beständigkeit der Daten in Logstash.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Amazon OpenSearch Service-Domain.	Erstellen Sie die Amazon OpenSearch Service-Domain mit einer Zugriffsrichtlinie , die keine Signierung von Anfragen mit AWS Identity and Access Management (IAM) -Anmeldeinformationen erfordert. Die Amazon OpenSearch Service-Domain muss innerhalb derselben VPC erstellt werden. Sie sollten auch die Instance-Typen auswählen und die Anzahl der dedizierten Knoten und Master-Knoten auf der Grundlage Ihrer Analyse festlegen.	Developer
Konfigurieren Sie die erforderlichen Amazon OpenSearch Service-Protokolle.	Weitere Informationen finden Sie in der OpenSearch Servicedokumentation.	
Erstellen Sie den Index.		Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie Logstash.	Führen Sie Logstash als Hintergrunddienst aus. Logstash führt die konfiguri erte SQL-Abfrage aus, ruft die Daten ab, konvertiert sie in das JSON-Format und leitet sie an Service weiter. OpenSearch Für den ersten Ladevorgang sollten Sie den Scheduler nicht in der Logstash-Konfigurationsdatei konfigurieren.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Dokumente.	Überprüfen Sie die Anzahl der Dokumente im Index und ob alle Dokumente in der Quelldatenbank vorhanden sind. Beim ersten Laden werden sie dem Index hinzugefügt und zum Stoppen von Logstash verwendet. Ändern Sie die Logstash-Konfiguration, um einen Scheduler hinzuzufügen, der je nach Client-Anforderung en in einem festen Intervall läuft, und starten Sie Logstash neu. Logstash wählt nur die Datensätze aus, die nach dem letzten Lauf aktualisi ert oder hinzugefügt wurden, und der Zeitstempel der letzten Ausführung wird in der Datei gespeichert, die mit der Eigenschaft in der Logstash-Konfigurationsdate i konfiguriert ist. `last_run_ metadata_path => “/usr/share/logsta sh/.logstash_jdbc_ last_run”`	Developer

Zugehörige Ressourcen

- Empfohlene CloudWatch Alarme
- Dedizierte Amazon OpenSearch Service Master Nodes

- Dimensionierung von Amazon OpenSearch Service-Domains
- Logstash-Dokumentation
- JDBC-Eingabe-Plugin
- Logstash-Ausgabe-Plugin
- Amazon OpenSearch Service-Webseite

Migrieren Sie eine lokale Oracle-Datenbank zu Amazon RDS for Oracle

Erstellt von Baji Shaik (AWS) und Pavan Pusuluri (AWS)

Übersicht

Dieses Muster beschreibt die Schritte für die Migration von lokalen Oracle-Datenbanken zu Amazon Relational Database Service (Amazon RDS) für Oracle. Im Rahmen des Migrationsprozesses erstellen Sie einen Migrationsplan und berücksichtigen wichtige Faktoren in Bezug auf Ihre Zieldatenbankinfrastruktur auf der Grundlage Ihrer Quelldatenbank. Sie können je nach Ihren Geschäftsanforderungen und Ihrem Anwendungsfall eine von zwei Migrationsoptionen wählen:

- AWS Database Migration Service (AWS DMS) — Mit AWS DMS können Sie Datenbanken schnell und sicher in die AWS-Cloud migrieren. Ihre Quelldatenbank bleibt während der Migration voll funktionsfähig, wodurch die Ausfallzeiten von Anwendungen, die auf die Datenbank angewiesen sind, minimiert werden. Sie können die Migrationszeit reduzieren, indem Sie mit AWS DMS eine Aufgabe erstellen, die laufende Änderungen erfasst, nachdem Sie eine erste Volllastmigration über einen Prozess namens Change Data Capture (CDC) abgeschlossen haben.
- Systemeigene Oracle-Tools — Sie können Datenbanken mithilfe systemeigener Oracle-Tools wie Oracle und Data Pump Export und Data Pump Import mit Oracle for GoldenGate CDC migrieren. Sie können auch native Oracle-Tools wie das ursprüngliche Export-Hilfsprogramm und das ursprüngliche Import-Hilfsprogramm verwenden, um die Vollladezeit zu reduzieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine lokale Oracle-Datenbank
- Eine Amazon RDS-Oracle-Datenbank-Instance (DB)

Einschränkungen

- Größenbeschränkung der Datenbank: 64 TB

Produktversionen

- Oracle-Versionen 11g (Versionen 11.2.0.3.v1 und höher) und bis zu 12.2 und 18c. Die aktuelle Liste der unterstützten Versionen und Editionen finden Sie in der AWS-Dokumentation unter Amazon RDS for Oracle. Informationen zu Oracle-Versionen, die von AWS DMS unterstützt werden, finden Sie unter Verwenden einer Oracle-Datenbank als Quelle für AWS DMS in der AWS DMS-Dokumentation.

Architektur

Quelltechnologie-Stack

- Lokale Oracle-Datenbanken

Zieltechnologie-Stack

- Amazon RDS für Oracle

Quell- und Zielarchitektur

Das folgende Diagramm zeigt, wie eine lokale Oracle-Datenbank mithilfe von AWS DMS zu Amazon RDS for Oracle migriert wird.

Das Diagramm zeigt den folgenden Workflow:

1. Erstellen oder verwenden Sie einen vorhandenen Datenbankbenutzer, gewähren Sie diesem Benutzer die erforderlichen AWS DMS-Berechtigungen, aktivieren Sie den ARCHIVELOG-Modus und richten Sie dann die zusätzliche Protokollierung ein.
2. Konfigurieren Sie das Internet-Gateway zwischen dem lokalen Netzwerk und dem AWS-Netzwerk.
3. Konfigurieren Sie Quell- und Zielendpunkte für AWS DMS.
4. Konfigurieren Sie AWS DMS-Replikationsaufgaben, um die Daten von der Quelldatenbank zur Zieldatenbank zu migrieren.
5. Schließen Sie die Aktivitäten nach der Migration in der Zieldatenbank ab.

Das folgende Diagramm zeigt, wie eine lokale Oracle-Datenbank mithilfe nativer Oracle-Tools zu Amazon RDS for Oracle migriert wird.

Das Diagramm zeigt den folgenden Workflow:

1. Erstellen oder verwenden Sie einen vorhandenen Datenbankbenutzer und gewähren Sie die erforderlichen Berechtigungen zum Sichern der Oracle-Datenbank mithilfe der Oracle-Dienstprogramme Export (`exp`) und Import (`imp`).
2. Konfigurieren Sie das Internet-Gateway zwischen dem lokalen Netzwerk und dem AWS-Netzwerk.
3. Konfigurieren Sie den Oracle-Client auf dem Bastion-Host so, dass er die Backup-Datenbank verwendet.
4. Laden Sie die Backup-Datenbank in einen Amazon Simple Storage Service (Amazon S3) -Bucket hoch.
5. Stellen Sie die Datenbanksicherung von Amazon S3 in einer Amazon RDS for Oracle Oracle-Datenbank wieder her.
6. Konfigurieren Sie Oracle GoldenGate für CDC.
7. Schließen Sie die Aktivitäten nach der Migration in der Zieldatenbank ab.

Tools

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS-Cloud oder zwischen Kombinationen von Cloud- und lokalen Setups.
- Native Oracle-Tools helfen Ihnen bei der Durchführung einer homogenen Migration. Sie können Oracle Data Pump verwenden, um Daten zwischen Ihren Quell- und Zieldatenbanken zu migrieren. Dieses Muster verwendet Oracle Data Pump, um den vollen Ladevorgang von der Quelldatenbank in die Zieldatenbank durchzuführen.
- Oracle GoldenGate unterstützt Sie bei der logischen Replikation zwischen zwei oder mehr Datenbanken. Dieses Muster wird verwendet GoldenGate , um die Delta-Änderungen nach dem ersten Laden mithilfe von Oracle Data Pump zu replizieren.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Projektdokumente und zeichnen Sie Datenbankdetails auf.	1. Dokumentieren Sie Ihre Migrationsziele, Migrationsanforderungen, wichtige Projektbeteiligte, Projektmeilensteine, Projektfristen, wichtige Kennzahlen, Migrationsrisiken und Pläne zur Risikominderung. 2. Dokumentieren Sie wichtige Informationen über Ihre Quelldatenbank, einschließlich RAM, IOPS und. CPUs Sie werden diese Informationen später verwenden, um die geeignete Ziel-DB-Instance zu ermitteln. 3. Überprüfen Sie die Versionen Ihrer Quell- und Zieldatenbanken.	DBA
Identifizieren Sie die Speicheranforderungen.	Identifizieren und dokumentieren Sie Ihre Speicheranforderungen, einschließlich der folgenden: 1. Berechnen Sie den für die Quell-DB-Instance zugewiesenen Speicher.	DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Sammeln Sie die historischen Wachstumskennzahlen aus der Quell-DB-Instance. 3. Forecast Sie das future Wachstum für die Ziel-DB-Instance. **Note** Für Allzweck-SSD-Volumes (GP2) erhalten Sie drei IOPS pro 1 GB Speicher. Ordnen Sie Speicherplatz zu, indem Sie die Gesamtzahl der Lese- und Schreib-IOPS in der Quelldatenbank berechnen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie den richtigen Instanztyp basierend auf den Rechenanforderungen aus.	1. Ermitteln Sie die Rechenanforderungen der Ziel-DB-Instance. 2. Identifizieren Sie Leistungsprobleme. 3. Berücksichtigen Sie die Faktoren bei der Bestimmung des geeigneten Instance-Typs: • CPU-Auslastung der Quell-DB-Instance • IOPS (Lesen und Schreiben) für die Quell-DB-Instance • Speicherbedarf auf der Quell-DB-Instance	SysAdmin
Identifizieren Sie die Sicherheitsanforderungen für den Netzwerkzugriff.	1. Identifizieren und dokumentieren Sie die Sicherheitsanforderungen für den Netzwerkzugriff für Ihre Quell- und Zieldatenbanken. 2. Konfigurieren Sie die entsprechenden Sicherheitsgruppen, damit die Anwendung mit der Datenbank kommunizieren kann.	DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Strategie zur Anwendungsmigration.	1. Ermitteln und dokumentieren Sie die Strategie zur Umstellung der Migration. 2. Ermitteln und dokumentieren Sie das Recovery Time Objective (RTO) und das Recovery Point Objective (RPO) für Ihre Anwendung und planen Sie dann die Umstellung entsprechend.	DBA, Besitzer der App SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie Migration srisiken.	Beurteilen Sie die Datenbank und dokumentieren Sie migrationsspezifische Risiken und Abhilfemaßnahmen. Zum Beispiel: • Identifizieren Sie Tabellen, die keine Protokollierung erfordern, und heben Sie das Risiko eines Datenverlusts im Falle einer Wiederherstellung hervor. • Extrahieren Sie die Benutzer und Rechte der Quelldatenbank und heben Sie die Konflikte mit den Amazon RDS-Rechten hervor. • Überprüfen Sie das Alert-Protokoll auf Oracle-spezifische Fehler und Warnungen. • Identifizieren Sie die unterstützten und nicht unterstützten Funktionen der Ziel-DB-Instance. • Überprüfen Sie die veraltete n Funktionen der Engine der Ziel-DB-Version.	DBA

Konfiguration der Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC.	Erstellen Sie eine neue Amazon Virtual Private Cloud (Amazon VPC) für die Ziel-DB-Instance.	SysAdmin
Erstellen Sie Sicherheitsgruppen.	Erstellen Sie eine Sicherheitsgruppe in Ihrer neuen VPC, um eingehende Verbindungen zur DB-Instance zuzulassen.	SysAdmin
Erstellen Sie eine Amazon RDS for Oracle DB-Instance.	Erstellen Sie die Ziel-DB-Instance mit der neuen VPC und Sicherheitsgruppe und starten Sie dann die Instance.	SysAdmin

Option 1: Verwenden Sie native Tools von Oracle oder Drittanbietern, um Daten zu migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Quelldatenbank vor.	1. Erstellen Sie ein Data Pump-Verzeichnis oder verwenden Sie ein vorhandenes. 2. Erstellen Sie einen Migrationsbenutzer und gewähren Sie ihm Berechtigungen zur Durchführung des Data Pump-Extrakts. 3. Extrahieren Sie Rollen, Benutzer und Tablespaces aus der Quelldatenbank als SQL-Skript.	DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Übertragen Sie den extrahierten Data Pump-Dump in das Ziel-DB-Instance-Verzeichnis. `data pump`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Zieldatenbank vor.	1. Vergewissern Sie sich, dass alle Datenbankoptionen (z. B. Text und Java) auf der Ziel-DB-Instance von Amazon RDS for Oracle installiert oder aktiviert sind. 2. Erstellen Sie ein Data Pump-Verzeichnis oder verwenden Sie ein vorhandenes. 3. Erstellen Sie einen Migrationsbenutzer und gewähren Sie ihm Berechtigungen zur Durchführung des Data Pump-Imports. 4. Erstellen Sie die erforderlichen Tablespaces, Benutzer und Rollen auf der Ziel-DB-Instance. 5. Importieren Sie den übertragenen Data Pump-Export-Dump in die Zieldatenbank. 6. Erstellen Sie alle Indizes, die beim Import oder bei der Objekterstellung ausgeschlossen wurden. 7. Erstellen Sie alle Einschränkungen, die beim Import ausgeschlossen wurden. 8. Validieren oder kompilieren Sie ungültige Objekte neu.	DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	9. Erstellen Sie die ungültigen Indizes neu. 10. Überprüfen Sie die Anzahl der Datenbankobjekte zwischen der Quell- und der Zieldatenbank. 11. Beheben Sie alle festgestellten Diskrepanzen zwischen der Objektanzahl.	

Option 2 — Verwenden Sie AWS DMS, um Daten zu migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Daten vor.	1. Bereinigen Sie die Daten in der Quelldatenbank. 2. Erstellen Sie eine Replikationsinstanz. 3. Erstellen Sie einen Quellendpunkt und einen Zielendpunkt. 4. Identifizieren Sie die Anzahl der Tabellen und Objekte, die migriert werden sollen.	DBA
Migrieren Sie die Daten.	1. Löschen Sie Fremdschlüsseleinschränkungen und Auslöser in der Zieldatenbank. 2. Löschen Sie sekundäre Indizes in der Zieldatenbank.	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Konfigurieren Sie die Einstellungen für AWS DMS-Vollladeaufgaben von der Quelldatenbank zur Zieldatenbank. 4. Aktivieren Sie Fremdschl üssel. 5. Ermöglichen Sie AWS DMS CDC, um laufende Änderungen zu replizieren. 6. Aktivieren Sie Auslöser. 7. Aktualisieren Sie die Sequenzen. 8. Überprüfen Sie die Quell- und Zieldaten.	

Wechseln Sie zur Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung sclients auf die neue Infrastru ktur um.	1. Stoppen Sie alle Anwendungsdienste und Client-Verbindungen, die auf Oracle verweisen. 2. Führen Sie die AWS DMS-Aufgaben aus. 3. Richten Sie eine Rollback-Aufgabe ein (z. B. CDC von der Amazon RDS-Daten bank zur lokalen Oracle-Datenbank rückgängig machen). 4. Validieren Sie die Daten.	DBA SysAdmin, Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Starten Sie die Anwendungsdienste in der neuen Zieldatenbank, indem Sie Amazon Route 53 für die neue Amazon RDS for Oracle Oracle-DB-Instance konfigurieren. 6. Fügen Sie Amazon CloudWatch Monitoring zu Ihrer neuen Amazon RDS for Oracle DB-Instance hinzu.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Implementieren Sie Ihren Rollback-Plan.	1. Beenden Sie alle Anwendungsdienste, die auf die Amazon RDS for Oracle Oracle-DB-Instance verweisen. 2. Machen Sie die Änderungen an der lokalen Oracle-Quelldatenbank mithilfe einer AWS DMS-Aufgabe rückgängig. 3. Beenden Sie die AWS-DMS-Aufgaben, die von der lokalen Oracle-Datenbank zur Amazon RDS for Oracle Oracle-Datenbank ausgeführt werden. 4. Konfigurieren Sie die Anwendungen wieder in der Oracle-Quelldatenbank. 5. Stellen Sie sicher, dass die Rollback-Bereitstellung abgeschlossen ist.	DBA, Besitzer der App

Schließen Sie das Migrationsprojekt ab

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereinigen von Ressourcen.	Fahren Sie die temporären AWS-Ressourcen herunter oder entfernen Sie sie, z. B. die AWS DMS-Replikationsinstanz und den S3-Bucket.	DBA, SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Projektdokumente.	Überprüfen Sie Ihre Dokumente und Ziele zur Migrationsplanung und stellen Sie dann sicher, dass Sie alle erforderlichen Migrationsschritte abgeschlossen haben.	DBA SysAdmin, Besitzer der App
Sammeln Sie Kennzahlen.	Erfassen Sie wichtige Migrationskennzahlen, wie lange es gedauert hat, bis die Migration abgeschlossen ist, wie viel Prozent manuelle Aufgaben im Vergleich zu toolbasierten Aufgaben haben, Kosteneinsparungen und andere relevante Kennzahlen.	DBA, Besitzer der SysAdmin App
Schließt das Projekt ab.	Schließen Sie das Migrationsprojekt ab und sammeln Sie Feedback zu den Bemühungen.	DBA SysAdmin, App-Besitzer

Zugehörige Ressourcen

Referenzen

- Migration von Oracle-Datenbanken in die AWS-Cloud (AWS Prescriptive Guidance)
- AWS Database Migration Service (AWS DMS-Dokumentation)
- Amazon RDS-Preise (Amazon RDS-Dokumentation)

Tutorials und Videos

- Erste Schritte mit AWS Database Migration Service (AWS DMS-Dokumentation)
- Amazon RDS-Ressourcen (Amazon RDS-Dokumentation)

- AWS Database Migration Service (DMS) (YouTube)

Migrieren Sie eine lokale Oracle-Datenbank mit Oracle Data Pump zu Amazon RDS for Oracle

Erstellt von Mohan Annam (AWS) und Brian Motzer (AWS)

Übersicht

Dieses Muster beschreibt, wie eine Oracle-Datenbank mithilfe von Oracle Data Pump von einem lokalen Rechenzentrum zu einer Amazon Relational Database Service (Amazon RDS) für Oracle-DB-Instance migriert wird.

Das Muster umfasst das Erstellen einer Datendumpdatei aus der Quelldatenbank, das Speichern der Datei in einem Amazon Simple Storage Service (Amazon S3) -Bucket und das anschließende Wiederherstellen der Daten in einer Amazon RDS for Oracle Oracle-DB-Instance. Dieses Muster ist nützlich, wenn Sie bei der Verwendung von AWS Database Migration Service (AWS DMS) für die Migration auf Einschränkungen stoßen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Die erforderlichen Berechtigungen zum Erstellen von Rollen in AWS Identity and Access Management (IAM) und für einen mehrteiligen Amazon S3 S3-Upload
- Die erforderlichen Berechtigungen zum Exportieren von Daten aus der Quelldatenbank
- AWS-Befehlszeilenschnittstelle (AWS CLI) installiert und konfiguriert

Produktversionen

- Oracle Data Pump ist nur für Oracle Database 10g Release 1 (10.1) und spätere Versionen verfügbar.

Architektur

Quelltechnologie-Stack

- Lokale Oracle-Datenbanken

Zieltechnologie-Stack

- Amazon RDS für Oracle
- SQL-Client (Oracle SQL Developer)
- Ein S3-Bucket

Quell- und Zielarchitektur

Tools

AWS-Services

- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie kontrollieren, wer authentifiziert und autorisiert ist, diese zu verwenden. In diesem Muster wird IAM verwendet, um die Rollen und Richtlinien zu erstellen, die für die Migration von Daten von Amazon S3 zu Amazon RDS for Oracle erforderlich sind.
- Amazon Relational Database Service (Amazon RDS) für Oracle unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Oracle-Datenbank in der AWS-Cloud.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere Tools

- Mit Oracle Data Pump können Sie Daten und Metadaten mit hoher Geschwindigkeit von einer Datenbank in eine andere verschieben. In diesem Muster wird Oracle Data Pump verwendet, um die Datendump-Datei (.dmp) auf den Oracle-Server zu exportieren und sie in Amazon RDS for Oracle zu importieren. Weitere Informationen finden Sie unter Daten in Oracle auf Amazon RDS importieren in der Amazon RDS-Dokumentation.
- Oracle SQL Developer ist eine integrierte Entwicklungsumgebung, die die Entwicklung und Verwaltung von Oracle-Datenbanken sowohl in herkömmlichen als auch in Cloud-basierten Bereitstellungen vereinfacht. Es interagiert sowohl mit der lokalen Oracle-Datenbank als auch mit Amazon RDS for Oracle, um die für den Export und Import von Daten erforderlichen SQL-Befehle auszuführen.

Epen

Erstellen eines S3-Buckets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Bucket.	Folgen Sie den Anweisungen in der AWS-Dokumentation, um den S3-Bucket zu erstellen .	AWS-Systemadministrator

Erstellen Sie die IAM-Rolle und weisen Sie Richtlinien zu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie IAM-Berechtigungen.	Folgen Sie den Anweisungen in der AWS-Dokumentation, um Berechtigungen zu konfigurieren.	AWS-Systemadministrator

Erstellen Sie die Amazon RDS for Oracle DB-Zielinstanz und ordnen Sie die Amazon S3 S3-Integrationsrolle zu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Amazon RDS-Ziel-DB-Instance für Oracle.	Folgen Sie den Anweisungen in der AWS-Dokumentation, um die Amazon RDS for Oracle Oracle-Instance zu erstellen.	AWS-Systemadministrator
Ordnen Sie die Rolle der DB-Instance zu.	Folgen Sie den Anweisungen in der AWS-Dokumentation, um die Rolle der Instance zuzuordnen.	DBA

Erstellen Sie den Datenbankbenutzer in der Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den Benutzer.	Stellen Sie von Oracle SQL Developer oder SQL*Plus eine Connect zur Amazon RDS for Oracle-Zieldatenbank her und führen Sie den folgenden SQL-Befehl aus, um den Benutzer zu erstellen, in den das Schema importiert werden soll.
	`create user SAMPLE_SCHEMA identified by <PASSWORD>;`
	`grant create session, resource to <USER NAME>;`
	`alter user <USER NAME> quota 100M on users;`
		DBA

Erstellen Sie die Exportdatei aus der Oracle-Quelldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine Datendump-Datei.	Verwenden Sie das folgende Skript, um eine Dump-Datei mit dem Namen `sample.dmp` des `DATA_PUMP_DIR` Verzeichnisses für den Export des `SAMPLE_SCHEMA` Benutzers zu erstellen.
	`DECLARE`
	`hdnl NUMBER;`
		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	BEGIN
	    hdnl := dbms_data
	pump.open(operation
	 => 'EXPORT',
	
	           job_mode =>
	 'SCHEMA',
	
	           job_name =>
	 NULL);
	
	    dbms_datapump.add_
	file(handle => hdnl,
	
	         filename =>
	 'sample.dmp',
	
	        directory =>
	 'DATA_PUMP_DIR',
	
	         filetype =>
	 dbms_datapump.ku$_
	file_type_dump_file);
	
	    dbms_datapump.add_
	file(handle => hdnl,
	
	         filename =>
	 'export.log',
	
	        directory =>
	 'DATA_PUMP_DIR',
	
	         filetype =>
	 dbms_datapump.ku$_
	file_type_log_file);
	
	    dbms_datapump.meta
	data_filter(hdnl,
	 'SCHEMA_EXPR', 'IN
	 (''SAMPLE_SCHEMA''
	)');	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`dbms_datapump.start_job(hdnl);`
	`END;`
	`/`
	
	Überprüfen Sie die Exportdetails, indem Sie die `export.log` Datei in Ihrem lokalen `DATA_PUMP_DIR` Verzeichnis überprüfen.	

Laden Sie die Dump-Datei in den S3-Bucket hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Datendump-Datei von der Quelle in den S3-Bucket hoch.	Führen Sie mit AWS CLI den folgenden Befehl aus. `aws s3 cp sample.dmp s3://<bucket_created_epic_1>/`	DBA

Laden Sie die Exportdatei aus dem S3-Bucket auf die RDS-Instance herunter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Datendump-Datei auf Amazon RDS herunter	Um die Dump-Datei `sample.dmp` aus dem S3-Bucket in die Amazon RDS for Oracle Oracle-Datenbank zu kopieren, führen Sie den folgenden SQL-Befehl aus. In diesem Beispiel wird die	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`sample.dmp` Datei aus dem S3-Bucket `my-s3-integration1` in das Oracle-Verzeichnis `DATA_PUMP_DIR` heruntergeladen. Stellen Sie sicher, dass Ihrer RDS-Instance ausreichend Festplattenspeicher zugewiesen ist, um sowohl die Datenbank als auch die Exportdatei aufzunehmen.
	`-- If you want to download all the files in the S3 bucket remove the p_s3_prefix line.`
	`SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3( p_bucket_name => 'my-s3-integration', p_s3_prefix => 'sample.dmp', p_directory_name => 'DATA_PUMP_DIR') AS TASK_ID FROM DUAL;`
	Der vorherige Befehl gibt eine Task-ID aus. Führen Sie den folgenden Befehl aus, um den Status des Downloads anhand der Daten in der Task-ID zu überprüfen.
	`SELECT text FROM table(rdsadmin.rds`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`_file_util.read_te xt_file('BDUMP','d btask-<task_id>.lo g'));`
	
	Führen Sie den folgenden Befehl aus, um die Dateien im `DATA_PUMP_DIR` Verzeichn is anzuzeigen.
	
	`SELECT filename, type,filesize/1024 /1024 size_megs ,to_char(mtime,'DD -MON-YY HH24:MI:SS') timestamp FROM TABLE(rdsadmin.rds _file_util.listdir (p_directory => upper('DATA_PUMP_D IR'))) order by 4;`	

Importieren Sie die Dump-Datei in die Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie das Schema und die Daten in Amazon RDS wieder her.	Um die Dump-Datei in das `sample_schema` Datenbank schema zu importieren, führen Sie den folgenden SQL-Befeh l von SQL Developer oder SQL*Plus aus. `DECLARE hdnl NUMBER; BEGIN`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>hdnl := DBMS_DATA
	PUMP.OPEN(operation
	 => 'IMPORT', job_mode
	 => 'SCHEMA', job_name=
	>null);
	
	DBMS_DATAPUMP.ADD_
	FILE(handle => hdnl,
	 filename => 'sample.d
	mp', directory =>
	 'DATA_PUMP_DIR',
	 filetype => dbms_data
	pump.ku$_file_type
	_dump_file);
	
	DBMS_DATAPUMP.ADD_FILE
	(handle => hdnl,
	 filename => 'import.l
	og', directory =>
	 'DATA_PUMP_DIR',
	 filetype => dbms_data
	pump.ku$_file_type
	_log_file);
	
	DBMS_DATAPUMP.
	METADATA_FILTER(hd
	nl,'SCHEMA_EXPR','
	IN (''SAMPLE_SCHEMA''
	)');
	
	DBMS_DATAPUMP.START_J
	OB(hdnl);
	
	END;
	/</pre>
	Führen Sie den folgenden Befehl aus, um die Protokoll datei aus dem Import anzuzeigen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('DATA_PUMP_DIR','import.log'));`	

Entfernen Sie die Dump-Datei aus dem Verzeichnis DATA_PUMP_DIR

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Listet die Exportdateien auf und bereinigt sie.	Führen Sie die folgenden Befehle aus, um die Exportdateien im `DATA_PUMP_DIR` Verzeichnis aufzulisten und zu entfernen.
	`-- List the files SELECT filename, type,filesize/1024/1024 size_megs ,to_char(mtime,'DD-MON-YY HH24:MI:SS') timestamp FROM TABLE(rdsadmin.rds_file_util.listdir(p_directory => upper('DATA_PUMP_DIR'))) order by 4;`
	`-- Remove the files EXEC UTL_FILE.FREMOVE('DATA_PUMP_DIR','sample.dmp'); EXEC UTL_FILE.FREMOVE('DATA_PUMP_DIR','import.log');`
		AWS-Systemadministrator

Zugehörige Ressourcen

- Amazon S3 S3-Integration
- Erstellen Sie eine DB-Instance
- Daten in Oracle auf Amazon RDS importieren
- Amazon S3 S3-Dokumentation
- IAM-Dokumentation
- Dokumentation zu Amazon RDS
- Dokumentation zu Oracle Data Pump
- Oracle SQL Developer

Migrieren Sie mit pglogical von PostgreSQL auf Amazon EC2 zu Amazon RDS for PostgreSQL

Erstellt von Rajesh Madiwale (AWS)

Übersicht

Dieses Muster beschreibt die Schritte für die Migration einer PostgreSQL-Datenbank (Version 9.5 und höher) von Amazon Elastic Compute Cloud (Amazon) zu Amazon Relational Database Service (Amazon RDS EC2) für PostgreSQL mithilfe der pglogischen PostgreSQL-Erweiterung. Amazon RDS unterstützt jetzt die Erweiterung pglogical für PostgreSQL Version 10.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Wählen Sie den richtigen Typ von Amazon RDS-Instance. Weitere Informationen finden Sie unter Amazon RDS-Instance-Typen.
- Stellen Sie sicher, dass die Quell- und Zielversion von PostgreSQL identisch sind.
- Installieren und integrieren Sie die Erweiterung pglogical mit PostgreSQL auf Amazon. EC2

Produktversionen

- PostgreSQL Version 10 und höher auf Amazon RDS, wobei die Funktionen auf Amazon RDS unterstützt werden (siehe PostgreSQL on Amazon RDS in der AWS-Dokumentation). Dieses Muster wurde durch die Migration von PostgreSQL 9.5 auf PostgreSQL Version 10 auf Amazon RDS getestet, gilt aber auch für spätere Versionen von PostgreSQL auf Amazon RDS.

Architektur

Architektur der Datenmigration

Tools

- logische Erweiterung
- Native PostgreSQL-Dienstprogramme: pg_dump und pg_restore

Epen

Migrieren Sie Daten mithilfe der Erweiterung pglogical

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon RDS PostgreSQL-DB-Instance.	Richten Sie eine PostgreSQL-DB-Instance in Amazon RDS ein. Anweisungen finden Sie in der Dokumentation zu Amazon RDS for PostgreSQL.	DBA
Rufen Sie einen Schema-Dump aus der PostgreSQL-Quelldatenbank ab und stellen Sie ihn in der PostgreSQL-Zieldatenbank wieder her.	1. Verwenden Sie das Hilfsprogramm pg_dump mit der `-s` Option, um eine Schemadatei aus der Quelldatenbank zu generieren. 2. Verwenden Sie das Hilfsprogramm psql mit der `-f` Option, um das Schema in die Zieldatenbank zu laden.	DBA
Schalten Sie die logische Dekodierung ein.	Setzen Sie in der Amazon RDS-DB-Parametergruppe den `rds.logical_replication` statischen Parameter auf 1. Anweisungen finden Sie in der Amazon RDS-Dokumentation.	DBA
Erstellen Sie die pglogische Erweiterung für die Quell- und Zieldatenbank.	1. Erstellen Sie die `pglogical` Erweiterung in der PostgreSQL-Quelldatenbank:	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`psql -h <amazon-ec2-endpoint> -d target-dbname -U target-dbuser -c "create extension pglogical ;"`
	2. Erstellen Sie die `pglogical` Erweiterung in der PostgreSQL-Zieldatenbank:
	`psql -h <amazon-rds-endpoint> -d source-dbname -U source-dbuser -c "create extension pglogical ;"`	

Erstellen Sie einen Herausgeber in der PostgreSQL-Quelldatenbank.	Um einen Herausgeber zu erstellen, führen Sie folgenden Befehl aus: `psql -d dbname -p 5432 <<EOF SELECT pglogical .create_node( node_name := 'provider1', dsn := 'host=<ec2-endpoint> port=5432 dbname=source-dbname user=source-dbuser' ); EOF`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Replikationssatz, fügen Sie Tabellen und Sequenzen hinzu.	Um einen Replikationssatz in der PostgreSQL-Quelldatenbank zu erstellen und dem Replikationssatz Tabellen und Sequenzen hinzuzufügen, führen Sie folgenden Befehl aus: `psql -d dbname -p 5432 <<EOF SELECT pglogical.replication_set_add_all_tables('default', '{public}'::text[],synchronize_data := true); EOF`	DBA
Erstellen Sie einen Abonnenten.	Um einen Abonnenten in der PostgreSQL-Zieldatenbank zu erstellen, führen Sie folgenden Befehl aus: `psql -h <rds-endpoint> -d target-dbname -U target-dbuser <<EOF SELECT pglogical.create_node( node_name := 'subscriber1', dsn := 'host=<rds-endpoint> port=5432 dbname=target-dbname password=postgres user=target-dbuser' ); EOF`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Abonnement.	Um ein Abonnement für die PostgreSQL-Zieldatenbank zu erstellen, führen Sie folgenden Befehl aus: `psql -h <rds-endpoint> -d target -U postgres <<EOF SELECT pglogical.create_subscription( subscription_name := 'subscription1', replication_sets := array['default'], provider_dsn := 'host=<ec2-endpoint> port=5432 dbname=<source-dbname> password=<password> user=source-dbuser' );`	DBA

Bestätigen Sie Ihre Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Quell- und Zieldatenbanken.	Überprüfen Sie die Quell- und Zieldatenbanken, um sicherzustellen, dass die Daten erfolgreich repliziert wurden. Sie können eine grundlegende Validierung durchführen, indem `select count(1)` Sie die Quell- und Zieltabellen verwenden.	DBA

Zugehörige Ressourcen

- Amazon RDS
- Logische Replikation für PostgreSQL auf Amazon RDS (Amazon RDS-Dokumentation)
- logisch (Repository) GitHub
- Einschränkungen von pglogical (README-Datei des Projektarchivs) GitHub
- Migration von PostgreSQL von lokal oder Amazon EC2 zu Amazon RDS mithilfe logischer Replikation (AWS-Datenbank-Blog)

Migrieren Sie eine lokale PostgreSQL-Datenbank zu Aurora PostgreSQL

Erstellt von Baji Shaik (AWS) und Jitender Kumar (AWS)

Übersicht

Die Amazon Aurora PostgreSQL-Compatible Edition kombiniert die Leistung und Verfügbarkeit kommerzieller High-End-Datenbanken mit der Einfachheit und Kosteneffizienz von Open-Source-Datenbanken. Aurora bietet diese Vorteile durch die Skalierung des Speichers auf drei Availability Zones in derselben AWS-Region und unterstützt bis zu 15 Read Replica-Instances zur Skalierung von Lese-Workloads und zur Bereitstellung von Hochverfügbarkeit innerhalb einer einzigen Region. Mithilfe einer globalen Aurora-Datenbank können Sie PostgreSQL-Datenbanken in bis zu fünf Regionen replizieren, um den Fernlesezugriff und die Notfallwiederherstellung im Falle eines Regionsausfalls zu ermöglichen. Dieses Muster beschreibt die Schritte zur Migration einer lokalen PostgreSQL-Quelldatenbank zu einer Aurora PostgreSQL-kompatiblen Datenbank. Das Muster umfasst zwei Migrationsoptionen: die Verwendung von AWS Data Migration Service (AWS DMS) oder die Verwendung nativer PostgreSQL-Tools (wie pg_dump, pg_restore und psql) oder Tools von Drittanbietern.

Die in diesem Muster beschriebenen Schritte gelten auch für PostgreSQL-Zieldatenbanken auf Amazon Relational Database Service (Amazon RDS) - und Amazon Elastic Compute Cloud (Amazon EC2) -Instances.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine PostgreSQL-Quelldatenbank in einem lokalen Rechenzentrum
- Eine Aurora PostgreSQL-kompatible DB-Instance oder eine Amazon RDS for PostgreSQL DB-Instance

Einschränkungen

- Die Größenbeschränkungen für Datenbanken sind 64 TB für Amazon RDS for PostgreSQL und 128 TB für Aurora PostgreSQL-kompatibel.
- Wenn Sie die AWS DMS-Migrationsoption verwenden, lesen Sie sich die AWS-DMS-Einschränkungen für die Verwendung einer PostgreSQL-Datenbank als Quelle durch.

Produktversionen

- Informationen zur Unterstützung von PostgreSQL-Haupt- und Nebenversionen in Amazon RDS finden Sie unter Amazon RDS for PostgreSQL PostgreSQL-Updates in der Amazon RDS-Dokumentation.
- Informationen zur PostgreSQL-Unterstützung in Aurora finden Sie unter Amazon Aurora PostgreSQL-Updates in der Aurora-Dokumentation.
- Wenn Sie die AWS DMS-Migrationsoption verwenden, finden Sie in der AWS DMS-Dokumentation Informationen zu den unterstützten PostgreSQL-Versionen.

Architektur

Quelltechnologie-Stack

- Lokale PostgreSQL-Datenbank

Zieltechnologie-Stack

- Aurora PostgreSQL-kompatible DB-Instance

Quellarchitektur

Zielarchitektur

Architektur der Datenmigration

Verwenden von AWS DMS

Verwendung nativer PostgreSQL-Tools

Tools

- AWS Database Migration Service (AWS DMS) unterstützt Sie bei der Migration von Datenspeichern in die AWS-Cloud oder zwischen Kombinationen von Cloud- und lokalen Konfigurationen. Dieser Service unterstützt verschiedene Quellen und Zieldatenbanken.

Informationen zur Validierung der Versionen und Editionen der PostgreSQL-Quell- und Zieldatenbank, die für die Verwendung mit AWS DMS unterstützt werden, finden Sie unter Verwenden einer PostgreSQL-Datenbank als AWS-DMS-Quelle. Wir empfehlen Ihnen, die neueste Version von AWS DMS zu verwenden, um die umfassendste Version von Versionen und Funktionen zu erhalten.

- Zu den nativen PostgreSQL-Tools gehören pg_dump, pg_restore und psql.

Epen

Analysieren Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversionen.	Wenn Sie AWS DMS verwenden, stellen Sie sicher, dass Sie eine unterstützte Version von PostgreSQL verwenden.	DBA
Identifizieren Sie den Speichertyp und die Kapazitätsanforderungen.	1. Berechnen Sie den für die Quelldatenbank-Instance zugewiesenen Speicher. 2. Sammeln Sie die historischen Wachstumskennzahlen für die Quelldatenbank-Instance. 3. Antizipieren Sie die future Wachstumsprognose für die Zieldatenbank-Instance. 4. Ordnen Sie Speicher zu, indem Sie die Gesamtzahl der Lese- und Schreib-IOPS in der Quelldatenbank berechnen. Ein Allzweck-SSD-Volume (gp2) bietet 3 IOPS pro 1 GB Speicher.	DBA, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie den richtigen Instanztyp, die Kapazität, die Speicherfunktionen und die Netzwerkfunktionen aus.	Ermitteln Sie die Rechenanforderungen der Zieldatenbank-Instance. Prüfen Sie bekannte Leistungsprobleme, die möglicherweise zusätzliche Aufmerksamkeit erfordern. Berücksichtigen Sie die folgenden Faktoren, um den geeigneten Instance-Typ zu bestimmen: • CPU-Auslastung der Quelldatenbank-Instance • IOPS (Lese- und Schreiboperationen) für die Quelldatenbankinstanz • Speicherbedarf auf der Quelldatenbankinstanz Weitere Informationen finden Sie unter Aurora-DB-Instance-Klassen in der Aurora-Dokumentation.	DBA, Systemadministrator
Identifizieren Sie die Sicherheitsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.	Ermitteln Sie die geeigneten Sicherheitsgruppen, die es der Anwendung ermöglichen würden, mit der Datenbank zu kommunizieren.	DBA, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Strategie zur Anwendungsmigration.	• Legen Sie die Strategie für die Umstellung der Migration auf der Grundlage der Komplexität Ihrer Anwendung fest. • Ermitteln Sie das Recovery Time Objective (RTO) und das Recovery Point Objective (RPO) für die Anwendung und planen Sie die Umstellung entsprech end.	DBA, Besitzer der App, Systemadministrator

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC.	Erstellen Sie eine neue Virtual Private Cloud (VPC) für die Zieldatenbank-Instance.	Systemadministrator
Erstellen Sie Sicherhei tsgruppen.	Erstellen Sie eine Sicherhei tsgruppe innerhalb der VPC (wie im vorherigen Epic festgelegt), um eingehende Verbindungen zur Datenbank-Instance zuzulassen.	Systemadministrator
Konfigurieren und starten Sie den Aurora-DB-Cluster.	Erstellen Sie die Zieldaten bank-Instance mit der neuen VPC und Sicherheitsgruppe und starten Sie die Instance.	Systemadministrator

Daten migrieren – Option 1 (mit AWS DMS)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Schritte vor der Migration durch.	1. Bereinigen Sie die Daten in der Quelldatenbank. 2. Erstellen Sie eine Replikationsinstanz. 3. Erstellen Sie Quell- und Zielendpunkte. 4. Identifizieren Sie die Anzahl der verfügbaren Tabellen und Objekte, die migriert werden sollen.	DBA
Schließen Sie die Migrationsschritte ab.	1. Löschen Sie Fremdschlüsseleinschränkungen und Auslöser in der Zieldatenbank. 2. Löschen Sie sekundäre Indizes in der Zieldatenbank. 3. Verwenden Sie eine Volllastaufgabe, um Daten von der Quell- zur Zieldatenbank zu migrieren. 4. Aktivieren Sie Fremdschlüssel. 5. Wenn Sie die Flash-Cut-Migration verwenden und Ihre Anwendung nur minimale Ausfallzeiten erfordert, aktivieren Sie Change Data Capture (CDC), um laufende Änderungen zu replizieren	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Aktivieren Sie Auslöser. 7. Sequenzen aktualisieren. 8. Überprüfen Sie die Quell- und Zieldaten.	
Daten validieren.	Um sicherzustellen, dass Ihre Daten korrekt von der Quelle zum Ziel migriert wurden, befolgen Sie die Schritte zur Datenvalidierung in der AWS DMS-Dokumentation.	DBA

Daten migrieren – Option 2 (mit pg_dump und pg_restore)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die Quelldatenbank vor.	1. Erstellen Sie ein Verzeichnis, um das pg_dump-Backup zu speichern, falls es noch nicht existiert. 2. Erstellen Sie einen Migrationsbenutzer, der berechtigt ist, pg_dump für Datenbankobjekte auszuführen. 3. Connect zur EC2 Instanz her und führen Sie pg_dump backup aus. Weitere Informationen finden Sie in der pg_dump-Dokumentation und in der exemplarischen Vorgehens	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	weise in der AWS DMS-Dokumentation.	
Bereiten Sie die Zieldatenbank vor.	1. Erstellen Sie einen Migrationsbenutzer, der berechtigt ist, pg_restore für Datenbankobjekte zu verwenden. 2. Importieren Sie den Datenbank-Dump mithilfe von pg_restore. Weitere Informationen finden Sie in der Dokumentation zu pg_restore und in der exemplarischen Vorgehens weise in der AWS DMS-Dokumentation.	DBA
Daten validieren.	1. Vergleichen Sie die Anzahl der Datenbankobjekte zwischen der Quell- und der Zieldatenbank. 2. Beheben Sie alle festgeste llten Diskrepanzen zwischen der Objektanzahl.	DBA

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Anwendungsmigration.	Implementieren Sie die Strategie zur Anwendung	DBA, App-Besitzer, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	smigration, die Sie im ersten Epic erstellt haben.	

Wechseln Sie zur Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung sclients auf die neue Infrastru ktur um.	1. Beenden Sie alle Anwendungsdienste und Clientverbindungen, die auf die lokale PostgreSQL-Datenbank verweisen. 2. Führen Sie die AWS DMS-Aufgaben aus. 3. Richten Sie bei Bedarf eine Rollback-Aufgabe ein (Rückwärts-CDC von Aurora PostgreSQ L-kompatibel zur lokalen PostgreSQL-Datenbank). 4. Daten validieren. 5. Starten Sie die Anwendung sdienste auf dem neuen Ziel, indem Sie Amazon Route 53 für die neue Aurora PostgreSQL-kompatible DB-Instance konfigurieren. 6. Fügen Sie Amazon CloudWatch - und Performance Insights Insights-Monitoring zu Ihrer neuen Aurora PostgreSQ	DBA, App-Besitzer, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	L-kompatiblen DB-Instance hinzu.	
Wenn Sie die Migration rückgängig machen müssen.	1. Beenden Sie alle Anwendungsdienste, die auf die Aurora PostgreSQL-kompatible Datenbank verweisen. 2. Machen Sie die Änderungen an der lokalen PostgreSQL-Quelldatenbank rückgängig, indem Sie die AWS DMS-Aufgabe verwenden, die Sie in der vorherigen Geschichte erstellt haben. 3. Beenden Sie die AWS-DMS-Aufgaben, die von der lokalen PostgreSQL-Datenbank zur Aurora PostgreSQL-kompatiblen Datenbank ausgeführt werden. 4. Konfigurieren Sie die Anwendung so, dass sie auf die lokale PostgreSQL-Quelldatenbank zurückverweist. 5. Vergewissern Sie sich, dass die gesamte Rollback-Bereitstellung abgeschlossen ist.	DBA, Besitzer der App

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ressourcen herunterfahren.	Fahren Sie die temporären AWS-Ressourcen herunter.	DBA, Systemadministrator
Dokumente validieren.	Überprüfen und validieren Sie die Projektdokumente.	DBA, App-Besitzer, Systemadministrator
Sammeln Sie Metriken.	Erfassen Sie Kennzahlen zum Zeitpunkt der Migration, zu den prozentualen Einsparungen bei den manuellen Kosten im Vergleich zu den Werkzeugkosten usw.	DBA, App-Besitzer, Systemadministrator
Schließt das Projekt.	Schließen Sie das Projekt und geben Sie Feedback.	DBA, App-Besitzer, Systemadministrator

Zugehörige Ressourcen

Referenzen

- AWS-Datenmigrationsservice
- VPCs und Amazon Aurora
- Amazon-Aurora-Preise
- Verwenden einer PostgreSQL-Datenbank als AWS-DMS-Quelle
- So erstellen Sie eine AWS DMS-Replikationsinstanz
- So erstellen Sie Quell- und Zielendpunkte mit AWS DMS

Weitere Ressourcen

- Erste Schritte mit AWS DMS
- Exemplarische Vorgehensweisen zur Datenmigration step-by-step
- Amazon Aurora Aurora-Ressourcen

Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Microsoft SQL Server auf Amazon EC2 unter Linux

Erstellt von Tirumala Dasari (AWS)

Übersicht

Dieses Muster beschreibt, wie Sie mithilfe von Sicherungs- und Wiederherstellungsdienstprogrammen von einer lokalen Microsoft SQL Server-Datenbank, die unter Microsoft Windows ausgeführt wird, zu Microsoft SQL Server auf einer Amazon Elastic Compute Cloud (Amazon EC2) Linux-Instance migrieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Amazon EC2 Linux AMI (Amazon Machine Image) mit Microsoft SQL Server
- AWS Direct Connect zwischen lokalem Windows und Microsoft SQL Server auf der Linux-Instance EC2

Architektur

Quelltechnologie-Stack

- Lokale Microsoft SQL Server-Datenbank

Zieltechnologie-Stack

- EC2 Linux-Instanz mit einer Microsoft SQL Server-Datenbank

Architektur der Datenbankmigration

Tools

- WinSCP - Mit diesem Tool können Windows-Benutzer Dateien problemlos mit Linux-Benutzern teilen.

- Sqlcmd — Mit diesem Befehlszeilenprogramm können Sie T-SQL-Anweisungen oder Batches an lokale und Remoteinstanzen von SQL Server senden. Das Hilfsprogramm ist äußerst nützlich für sich wiederholende Datenbankaufgaben wie Batchverarbeitung oder Komponententests.

Epen

Bereiten Sie die EC2 Linux-Instanz mit SQL Server vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie ein AMI aus, das das Linux-Betriebssystem bereitstellt und Microsoft SQL Server enthält.		Systemadministrator
Konfigurieren Sie das AMI, um eine EC2 Instanz zu erstellen.		Sysadmin
Erstellen Sie Regeln für eingehenden und ausgehend en Datenverkehr für Sicherhei tsgruppen.		Sysadmin
Konfigurieren Sie die EC2 Linux-Instanz für eine Microsoft SQL Server-Da tenbank.		DBA
Erstellen Sie Benutzer und gewähren Sie Berechtigungen wie in der Quelldatenbank.		Appowner, DBA
Installieren Sie die SQL Server-Tools und das Hilfsprogramm sqlcmd auf der Linux-Instanz. EC2		DBA

Sichern Sie die Datenbank und verschieben Sie die Sicherungsdatei auf die Linux-Instanz EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sichern Sie die lokale SQL Server-Datenbank.		DBA
Installieren Sie WinSCP auf Microsoft SQL Server.		DBA
Verschieben Sie die Sicherungsdatei auf die EC2 Linux-Instanz, auf der Microsoft SQL Server ausgeführt wird.		DBA

Stellen Sie die Datenbank auf einer EC2 Linux-Instanz wieder her, auf der SQL Server ausgeführt wird

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Datenbank mithilfe des Dienstprogramms sqlcmd aus der Datenbank-Backup-Datei wieder her.		DBA
Validieren Sie Datenbankobjekte und Daten.		Entwickler, Testingenieur

Wechseln Sie von Windows SQL Server zu Windows SQL Server auf einer EC2 Linux-Instanz

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie Datenbankobjekte und Daten.		Entwickler, Testingenieur
Wechseln Sie von der lokalen Microsoft SQL Server-Da		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
tenbank zur EC2 Linux-Ins tanz, auf der Microsoft SQL Server ausgeführt wird.		

Zugehörige Ressourcen

- So konfigurieren Sie SQL Server 2017 auf Amazon Linux und Ubuntu AMIs
- Installation von SQL-Tools auf einer Linux-Instanz
- Backup und Wiederherstellung von einer lokalen Microsoft SQL Server-Datenbank auf Microsoft SQL Server auf einer Linux-Instanz EC2

Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mithilfe von Verbindungsservern zu Amazon RDS for SQL Server

Erstellt von Kevin Yung (AWS), Vishal Singh (AWS) und Viqash Adwani (AWS)

Übersicht

Verbindungsserver ermöglichen es Microsoft SQL Server, SQL-Anweisungen auf anderen Instanzen von Datenbankservern auszuführen. Dieses Muster beschreibt, wie Sie Ihre lokale Microsoft SQL Server-Datenbank zu Amazon Relational Database Service (Amazon RDS) für Microsoft SQL Server migrieren können, um geringere Kosten und höhere Verfügbarkeit zu erzielen. Derzeit unterstützt Amazon RDS for Microsoft SQL Server keine Verbindungen außerhalb eines Amazon Virtual Private Cloud (Amazon VPC) -Netzwerks.

Sie können dieses Muster verwenden, um die folgenden Ziele zu erreichen:

- Um Microsoft SQL Server auf Amazon RDS for Microsoft SQL Server zu migrieren, ohne die Funktionen des Verbindungsservers zu beeinträchtigen.
- Um verknüpfte Microsoft SQL Server in verschiedenen Wellen zu priorisieren und zu migrieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Prüfen Sie, ob Microsoft SQL Server auf Amazon RDS die von Ihnen benötigten Funktionen unterstützt.
- Stellen Sie sicher, dass Sie entweder Amazon RDS for Microsoft SQL Server mit Standardsortierungen oder Sortierungen auf Datenbankebene verwenden können.

Architektur

Quelltechnologie-Stack

- Lokale Datenbanken (Microsoft SQL Server)

Zieltechnologie-Stack

- Amazon RDS für SQL Server

Architektur des Quellzustands

Architektur des Zielzustands

Im Zielstatus migrieren Sie Microsoft SQL Server mithilfe von Verbindungsservern zu Amazon RDS for Microsoft SQL Server. Diese Architektur verwendet einen Network Load Balancer, um den Datenverkehr von Amazon RDS for Microsoft SQL Server an lokale Server weiterzuleiten, auf denen Microsoft SQL Server ausgeführt wird. Das folgende Diagramm zeigt die Reverse-Proxy-Fähigkeit für den Network Load Balancer.

Tools

- AWS CloudFormation
- Network Load Balancer
- Amazon RDS for SQL Server in mehreren Availability Zones (Multi-AZs)
- AWS Database Migration Service (AWS DMS)

Epen

Erstellen Sie eine Landingzone-VPC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die CIDR-Zute ilung.		AWS SysAdmin
Erstellen einer Virtual Private Cloud (VPC).		AWS SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die VPC-Subnetze.		AWS SysAdmin
Erstellen Sie die Subnetz-Zugriffskontrolllisten (ACLs).		AWS SysAdmin
Erstellen Sie die Subnetz-Routing-Tabellen.		AWS SysAdmin
Stellen Sie eine Verbindung mit AWS Direct Connect oder AWS Virtual Private Network (VPN) her.		AWS SysAdmin

Migrieren Sie die Datenbank zu Amazon RDS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon RDS for Microsoft SQL Server Server-DB-Instance.		AWS SysAdmin
Erstellen Sie eine AWS DMS-Replikations-Instance.		AWS SysAdmin
Erstellen Sie die Quell- und Zieldatenbank-Endpunkte in AWS DMS.		AWS SysAdmin
Erstellen Sie die Migrationsaufgabe und setzen Sie die kontinuierliche Replikation nach einer Volllast auf ON.		AWS SysAdmin
Fordern Sie eine Firewall-Änderung an, damit Amazon		AWS SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
RDS for Microsoft SQL Server auf die lokalen SQL Server-Datenbanken zugreifen kann.		
Erstellen Sie einen Network Load Balancer.		AWS SysAdmin
Erstellen Sie eine Zielgruppe, die auf die Datenbankserver in Ihrem Rechenzentrum abzielt	Wir empfehlen, Hostnamen in der Zielkonfiguration zu verwenden, um Failover-Ereignisse im Rechenzentrum (DC) einzubeziehen.	AWS SysAdmin
Führen Sie die SQL-Anweisung für die Einrichtung des Verbindungsservers aus.	Führen Sie die SQL-Anweisungen zum Hinzufügen eines Verbindungsservers mithilfe des Microsoft SQL-Managementtools für die Amazon RDS for Microsoft SQL Server-DB-Instance aus. Legen Sie in der SQL-Anweisung @datasrc fest, um den Network Load Balancer Balancer-Hostnamen zu verwenden. Fügen Sie Anmeldeinformationen für verknüpfte Server hinzu, indem Sie das Microsoft SQL-Management-Tool für die Amazon RDS for Microsoft SQL Server-DB-Instance verwenden.	AWS SysAdmin
Testen und validieren Sie die SQL Server-Funktionen.		AWS SysAdmin

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Umstellung.		AWS SysAdmin

Zugehörige Ressourcen

- Allgemeine Verwaltungsaufgaben für Microsoft SQL Server auf Amazon RDS
- Sortierungen und Zeichensätze für Microsoft SQL Server
- Dokumentation zum Network Load Balancer
- Implementieren von Verbindungsservern mit Amazon RDS for Microsoft SQL Server (Blogbeitrag)

Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mit systemeigenen Sicherungs- und Wiederherstellungsmethoden zu Amazon RDS for SQL Server

Erstellt von Tirumala Dasari (AWS), David Queiroz (AWS) und Vishal Singh (AWS)

Übersicht

Dieses Muster beschreibt, wie eine lokale Microsoft SQL Server-Datenbank auf eine Amazon Relational Database Service (Amazon RDS) für SQL Server-DB-Instance migriert wird (homogene Migration). Der Migrationsprozess basiert auf systemeigenen Sicherungs- und Wiederherstellungsmethoden von SQL Server. Es verwendet SQL Server Management Studio (SSMS), um eine Datenbank-Backup-Datei zu erstellen, und einen Amazon Simple Storage Service (Amazon S3) -Bucket, um die Sicherungsdatei zu speichern, bevor sie in Amazon RDS for SQL Server wiederhergestellt wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS Identity and Access Management (IAM) -Rollenrichtlinien für den Zugriff auf den S3-Bucket und die Amazon RDS for SQL Server-DB-Instance.

Einschränkungen

- Der in diesem Muster beschriebene Prozess migriert nur die Datenbank. SQL-Anmeldungen oder Datenbankbenutzer, einschließlich aller SQL Server-Agent-Jobs, werden nicht migriert, da sie zusätzliche Schritte erfordern.

Produktversionen

- SQL Server 2012-2017. Die aktuelle Liste der unterstützten Versionen und Funktionen finden Sie in der AWS-Dokumentation unter Microsoft SQL Server on Amazon RDS.

Architektur

Quelltechnologie-Stack

- Eine lokale Microsoft SQL Server-Datenbank

Zieltechnologie-Stack

- Amazon RDS for SQL Server Server-DB-Instance

Architektur der Datenmigration

Tools

- Microsoft SQL Server Management Studio (SSMS) ist eine integrierte Umgebung für die Verwaltung der SQL Server-Infrastruktur. Es bietet eine Benutzeroberfläche und eine Gruppe von Tools mit umfangreichen Skripteditoren, die mit SQL Server interagieren.

Epen

Erstellen Sie eine Amazon RDS for SQL Server-DB-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie SQL Server als Datenbank-Engine in Amazon RDS for SQL Server aus.		DBA
Wählen Sie die SQL Server Express Edition.		DBA
Geben Sie Datenbankdetails an.	Weitere Informationen zum Erstellen einer DB-Instance finden Sie in der Amazon RDS-Dokumentation.	DBA, Besitzer der App

Erstellen Sie eine Sicherungsdatei aus der lokalen SQL Server-Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie über SSMS eine Connect zur lokalen SQL Server-Datenbank her.		DBA
Erstellen Sie eine Sicherungskopie der Datenbank.	Anweisungen finden Sie in der SSMS-Dokumentation.	DBA, Besitzer der App

Laden Sie die Sicherungsdatei auf Amazon S3 hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen eines Buckets in Amazon S3.	Weitere Informationen finden Sie in der Amazon S3-Dokumentation.	DBA
Laden Sie die Sicherungsdatei in den S3-Bucket hoch.	Weitere Informationen finden Sie in der Amazon S3-Dokumentation.	SysOps Administrator

Stellen Sie die Datenbank in Amazon RDS for SQL Server wieder her

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die Optionsgruppe zu Amazon RDS hinzu.	1. Öffnen Sie die Amazon RDS-Konsole unter https://console.aws.amazon.com/rds/. 2. Wählen Sie im Navigationsbereich Optionsgruppen, Gruppe erstellen aus. 3. Geben Sie die Informationen für die Optionsgruppe	SysOps Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ein, und wählen Sie dann Erstellen aus. 4. Fügen Sie die `SQLSERVER_BACKUP_RESTORE` Option der Optionsgruppe hinzu und wählen Sie dann Option hinzufügen. Weitere Informationen finden Sie in der Dokumentation zu Amazon RDS.	
Stellen Sie die Datenbank wieder her.	1. Stellen Sie über SSMS eine Connect zu Amazon RDS for SQL Server her. 2. Rufen Sie die `msdb.dbo.rds_restore_database` gespeicherte Prozedur auf, um die Datenbank wiederherzustellen.	DBA

Validieren Sie die Zieldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie Objekte und Daten.	Validieren Sie die Objekte und Daten zwischen der Quelldatenbank und Amazon RDS for SQL Server. **Note** Bei dieser Aufgabe wird nur die	App-Besitzer, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Datenbank migriert. Logins und Jobs werden nicht migriert.	

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Leiten Sie den Anwendungsverkehr um.	Leiten Sie nach der Validierung den Anwendungsdatenverkehr zur Amazon RDS for SQL Server-DB-Instance um.	Besitzer der App, DBA

Zugehörige Ressourcen

- Amazon S3 S3-Dokumentation
- Dokumentation zu Amazon RDS for SQL Server
- Optionen für die Microsoft SQL Server Database Engine

Migrieren Sie eine Microsoft SQL Server-Datenbank mithilfe von AWS DMS und AWS SCT zu Aurora MySQL

Erstellt von Mark Szalkiewicz (AWS) und Pavan Pusuluri (AWS)

Übersicht

Dieses Muster beschreibt, wie eine Microsoft SQL Server-Datenbank, die sich entweder lokal oder auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance befindet, zu Amazon Aurora MySQL migriert wird. Das Muster verwendet AWS Database Migration Service (AWS DMS) und AWS Schema Conversion Tool (AWS SCT) für die Datenmigration und Schemakonvertierung.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Microsoft SQL Server-Quelldatenbank in einem lokalen Rechenzentrum oder auf einer Instanz EC2
- Java Database Connectivity (JDBC) -Treiber für AWS SCT-Konnektoren, die entweder auf einem lokalen Computer oder auf einer EC2 Instanz installiert sind, auf der AWS SCT installiert ist

Einschränkungen

- Größenbeschränkung der Datenbank: 64 TB

Produktversionen

- Microsoft SQL Server 2008, 2008R2, 2012, 2014, 2016 und 2017 für die Enterprise, Standard, Workgroup und Developer Editionen. Die Web- und Express-Editionen werden von AWS DMS nicht unterstützt. Die aktuelle Liste der unterstützten Versionen finden Sie unter Verwenden einer Microsoft SQL Server-Datenbank als Quelle für AWS DMS. Wir empfehlen Ihnen, die neueste Version von AWS DMS zu verwenden, um die umfassendste Version von Versionen und Funktionen zu erhalten. Informationen zu den von AWS SCT unterstützten Microsoft SQL Server-Versionen finden Sie in der AWS SCT-Dokumentation.
- MySQL-Versionen 5.5, 5.6 und 5.7. Die aktuelle Liste der unterstützten Versionen finden Sie unter Verwenden einer MySQL-kompatiblen Datenbank als Ziel für AWS DMS.

Architektur

Quelltechnologie-Stack

Eine der beiden folgenden Komponenten:

- Eine lokale Microsoft SQL Server-Datenbank
- Eine Microsoft SQL Server-Datenbank auf einer EC2 Instanz

Zieltechnologie-Stack

- Aurora MySQL

Architektur der Datenmigration

- Aus einer Microsoft SQL Server-Datenbank, die in der AWS-Cloud läuft

- Aus einer Microsoft SQL Server-Datenbank, die in einem lokalen Rechenzentrum läuft

Tools

- AWS DMS — AWS Data Migration Service (AWS DMS) unterstützt Sie bei der Migration Ihrer Daten zu und von weit verbreiteten kommerziellen und Open-Source-Datenbanken, darunter Oracle, SQL Server, MySQL und PostgreSQL. Sie können AWS DMS verwenden, um Ihre Daten in die AWS Cloud, zwischen lokalen Instances (über eine AWS Cloud-Einrichtung) oder zwischen Kombinationen aus Cloud und lokalen Einrichtungen zu migrieren.
- AWS SCT — Das AWS Schema Conversion Tool (AWS SCT) vereinfacht heterogene Datenbankmigrationen, indem das Quelldatenbankschema und ein Großteil des benutzerdefinierten Codes automatisch in ein mit der Zieldatenbank kompatibles Format konvertiert werden.

Epen

Bereite dich auf die Migration vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Quell- und Zieldatenbankversion und die Engine.		DBA
Erstellen Sie eine Sicherhei tsgruppe für ausgehende Nachrichten für die Quell- und Zieldatenbanken.		SysAdmin
Erstellen und konfigurieren Sie bei Bedarf eine EC2 Instanz für AWS SCT.		DBA
Laden Sie die neueste Version von AWS SCT und die zugehörigen Treiber herunter.		DBA
Fügen Sie die erforderlichen Benutzer und Berechtigungen in der Quelldatenbank hinzu und validieren Sie sie.		DBA
Erstellen Sie ein AWS SCT-Projekt für den Workload und stellen Sie eine Verbindung zur Quelldatenbank her.		DBA
Erstellen Sie einen Bewertung sbericht und bewerten Sie die Machbarkeit.		DBA

Bereiten Sie die Zieldatenbank vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon RDS-DB-Zielinstanz mit Amazon Aurora als Datenbank-Engine.		DBA
Extrahieren Sie die Liste der Benutzer, Rollen und Berechtigungen aus der Quelle.		DBA
Ordnen Sie die vorhanden en Datenbankbenutzer den neuen Datenbankbenutzern zu.		Besitzer der App
Erstellen Sie Benutzer in der Zieldatenbank.		DBA
Wenden Sie Rollen aus dem vorherigen Schritt auf die Zieldatenbank an.		DBA
Überprüfen Sie die Datenbank optionen, Parameter , Netzwerkdateien und Datenbank-Links in der Quelldatenbank und bewerten Sie dann deren Anwendbarkeit auf die Zieldatenbank.		DBA
Wenden Sie alle relevanten Einstellungen auf das Ziel an.		DBA

Objekte übertragen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die AWS SCT-Konnektivität zur Zieldatenbank.		DBA
Konvertieren Sie das Schema mit AWS SCT.	AWS SCT konvertiert das Quelldatenbankschema und den größten Teil des benutzerdefinierten Codes automatisch in ein Format, das mit der Zieldatenbank kompatibel ist. Jeder Code, den das Tool nicht automatisch konvertieren kann, ist deutlich gekennzeichnet, sodass Sie ihn selbst konvertieren können.	DBA
Überprüfen Sie den generierten SQL-Bericht und speichern Sie alle Fehler und Warnungen.		DBA
Wenden Sie automatische Schemaänderungen auf das Ziel an oder speichern Sie sie als .sql-Datei.		DBA
Überprüfen Sie, ob AWS SCT die Objekte auf dem Ziel erstellt hat.		DBA
Alle Elemente, die nicht automatisch konvertiert werden konnten, können		DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
manuell neu geschrieben, zurückgewiesen oder neu gestaltet werden.		
Wenden Sie die generierten Rollen- und Benutzerberechtigungen an und überprüfen Sie alle Ausnahmen.		DBA

Migrieren Sie die Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie die Migrationsmethode.		DBA
Erstellen Sie eine Replikationsinstanz von der AWS DMS-Konsole aus.	Detaillierte Informationen zur Verwendung von AWS DMS finden Sie unter den Links im Abschnitt „Verwandte Ressourcen“.	DBA
Erstellen Sie die Quell- und Zielendpunkte.		DBA
Erstellen Sie eine Replikationsaufgabe.		DBA
Starten Sie die Replikationsaufgabe und überwachen Sie die Protokolle.		DBA

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie AWS SCT, um die SQL-Elemente im Anwendungscode zu analysieren und zu konvertieren.	Wenn Sie Ihr Datenbankschema von einer Engine in eine andere konvertieren, müssen Sie auch den SQL-Code in Ihren Anwendungen aktualisieren, damit diese mit der neuen Datenbank-Engine anstelle der alten interagieren. Sie können den konvertierten SQL-Code anzeigen, analysieren, bearbeiten und speichern. Detaillierte Informationen zur Verwendung von AWS SCT finden Sie unter den Links im Abschnitt „Verwandte Ressourcen“.	Besitzer der App
Erstellen Sie die neuen Anwendungsserver auf AWS.		Besitzer der App
Migrieren Sie den Anwendungscode auf die neuen Server.		Besitzer der App
Konfigurieren Sie den Anwendungsserver für die Zieldatenbank und die Treiber.		Besitzer der App
Korrigieren Sie jeglichen Code, der für die Quelldatenbank-Engine in der Anwendung spezifisch ist.		Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Optimieren Sie den Anwendungscode für die Ziel-Engine.		Besitzer der App

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wenden Sie alle neuen Benutzer, Zuschüsse und Codeänderungen auf das Ziel an.		DBA
Sperren Sie die Anwendung für alle Änderungen.		Besitzer der App
Stellen Sie sicher, dass alle Änderungen an die Zieldaten bank weitergegeben wurden.		DBA
Verweisen Sie den neuen Anwendungsserver auf die Zieldatenbank.		Besitzer der App
Überprüfe alles noch einmal.		Besitzer der App
Geh live.		Besitzer der App

Schließe das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die temporären AWS-Ressourcen herunter (AWS DMS-Replikationsin		DBA, Besitzer der App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
stanz und für AWS SCT verwendete EC2 Instanz).		
Aktualisieren Sie das Feedback zum AWS DMS-Prozess für interne Teams.		DBA, Besitzer der App
Überarbeiten Sie den AWS-DMS-Prozess und verbessern Sie gegebenenfalls die Vorlage.		DBA, Besitzer der App
Überprüfen und validieren Sie die Projektdokumente.		DBA, Besitzer der App
Erfassen Sie Kennzahlen zum Zeitpunkt der Migration, zu den prozentualen Einsparungen bei den manuellen Kosten im Vergleich zu den Werkzeugkosten usw.		DBA, Besitzer der App
Schließen Sie das Projekt und geben Sie Feedback.		DBA, Besitzer der App

Zugehörige Ressourcen

Referenzen

- AWS DMS-Benutzerhandbuch
- AWS SCT-Benutzerhandbuch
- Amazon Aurora Aurora-Preise

Tutorials und Videos

- Erste Schritte mit AWS Database Migration Service

- Erste Schritte mit dem AWS Schema Conversion Tool
- Amazon RDS-Ressourcen
- Exemplarische Vorgehensweisen zu AWS DMS Step-by-Step

Migrieren Sie eine lokale MariaDB-Datenbank mit nativen Tools zu Amazon RDS for MariaDB

Erstellt von Shyam Sunder Rakhecha (AWS)

Übersicht

Dieses Muster bietet Anleitungen für die Migration einer lokalen MariaDB-Datenbank zu Amazon Relational Database Service (Amazon RDS) für MariaDB mithilfe nativer Tools. Wenn Sie MySQL-Tools installiert haben, können Sie mysql und mysqldump verwenden. Wenn Sie MariaDB-Tools installiert haben, können Sie Mariadb und Mariadb-dump verwenden. MySQL- und MariaDB-Tools haben denselben Ursprung, aber es gibt geringfügige Unterschiede in MariaDB-Version 10.6 und höher.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine MariaDB-Quelldatenbank in einem lokalen Rechenzentrum

Einschränkungen

- Größenbeschränkung der Datenbank: 64 TB

Produktversionen

- MariaDB-Versionen 10.0-10.6 (die aktuelle Liste der unterstützten Versionen finden Sie unter MariaDB on Amazon RDS in der AWS-Dokumentation)

Architektur

Quelltechnologie-Stack

- MariaDB-Datenbank in einem lokalen Rechenzentrum

Zieltechnologie-Stack

- Amazon RDS for MariaDB MariaDB-DB-Instance

Zielarchitektur

Architektur der Datenmigration

Tools

- Native MySQL-Tools: mysql und mysqldump
- Native MariaDB-Tools: Mariadb und Mariadb-Dump

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Versionen und Engines der Quell- und Zieldatenbank.		DBA
Identifizieren Sie die Hardwareanforderungen für die Zielserverinstanz.		DBA, Systemadministrator
Identifizieren Sie die Speicheranforderungen (Speichertyp und Kapazität).		DBA, Systemadministrator
Wählen Sie den richtigen Instanztyp auf der Grundlage von Kapazität, Speicherf unktionen und Netzwerkf unktionen aus.		DBA, Systemadministrator
Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerkzugriff für Quell- und Zieldatenbanken.		DBA, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Strategie zur Anwendungsmigration.		DBA, App-Besitzer, Systemadministrator

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC).		Systemadministrator
Erstellen Sie Sicherhei tsgruppen.		Systemadministrator
Konfigurieren und starten Sie eine Amazon RDS-DB-Instance, auf der MariaDB ausgeführt wird.		Systemadministrator

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie native Tools, um Datenbankobjekte und Daten zu migrieren.	Verwenden Sie in der Quelldatenbank mysqldump oder mariadb-dump, um eine Ausgabedatei zu erstellen , die Datenbankobjekte und Daten enthält. Verwenden Sie in der Zieldatenbank mysql oder mariadb, um die Daten wiederherzustellen.	DBA
Validieren Sie die Daten.	Überprüfen Sie die Quell- und Zieldatenbanken, um	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	sicherzustellen, dass die Datenmigration erfolgreich war.	

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie zur Anwendungsmigration.		DBA, App-Besitzer, Systemadministrator

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendung sclients auf die neue Infrastru ktur um.		DBA, App-Besitzer, Systemadministrator

Schließen Sie das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fahren Sie die temporären AWS-Ressourcen herunter.		Systemadministrator
Überprüfen und validieren Sie die Projektdokumente.		DBA, App-Besitzer, Systemadministrator
Sammeln Sie Kennzahlen zum Zeitpunkt der Migration, zu den durch Tools erzielten Kosteneinsparungen usw.		DBA, App-Besitzer, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schließen Sie das Projekt ab und geben Sie Feedback.		DBA, App-Besitzer, Systemadministrator

Zugehörige Ressourcen

Amazon RDS-Referenzen

- Amazon RDS für MariaDB
- Amazon Virtual Private Cloud VPCs und Amazon RDS
- Amazon RDS Multi-AZ-Bereitstellungen
- Amazon RDS — Preise

MySQL- und MariaDB-Referenzen

- mariadb-dump/mysqldump
- mysql-Befehlszeilenclient

Anleitungen und Videos

- Erste Schritte mit Amazon RDS

Migrieren Sie eine lokale MySQL-Datenbank zu Aurora MySQL

Erstellt von Igor Obradovic (AWS)

Übersicht

Dieses Muster erklärt, wie eine lokale MySQL-Quelldatenbank zur Amazon Aurora MySQL-Compatible Edition migriert wird. Es beschreibt zwei Optionen für die Migration: die Verwendung von AWS Database Migration Service (AWS DMS) oder die Verwendung nativer MySQL-Tools wie mysqldbcopy und mysqldump.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Eine MySQL-Quelldatenbank in einem lokalen Rechenzentrum

Einschränkungen

- Größenbeschränkung der Datenbank: 128 TB

Produktversionen

- MySQL Version 8.0 (Aurora MySQL Version 3) ist im Rahmen der Standardunterstützung verfügbar.
- MySQL Version 5.7 (Aurora MySQL Version 2) ist im Rahmen des erweiterten Supports gegen Aufpreis erhältlich.

Die aktuelle Liste der unterstützten Versionen finden Sie in der AWS Dokumentation unter Amazon Aurora Aurora-Versionen. Wenn Sie verwenden AWS DMS, siehe auch Verwenden einer MySQL-kompatiblen Datenbank als Ziel für AWS DMS für MySQL-Versionen, die von unterstützt werden. AWS DMS

Architektur

Quelltechnologie-Stack

- Eine lokale MySQL-Datenbank

Zieltechnologie-Stack

- Amazon Aurora MySQL-Compatible Edition

Zielarchitektur

Aurora-Daten werden in einem Cluster-Volume gespeichert, bei dem es sich um ein einzelnes virtuelles Volume handelt, das Solid-State-Laufwerke (SSDs) verwendet. Ein Cluster-Volume besteht aus Datenkopien, die sich zwischen drei Availability Zones in einer einzelnen AWS-Region befinden. Da die Daten automatisch über Availability Zones hinweg repliziert werden, sind sie äußerst robust und die Wahrscheinlichkeit eines Datenverlusts ist geringer.

Aurora teilt Ihr Datenbankvolumen automatisch in 10-GB-Segmente auf, die auf viele Festplatten verteilt sind. Jeder 10-GB-Abschnitt Ihres Datenbankvolumens wird auf sechs Arten in drei Availability Zones repliziert. Das folgende Diagramm veranschaulicht die Beziehung zwischen dem Cluster-Volume, der Writer-DB-Instance und den Reader-DB-Instances in einem Aurora-DB-Cluster sowie die Trennung von Rechenkapazität und Speicher. Weitere Informationen zu dieser Architektur finden Sie in der Aurora-Dokumentation und in den häufig gestellten Fragen.

Architektur der Datenmigration

Verwenden von AWS DMS:

Das folgende Diagramm veranschaulicht die Migration einer lokalen MySQL-Datenbank zu einem Aurora MySQL-kompatiblen Cluster im, using. AWS Cloud AWS DMS

Verwendung nativer MySQL-Tools:

Das folgende Diagramm veranschaulicht die Migration einer lokalen MySQL-Datenbank zu einem Aurora MySQL-kompatiblen Cluster im AWS Cloud, wobei native MySQL-Tools wie mysqldbcopy und mysqldump verwendet werden.

Tools

- AWS Database Migration Service () unterstützt mehrere Quell AWS DMS - und Zieldatenbank-Engines. Hinweise zu MySQL-Quell- und Zieldatenbanken, die von unterstützt werden AWS

DMS, finden Sie unter MySQL-kompatible Datenbanken migrieren zu. AWS Wir empfehlen Ihnen, die neueste Version von zu verwenden, um die umfassendste AWS DMS Versions- und Funktionsunterstützung zu erhalten.

- mysqldbcopy ist ein MySQL-Hilfsprogramm, das eine MySQL-Datenbank auf einen einzelnen Server oder zwischen Servern kopiert.
- mysqldump ist ein MySQL-Hilfsprogramm, das zu Sicherungs- oder Migrationszwecken eine Dump-Datei aus einer MySQL-Datenbank erstellt.

Epen

Planen Sie die Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Version und die Engine.	Überprüfen Sie die Datenbank version und die Engine für die Quell- und Zieldatenbanken.	DBA
Identifizieren Sie die Hardwareanforderungen.	Identifizieren Sie die Hardwareanforderungen für die Zielserverinstanz.	DBA, Systemadministrator
Identifizieren Sie die Speicheranforderungen.	Identifizieren Sie die Speicheranforderungen (Speichertyp und Kapazität).	DBA, Systemadministrator
Wählen Sie den Instance-Typ aus.	Wählen Sie den richtigen Instanztyp basierend auf Ihren Rechen-, Speicher- und Netzwerkanforderungen.	DBA, Systemadministrator
Ermitteln Sie die Sicherhei tsanforderungen für den Netzwerkzugriff.	Identifizieren Sie die Sicherhei tsanforderungen für den Netzwerkzugriff für die Quell- und Zieldatenbanken.	DBA, Systemadministrator
Legen Sie die Strategie fest.	Identifizieren Sie die Strategie für die Anwendungsmigration.	DBA, App-Besitzer, Systemadministrator

Konfigurieren Sie die Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen einer Virtual Private Cloud (VPC).	Anweisungen finden Sie unter Erstellen einer VPC in der Dokumentation zu Amazon Virtual Private Cloud (Amazon VPC).	Systemadministrator
Erstellen Sie Sicherhei tsgruppen.	Anweisungen finden Sie unter Erstellen einer Sicherhei tsgruppe für Ihre VPC in der Amazon VPC-Dokumentation.	Systemadministrator
Konfigurieren und starten Sie einen Aurora MySQL-kom patiblen DB-Cluster in Ihrem. AWS-Konto	Anweisungen finden Sie in der Aurora-Dokumentation unter Erstellen eines Amazon Aurora Aurora-DB-Clusters.	Systemadministrator

Daten migrieren — Option 1

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie native MySQL-Tools oder Tools von Drittanbi etern, um Datenbankobjekte und Daten zu migrieren.	Anweisungen finden Sie in der Dokumentation für MySQL-Tools wie mysqldbcopy und mysqldump.	DBA

Daten migrieren — Option 2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren Sie Daten mit AWS DMS.	Anweisungen finden Sie in der Dokumentation unter Verwenden einer MySQL-kom	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	patiblen Datenbank als Quelle und Verwenden einer MySQL-kompatiblen Datenbank als Ziel. AWS DMS	

Migrieren Sie die Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie der Strategie.	Folgen Sie der Strategie zur Anwendungsmigration.	DBA, App-Besitzer, Systemadministrator

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wechseln Sie zwischen den Anwendungsclients.	Schalten Sie die Anwendung sclients um, um eine Verbindung zum neuen Aurora-Cluster-Endpunkt herzustellen.	DBA, App-Besitzer, Systemadministrator

Schließen Sie das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ressourcen herunterfahren.	Temporäre AWS Ressourcen herunterfahren.	DBA, Systemadministrator
Überprüfen Sie die Dokumentation.	Überprüfen und validieren Sie die Projektdokumente.	DBA, App-Besitzer, Systemadministrator
Sammeln Sie Metriken.	Erfassen Sie Kennzahlen zum Zeitpunkt der Migration, zum	DBA, App-Besitzer, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Prozentsatz manueller Schritte im Vergleich zur Nutzung der Tools, zu Kosteneinsparungen usw.	
Schließen Sie das Migration sprojekt ab.	Schließen Sie das Projekt ab und geben Sie Feedback.	App-Besitzer, DBA, Systemadministrator

Zugehörige Ressourcen

Referenzen

- Migrieren Sie Daten zum Amazon Aurora MySQL-DB-Cluster
- AWS DMS website
- AWS DMS Dokumentation
- Amazon Aurora Aurora-Preise
- Einen Aurora MySQL-DB-Cluster erstellen und eine Verbindung zu diesem herstellen
- Amazon VPC und Amazon RDS
- Amazon Aurora Aurora-Dokumentation

Tutorials und Videos

- Erste Schritte mit AWS DMS
- Erste Schritte mit Amazon Aurora

Migrieren Sie lokale MySQL-Datenbanken mit Percona XtraBackup, Amazon EFS und Amazon S3 zu Aurora MySQL

Erstellt von Rohan Jamadagni (AWS), Sajith Menon (AWS) und Udayasimha Theepireddy (AWS)

Übersicht

Dieses Muster beschreibt, wie große, lokale MySQL-Datenbanken mithilfe von XtraBackup Percona effizient zu Amazon Aurora MySQL migriert werden können. Percona XtraBackup ist ein quelloffenes, nicht blockierendes Backup-Programm für MySQL-basierte Server. Das Muster zeigt, wie Amazon Elastic File System (Amazon EFS) verwendet wird, um die Zeit für das Hochladen des Backups auf Amazon Simple Storage Service (Amazon S3) und das Wiederherstellen des Backups auf Amazon Aurora MySQL zu reduzieren. Das Muster enthält auch Details darüber, wie inkrementelle Percona-Backups erstellt werden können, um die Anzahl der Binärprotokolle zu minimieren, die auf die Aurora MySQL-Zieldatenbank angewendet werden sollen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Berechtigungen zum Erstellen von Rollen und Richtlinien für AWS Identity and Access Management (IAM)
- Netzwerkkonnektivität zwischen der lokalen MySQL-Datenbank und der Virtual Private Cloud (VPC) auf AWS

Einschränkungen

- Bei den Quellservern muss es sich um Linux-basierte Systeme handeln, die einen Network File System (NFS) -Client (nfs-utils/nfs-common) installieren können.
- Der S3-Bucket, der zum Hochladen von Backup-Dateien verwendet wird, unterstützt nur serverseitige Verschlüsselung (SSE-S3/SSE-KMS).
- Amazon S3 begrenzt die Größe der Backup-Dateien auf 5 TB. Wenn Ihre Backup-Datei 5 TB überschreitet, können Sie sie in mehrere kleinere Dateien aufteilen.
- Die Anzahl der in den S3-Bucket hochgeladenen Quelldateien darf eine Million Dateien nicht überschreiten.

- Das Muster unterstützt nur das XtraBackup vollständige und das inkrementelle Backup von Percona. Es unterstützt keine teilweisen Backups, die`--tables`,,`--tables-exclude`, `--tables-file` `--databases``--databases-exclude`, oder verwenden. `--databases-file`
- Aurora stellt keine Benutzer, Funktionen, gespeicherten Prozeduren oder Zeitzoneninformationen aus der MySQL-Quelldatenbank wieder her.

Produktversionen

- Die Quelldatenbank muss die MySQL-Version 5.5, 5.6 oder 5.7 sein.
- Für MySQL 5.7 müssen Sie Percona XtraBackup 2.4 verwenden.
- Für MySQL 5.6 und 5.6 müssen Sie Percona XtraBackup 2.3 oder 2.4 verwenden.

Architektur

Quelltechnologie-Stack

- Linux-basiertes Betriebssystem
- MySQL-Server
- Percona XtraBackup

Zieltechnologie-Stack

- Amazon Aurora
- Amazon S3
- Amazon EFS

Zielarchitektur

Tools

AWS-Services

- Amazon Aurora ist eine vollständig verwaltete relationale Datenbank-Engine, die es einfach und kostengünstig macht, MySQL-Bereitstellungen einzurichten, zu betreiben und zu skalieren. Aurora MySQL ist ein Drop-In-Ersatz für MySQL.

- Amazon Elastic File System (Amazon EFS) unterstützt Sie bei der Erstellung und Konfiguration gemeinsam genutzter Dateisysteme in der AWS-Cloud.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere Tools

- Percona XtraBackup ist ein Open-Source-Hilfsprogramm, das Streaming-, komprimierte und inkrementelle Backups von MySQL-Datenbanken durchführt, ohne Ihre Datenbanken zu stören oder zu blockieren.

Epen

Erstellen eines Amazon EFS-Dateisystems

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Sicherheitsgruppe, die Amazon EFS-Mount-Zielen zugeordnet werden soll.	Erstellen Sie eine Sicherheitsgruppe in der VPC, die mit einem VPN-Anhang zur lokalen Datenbank über AWS Transit Gateway konfiguriert ist. Weitere Informationen zu den in diesem und anderen Berichten beschriebenen Befehlen und Schritten finden Sie unter den Links im Abschnitt „Verwandte Ressourcen“ am Ende dieses Musters.	DevOpsAWS-/Datenbankadministrator
Bearbeiten Sie die Sicherheitsgruppenregeln.	Fügen Sie eine Regel für eingehenden Datenverkehr hinzu und verwenden Sie dabei den Typ NFS, Port 2049 und den IP-Bereich des lokalen Datenbankservers als	DevOpsAWS-/Datenbankadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Quelle. Standardmäßig erlaubt die Regel für ausgehenden Datenverkehr das Verlassen des gesamten Datenverkehrs. Wenn dies nicht der Fall ist, fügen Sie eine ausgehend e Regel hinzu, um eine Verbindung für den NFS-Port zu öffnen. Fügen Sie zwei weitere Regeln für eingehend en Datenverkehr hinzu: Port 2049 (Quelle: Sicherhei tsgruppen-ID derselben Sicherheitsgruppe) und Port 22 (Quelle: IP-Bereich, von dem aus Sie eine Verbindun g zu einer Instance herstellen werden). EC2	
Erstellen eines Dateisystems.	Verwenden Sie in den Mount-Zielen die VPC und die Sicherheitsgruppe, die Sie in der vorherigen Geschicht e erstellt haben. Wählen Sie den Durchsatzmodus und die Leistung auf der Grundlage der I/O-Anforderungen der lokalen Datenbank. Aktiviere n Sie optional die Verschlüs selung im Ruhezustand.	DevOpsAWS-/Datenba nkadministrator

Hängen Sie das Dateisystem ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Instanzprofilrolle, die einer EC2 Instanz zugeordnet werden soll.	Erstellen Sie eine IAM-Rolle, die über Berechtigungen zum Hochladen und Zugreifen auf Objekte in Amazon S3 verfügt. Wählen Sie den S3-Bucket aus, in dem das Backup als Richtlinienressource gespeichert werden soll.	AWS DevOps
Erstellen Sie eine EC2 Instanz.	Starten Sie eine Linux-basierte EC2 Instance und fügen Sie die IAM-Instance-Profilrolle, die Sie im vorherigen Schritt erstellt haben, sowie die Sicherheitsgruppe, die Sie zuvor erstellt haben, hinzu.	AWS DevOps
Installieren Sie den NFS-Client.	Installieren Sie den NFS-Client auf dem lokalen Datenbankserver und auf der EC2 Instance. Installationsanweisungen finden Sie im Abschnitt „Zusätzliche Informationen“.	DevOps
Mounten Sie das Amazon-EFS-Dateisystem ein.	Mounten Sie das Amazon EFS-Dateisystem lokal und auf der EC2 Instance. Erstellen Sie auf jedem Server ein Verzeichnis zum Speichern des Backups und mounten Sie das Dateisystem mithilfe des Mount-Zielendpunkts. Ein Beispiel finden	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie im Abschnitt „Zusätzliche Informationen“.	

Erstellen Sie eine Sicherungskopie der MySQL-Quelldatenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Percona XtraBackup.	Installieren Sie Percona XtraBackup 2.3 oder 2.4 (abhängig von der Version Ihrer MySQL-Datenbank) auf dem lokalen Datenbankserver. Links zur Installation finden Sie im Abschnitt „Verwandte Ressourcen“.	Datenbankadministrator
Zählen Sie die Schemas und Tabellen in der Quelldatenbank.	Erfassen und notieren Sie die Anzahl der Schemas und Objekte in der MySQL-Quelldatenbank. Sie werden diese Zählungen verwenden, um die Aurora MySQL-Datenbank nach der Migration zu validieren.	Datenbankadministrator
(Optional) Notieren Sie sich die neueste binäre Protokollsequenz aus der Quelldatenbank.	Führen Sie diesen Schritt aus, wenn Sie eine binäre Protokollreplikation zwischen der Quelldatenbank und Aurora MySQL einrichten möchten, um Ausfallzeiten zu minimieren. log-bin muss aktiviert sein und server_id muss eindeutig sein. Notieren Sie sich die aktuelle Binärprotokollsequ	Datenbankadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	enz aus der Quelldatenbank, kurz bevor Sie ein Backup initiieren. Führen Sie diesen Schritt unmittelbar vor der vollständigen Sicherung aus, wenn Sie nur die vollständ ige Sicherung verwenden möchten. Wenn Sie planen, nach einem vollständigen Backup inkrementelle Backups zu erstellen, führen Sie diesen Schritt unmittelbar vor dem letzten inkrementellen Backup aus, das Sie auf der Aurora MySQL-DB-Instance wiederherstellen werden.	
Starten Sie eine vollständige Sicherung der MySQL-Que lldatenbank.	Erstellen Sie mit Percona XtraBackup eine vollständ ige Sicherung der MySQL-Quelldatenbank. Befehle für vollständige und inkrementelle Backups finden Sie beispiels weise im Abschnitt „Zusätzli che Informationen“.	Datenbankadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Erstellen Sie inkrementelle Backups mit Percona. XtraBackup	Inkrementelle Backups können verwendet werden, um die Anzahl der Binärprotokolle zu reduzieren, die Sie anwenden müssen, um die Quelldatenbank mit Aurora MySQL zu synchronisieren. Große und transaktionsintensive Datenbanken können bei Backups eine große Anzahl von Binärprotokollen generieren. Indem Sie inkrementelle Backups erstellen und diese auf einem gemeinsam genutzten Amazon EFS-Dateisystem speichern, können Sie die Zeit für das Sichern und Hochladen Ihrer Datenbank erheblich reduzieren. Einzelheiten finden Sie im Abschnitt „Zusätzliche Informationen“. Erstellen Sie weiterhin inkrementelle Backups, bis Sie bereit sind, mit der Migration zu Aurora zu beginnen.	Datenbankadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie Backups vor.	In diesem Schritt werden Transaktionsprotokolle für Transaktionen, die während des Backups verarbeitet wurden, auf das Backup angewendet. Wenden Sie weiterhin Transakti onsprotokolle (--apply-log-only) auf jedes inkrement elle Backup an, um die Backups zusammenzuführen, mit Ausnahme des letzten Backups. Beispiele finden Sie im Abschnitt „Zusätzliche Informationen“. <efs_moun t_name>Nach diesem Schritt befindet sich das vollständige, zusammengeführte Backup in ~/ /fullbackup.	Datenbankadministrator
Komprimieren und teilen Sie das endgültige zusammeng eführte Backup auf.	Nachdem Sie das endgültig e, zusammengeführte Backup vorbereitet haben, verwenden Sie die Befehle tar, zip und split, um kleinere ZIP-Dateien des Backups zu erstellen. Beispiele finden Sie im Abschnitt „Zusätzliche Informationen“.	Datenbankadministrator

Stellen Sie das Backup auf einem Aurora MySQL-DB-Cluster wieder her

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das Backup auf Amazon S3 hoch.	Das Amazon EFS-Datei system, in dem die Sicherung sdateien gespeichert sind, wird sowohl in der lokalen Datenbank als auch in einer EC2 Instance bereitgestellt, sodass die Sicherungsdateien für die EC2 Instance jederzeit verfügbar sind. <bucket_n ame>Stellen Sie mithilfe von Secure Shell (SSH) eine Connect zur EC2 Instanz her und laden Sie die komprimie rten Backup-Dateien in einen neuen oder vorhandenen S3-Bucket hoch; zum Beispiel: aws s3 sync ~/ <efs_moun t_name>/fullbackup s3:///ful lbackup. Weitere Informati onen finden Sie unter den Links im Abschnitt „Verwandte Ressourcen“.	AWS DevOps
Erstellen Sie eine Servicerolle für Aurora, um auf Amazon S3 zuzugreifen.	Erstellen Sie eine IAM-Rolle mit dem Trust „rds.amaz onaws.com“ und einer Richtlini e, die Aurora den Zugriff auf den S3-Bucket ermöglicht, in dem die Backup-Dateien gespeichert sind. Die erforderl ichen Berechtigungen sind, und. ListBucket GetObject GetObjectVersion	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Netzwerkkonfiguration für Aurora.	Erstellen Sie eine Cluster-DB-Subnetzgruppe mit mindestens zwei Availability Zones und einer Subnetz-Routing-Tabellenkonfiguration, die ausgehende Konnektivität zur Quelldatenbank ermöglicht. Erstellen Sie eine Sicherheitsgruppe, die ausgehende Verbindungen zur lokalen Datenbank ermöglicht und es Administratoren ermöglicht, sich mit dem Aurora-DB-Cluster zu verbinden. Weitere Informationen finden Sie unter den Links im Abschnitt „Verwandte Ressourcen“.	DevOpsAWS-/Datenbankadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie das Backup auf einem Aurora MySQL-DB-Cluster wieder her.	Stellen Sie Ihre Daten aus dem Backup wieder her, das Sie auf Amazon S3 hochgeladen haben. Geben Sie die MySQL-Version Ihrer Quelldatenbank an, geben Sie den S3-Bucket-Namen und das Ordnerpfadpräfix an, in das Sie die Backup-Datei hochgeladen haben (z. B. „fullbackup“ für die Beispiele im Abschnitt „Zusätzliche Informationen“) und geben Sie die IAM-Rolle an, die Sie erstellt haben, um Aurora für den Zugriff auf Amazon S3 zu autorisieren.	DevOpsAWS-/Datenbankadministrator
Validieren Sie die Aurora MySQL-Datenbank.	Überprüfen Sie die Anzahl der Schemas und Objekte im wiederhergestellten Aurora-DB-Cluster anhand der Anzahl, die Sie aus der Quelldatenbank erhalten haben.	Datenbankadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Binlog-Replikation ein.	Verwenden Sie die binäre Protokollsequenz, die Sie zuvor notiert haben, bevor Sie das letzte Backup erstellen , das im Aurora-DB-Cluster wiederhergestellt wurde. Erstellen Sie einen Replikationsbenutzer in der Quelldatenbank und folgen Sie den Anweisungen im Abschnitt „Zusätzliche Informationen“, um die entsprechenden Rechte bereitzustellen, die Replikation auf Aurora zu aktivieren und zu bestätigen, dass die Replikation synchron ist.	DevOpsAWS-/Datenbankadministrator

Zugehörige Ressourcen

Erstellen eines Amazon-EFS-Dateisystems

- Eine Sicherheitsgruppe erstellen (Amazon VPC-Dokumentation)
- Transit-Gateway-VPN-Anhänge (Amazon VPC-Dokumentation)
- Skalierung des VPN-Durchsatzes mit AWS Transit Gateway (Blog Networking & Content Delivery)
- Erstellen eines Amazon EFS-Dateisystems (Amazon EFS-Dokumentation)
- Bereitstellungsziele erstellen (Amazon EFS-Dokumentation)
- Verschlüsseln von Daten im Ruhezustand (Amazon EFS-Dokumentation)

Mounten des Dateisystems

- IAM-Rollen für Amazon EC2 (EC2 Amazon-Dokumentation)
- Starten einer Amazon EC2 Linux-Instance (EC2 Amazon-Dokumentation)

- Installation des NFS-Clients (Amazon EFS-Dokumentation)
- Mounten des Amazon EFS-Dateisystems auf Ihrem lokalen Client (Amazon EFS-Dokumentation)
- Mounten von EFS-Dateisystemen (Amazon EFS-Dokumentation)

Erstellen einer Sicherungskopie der MySQL-Quelldatenbank

- Installation von Percona XtraBackup 2.3 (Percona-Dokumentation XtraBackup)
- Installation von Percona XtraBackup 2.4 (Percona-Dokumentation) XtraBackup
- Einstellung der Replikationsmasterkonfiguration (MySQL-Dokumentation)
- Daten von einer externen MySQL-Datenbank zu einem Aurora MySQL-DB-Cluster migrieren (Aurora-Dokumentation)
- Inkrementelles Backup (Percona-Dokumentation XtraBackup)

Wiederherstellung des Backups auf Amazon Aurora MySQL

- Einen Bucket erstellen (Amazon S3 S3-Dokumentation)
- Mit SSH eine Verbindung zu Ihrer Linux-Instance herstellen (Amazon Ec2-Dokumentation)
- Konfiguration der AWS-CLI (AWS-CLI-Dokumentation)
- Sync-Befehl (AWS-CLI-Befehlsreferenz)
- Erstellen einer IAM-Richtlinie für den Zugriff auf Amazon S3 S3-Ressourcen (Aurora-Dokumentation)
- Voraussetzungen für DB-Cluster (Aurora-Dokumentation)
- Arbeiten mit DB-Subnetzgruppen (Aurora-Dokumentation)
- Erstellen einer VPC-Sicherheitsgruppe für eine private DB-Instance (Aurora-Dokumentation)
- Wiederherstellen eines Aurora MySQL-DB-Clusters aus einem S3-Bucket (Aurora-Dokumentation)
- Einrichtung der Replikation mit MySQL oder einem anderen Aurora-DB-Cluster (Aurora-Dokumentation)
- mysql.rds_set_external_master-Prozedur (SQL-Referenz für MySQL auf Amazon RDS)
- mysql.rds_start_replication-Prozedur (SQL-Referenz für MySQL auf Amazon RDS)

Zusätzliche Verweise

- Daten von einer externen MySQL-Datenbank zu einem Aurora MySQL-DB-Cluster migrieren (Aurora-Dokumentation)
- MySQL-Server-Downloads (Oracle-Website)

Tutorials und Videos

- Migrieren von MySQL-Daten zu einem Aurora MySQL-DB-Cluster mithilfe von Amazon S3 (AWS Knowledge Center)
- Einrichtung und Bereitstellung von Amazon EFS (Video)

Zusätzliche Informationen

Installation eines NFS-Clients

- Wenn Sie Red Hat oder ein ähnliches Linux-Betriebssystem verwenden, verwenden Sie den folgenden Befehl:

```
$ sudo yum -y install nfs-utils
```

- Wenn Sie Ubuntu oder ein ähnliches Linux-Betriebssystem verwenden, verwenden Sie den folgenden Befehl:

```
$ sudo apt-get -y install nfs-common
```

Weitere Informationen finden Sie in der exemplarischen Vorgehensweise in der Amazon EFS-Dokumentation.

Mounten des Amazon EFS-Dateisystems

Verwenden Sie die folgenden Befehle:

```
mkdir ~/<efs_mount_name>
$ sudo mount -t nfs -o
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport mount-
target-IP:/ ~/<efs_mount_name>
```

Weitere Informationen finden Sie in der Anleitung und Mounten von EFS-Dateisystemen in der Amazon EFS-Dokumentation.

Backups der MySQL-Quelldatenbank erstellen

Vollständige Backups

Verwenden Sie einen Befehl wie den folgenden, der das Backup nimmt, komprimiert und in kleinere Teile von jeweils 1 GB aufteilt:

```
xtrabackup --backup --user=dbuser --password=<password> --binlog-info=AUTO --stream=tar
 --target-dir=~/<efs_mount_name>/fullbackup | gzip - | split -d --bytes=1024MB - ~/
<efs_mount_name>/fullbackup/backup.tar.gz &
```

Wenn Sie planen, nach dem vollständigen Backup weitere inkrementelle Backups zu erstellen, sollten Sie das Backup nicht komprimieren und teilen. Verwenden Sie stattdessen einen Befehl, der dem folgenden ähnelt:

```
xtrabackup --backup --user=dbuser --password=<password> --target-dir=~/
<efs_mount_name>/fullbackup/
```

Inkrementelle Backups

Verwenden Sie den vollständigen Backup-Pfad für den `--incremental-basedir` Parameter. Beispiel:

```
xtrabackup --backup --user=dbuser --password=<password> --target-dir=~/
<efs_mount_name>/incremental/backupdate --incremental-basedir=~/<efs_mount_name>/
fullbackup
```

wobei basedir der Pfad zur vollständigen Sicherung und zur Datei xtrabackup_checkpoints ist.

Weitere Informationen zum Erstellen von Backups finden Sie unter Migrieren von Daten aus einer externen MySQL-Datenbank zu einem Amazon Aurora MySQL-DB-Cluster in der Aurora-Dokumentation.

Backups vorbereiten

So bereiten Sie ein vollständiges Backup vor:

```
xtrabackup --prepare --apply-log-only --target-dir=~/<efs_mount_name>/fullbackup
```

So bereiten Sie ein inkrementelles Backup vor:

```
xtrabackup --prepare --apply-log-only --target-dir=~/<efs_mount_name>/fullbackup --
incremental-dir=~/<efs_mount_name>/incremental/06062020
```

So bereiten Sie das endgültige Backup vor:

```
xtrabackup --prepare --target-dir=~/<efs_mount_name>/fullbackup --incremental-dir=~/
<efs_mount_name>/incremental/06072020
```

Weitere Informationen finden Sie unter Inkrementelle Backups in der Percona-Dokumentation XtraBackup .

Das zusammengeführte Backup komprimieren und aufteilen

<efs_mount_name>Um das zusammengeführte Backup unter ~/ /fullbackup zu komprimieren:

```
tar -zcvf <backupfilename.tar.gz> ~/<efs_mount_name>/fullbackup
```

Um das Backup aufzuteilen:

```
split -d -b1024M --verbose  <backupfilename.tar.gz> <backupfilename.tar.gz>
```

Binlog-Replikation einrichten

Um einen Replikationsbenutzer in der Quelldatenbank zu erstellen und die entsprechenden Rechte bereitzustellen:

```
CREATE USER 'repl_user'@'' IDENTIFIED BY ''; GRANT REPLICATION CLIENT, REPLICATION
 SLAVE ON *.* TO 'repl_user'@'';
```

Um die Replikation auf Aurora durch eine Verbindung zum Aurora-DB-Cluster zu aktivieren, aktivieren Sie binäre Logs in der DB-Cluster-Parametergruppe. Set `binlog_format = mixed` (gemischter Modus wird bevorzugt). Diese Änderung erfordert, dass Sie die Instanz neu starten, um das Update anzuwenden.

```
CALL mysql.rds_set_external_master ('sourcedbinstanceIP', sourcedbport, 'repl_user',
 '', 'binlog_file_name', binlog_file_position, 0); CALL mysql.rds_start_replication;
```

Um zu überprüfen, ob die Replikation synchron ist:

```
SHOW Slave Status \G;
```

Das Feld Seconds behind master zeigt, wie weit Aurora von der lokalen Datenbank zurückliegt.

Migrieren Sie lokale Java-Anwendungen mit AWS App2Container zu AWS

Erstellt von Dhananjay Karanjkar (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

AWS App2Container (A2C) ist ein Befehlszeilentool, das dabei hilft, bestehende Anwendungen, die auf virtuellen Maschinen ausgeführt werden, in Container umzuwandeln, ohne dass Codeänderungen erforderlich sind. A2C erkennt Anwendungen, die auf einem Server laufen, identifiziert Abhängigkeiten und generiert relevante Artefakte für eine reibungslose Bereitstellung in Amazon Elastic Container Service (Amazon ECS) und Amazon Elastic Kubernetes Service (Amazon EKS).

Dieses Muster enthält die Schritte für die Remote-Migration von lokalen Java-Anwendungen, die auf einem Anwendungsserver bereitgestellt werden, zu AWS Fargate oder Amazon EKS mithilfe von App2Container über den Worker-Computer.

Der Arbeitscomputer kann in den folgenden Anwendungsfällen verwendet werden:

- Die Docker-Installation ist auf den Anwendungsservern, auf denen die Java-Anwendungen ausgeführt werden, nicht zulässig oder nicht verfügbar.
- Sie müssen die Migration mehrerer Anwendungen verwalten, die auf verschiedenen physischen oder virtuellen Servern bereitgestellt werden.

Dieses Muster verwendet AWS CodeCommit AWS CodePipeline, und AWS CodeBuild.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein Anwendungsserver mit einer Java-Anwendung, die auf einem Linux-Server läuft
- Ein Arbeitscomputer mit einem Linux-Betriebssystem
- Ein Arbeitscomputer mit mindestens 20 GB verfügbarem Festplattenspeicher

Einschränkungen

- Nicht alle Anwendungen werden unterstützt. Weitere Informationen finden Sie unter Unterstützte Anwendungen für Linux.

Architektur

Quelltechnologie-Stack

- Java-Anwendungen, die auf einem Linux-Server ausgeführt werden

Zieltechnologie-Stack

- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline
- Amazon Elastic Container Registry
- AWS Fargate

Zielarchitektur

Tools

Tools

- AWS App2Container — AWS App2Container (A2C) ist ein Befehlszeilentool, mit dem Sie Anwendungen, die in Ihren lokalen Rechenzentren oder auf virtuellen Maschinen ausgeführt werden, so verschieben können, dass sie in Containern ausgeführt werden, die von Amazon ECS oder Amazon EKS verwaltet werden.
- AWS CodeBuild — AWS CodeBuild ist ein vollständig verwalteter Build-Service in der Cloud. CodeBuild kompiliert Ihren Quellcode, führt Komponententests durch und produziert Artefakte, die sofort einsatzbereit sind.
- AWS CodeCommit — AWS CodeCommit ist ein von Amazon Web Services gehosteter Service zur Versionskontrolle, mit dem Sie Ressourcen (wie Dokumente, Quellcode und Binärdateien) privat in der Cloud speichern und verwalten können.

- AWS CodePipeline — AWS CodePipeline ist ein Continuous Delivery Service, mit dem Sie die zur Veröffentlichung Ihrer Software erforderlichen Schritte modellieren, visualisieren und automatisieren können.
- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service zum Ausführen, Stoppen und Verwalten von Containern in einem Cluster.
- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) ist ein von AWS verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon EKS — Amazon Elastic Kubernetes Service (Amazon EKS) ist ein verwalteter Service, mit dem Sie Kubernetes auf AWS ausführen können, ohne Ihre eigene Kubernetes-Steuerebene oder Knoten installieren, betreiben und warten zu müssen.
- AWS Fargate — AWS Fargate ist eine Technologie, die Sie mit Amazon ECS verwenden können, um Container auszuführen, ohne Server oder Cluster von Amazon Elastic Compute Cloud (Amazon EC2) -Instances verwalten zu müssen. Mit Fargate müssen Sie keine Cluster virtueller Maschinen mehr bereitstellen, konfigurieren oder skalieren, um Container auszuführen.

Epen

Anmeldeinformationen einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Geheimnis für den Zugriff auf den Anwendungsserver.	Um vom Arbeitscomputer aus remote auf den Anwendung sserver zuzugreifen, erstellen Sie ein Geheimnis in AWS Secrets Manager. Für Ihr Geheimnis können Sie entweder den privaten SSH-Schlüssel oder das Zertifikat und den privaten SSH-Schlü ssel verwenden. Weitere Informationen finden Sie unter Manage Secrets for AWS App2Container.	DevOps, Entwickler

Richten Sie die Arbeitsmaschine ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die TAR-Datei.	Führen Sie `sudo yum install -y tar`.	DevOps, Entwickler
Installieren Sie den AWS CLI.	Führen Sie den Befehl aus, um das Amazon Command Line Interface (AWS CLI) zu installieren`curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip" .` Extrahieren Sie `awscliv2.zip .` Führen Sie `sudo ./aws/install .`	DevOps, Entwickler
Installieren Sie App2Container.	Führen Sie die folgenden Befehle aus: `curl -o AWSApp2Container-installer-linux.tar.gz https://app2container-release-us-east-1.s3.us-east-1.amazonaws.com/latest/linux/AWSApp2Container-installer-linux.tar.gz`	DevOps, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`sudo tar xvf AWSApp2Container-installer-linux.tar.gz`
	
	`sudo ./install.sh`	

Konfigurieren Sie die Profile.	Führen Sie den Befehl aus, um das AWS-Standardprofil zu konfigurieren`sudo aws configure` . Führen Sie den Befehl aus, um das benannte AWS-Standardprofil zu konfigurieren`sudo aws configure --profile <profile name>`.	DevOps, Entwickler

Docker-Installation.	Führen Sie die folgenden Befehle aus.
	
	`sudo yum install -y docker`
	
	`sudo systemctl enable docker & sudo systemctl restart docker`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initialisieren Sie App2Container.	Um App2Container zu initialisieren, benötigen Sie die folgenden Informationen: • `workspace` : Um Artefakte zur Containerisierung von Anwendungen zu speichern. Wir empfehlen , einen Verzeichnispfad mit mindestens 20 GB freiem Festplattenspeicher anzugeben. • `awsProfile` : Auf dem Server konfiguriertes AWS-Profil. Dies ist erforderlich, um Artefakte auf Amazon S3 hochzuladen, den `containerize` Befehl auszuführen und AWS-Artefakte für die Bereitstellung auf Amazon ECS oder Amazon EKS zu generieren. • `s3Bucket`: Um AWS-Artefakte zu extrahieren und zu speichern. • `metricsReportPermission` : Um gemeldete Metriken zu sammeln und zu speichern. • `dockerContentTrust` : Um das Docker-Image zu signieren.	DevOps, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Führen Sie `sudo app2container init .`	

Konfigurieren Sie den Arbeitscomputer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Arbeitscomputer so, dass er eine Remoteverbindung herstellt und App2Container-Befehle auf dem Anwendungsserver ausführt.	Um den Arbeitscomputer zu konfigurieren, sind die folgenden Informationen erforderlich: • `Server FQDN`: Der vollqualifizierte Domänenname des Anwendungsservers. • `Server IP address`: Die IP-Adresse des Anwendungsservers. Entweder der FQDN oder die IP-Adresse ist ausreichend. • `SecretARN` : Der Amazon-Ressourcenname (ARN) des Secrets, das für die Verbindung mit dem Anwendungsserver verwendet wird und in Secrets Manager gespeichert ist. • `AuthMethod` : Die `cert` Authentifizierungsmethode `key` oder.	DevOps, Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Führen Sie `sudo app2container remote configure` .	

Entdecken, analysieren und extrahieren Sie Anwendungen auf dem Arbeitscomputer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entdecken Sie die lokalen Java-Anwendungen.	Führen Sie den folgenden Befehl aus, um per Fernzugriff alle Anwendungen zu ermitteln , die auf dem Anwendungsserver ausgeführt werden. `sudo app2container remote inventory --target <FQDN/IP of App server>` Dieser Befehl generiert eine Liste der bereitgestellten Anwendungen in`inventory.json` .	Entwickler, DevOps
Analysieren Sie die entdeckten Anwendungen.	Führen Sie den folgenden Befehl aus, um jede Anwendung mithilfe der in der Inventarphase erhaltenen Anwendungs-ID remote zu analysieren. `sudo app2container remote analyze --application-id <java-app-id> --target`	Entwickler, DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`<FQDN/IP of App Server>` Dadurch wird eine `analysis.json` Datei am Speicherort des Workspace generiert. Nachdem diese Datei generiert wurde, können Sie die Containerisierungsparameter Ihren Bedürfnissen entsprechend ändern.	
Extrahieren Sie die analysierten Anwendungen.	Um ein Anwendungsarchiv für die analysierte Anwendung zu generieren, führen Sie den folgenden Befehl remote aus, der das TAR-Bundle am Workspace-Speicherort generiert. `sudo app2container remote extract --application-id <application id> --target <FQDN/IP of App Server>` Extrahierte Artefakte können auf dem lokalen Arbeitscomputer generiert werden.	Entwickler, DevOps

Containeriere die extrahierten Artefakte auf dem Worker-Computer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Containerisieren Sie die extrahierten Artefakte.	Containerisieren Sie die im vorherigen Schritt extrahier ten Artefakte, indem Sie den folgenden Befehl ausführen. `sudo app2container containerize --input-archive <tar bundle location on worker machine>`	Entwickler, DevOps
Finalisieren Sie das Ziel.	Um das Ziel zu finalisie ren, öffnen Sie es. Es wird erstellt`deployment.json` , wenn der `container ize` Befehl ausgeführt wird. Um AWS Fargate als Ziel anzugeben, legen Sie `createEcsArtifacts` auf `true` fest. Um Amazon EKS als Ziel festzulegen, legen Sie den Wert `createEks Artifacts` auf true fest.	Entwickler, DevOps

AWS-Artefakte generieren und bereitstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie AWS-Berei tstellungsartefakte auf dem Arbeitscomputer.	Führen Sie den folgenden Befehl aus, um Bereitste llungsartefakte zu generieren.	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`sudo app2container generate app-deployment --application-id <application id>` Dadurch wird die `ecs-master.yml` CloudFormation AWS-Vorlage im Workspace generiert.	
Stellen Sie die Artefakte bereit.	Um die generierten Artefakte weiter bereitzustellen, stellen Sie die CloudFormation AWS-Vorlage bereit, indem Sie den folgenden Befehl ausführen. `aws cloudformation deploy --template-file <path to ecs-master.yml> --capabilities CAPABILITY_NAMED_IAM --stack-name <application id>-ECS`	DevOps
Generieren Sie die Pipeline.	Modifizieren Sie`pipeline.json` , was in der vorherigen Geschichte erstellt wurde, basierend auf Ihren Bedürfnissen. Führen Sie dann den `generate pipeline` Befehl aus, um die Artefakte für die Pipeline-Bereitstellung zu generieren.	DevOps

Zugehörige Ressourcen

- Was ist App2Container?
- Blogbeitrag zu AWS App2Container
- Grundlagen der AWS-CLI-Konfiguration
- Docker-Grundlagen für Amazon ECS
- Docker-Befehle

Migrieren Sie gemeinsam genutzte Dateisysteme in einer großen AWS-Migration

Erstellt von Amit Rudraraju (AWS), Sam Apa (AWS), Bheemeswararao Balla (AWS), Wally Lu (AWS) und Sanjeev Prakasam (AWS)

Übersicht

Die Migration von 300 oder mehr Servern wird als umfangreiche Migration angesehen. Der Zweck einer großen Migration besteht darin, Workloads von ihren bestehenden lokalen Rechenzentren in die AWS-Cloud zu migrieren. Diese Projekte konzentrieren sich in der Regel auf Anwendungs- und Datenbank-Workloads. Gemeinsam genutzte Dateisysteme erfordern jedoch besondere Aufmerksamkeit und einen separaten Migrationsplan. Dieses Muster beschreibt den Migrationsprozess für gemeinsam genutzte Dateisysteme und bietet bewährte Methoden für deren erfolgreiche Migration im Rahmen eines großen Migrationsprojekts.

Ein Shared File System (SFS), auch bekannt als Netzwerk - oder Cluster-Dateisystem, ist eine Dateifreigabe, die auf mehreren Servern bereitgestellt wird. Auf gemeinsam genutzte Dateisysteme wird über Protokolle wie Network File System (NFS), Common Internet File System (CIFS) oder Server Message Block (SMB) zugegriffen.

Diese Systeme werden nicht mit Standard-Migrationstools wie dem AWS Application Migration Service migriert, da sie weder für den zu migrierenden Host reserviert noch als Blockgerät dargestellt werden. Obwohl die meisten Host-Abhängigkeiten transparent migriert werden, müssen die Koordination und Verwaltung der abhängigen Dateisysteme separat erfolgen.

Sie migrieren gemeinsam genutzte Dateisysteme in den folgenden Phasen: Erkennung, Planung, Vorbereitung, Umstellung und Validierung. Mithilfe dieses Musters und der angehängten Arbeitsmappen migrieren Sie Ihr gemeinsam genutztes Dateisystem zu einem AWS-Speicherservice wie Amazon Elastic File System (Amazon EFS), Amazon FSx for NetApp ONTAP oder Amazon FSx for Windows File Server. Um das Dateisystem zu übertragen, können Sie AWS DataSync oder ein Drittanbieter-Tool verwenden, NetApp SnapMirror z.

> **Note**
>
> Dieses Muster ist Teil einer Reihe von AWS Prescriptive Guidance über große Migration en in die AWS-Cloud. Dieses Muster enthält bewährte Methoden und Anweisungen zur Integration SFSs in Ihre Wave-Pläne für Server. Wenn Sie ein oder mehrere gemeinsam genutzte Dateisysteme außerhalb eines großen Migrationsprojekts migrieren, lesen Sie

die Anweisungen zur Datenübertragung in der AWS-Dokumentation für Amazon EFS, Amazon FSx für Windows File Server und Amazon FSx für NetApp ONTAP.

Voraussetzungen und Einschränkungen

Voraussetzungen

Die Voraussetzungen können je nach Ihren gemeinsam genutzten Quell- und Zieldateisystemen und Ihrem Anwendungsfall variieren. Die folgenden sind am häufigsten:

- Ein aktives AWS-Konto.
- Sie haben die Suche nach dem Anwendungsportfolio für Ihr großes Migrationsprojekt abgeschlossen und mit der Entwicklung von Wave-Plänen begonnen. Weitere Informationen finden Sie im Portfolio-Playbook für große AWS-Migrationen.
- Virtuelle private Clouds (VPCs) und Sicherheitsgruppen, die eingehenden und ausgehenden Datenverkehr zwischen dem lokalen Rechenzentrum und Ihrer AWS-Umgebung ermöglichen. Weitere Informationen finden Sie unter Network-to-Amazon VPC-Konnektivitätsoptionen und DataSync AWS-Netzwerkanforderungen.
- Berechtigungen zum Erstellen von CloudFormation AWS-Stacks oder Berechtigungen zum Erstellen von Amazon EFS- oder FSx Amazon-Ressourcen. Weitere Informationen finden Sie in der CloudFormation Dokumentation, der Amazon EFS-Dokumentation oder der FSx Amazon-Dokumentation.
- Wenn Sie AWS verwenden DataSync , um die Migration durchzuführen, benötigen Sie die folgenden Berechtigungen:
  - Berechtigungen für AWS DataSync zum Senden von Protokollen an eine AWS CloudWatch Logs-Protokollgruppe. Weitere Informationen finden Sie unter Zulassen DataSync des Hochladens von Protokollen in CloudWatch Protokollgruppen.
  - Berechtigungen für den Zugriff auf die CloudWatch Protokollgruppe Logs. Weitere Informationen finden Sie unter Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre CloudWatch Logs-Ressourcen.
  - Berechtigungen zum Erstellen von Agenten und Aufgaben in DataSync. Weitere Informationen finden Sie unter Erforderliche IAM-Berechtigungen für die Nutzung von AWS DataSync.

Einschränkungen

- Dieses Muster ist für die Migration im SFSs Rahmen eines großen Migrationsprojekts konzipiert. Es enthält bewährte Methoden und Anweisungen für die Integration SFSs in Ihre Wave-Pläne für die Migration von Anwendungen. Wenn Sie ein oder mehrere gemeinsam genutzte Dateisysteme außerhalb eines großen Migrationsprojekts migrieren, lesen Sie die Anweisungen zur Datenübertragung in der AWS-Dokumentation für Amazon EFS, Amazon FSx für Windows File Server und Amazon FSx für NetApp ONTAP.
- Dieses Muster basiert auf häufig verwendeten Architekturen, Services und Migrationsmustern. Große Migrationsprojekte und -strategien können jedoch von Unternehmen zu Unternehmen variieren. Möglicherweise müssen Sie diese Lösung oder die bereitgestellten Arbeitsmappen an Ihre Anforderungen anpassen.

Architektur

Quelltechnologie-Stack

Eine oder mehrere der folgenden Optionen:

- Linux-Dateiserver (NFS)
- Windows (SMB) -Dateiserver
- NetApp Speicher-Array
- Dell EMC Isilon-Speicher-Array

Zieltechnologie-Stack

Eine oder mehrere der folgenden Optionen:

- Amazon Elastic File System
- Amazon FSx für NetApp ONTAP
- Amazon FSx für Windows-Dateiserver

Zielarchitektur

Das Diagramm zeigt den folgenden Prozess:

1. Sie stellen eine Verbindung zwischen dem lokalen Rechenzentrum und der AWS-Cloud her, indem Sie einen AWS-Service wie AWS Direct Connect oder AWS Site-to-Site VPN verwenden.

2. Sie installieren den DataSync Agenten im lokalen Rechenzentrum.
3. Gemäß Ihrem Wave-Plan DataSync replizieren Sie Daten aus dem gemeinsam genutzten Quelldateisystem auf die AWS-Zieldateifreigabe.

Migrationsphasen

Die folgende Abbildung zeigt die Phasen und allgemeinen Schritte für die Migration eines SFS in einem großen Migrationsprojekt.

Der Abschnitt Epics dieses Musters enthält detaillierte Anweisungen zum Abschließen der Migration und zur Verwendung der beigefügten Arbeitsmappen. Im Folgenden finden Sie einen allgemeinen Überblick über die Schritte dieses schrittweisen Ansatzes.

Phase	Schritte
Erkennen	1. Mithilfe eines Discoverytools sammeln Sie Daten über das gemeinsam genutzte Dateisystem, einschließlich Server, Bereitstellungspunkte und IP-Adressen. 2. Mithilfe einer Configuration Management Database (CMDB) oder Ihres Migrationstools erfassen Sie Details über den Server, einschließlich Informationen zur Migrationswelle, zur Umgebung, zum Anwendungsbesitzer, zum IT-Servicemanagement (ITSM) -Dienstnamen, zur Organisationseinheit und zur Anwendungs-ID.
Plan	3. Erstellen Sie anhand der gesammelten Informationen über die SFSs und die Server den SFS-Wellenplan. 4. Wählen Sie anhand der Informationen im Build-Arbeitsblatt für jedes SFS einen AWS-Zielservice und ein Migrationstool aus.

Vorbereitung	5. Richten Sie die Zielinfrastruktur in Amazon EFS, Amazon FSx for NetApp ONTAP oder Amazon FSx for Windows File Server ein. 6. Richten Sie den Datenübertragungsdienst ein, z. B. DataSync, und starten Sie dann die erste Datensynchronisierung. Wenn die erste Synchronisierung abgeschlossen ist, können Sie wiederkehrende Synchronisierungen so einrichten, dass sie nach einem Zeitplan ausgeführt werden. 7. Aktualisieren Sie den SFS-Wellenplan mit Informationen zur Zieldateifreigabe, z. B. der IP-Adresse oder dem Pfad.
Überschneiden	8. Stoppen Sie Anwendungen, die aktiv auf das Quell-SFS zugreifen. 9. Führen Sie im Datenübertragungsdienst eine letzte Datensynchronisierung durch. 10. Wenn die Synchronisierung abgeschlo ssen ist, überprüfen Sie, ob sie vollständig erfolgreich war, indem Sie die Protokolldaten in CloudWatch Logs überprüfen.
Bestätigen	11. Ändern Sie auf den Servern den Bereitste llungspunkt auf den neuen SFS-Pfad. 12. Starten Sie die Anwendungen neu und validieren Sie sie.

Tools

AWS-Services

- Amazon CloudWatch Logs hilft Ihnen dabei, die Protokolle all Ihrer Systeme, Anwendungen und AWS-Services zu zentralisieren, sodass Sie sie überwachen und sicher archivieren können.

- AWS DataSync ist ein Online-Datenübertragungs- und Erkennungsservice, mit dem Sie Dateien oder Objektdaten zu, von und zwischen AWS-Speicherservices verschieben können.
- Amazon Elastic File System (Amazon EFS) unterstützt Sie bei der Erstellung und Konfiguration gemeinsam genutzter Dateisysteme in der AWS-Cloud.
- Amazon FSx bietet Dateisysteme, die branchenübliche Konnektivitätsprotokolle unterstützen und Hochverfügbarkeit und Replikation in allen AWS-Regionen bieten.

Andere Tools

- SnapMirrorist ein NetApp Datenreplikationstool, das Daten von bestimmten Quell-Volumes oder QTrees auf Ziel-Volumes bzw. QTrees repliziert. Sie können dieses Tool verwenden, um ein NetApp Quelldateisystem FSx für ONTAP zu Amazon zu migrieren.
- Robocopy, kurz für Robust File Copy, ist ein Befehlszeilenverzeichnis und ein Befehl für Windows. Sie können dieses Tool verwenden, um ein Windows-Quelldateisystem zu Amazon FSx for Windows File Server zu migrieren.

Bewährte Methoden

Ansätze zur Wellenplanung

Berücksichtigen Sie bei der Planung von Wellen für Ihr großes Migrationsprojekt die Latenz und die Anwendungsleistung. Wenn das SFS und die abhängigen Anwendungen an unterschiedlichen Standorten betrieben werden, z. B. an einem Standort in der Cloud und einem im lokalen Rechenzentrum, kann dies die Latenz erhöhen und die Anwendungsleistung beeinträchtigen. Bei der Erstellung von Wellenplänen stehen die folgenden Optionen zur Verfügung:

1. Migrieren Sie das SFS und alle abhängigen Server innerhalb derselben Welle — Dieser Ansatz verhindert Leistungsprobleme und minimiert Nacharbeiten, wie z. B. die mehrfache Neukonfiguration von Mount-Points. Es wird empfohlen, wenn eine sehr geringe Latenz zwischen der Anwendung und dem SFS erforderlich ist. Die Wellenplanung ist jedoch komplex, und das Ziel besteht in der Regel darin, Variablen aus Abhängigkeitsgruppierungen zu entfernen und nicht zu ihnen hinzuzufügen. Außerdem wird dieser Ansatz nicht empfohlen, wenn viele Server auf dasselbe SFS zugreifen, da die Welle dadurch zu groß wird.
2. Migrieren Sie das SFS, nachdem der letzte abhängige Server migriert wurde. Wenn beispielsweise mehrere Server auf ein SFS zugreifen und diese Server für die Migration in den Wellen 4, 6 und 7 geplant sind, planen Sie das SFS so, dass es in Welle 7 migriert wird.

Dieser Ansatz ist bei großen Migrationen oft am logischsten und wird für latenzempfindliche Anwendungen empfohlen. Es reduziert die mit der Datenübertragung verbundenen Kosten. Es minimiert auch die Latenzzeit zwischen dem SFS und Anwendungen höherer Ebenen (wie z. B. Produktionsanwendungen), da Anwendungen höherer Stufen in der Regel erst nach der Entwicklung und der Qualitätssicherung migriert werden.

Dieser Ansatz erfordert jedoch immer noch Entdeckung, Planung und Agilität. Möglicherweise müssen Sie das SFS in einer früheren Welle migrieren. Vergewissern Sie sich, dass die Anwendungen die zusätzliche Latenz für den Zeitraum zwischen der ersten abhängigen Welle und der Welle, die das SFS enthält, aushalten können. Führen Sie eine Ermittlungssitzung mit den Besitzern der Anwendung durch und migrieren Sie die Anwendung in derselben Welle, der Anwendung mit der höchsten Latenzempfindlichkeit. Wenn nach der Migration einer abhängigen Anwendung Leistungsprobleme festgestellt werden, sollten Sie darauf vorbereitet sein, schnell umzusteigen, um das SFS so schnell wie möglich zu migrieren.

3. Migrieren Sie das SFS am Ende des großen Migrationsprojekts — Dieser Ansatz wird empfohlen, wenn die Latenz keine Rolle spielt, z. B. wenn auf die Daten im SFS selten zugegriffen wird oder wenn sie für die Anwendungsleistung nicht entscheidend sind. Dieser Ansatz rationalisiert die Migration und vereinfacht Umstellungsaufgaben.

Sie können diese Ansätze je nach Latenzempfindlichkeit der Anwendung kombinieren. Sie können z. B. latenzabhängig migrieren, SFSs indem Sie die Ansätze 1 oder 2 verwenden, und dann den Rest mit Ansatz 3 migrieren. SFSs

Auswahl eines AWS-Dateisystem-Service

AWS bietet mehrere Cloud-Services für die Dateispeicherung an. Jeder bietet unterschiedliche Vorteile und Einschränkungen in Bezug auf Leistung, Skalierbarkeit, Zugänglichkeit, Integration, Compliance und Kostenoptimierung. Es gibt einige logische Standardoptionen. Wenn auf Ihrem aktuellen lokalen Dateisystem beispielsweise Windows Server ausgeführt wird, ist Amazon FSx for Windows File Server die Standardauswahl. Oder wenn auf dem lokalen Dateisystem NetApp ONTAP ausgeführt wird, ist Amazon FSx for NetApp ONTAP die Standardoption. Sie können jedoch einen Zieldienst wählen, der auf den Anforderungen Ihrer Anwendung basiert oder um andere Vorteile des Cloud-Betriebs zu nutzen. Weitere Informationen finden Sie unter Auswahl des richtigen AWS-Dateispeicherservices für Ihre Bereitstellung (AWS Summit-Präsentation).

Auswahl eines Migrationstools

Amazon EFS und Amazon FSx unterstützen die Verwendung von AWS DataSync zur Migration gemeinsam genutzter Dateisysteme in die AWS-Cloud. Weitere Informationen zu unterstützten Speichersystemen und Services, Vorteilen und Anwendungsfällen finden Sie unter Was ist AWS DataSync. Einen Überblick über den Prozess der Übertragung Ihrer Dateien finden Sie unter So funktionieren DataSync AWS-Übertragungen. DataSync

Es sind auch mehrere Tools von Drittanbietern verfügbar, darunter die folgenden:

- Wenn Sie Amazon FSx for NetApp ONTAP wählen, können Sie NetApp SnapMirror damit die Dateien vom lokalen Rechenzentrum in die Cloud migrieren. SnapMirror verwendet eine Replikation auf Blockebene, die schneller als der Datenübertragungsprozess sein DataSync und dessen Dauer verkürzen kann. Weitere Informationen finden Sie unter Migration zu FSx ONTAP using. NetApp SnapMirror
- Wenn Sie sich FSx für Amazon for Windows File Server entscheiden, können Sie Robocopy verwenden, um Dateien in die Cloud zu migrieren. Weitere Informationen finden Sie unter Migrieren vorhandener Dateien auf einen FSx Windows-Dateiserver mithilfe von Robocopy.

Epen

Erkennen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die SFS-Discovery-Arbeitsmappe vor.	1. Laden Sie die Arbeitsmappen im Abschnitt Anlagen dieses Musters herunter. Es enthält zwei Dateien, SFS-Discovery-Workbook.xlsx und SFS-Wave-Plan-Workbook.xlsx. 2. Öffnen Sie die SFS-Discovery-Workbook-Datei in Microsoft Excel. 3. Gehen Sie im Dashboard-Arbeitsblatt wie folgt vor:	Migrationsingenieur, Migrationsleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Aktualisieren Sie in Spalte A den Namen der Umgebung. • Aktualisieren Sie in Spalte B die Reihenfolge der Umgebungen, sodass sie in der Reihenfol ge von niedrigster (1) Priorität bis zur höchsten Priorität angeordnet sind. • Aktualisieren Sie in den Spalten D—E den Wave-Zeitplan. • Aktualisieren Sie in den Spalten C und K die AWS-Kontonamen. • Aktualisieren Sie in Spalte L die VPC IDs. • Aktualisieren Sie in den Spalten M—O das Subnetz. IDs 4. Überprüfen Sie den Rest der Arbeitsmappenvorlage und aktualisieren Sie alle anderen Werte, die für Ihre Organisation oder Ihren Anwendungsfall erforderlich sind. 5. Speichern Sie die Arbeitsmappe.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sammeln Sie Informationen über das Quell-SFS.	1. Identifizieren Sie mit Ihrem bevorzugten Discovery -Tool alle SFS-Mounts auf allen entsprechenden Speichergeräten, Linux-Servern und Windows-Servern. In der Regel müssen Sie die folgenden Informationen sammeln: • Client-Geräte • Client-IP-Adresse • SFS-Einzelheiten • Befestigungspunkt **Note** Sie können Ihrem Migrations-Runbook Details zum Bereitstellungspunkt hinzufügen, um das SFS nach der Migration erneut zu mounten. 2. Öffnen Sie die SFS-Discovery-Workbook-Datei. 3. Gehen Sie auf dem Wave-Sheet-Arbeitsblatt wie folgt vor: • Vergewissern Sie sich in der Formel in der Spalte Serverstandort (D), dass	Migrationsingenieur, Migrationsleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	das Format des CIDR-Bereichs für die lokale Quelle für Ihren Bereich geeignet ist. Wenn Ihr CIDR-Bereich beispielsweise lautet`10.0.0.0/8` , geben Sie ein. `10.*.*.*` • Vergewissern Sie sich in der Spalte SFS-Standort (E) in der Formel, dass das Format des CIDR-Bereichs für die Ziel-VPC für Ihren Bereich funktioniert. Wenn Ihr CIDR-Bereich beispielsweise lautet, geben Sie ein. `176.16.0.0/16` `176.16.*.*` 4. Gehen Sie auf dem Arbeitsblatt SFS-Data wie folgt vor: • Geben Sie in der Spalte Servername (A) den Namen des Servers ein, auf dem das SFS bereitgestellt ist. • Geben Sie in der Spalte SFS-Pfad (B) den Namen des SFS ein. • Geben Sie in der Spalte IP-Adresse (C) die IP-Adresse des Servers ein.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Fügen Sie alle anderen relevanten Informationen hinzu, die Sie bei der Erkennung gesammelt haben, z. B. den Bereitstellungspunkt und die SFS-Größe. Sie können diese Daten später verwenden, um die Berechnungen zur Wellenplanung zu ändern. 5. Speichern Sie die Arbeitsmappe.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sammeln Sie Informationen über die Server.	1. Identifizieren Sie mithilfe Ihrer CMDB oder der in Ihrem Migrationstool aufgezeichneten Daten alle folgenden Informationen zu den Servern, die über SFS-Mounts verfügen: • Server name • IP-Adresse • Welle • Organisationseinheit (OU) • Serverumgebung, wie`DEV`,`QA`, oder `PROD` • Anwendungsname • Inhaber der Anwendung und Kontaktinformationen 2. Öffnen Sie die SFS-Disco very-Workbook-Datei. 3. Geben Sie im Arbeitsblatt Serverdaten in den Spalten A—H die Informationen ein, die Sie über die Quellserv er gesammelt haben. Beachten Sie Folgendes: • Geben Sie in der Spalte Welle Nr. (C) den Wellennamen ein (z. B.`Wave1`), out-of-scope (`OOS`) oder. `Retire` • Vergewissern Sie sich, dass die E-Mail-Adresse	Migrationsingenieur, Migration sleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in der Spalte Kontakt (H) des App-Besitzers richtig ist. Diese E-Mail-Adresse wird automatisch auf der Grundlage des Namens generiert, den Sie in der Spalte App-Besitzer (G) angegeben haben. Falls erforderlich, aktualisieren Sie den Wert manuell, sodass er die richtige E-Mail-Adresse wiedergibt. • Ändern Sie nicht die Spalten I—J, die Formeln enthalten. 4. Speichern Sie die Arbeitsmappe.	

Plan

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den SFS-Welle nplan.	1. Öffnen Sie die SFS-Disco very-Workbook-Datei. 2. Stellen Sie sicher, dass alle in der Ermittlungsphase gesammelten Informationen korrekt und aktuell sind. 3. Filtern Sie im Wave-Sheet-Arbeitsblatt die Spalte SFS-Welle (K) nach dem Wert. 1 Dies ist eine Liste aller	Leiter Aufbau, Leiter der Umstellung, Migration singenieur, Migrationsleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Objekte SFSs in der ersten Welle. **Note** Ein Wert von `0` in dieser Spalte gibt an, dass das SFS außerhalb des Migrationsbereichs liegt. Dies kann daran liegen, dass das SFS bereits auf AWS gehostet wird oder dass die Server, die auf das Share zugreifen, nicht in den Geltungsbereich der Migration fallen. 4. Vergewissern Sie sich, dass Sie diese SFSs in dieser Phase migrieren möchten. Weitere Informationen zur Zuweisung SFSs zu Wellen finden Sie unter Ansätze zur Wellenplanung im Abschnitt Bewährte Methoden. 5. Wählen Sie die Zellen aus, die die gefilterten Werte enthalten, und kopieren Sie sie. Kopieren Sie nicht die	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Kopfzeile mit den Spaltenti teln. 6. Öffnen Sie die SFS-Wave-Plan-Workbook-Datei, die Sie zuvor heruntergeladen haben. 7. Wählen Sie im Arbeitsblatt „Exportieren aus Discovery“ die Zelle A2 aus. 8. Fügen Sie die kopierten Daten ein. 9. Speichern Sie die Dateien SFS-Discovery-Workbook und SFS-Wave-Plan-Work book.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie den AWS-Service und das Migrationstool als Ziel aus.	1. Wählen Sie in der SFS-Wave-Plan-Workbook Datei auf dem Exported-from-Discovery Arbeitsblatt die Werte in der Spalte Alter Pfad (C) aus und kopieren Sie sie. 2. Wählen Sie auf dem Build-Wave-Arbeitsblatt die Zelle A2 aus. 3. Fügen Sie die kopierten Daten ein. Die Spalten B—M in diesem Arbeitsblatt werden automatisch aktualisiert, um andere mit diesem Pfad verknüpfte Daten widerzuspiegeln. 4. Entfernen Sie alle doppelten Werte in Spalte A. Anweisungen finden Sie unter Doppelte Werte entfernen (Microsoft-Support-Website). 5. Überprüfen Sie in der Spalte Zielmuster oder Service (F) den empfohlenen AWS-Zielservice und aktualisieren Sie ihn bei Bedarf. Weitere Informationen finden Sie unter Auswahl eines AWS-Dateisystem-Service im Abschnitt Bewährte Methoden dieses Musters.	Migrationsingenieur, Migrationsleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Sehen Sie sich in der Spalte Migrationsmethode (G) das empfohlene Migrationstool an und aktualisieren Sie es bei Bedarf. Weitere Informationen finden Sie unter Auswahl eines Migrationstools im Abschnitt Bewährte Methoden dieses Musters. 7. Speichern Sie die SFS-Discovery-Workbook-Date i. Sie haben die Erstellung eines Wellenplans für diese Welle abgeschlossen. 8. Wiederholen Sie diese Anweisungen, um für jede Welle einen Wellenplan zu erstellen. Da sich die Wellenpläne während der Migration ändern können, empfehlen wir, nicht mehr als 5 Wellen im Voraus zu planen.	

Vorbereitung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie das Zieldatei system ein.	Richten Sie gemäß den in Ihrem Wave-Plan aufgezeic hneten Details die Zieldatei systeme im AWS-Zielk	Migrationsingenieur, Migration sleiter, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	onto, in der VPC und in den Subnetzen ein. Anweisungen finden Sie in der folgenden AWS-Dokumentation: • Amazon EFS • Amazon FSx für NetApp ONTAP • Amazon FSx für Windows-Dateiserver	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie das Migrationstool ein und übertragen Sie Daten.	1. Wenn Sie AWS verwenden DataSync, konfigurieren Sie die Protokollierung für DataSync Aufgaben. Anweisungen finden Sie unter Protokollieren Ihrer DataSync AWS-Aufgabenaktivitäten. 2. Richten Sie das Migration stool ein und führen Sie eine erste Datenübertragung gemäß den Anweisungen für Ihr ausgewähltes Tool durch: • Informationen zu Amazon EFS finden Sie im Folgenden: • Dateien mithilfe von AWS an Amazon EFS übertragen DataSync • Informationen zu Amazon FSx für ONTAP finden Sie im Folgenden: • Migration zu FSx for ONTAP mit NetApp SnapMirror • Migration zu FSx for ONTAP mithilfe von AWS DataSync • Informationen zu Amazon FSx für Windows File Server finden Sie im Folgenden:	AWS-Administrator, Cloud-Administrator, Migrationsingenieur, Migrationsleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Migrieren vorhandener Dateien auf einen FSx Windows-Dateiserver mithilfe von AWS DataSync • Migrieren vorhandener Dateien auf einen FSx Windows-Dateiserver mithilfe von Robocopy 3. Änderungen am Quell-SFS können während oder nach der ersten Übertragung auftreten. Richten Sie wiederkehrende Datenübertragungen zwischen dem Quell- und dem Zieldateisystem ein, um die Daten synchron zu halten: • Wenn Sie dies verwenden DataSync, finden Sie weitere Informationen unter Planen Ihrer DataSync AWS-Aufgabe. DataSync überträgt nur die geänderten oder neuen Dateien im Quell-SFS. • Wenn Sie ein Drittanbieter-Tool verwenden, lesen Sie in der Dokumentation des ausgewählten Tools nach.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie den Wave-Plan.	1. Öffnen Sie die SFS-Wave-Plan-Workbook-Datei für die aktuelle Welle. 2. Geben Sie auf dem Build-Wave-Arbeitsblatt in der Spalte Neue Pfad-IP-Adresse (N) die IP-Adresse des Zieldateisystems ein. Gehen Sie wie folgt vor, um die IP-Adresse zu ermitteln: • Wählen Sie FSx für Windows File Server auf der FSx Amazon-Konsole Dateisysteme, wählen Sie Ihr Dateisystem aus und sehen Sie sich dann den Abschnitt Netzwerk und Sicherheit an. • Informationen FSx zu ONTAP finden Sie unter Mounten von Volumes. • Informationen zu Amazon EFS finden Sie unter Mounten mit einer IP-Adresse. 3. Geben Sie in der Spalte Neuer Pfad (O) den neuen Bereitstellungspfad ein. Der Mountpfad ist der DNS-Name des Dateisystems. Gehen Sie wie folgt vor, um den Bereitstellungspfad zu finden:	Migrationsingenieur, Migration sleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wählen Sie FSx für Windows File Server auf der FSx Amazon-Konsole Dateisysteme, wählen Sie Ihr Dateisystem und dann Attach aus. • Informationen FSx zu ONTAP finden Sie auf der Seite mit den Dateisystemdetails. Anweisungen finden Sie unter Volumen einbinden. • Informationen zu Amazon EFS finden Sie unter Informationen sammeln. 4. Vergewissern Sie sich im Arbeitsblatt Remount-S ummary, dass die Spalten Neuer Pfad (C) und Neuer Pfad IP-Adresse (D) die aktualisierten Werte wiedergeben. 5. Vergewissern Sie sich, dass Ihr Unternehmen Runbooks für die erneute Bereitstellung der Linux- und Windows-Dateisyste me nach der Umstellung vorbereitet hat. Allgemeine Anweisungen finden Sie im Folgenden: • Mounten von EFS-Datei systemen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Zugreifen auf Dateifreigaben FSx für Windows-Dateiserver • Montage FSx für ONTAP-Volumes 6. Falls abhängige Server nicht in dieser Welle enthalten sind, notieren Sie sie im Arbeitsblatt App-Team-Communication. Informieren Sie die jeweiligen Anwendungs- oder Serverbesitzer, da diese möglicherweise nicht in der Standard-Wave-Kommunikation enthalten sind. 7. Falls SFSs sie nach Abschluss des Wellenplans aus der Welle entfernt wurden, können Sie diese im Arbeitsblatt Descoped nachverfolgen.	

Überschneiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stoppen Sie Anwendungen.	Wenn Anwendungen oder Clients aktiv Lese- und Schreibvorgänge im Quell-SFS ausführen, beenden Sie sie, bevor Sie die endgültig	App-Besitzer, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	e Datensynchronisierung durchführen. Anweisungen finden Sie in der Anwendungsdokumentation oder in Ihren internen Prozessen zum Stoppen von Lese- und Schreibaktivitäten. Siehe beispielsweise Starten oder Beenden des Webservers (IIS 8) (Microsoft-Dokumentation) oder Systemdienste mit systemctl verwalten (Red Hat-Dokumentation).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die endgültige Datenübertragung durch.	1. Führen Sie im Migration stool manuell eine letzte Datenübertragungsaufgabe oder einen Job aus, um das Zieldateisystem mit dem Quell-SFS zu synchroni sieren. Anweisungen finden Sie unter Starten Ihrer DataSync Aufgabe oder in der Dokumentation des ausgewählten Migration stools eines Drittanbieters. 2. Warten Sie, bis die Datenübertragungsa ufgabe abgeschlossen ist. Weitere Informati onen finden Sie unter AWS-Überwachung der DataSync AWS-Aktivitäten mit Amazon CloudWatc h und Überwachen Ihrer DataSync Aufgabe von der Befehlszeile aus.	Migrationsingenieur, Migration sleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Datenübertragung.	Wenn Sie AWS verwenden DataSync, gehen Sie wie folgt vor, um zu überprüfen, ob die endgültige Datenübertragung erfolgreich abgeschlossen wurde: 1. Notieren Sie sich in der DataSync AWS-Konsole die Aufgabe und die Ausführungs-ID, z. `task-0000-exec-1111` B. 2. Navigieren Sie zum Abschnitt „Aufgabenprotokollierung“ der DataSync Aufgabe. 3. Wählen Sie den Link zur CloudWatch Protokollgruppe. 4. Suchen Sie in den Protokollen nach der Task- und Ausführungs-ID. 5. Notieren Sie sich alle Übertragungsfehler. Weitere Informationen finden Sie in der DataSync Dokumentation unter Häufige Fehler. 6. Überprüfen Sie Folgendes: • Vergleichen Sie die Dateilisten von Quelle und Ziel, SFSs um sicherzustellen, dass alle Daten übertragen wurden	Migrationsingenieur, Migrationsleiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Vergleichen Sie die Dateizugriffsberec htigungen zwischen Quelle und Ziel SFSs. Wenn Sie ein Drittanbieter-Tool verwenden, lesen Sie die Anweisungen zur Validieru ng der Datenübertragung in der Dokumentation zum ausgewählten Migrationstool.	

Validieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Hängen Sie das Dateisystem erneut ein und überprüfen Sie die Funktion und Leistung der Anwendung.	1. Wenn abhängige Server in dieser Welle migriert wurden, geben Sie in der Datei SFS-Wave-Plan-Workbook im Arbeitsbl att Remount-Summary die neue IP-Adresse des Servers in die Spalte Neue Server-IP-Adresse (F) ein. 2. Aktualisieren Sie auf allen Servern den Bereitste llungspunkt für das Dateisystem vom alten Pfad auf den neuen Pfad. Verwenden Sie für die erneute Installation das Runbook Ihrer Organisat ion, das bereits in der	AWS-Systemadministrator, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Vorbereitungsphase beschrieben wurde. 3. Vergewissern Sie sich, dass das Dateisystem ordnungsgemäß gemountet ist und dass der Zugriff darauf möglich ist, indem Sie die Mounts überprüfen und überprüfen, ob Dateien vorhanden sind. In der Regel führt das Infrastrukturteam diese Aktivitäten durch. 4. Starten Sie die Anwendungen neu und beauftragen Sie die Anwendungseigentümer oder das QA-Team, die für die Anwendung erforderlichen Funktions- und Leistungstests durchzuführen.	

Fehlerbehebung

Problem	Lösung
Zellenwerte in Microsoft Excel werden nicht aktualisiert.	Kopieren Sie die Formeln in den Beispielzeilen, indem Sie das Ausfüllkästchen ziehen. Weitere Informationen finden Sie in den Anweisungen für Windows oder für Mac (Microsoft-Support-Website).

Zugehörige Ressourcen

AWS-Dokumentation

- DataSync AWS-Dokumentation
- Amazon EFS-Dokumentation
- FSx Amazon-Dokumentation
- Große Migrationen zur AWS-Cloud
  - Leitfaden für große AWS-Migrationen
  - Portfolio-Playbook für große AWS-Migrationen

Fehlersuche

- Behebung von DataSync AWS-Problemen
- Problembehandlung bei Amazon EFS
- Problembehebung bei Amazon FSx für Windows File Server
- Problembehebung bei Amazon FSx für NetApp ONTAP

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Migrieren Sie eine Oracle-Datenbank mithilfe von GoldenGate Oracle-Flatfile-Adaptern zu Amazon RDS for Oracle

Erstellt von Dhairya Jindani (AWS) und Baji Shaik (AWS)

Übersicht

Oracle GoldenGate ist ein Datenerfassungs- und Replikationsservice in Echtzeit für heterogene Datenbanken und IT-Umgebungen. Dieser Service unterstützt derzeit jedoch nicht Amazon Relational Database Service (Amazon RDS) für Oracle. Eine Liste der unterstützten Datenbanken finden Sie unter Oracle GoldenGate for Heterogeneous Databases (Oracle-Dokumentation). Dieses Muster beschreibt, wie Oracle GoldenGate - und GoldenGate Oracle-Flatfile-Adapter verwendet werden, um Flatfiles aus der Oracle-Quelldatenbank zu generieren, die sich lokal oder auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance befinden kann. Sie können diese Flatfiles dann in eine Amazon RDS for Oracle Oracle-Datenbank-Instance importieren.

In diesem Muster verwenden Sie Oracle, GoldenGate um die Traildateien aus Ihrer Oracle-Quelldatenbank zu extrahieren. Die Datenpumpe kopiert die Traildateien auf einen Integrationsserver, bei dem es sich um eine EC2 Amazon-Instance handelt. Auf dem Integrationsserver GoldenGate verwendet Oracle den Flatfile-Adapter, um eine Reihe sequentieller Flatfiles auf der Grundlage der transationalen Datenerfassung der Traildateien zu generieren. Oracle GoldenGate formatiert die Daten entweder als durch Trennzeichen getrennte Werte oder als durch Länge getrennte Werte. Anschließend verwenden Sie Oracle SQL*Loader, um die Flatfiles in die Amazon RDS for Oracle Oracle-Zieldatenbank-Instance zu importieren.

Beabsichtigte Zielgruppe

Dieses Muster richtet sich an Personen, die Erfahrung mit den grundlegenden Bausteinen eines GoldenGate Orakels haben und diese kennen. Weitere Informationen finden Sie unter Überblick über die GoldenGate Oracle-Architektur (Oracle-Dokumentation).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto.
- Eine GoldenGate Oracle-Lizenz.
- Eine separate Lizenz für einen GoldenGate Oracle-Adapter.

- Eine Oracle-Quelldatenbank, die entweder vor Ort oder auf einer EC2 Amazon-Instance ausgeführt wird.
- Eine Amazon EC2 Linux-Instance, die als Integrationsserver verwendet wird. Weitere Informationen finden Sie unter Erste Schritte mit Amazon EC2 Linux-Instances (EC2 Amazon-Dokumentation).
- Eine Ziel-Instance der Amazon RDS for Oracle Oracle-Datenbank. Weitere Informationen finden Sie unter Eine Oracle-DB-Instance erstellen (Amazon RDS-Dokumentation).

Produktversionen

- Oracle Database Enterprise Edition Version 10g, 11g, 12c oder höher
- Oracle GoldenGate Version 12.2.0.1.1 oder höher

Architektur

Quelltechnologie-Stack

Eine Oracle-Datenbank (vor Ort oder auf einer EC2 Amazon-Instance)

Zieltechnologie-Stack

Amazon RDS für Oracle

Quell- und Zielarchitektur

1. Oracle GoldenGate extrahiert Pfade aus den Quelldatenbank-Logs.
2. Die Datenpumpe extrahiert die Trails und migriert sie auf einen Integrationsserver.
3. Der GoldenGate Oracle-Flatfile-Adapter liest die Trails, Quelldefinitionen und Extraktparameter.
4. Sie beenden die Extraktion, wodurch eine Steuerdatei und Flat-Datendateien generiert werden.
5. Sie migrieren die Flat-Datendateien auf eine Amazon RDS for Oracle Oracle-Datenbank-Instance in der AWS Cloud.

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Relational Database Service (Amazon RDS) für Oracle unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Oracle-Datenbank in der. AWS Cloud

Andere Dienste

- Oracle GoldenGate ist ein Dienst, der Sie dabei unterstützt, Daten von einer Datenbank in eine andere heterogene Datenbank oder in eine andere Zieltopologie, wie z. B. Flatfiles, zu replizieren, zu filtern und zu transformieren.
- Mit GoldenGate Oracle-Anwendungsadaptern GoldenGate kann Oracle aus Transaktionsdaten, die in den Traildateien einer Quelldatenbank erfasst wurden, eine Reihe von sequentiellen Flatfiles und Kontrolldateien erstellen. Diese Adapter werden häufig für Extraktions-, Transformations- und Ladevorgänge (ETL) in Data Warehouse-Anwendungen und proprietären oder älteren Anwendungen verwendet. Oracle GoldenGate führt diese Erfassung durch und wendet sie nahezu in Echtzeit auf heterogene Datenbanken, Plattformen und Betriebssysteme an. Die Adapter unterstützen verschiedene Formate für die Ausgabedateien, wie CSV oder Apache Parquet. Sie können diese generierten Dateien laden, um die Daten in verschiedene heterogene Datenbanken zu laden.

Epen

Richten Sie Oracle GoldenGate auf dem Quelldatenbankserver ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie Oracle herunter GoldenGate.	Laden Sie auf dem Quelldatenbankserver die GoldenGate Oracle-Version 12.2.0.1.1 oder höher herunter. Anweisungen finden Sie unter Oracle herunterladen GoldenGate (Oracle-Dokumentation).	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Oracle GoldenGate.	Anweisungen finden Sie unter Oracle installieren GoldenGate (Oracle-Dokumentation).	DBA
Richten Sie Oracle GoldenGat e ein.	Anweisungen finden Sie unter Preparing the Database for Oracle GoldenGate (Oracle-D okumentation).	DBA

Richten Sie Oracle GoldenGate auf dem Integrationsserver ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie Oracle herunter GoldenGate.	Laden Sie auf dem Integrati onsserver die GoldenGate Oracle-Version 12.2.0.1.1 oder höher herunter. Anweisung en finden Sie unter Oracle herunterladen GoldenGate (Oracle-Dokumentation).	DBA
Installieren Sie Oracle GoldenGate.	Erstellen Sie Verzeichnisse, richten Sie den Manager-Prozess ein und erstellen Sie die `defgen` Datei für eine heterogene Umgebung. Anweisungen finden Sie unter Oracle installieren GoldenGate (Oracle-Dokumentation).	DBA

Ändern Sie die GoldenGate Oracle-Datenerfassungskonfiguration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie die GoldenGate Oracle-Adapter vor.	Richten Sie auf dem Integrationsserver die GoldenGate Oracle-Adaptersoftware ein. Gehen Sie wie folgt vor: 1. Laden Sie ggs_Adapters_Linux_x64.zip von der Oracle Software Delivery Cloud herunter. 2. Entpacken Sie die Datei ggs_Adapters_Linux_x64.zip. 3. Führen Sie den folgenden Befehl aus, um die Adapter zu installieren: `tar -xvf ggs_Adapters_Linux_x64.tar`	DBA
Konfigurieren Sie die Datenpumpe.	Konfigurieren Sie auf dem Quellserver die Datenpumpe so, dass sie die Traildatei vom Quellserver zum Integrationsserver überträgt. Erstellen Sie die Datenpumpen-Parameterdatei und das Trails-Datenverzeichnis. Anweisungen finden Sie unter Konfiguration des Flatfile-Adapters (Oracle-Dokumentation).	DBA

Generieren und migrieren Sie die Flatfiles

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie die Flatfiles.	Erstellen Sie die Extraktdatei und die Kontrolldatei und starten Sie dann den Extraktionsprozess auf dem Integrationsserver. Dadurch werden die Datenbankänderungen extrahiert und die Quelldatenbank in die Flatfiles geschrieben. Anweisungen finden Sie unter Using the Flat File Adapter (Oracle-Dokumentation).	DBA
Laden Sie die Flatfiles in die Zieldatenbank.	Laden Sie die Flatfiles in die Ziel-Instance der Amazon RDS for Oracle Oracle-Datenbank. Weitere Informationen finden Sie unter Import mit Oracle SQL*Loader (Amazon RDS-Dokumentation).	DBA

Fehlerbehebung

Problem	Lösung
Der GoldenGate Oracle-Flatfile-Adapter generiert einen Fehler.	Eine Beschreibung der Adapterfehler finden Sie unter Locating Error Messages (Oracle-Dokumentation). Anweisungen zur Problembehandlung finden Sie unter Troubleshooting the Flat File Adapter (Oracle-Dokumentation).

Zugehörige Ressourcen

- Oracle installieren GoldenGate (Oracle-Dokumentation)
- Oracle konfigurieren GoldenGate (Oracle-Dokumentation)
- Grundlegendes zu GoldenGate Oracle-Adaptern (Oracle-Dokumentation)
- Konfiguration des Flatfile-Adapters (Oracle-Dokumentation)

Ändern Sie Python- und Perl-Anwendungen, um die Datenbankmigration von Microsoft SQL Server zur Amazon Aurora PostgreSQL-Compatible Edition zu unterstützen

Erstellt von Dwarika Patra (AWS) und Deepesh Jayaprakash (AWS)

Übersicht

Dieses Muster beschreibt Änderungen an Anwendungs-Repositorys, die möglicherweise erforderlich sind, wenn Sie Datenbanken von Microsoft SQL Server zu Amazon Aurora PostgreSQL-Compatible Edition migrieren. Das Muster geht davon aus, dass diese Anwendungen auf Python oder Perl basieren, und enthält separate Anweisungen für diese Skriptsprachen.

Die Migration von SQL Server-Datenbanken zu Aurora PostgreSQL-kompatibel umfasst die Schemakonvertierung, die Konvertierung von Datenbankobjekten, die Datenmigration und das Laden von Daten. Aufgrund der Unterschiede zwischen PostgreSQL und SQL Server (in Bezug auf Datentypen, Verbindungsobjekte, Syntax und Logik) besteht die schwierigste Migrationsaufgabe darin, die erforderlichen Änderungen an der Codebasis vorzunehmen, damit sie ordnungsgemäß mit PostgreSQL funktioniert.

Bei einer Python-basierten Anwendung sind Verbindungsobjekte und Klassen im gesamten System verstreut. Außerdem verwendet die Python-Codebasis möglicherweise mehrere Bibliotheken, um eine Verbindung zur Datenbank herzustellen. Wenn sich die Datenbankverbindungsschnittstelle ändert, müssen auch die Objekte, die die Inline-Abfragen der Anwendung ausführen, geändert werden.

Bei einer Perl-basierten Anwendung betreffen die Änderungen Verbindungsobjekte, Datenbankverbindungstreiber, statische und dynamische Inline-SQL-Anweisungen und die Art und Weise, wie die Anwendung komplexe dynamische DML-Abfragen und Ergebnismengen verarbeitet.

Wenn Sie Ihre Anwendung migrieren, können Sie auch mögliche Verbesserungen auf AWS in Betracht ziehen, z. B. den FTP-Server durch Amazon Simple Storage Service (Amazon S3) -Zugriff zu ersetzen.

Der Prozess der Anwendungsmigration beinhaltet die folgenden Herausforderungen:

- Verbindungsobjekte. Wenn Verbindungsobjekte im Code mit mehreren Bibliotheken und Funktionsaufrufen verstreut sind, müssen Sie möglicherweise einen generalisierten Weg finden, sie so zu ändern, dass sie PostgreSQL unterstützen.
- Fehler- oder Ausnahmebehandlung beim Abrufen oder bei Aktualisierungen von Datensätzen. Wenn Sie in der Datenbank bedingte Erstellungs-, Lese-, Aktualisierungs- und Löschvorgänge

(CRUD) ausführen, die Variablen, Ergebnissätze oder Datenrahmen zurückgeben, können Fehler oder Ausnahmen zu Anwendungsfehlern mit kaskadierenden Effekten führen. Diese sollten sorgfältig behandelt und mit geeigneten Validierungen und Speicherpunkten versehen werden. Ein solcher Speicherpunkt ist das Aufrufen großer Inline-SQL-Abfragen oder Datenbankobjekte innerhalb `BEGIN...EXCEPTION...END` von Blöcken.

- Steuerung von Transaktionen und deren Validierung. Dazu gehören manuelle und automatische Commits und Rollbacks. Der PostgreSQL-Treiber für Perl verlangt, dass Sie das Auto-Commit-Attribut immer explizit setzen.
- Umgang mit dynamischen SQL-Abfragen. Dies erfordert ein fundiertes Verständnis der Abfragelogik und iterative Tests, um sicherzustellen, dass Abfragen wie erwartet funktionieren.
- Leistung. Sie sollten sicherstellen, dass Codeänderungen nicht zu einer Beeinträchtigung der Anwendungsleistung führen.

Dieses Muster erklärt den Konvertierungsprozess im Detail.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Grundkenntnisse der Python- und Perl-Syntax.
- Grundkenntnisse in SQL Server und PostgreSQL.
- Verständnis Ihrer bestehenden Anwendungsarchitektur.
- Zugriff auf Ihren Anwendungscode, Ihre SQL Server-Datenbank und Ihre PostgreSQL-Datenbank.
- Zugriff auf die Windows- oder Linux-Entwicklungsumgebung (oder eine andere Unix-) Entwicklungsumgebung mit Anmeldeinformationen zum Entwickeln, Testen und Validieren von Anwendungsänderungen.
- Für eine Python-basierte Anwendung Standard-Python-Bibliotheken, die Ihre Anwendung möglicherweise benötigt, wie Pandas zur Verarbeitung von Datenframes und psycopg2 oder für Datenbankverbindungen. SQLAlchemy
- Für eine Perl-basierte Anwendung sind Perl-Pakete mit abhängigen Bibliotheken oder Modulen erforderlich. Das Modul Comprehensive Perl Archive Network (CPAN) kann die meisten Anwendungsanforderungen unterstützen.
- Alle erforderlichen abhängigen benutzerdefinierten Bibliotheken oder Module.
- Datenbankanmeldedaten für den Lesezugriff auf SQL Server und Lese-/Schreibzugriff auf Aurora.

- PostgreSQL zum Validieren und Debuggen von Anwendungsänderungen mit Diensten und Benutzern.
- Zugriff auf Entwicklungstools während der Anwendungsmigration wie Visual Studio Code, Sublime Text oder pgAdmin.

Einschränkungen

- Einige Python- oder Perl-Versionen, Module, Bibliotheken und Pakete sind nicht mit der Cloud-Umgebung kompatibel.
- Einige Bibliotheken und Frameworks von Drittanbietern, die für SQL Server verwendet werden, können nicht ersetzt werden, um die PostgreSQL-Migration zu unterstützen.
- Leistungsschwankungen erfordern möglicherweise Änderungen an Ihrer Anwendung, an Inline-Transact-SQL (T-SQL) -Abfragen, Datenbankfunktionen und gespeicherten Prozeduren.
- PostgreSQL unterstützt Kleinbuchstaben für Tabellennamen, Spaltennamen und andere Datenbankobjekte.
- Einige Datentypen, wie z. B. UUID-Spalten, werden nur in Kleinbuchstaben gespeichert. Python- und Perl-Anwendungen müssen mit solchen Fallunterschieden umgehen.
- Unterschiede in der Zeichenkodierung müssen mit dem richtigen Datentyp für die entsprechenden Textspalten in der PostgreSQL-Datenbank behandelt werden.

Produktversionen

- Python 3.6 oder höher (verwenden Sie die Version, die Ihr Betriebssystem unterstützt)
- Perl 5.8.3 oder höher (verwenden Sie die Version, die Ihr Betriebssystem unterstützt)
- Aurora PostgreSQL-kompatible Edition 4.2 oder höher (siehe Details)

Architektur

Quelltechnologie-Stack

- Skriptsprache (Anwendungsprogrammiersprache): Python 2.7 oder höher oder Perl 5.8
- Datenbank: Microsoft SQL Server Version 13
- Betriebssystem: Red Hat Enterprise Linux (RHEL) 7

Zieltechnologie-Stack

- Skriptsprache (Anwendungsprogrammiersprache): Python 3.6 oder höher oder Perl 5.8 oder höher
- Datenbank: Aurora PostgreSQL-kompatibel 4.2
- Betriebssystem: RHEL 7

Migrationsarchitektur

Tools

AWS-Services und -Tools

- Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, PostgreSQL-kompatible und ACID-konforme relationale Datenbank-Engine, die die Geschwindigkeit und Zuverlässigkeit kommerzieller High-End-Datenbanken mit der Wirtschaftlichkeit von Open-Source-Datenbanken kombiniert. Aurora PostgreSQL ist ein direkter Ersatz für PostgreSQL und macht es einfacher und kostengünstiger, Ihre neuen und bestehenden PostgreSQL-Implementierungen einzurichten, zu betreiben und zu skalieren.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

Andere Tools

- Python - und PostgresSQL-Datenbankverbindungsbibliotheken wie psycopg2 und SQLAlchemy
- Perl und seine DBI-Module
- Interaktives PostgreSQL-Terminal (psql)

Epen

Migrieren Sie Ihr Anwendungs-Repository zu PostgreSQL — grundlegende Schritte

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Folgen Sie diesen Schritten zur Codekonvertierung, um Ihre Anwendung zu PostgreSQL zu migrieren.	1. Legen Sie datenbank spezifische ODBC-Trei ber und -Bibliotheken für PostgreSQL fest. Sie	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	können beispielsweise eines der CPAN-Module für Perl und pyodbc, psycopg2 oder für Python verwenden. SQLAlchemy 2. Konvertieren Sie Datenbank objekte mithilfe dieser Bibliotheken, um eine Verbindung zu Aurora PostgreSQL-Compatible herzustellen. 3. Wenden Sie Codeänder ungen in vorhandenen Anwendungsmodulen an, um kompatible T-SQL-Anw eisungen zu erhalten. 4. Schreiben Sie datenbank spezifische Funktions aufrufen und gespeicherte Prozeduren im Anwendung scode neu. 5. Behandeln Sie Änderunge n an den Variablen Ihrer Anwendung und ihren Datentypen, die für Inline-SQL-Abfragen verwendet werden. 6. Behandeln Sie inkompati ble datenbankspezifische Funktionen. 7. Vollständige end-to-end Prüfung des konvertierten Anwendungscodes für die Datenbankmigration.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Vergleichen Sie die Ergebnisse von Microsoft SQL Server mit der Anwendung, die Sie zu PostgreSQL migriert haben. 9. Führen Sie ein Benchmarking der Anwendungsleistung zwischen Microsoft SQL Server und PostgreSQL durch. 10. Überarbeiten Sie gespeicherte Prozeduren oder Inline-T-SQL-Anweisungen, die von der Anwendung aufgerufen werden, um die Leistung zu verbessern. Die folgenden Epics enthalten detaillierte Anweisungen für einige dieser Konvertierungsaufgaben für Python- und Perl-Anwendungen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie für jeden Schritt der Migration eine Checkliste.	Fügen Sie Ihrer Checkliste für jeden Schritt der Anwendung smigration, einschließlich des letzten Schritts, Folgendes hinzu: • Lesen Sie die PostgreSQ L-Dokumentation, um sicherzustellen, dass alle Ihre Änderungen mit dem PostgreSQL-Standard kompatibel sind. • Suchen Sie nach Integer- und Gleitkommawerten für Spalten. • Identifizieren Sie die Anzahl der eingefügten, aktualisi erten und extrahierten Zeilen sowie die Spaltenna men und Datums-/Z eitstempel. Sie können ein Diff-Hilfsprogramm verwenden oder ein Skript schreiben, um diese Prüfungen zu automatis ieren. • Führen Sie Leistungs prüfungen für große Inline-SQL-Anweisungen durch und überprüfen Sie die Gesamtleistung der Anwendung. • Überprüfen Sie die korrekte Fehlerbehandlung bei	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Datenbankoperationen und das ordnungsgemäße Beenden des Programms, indem Sie mehrere Try/Catch-Blöcke verwenden. • Stellen Sie sicher, dass die richtigen Protokollierungsprozesse vorhanden sind.	

Analysieren und aktualisieren Sie Ihre Anwendung — Python-Codebasis

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie Ihre bestehende Python-Codebasis.	Ihre Analyse sollte Folgendes beinhalten, um den Migrationsprozess der Anwendung zu erleichtern: • Identifizieren Sie alle Verbindungsobjekte im Code. • Identifizieren Sie alle inkompatiblen Inline-SQL-Abfragen (wie T-SQL-Anweisungen und gespeicherte Prozeduren) und analysieren Sie die erforderlichen Änderungen. • Lesen Sie die Dokumentation zu Ihrem Code und verfolgen Sie den Kontrollablauf, um die Codefunktionalität zu verstehen. Dies ist später hilfreich, wenn	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie die Anwendung auf Leistungs- oder Lastvergl eiche testen. • Machen Sie sich mit dem Zweck der Anwendung vertraut, damit Sie sie nach der Datenbankkonvertie rung effektiv testen können. Die meisten Python-Anwendungen, die für eine Konvertierung mit Datenbankmigrationen in Frage kommen, sind entweder Feeds, die Daten aus anderen Quellen in Datenbanktabellen laden, oder Extraktoren, die Daten aus den Tabellen abrufen und sie in verschiedene Ausgabeformate (wie CSV, JSON oder Flatfiles) umwandeln, die sich für die Erstellung von Berichten oder für API-Aufrufe zur Durchführung von Validieru ngen eignen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konvertieren Sie Ihre Datenbankverbindungen zur Unterstützung von PostgreSQL.	Die meisten Python-Anwendungen verwenden die pyodbc-Bibliothek, um wie folgt eine Verbindung mit SQL Server-Datenbanken herzustellen.
	
	`import pyodbc`
	`....`
	`try:`
	`conn_string = "Driver=ODBC Driver 17 for SQL Server;UID={};PWD={};Server={};Database={}".format (conn_user, conn_password, conn_server, conn_database)`
	`conn = pyodbc.connect(conn_string)`
	`cur = conn.cursor()`
	`result = cur.execute(query_string)`
	`for row in result:`
	`print (row)`
	`except Exception as e:`
	`print(str(e))`
	
	Konvertieren Sie die Datenbankverbindung wie folgt zur Unterstützung von PostgreSQL.
	
	`import pyodbc`
	`import psycopg2`
	`....`
	`try:`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> conn_string =
	 'postgresql+psycop
	g2://'+
	    conn_user+':'+conn
	_password+'@'+conn
	_server+'/'+conn_d
	atabase
	    conn = pyodbc.co
	nnect(conn_string,
	 connect_args={'opt
	ions':'-csearch_pa
	th=dbo'})
	    cur = conn.cursor()
	    result = cur.execu
	te(query_string)
	    for row in result:
	    print (row)
	except Exception as e:
	    print(str(e))</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie Inline-SQL-Abfragen in PostgreSQL.	Konvertieren Sie Ihre Inline-SQL-Abfragen in ein PostgreSQL-kompatibles Format. Die folgende SQL Server-Abfrage ruft beispiels weise eine Zeichenfolge aus einer Tabelle ab. `dtype = “type1” stm = ‘“SELECT TOP 1 searchcode FROM TypesTable (NOLOCK) WHERE code=”’ + “’” + str(dtype) + “’” # For Microsoft SQL Server Database Connection engine = create_en gine(‘mssql+pyodbc :///?odbc_connect=%s’ % urllib.parse.quote _plus(conn_string) , connect_args={‘con nect_timeout’:logi n_timeout}) conn = engine_connect() rs = conn.execute(stm) for row in rs: print(row)`  Nach der Konvertierung sieht die PostgreSQL-kompatible Inline-SQL-Abfrage wie folgt aus.  `dtype = “type1”`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`stm = '"SELECT searchcode FROM TypesTable WHERE code="' + "'" + str(dtype) + "' LIMIT 1"`
	`# For PostgreSQL Database Connection`
	`engine = create_engine('postgres+psycopg2://%s' %conn_string, connect_args={'connect_timeout':login_timeout})`
	`conn = engine.connect()`
	`rs = conn.execute(stm)`
	`for row in rs:`
	`  print(row)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Verarbeitet dynamische SQL-Abfragen.	Dynamisches SQL kann in einem Skript oder in mehreren Python-Skripten vorhanden sein. Frühere Beispiele zeigten, wie die Zeichenke ttenersetzungsfunktion von Python verwendet werden kann, um Variablen für die Erstellung dynamischer SQL-Abfragen einzufügen. Ein alternativer Ansatz besteht darin, die Abfragezeichenfolge gegebenenfalls mit Variablen anzuhängen.
	
	Im folgenden Beispiel wird die Abfragezeichenfolge spontan auf der Grundlage der von einer Funktion zurückgeg ebenen Werte erstellt.
	
	`query = '"SELECT id from equity e join issues i on e.permId=i.permId where e.id'"`
	`query += get_id_filter(ids) + " e.id is NOT NULL`
	
	Diese Arten von dynamisch en Abfragen sind bei der Anwendungsmigration sehr verbreitet. Gehen Sie wie folgt vor, um dynamische Abfragen zu verarbeiten:
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Überprüfen Sie die allgemeine Syntax (z. B. die Syntax für die `SELECT` Anweisung mit einer `JOIN` Klausel). • Überprüfen Sie alle in der Abfrage verwendeten Variablen oder Spaltennamen, z. B. `i` und`id`. • Überprüfen Sie die in der Abfrage verwendeten Funktionen, Argumente und Rückgabewerte (z. B. `get_id_filter` und ihr Argument`ids`).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Behandelt Ergebnismengen, Variablen und Datenrahmen.	Für Microsoft SQL Server verwenden Sie Python-Methoden wie `fetchone()` oder`fetchall()` , um den Ergebnissatz aus der Datenbank abzurufen. Sie können auch die Anzahl der Datensätze verwenden `fetchmany(size)` und angeben, die aus dem Ergebnissatz zurückgegeben werden sollen. Dazu können Sie das Verbindungsobjekt pyodbc verwenden, wie im folgenden Beispiel gezeigt. pyodbc (Microsoft SQL Server) `import pyodbc server = 'tcp:myserver.database.windows.net' database = 'exampledb' username = 'exampleusername' password = 'examplepassword' conn = pyodbc.connect('DRIVER={ODBC Driver 17 for SQL Server};SERVER='+server+';DATABASE='+database+';UID='+username+';PWD='+ password) cursor = conn.cursor()`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`cursor.execute("SELECT * FROM ITEMS")`
	`row = cursor.fetchone()`
	`while row:`
	`  print(row[0])`
	`  row = cursor.fetchone()`	

	Um in Aurora ähnliche Aufgaben wie das Herstellen einer Verbindung zu PostgreSQL und das Abrufen von Ergebnismengen auszuführen, können Sie entweder psycopg2 oder verwenden. SQLAlchemy Diese Python-Bibliotheken stellen das Verbindungsmodul und das Cursorobjekt bereit, um die PostgreSQL-Datenbankeinträge zu durchsuchen, wie im folgenden Beispiel gezeigt.
	
	psycopg2 (Aurora PostgreSQL-kompatibel)
	
	`import psycopg2`
	`query = "SELECT * FROM ITEMS;"`
	`//Initialize variables`
	`host=dbname=user=password=port=sslmode=connect_timeout=""`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`connstring = "host='{host}' dbname='{dbname}' user='{user}' \ password='{password}'port='{port}' ".format(host=host,dbname=dbname,\ user=user,password=password,port=port) conn = psycopg2.connect(connstring) cursor = conn.cursor() cursor.execute(query) column_names = [column[0] for column in cursor.description] print("Column Names: ", column_names) print("Column values: " for row in cursor: print("itemid :", row[0]) print("itemdescrption :", row[1]) print("itemprice :", row[3]))`  SQLAlchemy (Aurora PostgreSQL-kompatibel)  `from sqlalchemy import create_engine from pandas import DataFrame conn_string = 'postgresql://core:database@localhost:5432/exampledatabase'`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`engine = create_engine(conn_string)`
	`conn = engine.connect()`
	`dataid = 1001`
	`result = conn.execute("SELECT * FROM ITEMS")`
	`df = DataFrame(result.fetchall())`
	`df.columns = result.keys()`
	`df = pd.DataFrame()`
	`engine.connect()`
	`df = pd.read_sql_query(sql_query, engine, coerce_float=False)`
	`print(“df=”, df)`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie Ihre Anwendung während und nach der Migration.	Das Testen der migrierten Python-Anwendung ist ein fortlaufender Prozess. Da die Migration Änderunge n an Verbindungsobjekten (psycopg2 oder SQLAlchem y), Fehlerbehandlung, neue Funktionen (Datenrahmen), Inline-SQL-Änderungen, Funktionen zum Massenkop ieren (`bcpstattC0PY`) und ähnliche Änderungen umfasst, muss sie während und nach der Anwendungsmigration sorgfältig getestet werden. Suchen Sie nach: • Bedingungen und Behandlung von Fehlern • Alle Datensätze stimmen nach der Migration nicht überein • Aktualisierungen oder Löschungen von Datensätz en • Zeit, die für die Ausführun g der Anwendung benötigt wird	App-Developer

Analysieren und aktualisieren Sie Ihre Anwendung — Perl-Codebasis

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie Ihre bestehende Perl-Codebasis.	Ihre Analyse sollte Folgendes beinhalten, um den Anwendungsmigratio nsprozess zu erleichtern. Sie sollten Folgendes identifiz ieren: • Beliebiger INI- oder konfigurationsbasierter Code • Datenbankspezifische Standard-Perl-Treiber für Open Database Connectiv ity (ODBC) oder beliebige benutzerdefinierte Treiber • Für Inline- und T-SQL-Abf ragen sind Codeänderungen erforderlich • Interaktionen zwischen verschiedenen Perl-Modu len (z. B. ein einzelnes Perl-ODBC-Verbindungsobjekt, das von mehreren Funktions komponenten aufgerufen oder von diesen verwendet wird) • Umgang mit Datensätzen und Ergebnismengen • Externe, abhängige Perl-Bibliotheken	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Alle APIs , die in der Anwendung verwendet werden • Perl-Versionskompatibilität und Treiberkompatibilität mit Aurora PostgreSQL-kompatibel	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konvertiert die Verbindungen aus der Perl-Anwendung und dem DBI-Modul zur Unterstützung von PostgreSQL.	Perl-basierte Anwendungen verwenden im Allgemeinen das Perl-DBI-Modul, ein Standard-Datenbankzugriffsmodul für die Programmiersprache Perl. Sie können dasselbe DBI-Modul mit unterschiedlichen Treibern für SQL Server und PostgreSQL verwenden.
	
	Weitere Informationen zu den erforderlichen Perl-Modulen, Installationen und anderen Anweisungen finden Sie in der DBD: :Pg-Dokumentation. Das folgende Beispiel stellt eine Verbindung zu Aurora PostgreSQL-Compatible unter her. `exampletest-aurorapg-database.cluster-sampleclusture.us-east-.rds.amazonaws.com`
	
	`#!/usr/bin/perl`
	`use DBI;`
	`use strict;`
	`my $driver = "Pg";`
	`my $hostname = “examplet`
	`est-aurorapg-datab`
	`ase-sampleclusture`
	`.us-east.rds.amazo`
	`naws.com”`
	`my $dsn = "DBI:$driver:`
	` dbname = $hostname`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	;host = 127.0.0.1;port = 5432"; my $username = "postgres"; my $password = "pass123"; $dbh = DBI->connect("dbi:Pg:dbname=$hostname;host=$host;port=$port;options=$options", $username, $password, {AutoCommit => 0, RaiseError => 1, PrintError => 0});	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie Inline-SQL-Abfragen in PostgreSQL.	Ihre Anwendung verfügt möglicherweise über Inline-SQL-Abfragen mit`SELECT`, `DELETE``UPDATE`, und ähnlichen Anweisungen, die Abfrageklauseln enthalten, die PostgreSQL nicht unterstützt. Beispielsweise werden Abfrageschlüsselwörter wie `TOP` und in PostgreSQL `NOLOCK` nicht unterstützt. Die folgenden Beispiele zeigen, wie Sie mit`TOP`, und boolesche n `NOLOCK` Variablen umgehen können.  In SQL Server:  `$sqlStr = $sqlStr . "WHERE a.student _id in (SELECT TOP $numofRecords c_student_id \ FROM active_student_rec ord b WITH (NOLOCK) \ INNER JOIN student_c ontributor c WITH (NOLOCK) on c.contrib utor_id = b.c_st)`  Für PostgreSQL konvertieren Sie in:  `$sqlStr = $sqlStr . "WHERE a.student _id in (SELECT`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	TOP $numofRecords c_student_id \ FROM active_student_rec ord b INNER JOIN student_contributor c \ on c.contributor_id = b.c_student_contr_id WHERE b_current_1 is true \ LIMIT $numofRecords)"	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verarbeitet dynamische SQL-Abfragen und Perl-Variablen.	Dynamische SQL-Abfragen sind SQL-Anweisungen, die zur Laufzeit der Anwendung erstellt werden. Diese Abfragen werden je nach bestimmten Bedingungen dynamisch erstellt, wenn die Anwendung ausgeführt wird, sodass der vollständige Text der Abfrage erst zur Laufzeit bekannt ist. Ein Beispiel ist eine Finanzanalyseanwendung, die täglich die zehn wichtigsten Aktien analysiert, und diese Aktien ändern sich täglich. Die SQL-Tabellen werden auf der Grundlage von Top-Performern erstellt, und die Werte sind erst zur Laufzeit bekannt. Nehmen wir an, dass die Inline-SQL-Abfragen für dieses Beispiel an eine Wrapper-Funktion übergeben werden, um die Ergebnisse in einer Variablen zu erhalten, und dann verwendet eine Variable eine Bedingung, um zu bestimmen, ob die Tabelle existiert: • Wenn die Tabelle existiert, erstellen Sie sie nicht,	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	sondern führen Sie einige Bearbeitungen durch.
	• Wenn die Tabelle nicht existiert, erstellen Sie die Tabelle und führen Sie auch einige Bearbeitungen durch.
	
	Hier ist ein Beispiel für die Variablenbehandlung, gefolgt von den SQL Server- und PostgreSQL-Abfragen für diesen Anwendungsfall.
	
	`my $tableexists = db_read( arg 1, $sql_qry, undef, 'writer'); my $table_already_exists = $tableexists->[0]{table_exists}; if ($table_already_exists){ # do some thing } else { # do something else }`
	
	SQL Server:
	
	`my $sql_qry = “SELECT OBJECT_ID('$backendTable', 'U') table_exists", undef, 'writer') ";`
	
	PostgreSQL:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`my $sql_qry = “SELECT TO_REGCLASS('$backendTable', 'U') table_exists", undef, 'writer')";`
	
	Im folgenden Beispiel wird eine Perl-Variable in Inline-SQL verwendet, die eine `SELECT` Anweisung mit a ausführt, `JOIN` um den Primärschlüssel der Tabelle und die Position der Schlüsselspalte abzurufen.
	
	SQL Server:
	
	`my $sql_qry = "SELECT column_name', character_maximum_length \ FROM INFORMATION_SCHEMA.COLUMNS \ WHERE TABLE_SCHEMA='$example_scheme maInfo' \ AND TABLE_NAME='$example_table' \ AND DATA_TYPE IN ('varchar','nvarchar');";`
	
	PostgreSQL:
	
	`my $sql_qry = "SELECT c1.column_name, c1.ordinal_position \ FROM information_schema.key_column_usage AS c LEFT \`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`JOIN information_schema .table_constraints AS t1 \ ON t1.constraint_name = c1.constraint_name \ WHERE t1.table_name = $example_schemaInf o'.'$example_table' \ AND t1.constraint_type = 'PRIMARY KEY' ;";`	

Nehmen Sie zusätzliche Änderungen an Ihrer Perl- oder Python-basierten Anwendung vor, um PostgreSQL zu unterstützen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konvertiert zusätzliche SQL Server-Konstrukte nach PostgreSQL.	Die folgenden Änderungen gelten für alle Anwendungen, unabhängig von der Programmiersprache. • Qualifizieren Sie Datenbankobjekte, die Ihre Anwendung verwendet, mit neuen und geeigneten Schemanamen. • Behandeln Sie LIKE-Operatoren für den Abgleich unter Berücksichtigung der Groß- und Kleinschreibung mit der Kollationsfunktion in PostgreSQL. • Behandelt nicht unterstützte datenbankspezifische Funktionen wie`DATEDIFF`,,`DATEADD`,	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`GETDATE` und Operatoren. `CONVERT` `CAST` Entsprechende PostgreSQL-kompatible Funktionen finden Sie unter Systemeigene oder integrierte SQL-Funktionen im Abschnitt Zusätzliche Informationen. • Behandeln Sie boolesche Werte in Vergleichsanweisungen. • Behandelt Rückgabewerte von Funktionen. Dies können Datensätze, Datenrahmen, Variablen und boolesche Werte sein. Behandeln Sie diese entsprechend den Anforderungen Ihrer Anwendung und zur Unterstützung von PostgreSQL. • Behandeln Sie anonyme Blöcke (z. B.`BEGIN TRAN`) mit neuen, benutzerdefinierten PostgreSQL-Funktionen. • Konvertiert Masseneinfügungen für Zeilen. Das PostgreSQL-Äquivalent des SQL Server-Dienstprogramms bulk copy (`bcp`), das aus der Anwendung heraus aufgerufen wird, ist. `COPY`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Konvertiert Operatoren zur Spaltenverkettung. SQL Server verwendet + für die Verkettung von Zeichenfolgen, PostgreSQL verwendet sie jedoch. | |	

Verbessern Sie die Leistung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Nutzen Sie die AWS-Services, um die Leistung zu verbesser n.	Wenn Sie zur AWS-Cloud migrieren, können Sie Ihr Anwendungs- und Datenbank design verfeinern, um die Vorteile der AWS-Services zu nutzen. Wenn beispiels weise die Abfragen Ihrer Python-Anwendung, die mit einem Aurora PostgreSQ L-kompatiblen Datenbank server verbunden ist, mehr Zeit in Anspruch nehmen als Ihre ursprünglichen Microsoft SQL Server-Ab fragen, könnten Sie erwägen, einen Feed mit historischen Daten direkt vom Aurora-Se rver in einen Amazon Simple Storage Service (Amazon S3) -Bucket zu erstellen und Amazon Athena-basierte SQL-Abfragen zu verwenden , um Berichte und analytisc	App-Entwickler, Cloud-Arc hitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	he Datenabfragen für Ihre Benutzer-Dashboards zu generieren.	

Zugehörige Ressourcen

- Perl
- Perl DBI-Modul
- Python
- psycopg2
- SQLAlchemy
- Massenkopie - PostgreSQL
- Massenkopie — Microsoft SQL Server
- PostgreSQL
- Arbeiten mit Amazon Aurora PostgreSQL

Zusätzliche Informationen

Sowohl Microsoft SQL Server als auch Aurora PostgreSQL-kompatibel sind ANSI SQL-kompatibel. Sie sollten sich jedoch dennoch aller Inkompatibilitäten in Bezug auf Syntax, Spaltendatentypen, systemeigene datenbankspezifische Funktionen, Masseneinfügungen und Berücksichtigung der Groß- und Kleinschreibung bewusst sein, wenn Sie Ihre Python- oder Perl-Anwendung von SQL Server zu PostgreSQL migrieren.

In den folgenden Abschnitten finden Sie weitere Informationen zu möglichen Inkonsistenzen.

Vergleich der Datentypen

Datentypänderungen von SQL Server zu PostgreSQL können zu erheblichen Unterschieden in den resultierenden Daten führen, mit denen Anwendungen arbeiten. Einen Vergleich der Datentypen finden Sie in der Tabelle auf der Sqlines-Website.

Systemeigene oder integrierte SQL-Funktionen

Das Verhalten einiger Funktionen unterscheidet sich zwischen SQL Server- und PostgreSQL-Datenbanken. Die folgende Tabelle bietet einen Vergleich.

Microsoft SQL Server	Beschreibung	PostgreSQL
`CAST`	Konvertiert einen Wert von einem Datentyp in einen anderen.	PostgreSQL `type ::` `operator`
`GETDATE()`	Gibt Datum und Uhrzeit des aktuellen Datenbanksystems in einem `YYYY-MM-DD` `hh:mm:ss.mmm` Format zurück.	`CLOCK_TIMESTAMP`
`DATEADD`	Fügt einem Datum ein Zeit-/Datumsintervall hinzu.	`INTERVAL`Ausdruck
`CONVERT`	Konvertiert einen Wert in ein bestimmtes Datenformat.	`TO_CHAR`
`DATEDIFF`	Gibt die Differenz zwischen zwei Daten zurück.	`DATE_PART`
`TOP`	Beschränkt die Anzahl der Zeilen in einem `SELECT` Ergebnissatz.	`LIMIT/FETCH`

Anonyme Blöcke

Eine strukturierte SQL-Abfrage ist in Abschnitte wie Deklaration, ausführbare Dateien und Ausnahmebehandlung unterteilt. In der folgenden Tabelle werden die Microsoft SQL Server- und PostgreSQL-Versionen eines einfachen anonymen Blocks verglichen. Für komplexe anonyme Blöcke empfehlen wir, dass Sie eine benutzerdefinierte Datenbankfunktion in Ihrer Anwendung aufrufen.

Microsoft SQL Server

```
my $sql_qry1=
```

PostgreSQL

```
my $sql_qry1=
```

```
my $sql_qry2 =
my $sqlqry = "BEGIN TRAN
$sql_qry1 $sql_qry2
if @\@error !=0 ROLLBACK
TRAN
else COMIT TRAN";
```

```
my $sql_qry2 =
my $sql_qry = " DO \$\$
BEGIN
$header_sql $content_sql
END
\$\$";
```

Andere Unterschiede

- Masseneinfügungen von Zeilen: Das PostgreSQL-Äquivalent des Microsoft SQL Server-Dienstprogramms BCP ist COPY.
- Berücksichtigung von Groß- und Kleinschreibung: Bei Spaltennamen wird in PostgreSQL zwischen Groß- und Kleinschreibung unterschieden, sodass Sie Ihre SQL Server-Spaltennamen in Klein- oder Großbuchstaben konvertieren müssen. Dies wird zu einem Faktor, wenn Sie Daten extrahieren oder vergleichen oder Spaltennamen in Ergebnismengen oder Variablen platzieren. Das folgende Beispiel identifiziert Spalten, in denen Werte in Groß- oder Kleinbuchstaben gespeichert werden könnten.

```
my $sql_qry = "SELECT $record_id FROM $exampleTable WHERE LOWER($record_name) =
 \'failed transaction\'";
```

- Verkettung: SQL Server verwendet + als Operator für die Verkettung von Zeichenketten, während PostgreSQL dies verwendet. | |
- Validierung: Sie sollten Inline-SQL-Abfragen und -Funktionen testen und validieren, bevor Sie sie im Anwendungscode für PostgreSQL verwenden.
- Inklusion der ORM-Bibliothek: Sie können auch danach suchen, eine bestehende Datenbankverbindungsbibliothek durch Python-ORM-Bibliotheken wie SQLAlchemyPynomoDB einzubeziehen oder zu ersetzen. Dies wird dazu beitragen, Daten aus einer Datenbank mithilfe eines objektorientierten Paradigmas einfach abzufragen und zu bearbeiten.

Streamen Sie Daten von IBM Db2, SAP, Sybase und anderen Datenbanken nach MongoDB Atlas auf AWS

Erstellt von Battulga Purevragchaa (AWS), Babu Srinivasan (MongoDB) und Igor Alekseev (AWS)

Übersicht

Dieses Muster beschreibt die Schritte zur Migration von Daten aus IBM Db2 und anderen Datenbanken wie Mainframe-Datenbanken und Sybase zu MongoDB Atlas auf dem. AWS Cloud Es hilft AWS Glue, die Datenmigration zu MongoDB Atlas zu beschleunigen.

Das Muster ist Teil des Leitfadens Migration zu MongoDB Atlas AWS auf der AWS Prescriptive Guidance-Website. Es enthält die Implementierungsschritte für eines der Migrationsszenarien, die in diesem Leitfaden erörtert werden. Weitere Migrationsszenarien finden Sie in den folgenden Mustern auf der AWS Prescriptive Guidance-Website:

- Migrieren Sie eine selbst gehostete MongoDB-Umgebung zu MongoDB Atlas am AWS
- Migrieren Sie relationale Datenbanken zu MongoDB Atlas auf AWS

Das Muster ist für AWS Managed Services Services-Partner und AWS Benutzer vorgesehen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Quelldatenbank wie SAP, Sybase, IBM Db2 und andere für die Migration zu MongoDB Atlas.
- Vertrautheit mit Datenbanken wie SAP, Sybase, IBM Db2, MongoDB Atlas und. AWS-Services

Produktversionen

- MongoDB Version 5.0 oder höher.

Architektur

Das folgende Diagramm veranschaulicht das Laden und Streamen von Batch-Daten mithilfe AWS Glue Studio von Amazon Kinesis Data Streams und MongoDB Atlas.

Diese Referenzarchitektur verwendet, AWS Glue Studio um ETL-Pipelines (Extrahieren, Transformieren und Laden) zu erstellen, um Daten zu MongoDB Atlas zu migrieren. An AWS-Glue-

Crawler lässt sich in MongoDB Atlas integrieren, um die Datenverwaltung zu erleichtern. Die Daten können entweder im Batch portiert oder mithilfe von Amazon Kinesis Data Streams nach MongoDB Atlas gestreamt werden.

Batch-Daten laden

Weitere Informationen zur Batch-Datenmigration finden Sie im AWS Blogbeitrag Compose your ETL jobs for MongoDB Atlas with AWS Glue.

Datenstreaming

Informationen zu MongoDB Atlas-Referenzarchitekturen, die verschiedene Nutzungsszenarien unterstützen, finden Sie unter Migration zu MongoDB Atlas AWS auf der AWS Prescriptive Guidance-Website.

Tools

- AWS Glueist ein vollständig verwalteter ETL-Service. Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben.
- Amazon Kinesis Data Streams hilft Ihnen dabei, große Datenströme in Echtzeit zu sammeln und zu verarbeiten.
- MongoDB Atlas ist ein vollständig verwalteter Database-as-a-Service (DBaaS) für die Bereitstellung und Verwaltung von MongoDB-Datenbanken in der Cloud.

Bewährte Methoden

Richtlinien finden Sie im Best Practices Guide for MongoDB im MongoDB-Repository GitHub .

Epen

Entdeckung und Bewertung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie die Clustergröße.	Schätzen Sie die Größe des Arbeitssets, indem Sie die Informationen `db.stats()`	MongoDB DBA, Anwendung sarchitekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	für den gesamten Indexraum verwenden. Gehen Sie davon aus, dass auf einen Prozentsatz Ihres Datenspeichers häufig zugegriffen wird. Oder Sie können Ihren Speicherbedarf auf der Grundlage Ihrer Annahmen abschätzen. Diese Aufgabe sollte ungefähr eine Woche dauern. Weitere Informationen und Beispiele für diese und die anderen Geschichten in diesem Epos finden Sie unter den Links im Abschnitt Verwandte Ressourcen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schätzen Sie die Anforderungen an die Netzwerkbandbreite.	Um Ihre Netzwerkbandbreitenanforderungen zu schätzen, multiplizieren Sie die durchschnittliche Dokumentengröße mit der Anzahl der pro Sekunde bereitgestellten Dokumente. Berücksichtigen Sie den maximalen Datenverkehr, den jeder Knoten in Ihrem Cluster als Grundlage tragen kann. Um die Downstream-Datenübertragungsraten von Ihrem Cluster zu den Client-Anwendungen zu berechnen, verwenden Sie die Summe aller Dokumente, die über einen bestimmten Zeitraum zurückgegeben wurden. Wenn Ihre Anwendungen von sekundären Knoten lesen, dividieren Sie diese Gesamtzahl der Dokumente durch die Anzahl der Knoten, die Lesevorgänge ausführen können. Verwenden Sie den `db.stats().avgObjSize` Befehl, um die durchschnittliche Dokumentgröße für eine Datenbank zu ermitteln. Diese Aufgabe dauert in der Regel einen Tag.	MongoDB DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie die Atlas-Stufe aus.	Folgen Sie den Anweisungen in der MongoDB-Dokumentation, um die richtige Atlas-Clusterstufe auszuwählen.	MongoDB DBA
Plan für die Umstellung.	Plan für die Umstellung der Anwendung.	MongoDB DBA, Anwendungsarchitekt

Richten Sie eine neue MongoDB Atlas-Umgebung auf AWS ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen neuen MongoDB Atlas-Cluster auf AWS.	Wählen Sie in MongoDB Atlas Build a Cluster und dann AWS als Cloud-Anbieter aus.	MongoDB DBA
Wählen Sie AWS-Regionen eine globale Clusterkonfiguration aus.	Wählen Sie aus der Liste der AWS-Regionen für Ihren Atlas-Cluster verfügbaren aus. Konfigurieren Sie bei Bedarf globale Cluster.	MongoDB DBA
Wählen Sie die Clusterebene aus.	Wählen Sie Ihre bevorzugte Clusterstufe aus. Ihre Tierauswahl bestimmt Faktoren wie Arbeitsspeicher, Speicher und IOPS-Spezifikation.	MongoDB DBA
Konfigurieren Sie zusätzliche Cluster-Einstellungen.	Konfigurieren Sie zusätzliche Clustereinstellungen wie MongoDB-Version, Sicherungs- und Verschlüsselungsoptionen. Weitere Informationen zu diesen Optionen finden	MongoDB DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie im Abschnitt Verwandte Ressourcen.	

Konfigurieren Sie Sicherheit und Compliance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Zugriffsliste.	Um eine Verbindung zum Atlas-Cluster herzustellen, müssen Sie der Zugriffsliste des Projekts einen Eintrag hinzufügen. Atlas verwendet Transport Layer Security (TLS)/Secure Sockets Layer (SSL), um die Verbindungen zur Virtual Private Cloud (VPC) für Ihre Datenbank zu verschlüsseln. Um die Zugriffsliste für das Projekt einzurichten und weitere Informationen zu den Geschichten in diesem Epos zu erhalten, klicken Sie auf die Links im Abschnitt Verwandte Ressourcen.	MongoDB DBA
Authentifizieren und autorisieren Sie Benutzer.	Sie müssen die Datenbankbenutzer, die auf die MongoDB Atlas-Cluster zugreifen, erstellen und authentifizieren. Um auf die Cluster in einem Projekt zugreifen zu können, müssen Benutzer zu diesem Projekt gehören, und sie können mehreren Projekten	MongoDB DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	angehören. Sie können die Autorisierung auch mit AWS Identity and Access Management (IAM) aktiviere n. Weitere Informationen finden Sie unter Authentif izierung mit IAM einrichten in der MongoDB-Dokumentation.	
Erstellen Sie benutzerd efinierte Rollen.	(Optional) Atlas unterstützt die Erstellung benutzerdefinierte r Rollen, wenn die integrierten Atlas-Datenbank-Benutzerrec hte Ihre gewünschten Rechte nicht abdecken.	MongoDB DBA
Richten Sie VPC-Peering ein.	(Optional) Atlas unterstützt VPC-Peering mit anderen AWS. VPCs	MongoDB DBA
Richten Sie einen Endpunkt ein AWS PrivateLink .	(Optional) Sie können private Endpunkte einrichten, AWS indem Sie AWS PrivateLink	MongoDB DBA
Aktivieren Sie die Zwei-Faktor-Authentifizierung.	(Optional) Atlas unterstützt die Zwei-Faktor-Authentifizieru ng (2FA), damit Benutzer den Zugriff auf ihre Atlas-Konten kontrollieren können.	MongoDB DBA
Richten Sie die Benutzera uthentifizierung und -autorisi erung mit LDAP ein.	(Optional) Atlas unterstützt die Benutzerauthentifizierung und -autorisierung mit dem Lightweight Directory Access Protocol (LDAP).	MongoDB DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie vereinheitlichten AWS Zugriff ein.	(Optional) Einige Atlas-Funktionen, darunter Atlas Data Lake und Verschlüsselung im Ruhezustand mithilfe der Kundenschlüsselverwaltung, verwenden IAM-Rollen für die Authentifizierung.	MongoDB DBA
Richten Sie die Verschlüsselung im Ruhezustand ein, indem Sie AWS KMS	(Optional) Atlas unterstützt die Verwendung von AWS Key Management Service (AWS KMS) zur Verschlüsselung von Speicher-Engines und Backups von Cloud-Anbietern.	MongoDB DBA
Richten Sie CSFLE ein.	(Optional) Atlas unterstützt die clientseitige Verschlüsselung auf Feldebene (CSFLE), einschließlich der automatischen Verschlüsselung von Feldern.	MongoDB DBA

Daten migrieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie Ihren Zielreplikatsatz in MongoDB Atlas.	Starten Sie Ihren Zielreplikatsatz in MongoDB Atlas. Wählen Sie im Atlas Live Migration Service die Option Ich bin bereit zur Migration aus.	MongoDB DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Verbindung AWS Glue mit MongoDB Atlas her.	Verwenden Sie an AWS-Glue-Crawler , um eine Verbindung AWS Glue mit MongoDB Atlas (Zieldatenbank) herzustellen. Dieser Schritt hilft, die Zielumgebung auf die Migration vorzubereiten. Weitere Informationen finden Sie in der AWS Glue - Dokumentation.	MongoDB DBA
Stellen Sie die Verbindung von AWS Glue mit der Quelldatenbank oder dem Quellstream her.	Dies hilft, die Zielumgebung auf die Migration vorzubereiten.	MongoDB DBA
Richten Sie die Datentransformation ein.	Konfigurieren Sie die Transformationslogik, um die Daten vom strukturierten Legacy-Schema zum flexiblen Schema von MongoDB zu migrieren.	MongoDB DBA
Migrieren Sie die Daten.	Planen Sie die Migration in AWS Glue Studio.	MongoDB DBA

Konfigurieren Sie die betriebliche Integration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Connect zum Cluster her.	Connect zum MongoDB Atlas-Cluster her.	App-Developer
Interagieren Sie mit Daten.	Interagieren Sie mit Clusterdaten.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überwachen Sie die Cluster.	Überwachen Sie Ihre MongoDB Atlas-Cluster.	MongoDB DBA
Daten sichern und wiederherstellen.	Clusterdaten sichern und wiederherstellen.	MongoDB DBA

Fehlerbehebung

Problem	Lösung
Wenn Sie auf Probleme stoßen	Weitere Informationen finden Sie unter Problembehandlung im MongoDB Atlas CloudFormation Resources Repository.

Zugehörige Ressourcen

Alle folgenden Links führen, sofern nicht anders angegeben, zu Webseiten in der MongoDB-Dokumentation.

Leitfaden zur Migration

- Migration zu MongoDB Atlas on AWS (AWS Prescriptive Guidance)

Entdeckung und Bewertung

- Arbeitsspeicher
- Beispiel zur Größenbestimmung mit Atlas-Beispieldatensätzen
- Beispiel zur Größenbestimmung für mobile Anwendungen
- Netzwerkverkehr
- Automatische Cluster-Skalierung
- Vorlage für die Größenbestimmung von Atlas

Konfiguration von Sicherheit und Compliance

- Einträge in der IP-Zugriffsliste konfigurieren
- Datenbankbenutzer konfigurieren
- Konfigurieren Sie den Zugriff auf die Atlas-Benutzeroberfläche
- Konfigurieren Sie benutzerdefinierte Datenbankrollen
- Datenbankbenutzer konfigurieren
- Richten Sie eine Netzwerk-Peering-Verbindung ein
- Erfahren Sie mehr über private Endpunkte in Atlas
- Verwalten Sie Ihre Multi-Faktor-Authentifizierungsoptionen
- Richten Sie die Benutzerauthentifizierung und -autorisierung mit LDAP ein
- Atlas Data Lake
- Verschlüsselung im Ruhezustand mithilfe von Customer Key Management
- Methoden zur Übernahme einer Rolle (IAM-Dokumentation)
- Clientseitige Verschlüsselung auf Feldebene
- Automatische Verschlüsselung
- MongoDB Atlas Sicherheitskontrollen
- MongoDB-Vertrauenszentrum
- Konfigurieren Sie Sicherheitsfunktionen für Cluster

Einrichtung einer neuen MongoDB Atlas-Umgebung auf AWS

- Cloud-Anbieter und Regionen
- Globale Cluster verwalten
- Wählen Sie die Clusterebene
- Konfigurieren Sie zusätzliche Einstellungen
- Fangen Sie mit Atlas an
- Konfigurieren Sie den Zugriff auf die Atlas-Benutzeroberfläche
- Cluster verwalten

Daten migrieren

- Daten migrieren oder importieren

Cluster überwachen

- Überwachen Sie Ihre Cluster

Integrieren von Abläufen

- Stellen Sie eine Connect zu einem Cluster her
- Interagieren Sie mit Ihren Daten
- Überwachen Sie Ihre Cluster
- Daten sichern, wiederherstellen und archivieren

GitHub Repositorium

- Streamen Sie Daten in MongoDB Atlas mit AWS Glue

Migrationsmuster nach Arbeitslast

Themen

- IBM
- Microsoft
- N/A
- Open-Source
- Oracle
- SAP

IBM

- Migrieren Sie mithilfe von AWS DMS eine Db2-Datenbank von Amazon EC2 zu Aurora MySQL-kompatibel
- Migrieren Sie Db2 for LUW zu Amazon mithilfe EC2 von Protokollversand, um Ausfallzeiten zu reduzieren
- Migrieren Sie Db2 for LUW zu Amazon EC2 mit Disaster Recovery mit hoher Verfügbarkeit
- Migrieren Sie mithilfe von AWS DMS und AWS SCT von IBM Db2 auf Amazon EC2 zu Aurora PostgreSQL-kompatibel
- Migrieren Sie von IBM WebSphere Application Server zu Apache Tomcat auf Amazon EC2
- Streamen Sie Daten von IBM Db2, SAP, Sybase und anderen Datenbanken nach MongoDB Atlas auf AWS

Microsoft

- Beschleunigen Sie die Erkennung und Migration von Microsoft-Workloads zu AWS
- Ändern Sie Python- und Perl-Anwendungen, um die Datenbankmigration von Microsoft SQL Server zur Amazon Aurora PostgreSQL-Compatible Edition zu unterstützen
- Erstellen Sie CloudFormation AWS-Vorlagen für AWS DMS-Aufgaben mit Microsoft Excel und Python
- Exportieren Sie eine Microsoft SQL Server-Datenbank mithilfe von AWS DMS nach Amazon S3
- Implementieren Sie SHA1 Hashing für PII-Daten bei der Migration von SQL Server zu PostgreSQL
- EC2 Windows-Instances in ein AWS Managed Services Services-Konto aufnehmen und migrieren
- Migrieren Sie eine Messaging-Warteschlange von Microsoft Azure Service Bus zu Amazon SQS
- Migrieren Sie mithilfe von AWS DMS eine Microsoft SQL Server-Datenbank von Amazon EC2 zu Amazon DocumentDB
- Migrieren Sie eine Microsoft SQL Server-Datenbank mithilfe von AWS DMS und AWS SCT zu Aurora MySQL
- Migrieren Sie eine.NET-Anwendung von Microsoft Azure App Service zu AWS Elastic Beanstalk
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Amazon EC2
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Amazon RDS for SQL Server
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mithilfe von Verbindungsservern zu Amazon RDS for SQL Server
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mit systemeigenen Sicherungs- und Wiederherstellungsmethoden zu Amazon RDS for SQL Server
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mit AWS DMS zu Amazon Redshift
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank mithilfe von AWS SCT-Datenextraktionsagenten zu Amazon Redshift
- Migrieren Sie eine lokale Microsoft SQL Server-Datenbank zu Microsoft SQL Server auf Amazon EC2 unter Linux
- Migrieren Sie Daten mithilfe von Rclone von Microsoft Azure Blob zu Amazon S3
- Migrieren Sie EC2 mithilfe des Application Migration Service eine lokale Microsoft SQL Server-Datenbank zu Amazon
- Migrieren Sie eine relationale Datenbank zu MongoDB Atlas am AWS
- Migrieren Sie Windows-SSL-Zertifikate mithilfe von ACM zu einem Application Load Balancer

- Rehosten Sie lokale Workloads in der AWS-Cloud: Migrationscheckliste
- Verbindungsfehler nach der Migration von Microsoft SQL Server zur AWS-Cloud beheben
- Richten Sie mithilfe von Amazon eine Multi-AZ-Infrastruktur für einen SQL Server Always On FCI ein FSx

N/A

- Erstellen Sie einen Genehmigungsprozess für Firewallanfragen während einer Rehost-Migration zu AWS

Open-Source

- Anwendungsbenutzer und Rollen in Aurora PostgreSQL-Compatible erstellen
- Migrieren Sie Amazon RDS for Oracle zu Amazon RDS for PostgreSQL mit AWS SCT und unter Verwendung von und AWS DMSAWS CLIAWS CloudFormation
- Migrieren Sie eine lokale MariaDB-Datenbank mit nativen Tools zu Amazon RDS for MariaDB
- Migrieren Sie eine lokale MySQL-Datenbank zu Amazon EC2
- Migrieren Sie eine lokale MySQL-Datenbank zu Amazon RDS for MySQL
- Migrieren Sie eine lokale MySQL-Datenbank zu Aurora MySQL
- Migrieren Sie eine lokale PostgreSQL-Datenbank zu Aurora PostgreSQL
- Migrieren Sie eine Couchbase Server-Datenbank zu Amazon EC2
- Migrieren Sie EC2 mit Auto Scaling von IBM WebSphere Application Server zu Apache Tomcat auf Amazon
- Migrieren Sie von Oracle GlassFish zu AWS Elastic Beanstalk
- Migrieren Sie mit pglogical von PostgreSQL auf Amazon EC2 zu Amazon RDS for PostgreSQL
- Migrieren Sie ML-Workloads zum Erstellen, Trainieren und Bereitstellen zu Amazon SageMaker mithilfe der AWS-Entwicklertools
- Migrieren Sie lokale Java-Anwendungen mit AWS App2Container zu AWS
- Migrieren Sie lokale MySQL-Datenbanken mit Percona XtraBackup, Amazon EFS und Amazon S3 zu Aurora MySQL
- Migrieren Sie externe Oracle-Tabellen zu Amazon Aurora PostgreSQL-kompatibel
- Migrieren Sie Redis-Workloads zu Redis Enterprise Cloud auf AWS
- Starten Sie den AWS Replication Agent SELinux nach dem Neustart eines RHEL-Quellservers automatisch neu, ohne ihn zu deaktivieren.
- Transportieren Sie PostgreSQL-Datenbanken zwischen zwei Amazon RDS-DB-Instances mithilfe von pg_transport

Oracle

- Konvertiert VARCHAR2 (1) den Datentyp für Oracle in den booleschen Datentyp für Amazon Aurora PostgreSQL
- Emulieren Sie Oracle DR mithilfe einer PostgreSQL-kompatiblen globalen Aurora-Datenbank
- Schrittweise Migration von Amazon RDS for Oracle zu Amazon RDS for PostgreSQL mithilfe von Oracle SQL Developer und AWS SCT
- Laden Sie BLOB-Dateien in TEXT, indem Sie die Dateikodierung in Aurora PostgreSQL-kompatibel verwenden
- Migrieren Sie Amazon RDS for Oracle zu Amazon RDS for PostgreSQL im SSL-Modus mithilfe von AWS DMS
- Migrieren Sie eine Amazon RDS for Oracle Oracle-Datenbank zu einer anderen AWS-Konto und AWS-Region verwenden Sie sie AWS DMS für die laufende Replikation
- Migrieren Sie eine Amazon RDS for Oracle DB-Instance zu einer anderen VPC
- Migrieren Sie eine lokale Oracle-Datenbank mithilfe EC2 von Oracle Data Pump zu Amazon
- Migrieren Sie eine lokale Oracle-Datenbank mit Logstash zu Amazon OpenSearch Service
- Migrieren Sie eine lokale Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon RDS for MySQL
- Migrieren Sie eine lokale Oracle-Datenbank zu Amazon RDS for Oracle
- Migrieren Sie eine lokale Oracle-Datenbank zu Amazon RDS for Oracle, indem Sie den direkten Oracle Data Pump-Import über einen Datenbank-Link verwenden
- Migrieren Sie eine lokale Oracle-Datenbank mit Oracle Data Pump zu Amazon RDS for Oracle
- Migrieren Sie eine lokale Oracle-Datenbank mithilfe eines Oracle-Bystanders und AWS DMS zu Amazon RDS for PostgreSQL
- Migrieren Sie eine lokale Oracle-Datenbank zu Oracle auf Amazon EC2
- Migrieren Sie mithilfe von AWS DMS und AWS SCT eine Oracle-Datenbank von Amazon EC2 zu Amazon RDS for MariaDB
- Migrieren Sie mithilfe von AWS DMS eine Oracle-Datenbank von Amazon EC2 zu Amazon RDS for Oracle
- Migrieren Sie eine Oracle-Datenbank mit AWS DMS zu Amazon DynamoDB
- Migrieren Sie eine Oracle-Datenbank mithilfe von GoldenGate Oracle-Flatfile-Adaptern zu Amazon RDS for Oracle
- Migrieren Sie eine Oracle-Datenbank mit AWS DMS und AWS SCT zu Amazon Redshift

- Migrieren Sie eine Oracle-Datenbank mit AWS DMS und AWS SCT zu Aurora PostgreSQL
- Migrieren Sie eine Oracle JD EnterpriseOne Edwards-Datenbank mithilfe von Oracle Data Pump und AWS DMS zu AWS
- Migrieren Sie eine partitionierte Oracle-Tabelle mithilfe von AWS DMS zu PostgreSQL
- Migrieren Sie eine PeopleSoft Oracle-Datenbank mithilfe von AWS DMS zu AWS
- Migrieren Sie Daten von einer lokalen Oracle-Datenbank zu Aurora PostgreSQL
- Migrieren Sie von Amazon RDS for Oracle zu Amazon RDS for MySQL
- Migrieren Sie mithilfe von Materialized Views und AWS DMS von Oracle 8i oder 9i zu Amazon RDS for PostgreSQL
- Migrieren Sie mithilfe von AWS DMS von Oracle 8i oder 9i zu Amazon RDS for PostgreSQL SharePlex
- Migrieren Sie mithilfe von Oracle von Oracle Database zu Amazon RDS for PostgreSQL GoldenGate
- Migrieren Sie mithilfe von AWS DMS und AWS SCT von Oracle auf Amazon EC2 zu Amazon RDS for MySQL
- Migrieren Sie mit AWS DMS von Oracle zu Amazon DocumentDB
- Migrieren Sie von Oracle WebLogic zu Apache Tomcat (ToMEE) auf Amazon ECS
- Migrieren Sie funktionsbasierte Indizes von Oracle nach PostgreSQL
- Migrieren Sie Legacy-Anwendungen von Oracle Pro*C zu ECPG
- Migrieren Sie Oracle CLOB-Werte in einzelne Zeilen in PostgreSQL auf AWS
- Migrieren Sie Oracle-Datenbank-Fehlercodes in eine Amazon Aurora PostgreSQL-kompatible Datenbank
- Migrieren Sie die Oracle E-Business Suite zu Amazon RDS Custom
- Migrieren Sie native Oracle-Funktionen mithilfe von Erweiterungen zu PostgreSQL
- Migrieren Sie Oracle PeopleSoft zu Amazon RDS Custom
- Migrieren Sie die Oracle ROWID-Funktionalität zu PostgreSQL auf AWS
- Migrieren Sie Oracle SERIALLY_REUSABLE Pragma-Pakete nach PostgreSQL
- Migrieren Sie virtuell generierte Spalten von Oracle nach PostgreSQL
- Richten Sie die Oracle UTL_FILE-Funktionalität auf Aurora PostgreSQL-Compatible ein
- Datenbankobjekte nach der Migration von Oracle zu Amazon Aurora PostgreSQL validieren

SAP

- Migrieren Sie eine lokale SAP ASE-Datenbank zu Amazon EC2
- Migrieren Sie mithilfe von AWS DMS von SAP ASE zu Amazon RDS for SQL Server
- Migrieren Sie SAP ASE auf Amazon EC2 zu Amazon Aurora PostgreSQL-kompatibel mit AWS SCT und AWS DMS
- Reduzieren Sie die Umstellungszeit für homogene SAP-Migrationen mithilfe des Application Migration Service

Mehr Muster

- Zugriff AWS-Services von IBM z/OS aus durch Installation des AWS CLI
- Beurteilen Sie die Anwendungsbereitschaft für die Migration in die AWS-Cloud mithilfe von CAST Highlight
- Beurteilen Sie die Abfrageleistung für die Migration von SQL Server-Datenbanken zu MongoDB Atlas auf AWS
- Automatisieren Sie regionsübergreifendes Failover und Failback mithilfe des DR Orchestrator Framework
- Automatisieren Sie Datenbankaufgaben in der SQL Server Express Edition, die auf Amazon ausgeführt wird, EC2 mithilfe eines AWS Lambda Taskplaners
- Erstellen Sie einen fortschrittlichen Mainframe-Dateiviewer in der AWS-Cloud
- Konfiguration einer Rechenzentrumserweiterung für VMware Cloud on AWS mithilfe des Hybrid Linked Mode
- Stellen Sie über ein privates Netzwerk eine Connect zu Daten- und Steuerungsebenen des Application Migration Service her
- Containerisieren Sie Mainframe-Workloads, die von Blu Age modernisiert wurden
- JSON-Oracle-Abfragen in PostgreSQL-Datenbank-SQL konvertieren
- Konvertieren Sie die temporale Funktion Teradata NORMALIZE in Amazon Redshift SQL
- Konvertieren Sie die Teradata RESET WHEN-Funktion in Amazon Redshift SQL
- Kopieren Sie Amazon DynamoDB-Tabellen zwischen Konten mit AWS Backup
- Stellen Sie einen Cassandra-Cluster auf Amazon EC2 mit Private Static bereit, um ein IPs Rebalancing zu vermeiden
- Stellen Sie Anwendungen mit mehreren Stacks mithilfe von AWS CDK bereit mit TypeScript
- Stellen Sie mithilfe von Terraform SQL Server-Failover-Cluster-Instances auf Amazon EC2 und Amazon FSx bereit
- Emulieren Sie Oracle RAC-Workloads mithilfe benutzerdefinierter Endpunkte in Aurora PostgreSQL
- Schätzen Sie die Größe der Amazon RDS-Engine für eine Oracle-Datenbank mithilfe von AWR-Berichten
- Generieren Sie Dateneinblicke mithilfe von AWS Mainframe Modernization und Amazon Q in QuickSight
- Behandeln Sie anonyme Blöcke in dynamischen SQL-Anweisungen in Aurora PostgreSQL

- Behandeln Sie überladene Oracle-Funktionen in Aurora PostgreSQL-kompatibel
- Automatische Identifizierung doppelter Container-Images bei der Migration zu einem Amazon ECR-Repository
- Integrieren Sie VMware vRealize Network Insight mit VMware Cloud on AWS
- Migrieren Sie Amazon RDS for Oracle DB-Instances zu anderen Konten, die AMS verwenden
- Migrieren Sie einen lokalen Apache Kafka-Cluster zu Amazon MSK mithilfe von MirrorMaker
- Migrieren Sie Apache Cassandra-Workloads mithilfe von AWS Glue zu Amazon Keyspaces
- Migrieren Sie Ihre Container-Workloads von Azure Red Hat OpenShift (ARO) zu Red Hat OpenShift Service in AWS (ROSA)
- Migrieren Sie mithilfe von AWS DMS von Oracle 8i oder 9i zu Amazon RDS for Oracle SharePlex
- Migrieren Sie Hadoop-Daten mithilfe WANdisco LiveData von Migrator zu Amazon S3
- Migrieren Sie Oracle-Funktionen und -Prozeduren mit mehr als 100 Argumenten nach PostgreSQL
- Migrieren Sie Oracle OUT-Bind-Variablen in eine PostgreSQL-Datenbank
- Migrieren Sie SAP HANA zu AWS mithilfe von SAP HSR mit demselben Hostnamen
- Migrieren Sie SQL Server mithilfe verteilter Verfügbarkeitsgruppen zu AWS
- Migrieren VMs Sie mithilfe von HCX OS Assisted Migration zur VMware Cloud auf AWS
- Modernisieren Sie Mainframe-Online-Druck-Workloads auf AWS mithilfe von Micro Focus Enterprise Server und LRS VPSX/MFI
- Modernisieren Sie das Mainframe-Output-Management mithilfe AWS von Rocket Enterprise Server und LRS X PageCenter
- Ändern Sie HTTP-Header, wenn Sie von F5 zu einem Application Load Balancer auf AWS migrieren
- Multi-AZ-Failover für EMR-Cluster mithilfe von Application Recovery Controller verwalten
- Senden Sie mithilfe von VMware Aria Operations AWS for Logs Logs von VMware Cloud on an Splunk
- Richten Sie mithilfe von Terraform eine CI/CD-Pipeline für die Datenbankmigration ein
- Richten Sie die Notfallwiederherstellung für Oracle JD Edwards EnterpriseOne mit AWS Elastic Disaster Recovery ein
- Vereinfachen Sie die Verwaltung privater Zertifikate mithilfe von AWS Private CA und AWS RAM
- Übertragung umfangreicher Db2 z/OS-Daten in CSV-Dateien nach Amazon S3

Modernisierung

Themen

- Analysieren und visualisieren Sie die Softwarearchitektur in CAST Imaging
- Beurteilen Sie die Anwendungsbereitschaft für die Migration in die AWS-Cloud mithilfe von CAST Highlight
- Automatisches Archivieren von Elementen in Amazon S3 mithilfe von DynamoDB TTL
- Erstellen Sie eine serverlose Architektur mit mehreren Mandanten in Amazon Service OpenSearch
- Stellen Sie Anwendungen mit mehreren Stacks mithilfe von AWS CDK bereit mit TypeScript
- Automatisieren Sie die Bereitstellung verschachtelter Anwendungen mit AWS SAM
- Implementieren Sie die SaaS-Mandantenisolierung für Amazon S3 mithilfe eines AWS Lambda Lambda-Token-Verkaufsautomaten
- Implementieren Sie das serverlose Saga-Muster mithilfe von AWS Step Functions
- Verwalten Sie lokale Containeranwendungen, indem Sie Amazon ECS Anywhere mit dem AWS CDK einrichten
- Modernisieren Sie ASP.NET Web Forms-Anwendungen auf AWS
- Führen Sie ereignisgesteuerte und geplante Workloads in großem Umfang mit AWS Fargate aus
- Mandanten-Onboarding in der SaaS-Architektur für das Silomodell mit C# und AWS CDK
- Zerlegen Sie Monolithen mithilfe von CQRS und Event Sourcing in Microservices
- Mehr Muster

Analysieren und visualisieren Sie die Softwarearchitektur in CAST Imaging

Erstellt von Arpita Sinha (Cast Software) und James Hurrell (Cast Software)

Übersicht

Dieses Muster zeigt, wie Sie mit CAST Imaging ein komplexes Softwaresystem visuell steuern und eine genaue Analyse der Softwarestruktur durchführen können. Wenn Sie CAST Imaging auf diese Weise verwenden, können Sie fundiertere Entscheidungen über die Architektur Ihrer Anwendung treffen, insbesondere zu Modernisierungszwecken.

Um die Architektur Ihrer Anwendung in CAST Imaging anzuzeigen, müssen Sie zunächst den Quellcode Ihrer Anwendung über die CAST-Konsole einbinden. Die Konsole veröffentlicht dann die Daten Ihrer Anwendung in CAST Imaging, wo Sie Ihre Anwendungsarchitektur Schicht für Schicht visualisieren und darin navigieren können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Das Amazon Machine Image (AMI) für CAST Imaging
- Eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance, die Folgendes beinhaltet (eine speicheroptimierte r5.xlarge EC2 Amazon-Instance wird empfohlen):
  - 4 vCPU
  - 32 GB RAM
  - Mindestvolumen von 500 GB für Allzweck-Solid-State-Laufwerke (SSD) (GP3)
- Lizenzschlüssel für CAST Console und CAST Imaging (um die erforderlichen Lizenzschlüssel zu erhalten, wenden Sie sich an CAST unter aws.contact-me@castsoftware.com)
- Der vollständige Quellcode der Anwendung, die Sie analysieren möchten, im komprimierten Format (.zip)
- Microsoft Edge, Mozilla Firefox oder Google Chrome

Architektur

Das folgende Diagramm zeigt einen Beispiel-Workflow für das Onboarding des Quellcodes einer Anwendung über die CAST-Konsole und die anschließende Anzeige in CAST Imaging:

Das Diagramm zeigt den folgenden Workflow:

1. CAST generiert Metadaten des Anwendungsquellcodes durch Reverse-Engineering von Frontend-, Middleware- und Back-End-Code.
2. Die von CAST generierten Anwendungsdaten werden automatisch in CAST Imaging importiert, wo sie visualisiert und analysiert werden können.

Hier ist eine Momentaufnahme der Funktionsweise dieses Prozesses:

Tools

- CAST Imaging ist eine browserbasierte Anwendung, mit der Sie Ihr Softwaresystem visuell betrachten und darin navigieren können, sodass Sie fundierte Entscheidungen über die Architektur treffen können.
- CAST Console ist eine browserbasierte Anwendung, mit der Sie CAST-AIP-Analysen konfigurieren, ausführen und verwalten können.

> **Note**
>
> CAST Imaging und CAST Console sind im AMI für CAST Imaging enthalten.

Epen

Richten Sie die CAST Imaging-Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die anfängliche Konfiguration der CAST-Konsole aus.	1. Öffnen Sie Ihren Webbrowser und stellen Sie eine Verbindung zur CAST-Konsole her, indem Sie die folgende URL eingeben: http://localhost:8081	Softwarearchitekten, Entwickler, technische Führungskräfte

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wenn Sie dazu aufgefordert werden, geben Sie Ihren CAST Console-Lizenzschlüssel ein. Wählen Sie anschließend Weiter. 3. Überprüfen Sie die Konfigurationseinstellungen. Wenn keine Änderungen erforderlich sind, wählen Sie Speichern und beenden.	
Führen Sie die erste CAST Imaging-Konfiguration aus.	1. Öffnen Sie Ihren Webbrowser und stellen Sie eine Verbindung zu CAST Imaging her, indem Sie die folgende URL eingeben: http://localhost:8083 2. Wenn Sie dazu aufgefordert werden, melden Sie sich an, indem Sie admin sowohl für den Benutzernamen als auch für das Passwort eingeben. 3. Wenn Sie dazu aufgefordert werden, geben Sie Ihren CAST Imaging-Lizenzschlüssel ein. Wählen Sie dann Update, um den Schlüssel zu speichern.	Softwarearchitekten, Entwickler, technische Führungskräfte

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den lokalen CAST Extend-Server.	(Optional) Standardmäßig ist der lokale CAST Extend-Server so konfiguriert, dass er im Offline-Modus funktioniert. Wenn dies akzeptabel ist, ist keine zusätzliche Konfiguration erforderlich. Wenn Sie es jedoch vorziehen, den lokalen CAST Extend-Server im Online-/Proxymodus mit einer direkten Verbindung zu CAST Extend zu konfigurieren, gehen Sie wie folgt vor. **Note** Die Anmeldeinformationen für CAST Extend finden Sie auf der CAST Extend-Registrierungsseite. 1. Verwenden Sie die Verknüpfung CAST Extend Admin Center auf dem Desktop, um Ihren Webbrowser zu laden und eine Verbindung zum lokalen CAST Extend-Server herzustellen. 2. Wählen Sie die Option Online.	Softwarearchitekten, Entwickler, technische Führungskräfte

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Geben Sie Ihre CAST Extend-Anmeldeinfo rmationen (E-Mail und Passwort) ein und wählen Sie Speichern, um den Vorgang abzuschließen.	

Integrieren Sie Ihre Anwendung in CAST Imaging

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie den Quellcode für Ihre Anwendung vor.	Speichern Sie den Quellcode Ihrer Anwendung in einer einzigen, komprimierten ZIP-Datei.	Softwarearchitekten, Entwickle r, technische Führungskräfte
Fügen Sie Ihre Anwendung zur CAST-Konsole hinzu.	1. Öffnen Sie Ihren Webbrowser und stellen Sie eine Verbindung zur CAST-Konsole her, indem Sie die folgende URL eingeben: http://localhost:8081 2. Wenn Sie dazu aufgeford ert werden, melden Sie sich an, indem Sie admin sowohl für den Benutzernamen als auch für das Passwort eingeben. 3. Wählen Sie Anwendung hinzufügen. Geben Sie dann den Namen der Anwendung ein und wählen Sie Hinzufügen.	Softwarearchitekten, Entwickle r, technische Führungskräfte

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Öffnen Sie den Assistenten für die Quellcode-Bereitstellung.	Suchen Sie die Anwendung, die Sie in der CAST-Konsole erstellt haben. Wählen Sie dann Version hinzufügen.	Softwarearchitekten, Entwickler, technische Führungskräfte
Laden Sie den Quellcode für Ihre Anwendung hoch.	Führen Sie eine der folgenden Aktionen aus: • Ziehen Sie die ZIP-Datei, die den Quellcode Ihrer Anwendung enthält, per Drag & Drop in den Assistenten für die Quellcodebereitstellung. – oder – • Wählen Sie das Symbol „Cloud hochladen“. Öffnen Sie dann die ZIP-Datei, die den Quellcode Ihrer Anwendung enthält.	Softwarearchitekten, Entwickler, technische Führungskräfte

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie den Analysepr ozess.	1. Geben Sie im Lieferass istenten die Versionsd etails an und geben Sie die Konfigurationsopti onen an. Weitere Informati onen finden Sie unter Standard Onboarding for CAST Imaging in der CAST Imaging-Dokumentation. 2. Vergewissern Sie sich, dass die Option In CAST Imaging veröffentlichen ausgewählt ist. Wählen Sie dann „Fortfahren“. **Note** Wenn Sie Weiter wählen, wird der Analyseprozess für den Quellcode gestartet. Das Fortschrittsfenster in der CAST-Konsole zeigt jeden Schritt des Analyseprozesses und zeigt eine Benachric htigung an, wenn die Analyse abgeschlo ssen ist.	Softwarearchitekten, Entwickle r, technische Führungskräfte

Überprüfen Sie die Analyseergebnisse und Daten, die auf CAST Imaging veröffentlicht wurden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Status und die Protokolle.	Wenn alle Analyseaktionen abgeschlossen sind, stellen Sie sicher, dass im Fortschritt tsfenster eine Erfolgsmeldung angezeigt wird. **Note** Sie können die einzelnen Protokolle für jede Analyseaktion unmittelbar nach deren Abschluss überprüfen. Um die Protokolle für eine bestimmte Aktion zu überprüfen, wählen Sie im Fortschritt tsfenster die Option Protokoll anzeigen.	Softwarearchitekten, Entwickler, technische Führungskräfte
Überprüfen Sie die Anwendungsdetails.	Überprüfen Sie im Bereich Anwendungsdetails die Details zu den Analyseergebnissen. Achten Sie darauf, dass Sie sich die entdeckten Technologien und die Organisation des Quellcodes ansehen.	Softwarearchitekten, Entwickler, technische Führungskräfte
Überprüfen Sie CAST Imaging und greifen Sie darauf zu.	1. Vergewissern Sie sich in der CAST-Konsole im Bereich Anwendungsverwaltung, dass der	Softwarearchitekten, Entwickler, technische Führungskräfte

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Versionsstatus Ihrer Anwendung „Imaging verarbeitet“ lautet. Ein CAST Imaging-Symbol wird angezeigt. 2. Wählen Sie das CAST Imaging-Symbol, um direkt zu Ihren Anwendung sdaten in CAST Imaging zu gelangen. **Note** Der Status „Imaging verarbeitet“ bedeutet, dass der Quellcode analysiert und in Ihre CAST Imaging-Instanz hochgeladen wurde.	

Beginnen Sie mit der Analyse Ihrer Anwendung mit CAST Imaging

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie sich bei CAST Imaging an.	Öffnen Sie Cast Imaging und geben Sie die standardm äßigen Administratoranmel dedaten ein (admin/admin). Die Daten Ihrer Anwendung werden angezeigt.	Softwarearchitekten, Entwickle r, technische Führungskräfte
Erkunden Sie die Daten Ihrer Anwendung in CAST Imaging.	Beginnen Sie mit der Anzeige Ihrer Softwarearchitektur	Softwarearchitekten, Entwickle r, technische Führungskräfte

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	mithilfe der Funktionen von CAST Imaging. Für eine kurze Anleitung zur Verwendung der Funktione n von CAST Imaging wählen Sie das Hilfesymbol, um den CAST Imaging Helper aufzurufen. Weitere Informationen finden Sie im CAST Imaging-B enutzerhandbuch.	

Zugehörige Ressourcen

Dokumentation zur CAST-Konsole

- Einloggen
- Konfiguration von Optionen über die CAST-Konsole

Dokumentation zu CAST Imaging

- Onboarding von Bewerbungen für CAST Imaging — Voraussetzungen
- Fügen Sie eine neue Anwendung für CAST Imaging hinzu
- Standard-Onboarding für CAST Imaging — Ergebnisse überprüfen
- Einloggen
- Konfigurationsoptionen — Admin Center GUI

Weitere Ressourcen zu CAST Imaging auf AWS

- Anwendungsmodernisierung auf AWS Accelerated by CAST — Technisch (PartnerCast AWS-Webinar, kostenloses Konto erforderlich)

- Verwendung von CAST und AWS Migration Hub Refactor Spaces zur Modernisierung älterer Anwendungen (AWS-Blogbeitrag)
- Modernisieren Sie Anwendungen für AWS-Architekturen mit CAST Imaging (AWS-Workshop)
- AWS Marketplace: CAST-Bildgebung
- Alle CAST auf AWS-Ressourcen

Beurteilen Sie die Anwendungsbereitschaft für die Migration in die AWS-Cloud mithilfe von CAST Highlight

Erstellt von Greg Rivera (Cast Software)

Übersicht

CAST Highlight ist eine Software-as-a-Service-Lösung (SaaS) zur schnellen Analyse des Anwendungsportfolios. Dieses Muster beschreibt, wie CAST Highlight konfiguriert und verwendet wird, um die Cloud-Eignung benutzerdefinierter Softwareanwendungen im gesamten IT-Portfolio eines Unternehmens zu bewerten und die Modernisierung oder Migration zur Amazon Web Services (AWS) Cloud zu planen.

CAST Highlight generiert Einblicke in die Cloud-Bereitschaft einer Anwendung, identifiziert Codeblocker, die vor einer Migration entfernt werden müssen, schätzt den Aufwand zur Entfernung dieser Blocker und empfiehlt AWS-Services, die einzelne Anwendungen nach der Migration nutzen könnten.

Dieses Muster beschreibt das Verfahren zur Einrichtung und Verwendung von CAST Highlight, das aus fünf Schritten besteht: Einrichtung neuer Benutzer, Anwendungsmanagement, Kampagnenmanagement, Quellcode-Analyse und Ergebnisanalyse. Sie müssen alle Schritte im Abschnitt „Epics“ dieses Musters ausführen, um einen erfolgreichen Anwendungsscan und eine erfolgreiche Analyse sicherzustellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives CAST-Highlight-Konto mit Portfoliomanager-Berechtigungen.
- Mindestens 300 MB freier Festplattenspeicher und 4 GB Arbeitsspeicher auf Ihrem lokalen Computer, um den CAST Highlight Local Agent zu installieren.
- Microsoft Windows 8 oder höher.
- Der Quellcode Ihrer Anwendung muss in Textdateien gespeichert werden, auf die von dem Computer aus zugegriffen werden kann, auf dem der Local Agent installiert ist. Kein Quellcode verlässt die Räumlichkeiten und der gesamte Code wird lokal gescannt.

Architektur

Das folgende Diagramm veranschaulicht den Arbeitsablauf für die Verwendung von CAST Highlight.

Der Workflow besteht aus folgenden Schritten:

1. Melden Sie sich beim CAST Highlight-Portal an, laden Sie den Local Agent herunter und installieren Sie ihn auf Ihrem lokalen Computer. Amazon Simple Storage Service (Amazon S3) speichert das Local Agent-Installationspaket.
2. Scannen Sie Ihre Quellcodedateien und erstellen Sie eine Ergebnisdatei.
3.
> **Important**
>
> Laden Sie die Ergebnisdatei in das CAST Highlight-Portal hoch. : In der Ergebnisdatei ist kein Quellcode enthalten.

4. Beantworten Sie die Fragen der Umfrage für jede Anwendung, die Sie gescannt haben.
5. Sehen Sie sich die Dashboards und Berichte an, die im CAST Highlight-Portal verfügbar sind. Amazon Relational Database Service (Amazon RDS) speichert den Codescan, die Analyseergebnisse und die CAST Highlight-Softwaredaten.

Technologie-Stack

CAST Highlight unterstützt die folgenden Technologien zur Analyse der Eignung von Anwendungen für die Cloud:

- Java
- COBOL
- C#
- C++
- Clojure
- PHP
- JavaScript
- TypeScript
- Python
- Microsoft Transact-SQL

- VB.Net
- Kotlin
- Scala
- Swift

Automatisierung und Skalierung

- Ein CLI-Analyzer kann verwendet werden, um den CAST-Highlight-Analyseprozess zu automatisieren.

Tools

Für dieses Muster sind keine Tools erforderlich, wenn alle Voraussetzungen erfüllt sind. Sie können jedoch optionale Tools wie SCM-Dienstprogramme (Source Code Management), Codeextraktoren oder andere Tools zur Verwaltung Ihrer Quellcodedateien verwenden.

Epen

Neues Benutzer-Setup

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie Ihr CAST Highlight-Konto und wählen Sie Ihr Passwort.	Alle CAST Highlight-Benutzer zum ersten Mal erhalten eine E-Mail zur Kontoaktivierung. Folgen Sie dem Aktivieru ngslink, um Ihr CAST Highlight -Konto zu aktivieren, und geben Sie ein Passwort ein, um den Aktivierungsvorgang abzuschließen.	N/A
Melden Sie sich im CAST Highlight-Portal an.	Die CAST Highlight-Homepage erscheint, nachdem Sie Ihr neues Passwort eingegeben haben. Melden Sie sich mit Ihren	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Benutzeranmeldeinformationen beim CAST Highlight-Portal an.	

Application Management

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Bewerbungsdatensatz.	Navigieren Sie im CAST Highlight-Portal zur Registerkarte „Anwendung verwalten“ im Abschnitt „Portfolio verwalten“. Wählen Sie in der Kachel „Anwendungen“ oben auf dem Bildschirm die Option Hinzufügen aus.	N/A
Wählen Sie einen Namen für die Anwendung.	Geben Sie einen Namen für Ihre Anwendung ein und wählen Sie dann Speichern. Dieser Name wird für Ihren Anwendungsdatensatz in CAST Highlight verwendet.	N/A
Wiederholen Sie die Schritte für alle Anwendungen.	Wiederholen Sie diese Schritte für jede Anwendung, die Sie scannen möchten.	N/A

Verwaltung von Kampagnen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Kampagne.	CAST Highlight verwendet den Begriff „Kampagne“, um	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eine Reihe von Anwendung en zu beschreiben, die zu einem bestimmten Zeitpunkt analysiert werden. Navigieren Sie im CAST Highlight-Portal im Bereich Portfolio verwalten zum Tab Kampagnen verwalten. Wählen Sie Kampagne erstellen, um den Bildschirm zur Kampagnen erstellung aufzurufen.	
Geben Sie einen Namen ein und wählen Sie ein Abschluss datum für die Kampagne.	Geben Sie einen Namen für Ihre Kampagne ein und wählen Sie ein Abschluss datum. **Important** Mitwirkende können nach dem Schlusste rmin der Kampagne keine Ergebnisse der Anwendungsanalyse einreichen.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entscheiden Sie sich dafür, den Quellcode, die Antworten auf die Umfrage sowie den Bereich und den Anwendungsbereich mit einzubeziehen.	Wählen Sie eine oder mehrere der Standardumfragen aus, die verwendet werden, um die Quellcode-Analysedaten um qualitative Informationen zu erweitern. Die Umfragekategorien lauten: Auswirkungen auf den Geschäftsbetrieb, Softwarewartungsaufwand CloudReady, Anwendungseigenschaften und Umweltverträglichkeit. Wählen Sie die Domain und die Anwendungen aus, die während der Kampagne analysiert werden. **Important** Stellen Sie sicher, dass Sie alle Anwendungen, die Sie scannen möchten, im Bereich Anwendungen verwalten hinzufügen, bevor Sie mit der Kampagne beginnen.	N/A
Passen Sie die Startnachricht an.	Passen Sie die Startnachricht an, die per E-Mail an alle Mitwirkenden gesendet wird, die mit den Anwendungen in der Kampagne verknüpft sind.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starte die Kampagne.	Wählen Sie Abgeschlossen, um die Kampagne zu starten.	N/A

Analyse des Quellcodes

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den CAST Highlight Local Agent herunter.	Wählen Sie im CAST Highlight -Portal die Option Anwendungsscans und laden Sie den Local Agent auf Ihren lokalen Computer herunter.	N/A
Installieren Sie den Local Agent.	Starten Sie das Installationsprogramm CASTHighlight Setup.exe und folgen Sie den angezeigten Installationsanweisungen. Nachdem der Local Agent installiert wurde, können Sie Ihre Anwendungen analysieren.	N/A
Definieren Sie den Umfang des Local Agent-Codescans.	Die Codeanalyse wird auf Dateiebene durchgeführt und berücksichtigt nicht die logischen Verknüpfungen oder Abhängigkeiten zwischen Dateien. Alle Dateien werden als gleichwertig betrachtet und sind Teil der Anwendung. Um genaue und konsistente Ergebnisse zu erzielen, bereiten Sie Ihren Codescanbereich vor, indem Sie die	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	im Local Agent verfügbaren Funktionen zum Ausschlie ßen von Dateien oder Ordnern verwenden.	
Schließen Sie Open-Source-Pakete oder COTS-Pakete ein.	(Optional) Wenn Sie Open-Source-Pakete oder kommerzielle Pakete off-the-shelf (COTS) einbeziehen möchten, stellen Sie sicher, dass sie in den Ordnern enthalten sind, die Sie scannen möchten. In der Regel sind externe Bibliothe ken in einem Unterordner mit dem Namen „Drittanbieter“ oder ähnlichem gruppiert, und der Hauptcode befindet sich häufig im Dateiordner „src/ main“.	N/A
Schließt Testklassen aus.	Testklassen werden in der Regel von der Quellcode analyse ausgeschlossen, da sie im Allgemeinen nicht Teil der kompilierten Anwendung sind. Sie können sich jedoch bei Bedarf dafür entscheid en, sie in den Scan einzubezi ehen.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schließen Sie SCM-, Build- und Deployment-Ordner aus.	Um konsistentere Ergebnisse zu erzielen, sollten Sie vermeiden, SCM-, Build- oder Deployment-Ordner (z. B. .git- oder .svn-Dateien) in Ihren Scan aufzunehmen.	N/A
Fügen Sie Abhängigkeitsdateien hinzu.	Wenn Sie Einblicke in Frameworks und Abhängigkeiten wünschen, deren physische Dateien nicht Teil des Ordners sind, den Sie scannen, stellen Sie sicher, dass Sie die Abhängigkeitsdateien (wie pom.xml-, build.gradle-, package.json- oder .vcsproj-Dateien) einbeziehen.	N/A
Rufen Sie den Local Agent auf.	Führen Sie den Local Agent auf Ihrem lokalen Windows-Computer aus.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie den Ordner, der Ihren Quellcode enthält.	Wählen Sie den Ordner, der Ihren Quellcode enthält. Sie können mehrere Ordner hinzufügen, die vom Local Agent erkannt werden sollen. Obwohl der Local Agent die Quellensuche über Netzwerkp fade unterstützt, sollten Sie sicherstellen, dass sich die Quellordner auf Ihrem lokalen Computer befinden. **Important** Wir empfehlen , mehrere Scans durchzuführen, wenn sich mehr als 10.000 Dateien in Ihren Quellordnern befinden.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Dateierkennung.	Wählen Sie im Local Agent-Dashboard die Option Discover Files aus. Der Local Agent erkennt Dateien in Ihren Ordnern und Unterordnern und erkennt deren Technologien. Sie können die Suche jederzeit mit der Schaltfläche Abbrechen abbrechen. Nach Abschluss der Dateisuche listet der Local Agent die gefundenen Ordner und Dateien auf. In der Spalte Technologien werden die zugehörigen Technologien und die Anzahl der Dateien angezeigt. In der Spalte Pfad wird der Speicherort der Ordner und Dateien angezeigt.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verfeinern Sie die Konfiguration für den Quellcode-Scan.	(Optional) Um den Local Agent-Scan zu verfeinern, können Sie eine oder mehrere Technologien für einen bestimmten Ordner oder eine bestimmte Datei deaktivieren. Wenn alle Technologien deaktiviert sind, wird Ihr Ordner oder Ihre Datei vom Scanbereich ausgeschlossen. Um Technologien zu deaktivieren, wählen Sie das gelbe Etikett der Technologie aus, die Sie deaktivieren möchten. Sie können auch das Filtersymbol auswählen, wenn Sie den Mauszeiger über eine Datei oder einen Ordner bewegen, um eine Technologie einer bestimmten Datei oder einem bestimmten Ordner zuzuordnen. Diese Einstellungen werden gespeichert und beschleunigen den Erkennungsprozess für den Ordner oder die Datei.	N/A
Starten Sie den Quellcode scan.	Nachdem Sie Ihren Scan konfiguriert haben, wählen Sie „Dateien scannen“, um den Scanvorgang zu starten.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Suchen Sie nach grünen oder grauen Etiketten.	Nach Abschluss des Quellcodescans wird auf Ordner- und Dateiebene ein Statuslabel angezeigt. Ein grünes Etikett bedeutet, dass die Dateien mit der zugehörigen Technologie korrekt gescannt wurden. Ein graues Etikett bedeutet, dass Dateien nicht gescannt wurden und ausgeschlossen sind. Der Grund für ihren Ausschluss wird angezeigt , wenn Sie den Mauszeiger über die Bezeichnung jeder Datei bewegen. Mögliche Gründe für den Ausschluss von Dateien sind Binärdateien, unlesbare Dateien, fehlende Dateien, externe Bibliothek, kodierte Dateien, generierte Dateien, Syntaxfehler, Inhalt, der nicht in der erwarteten Sprache verfasst ist, Code, der nicht genügend Analysekr iterien erfüllt, Dateien, die die Größenbeschränkung (10 MB) überschreiten, Timeout-Probleme oder die Nichtverf ügbarkeit des Analyzers.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Scankonfiguration und scannen Sie den Code erneut.	(Optional) Sie können Ihre Einstellungen für die Scankonfiguration ändern und Dateien scannen wählen, um die Dateien erneut zu scannen.	N/A
Bestätigen Sie die Scanergebnisse.	Wählen Sie Ergebnisse bestätigen, wenn die Scanergebnisse Ihren Anforderungen entsprechen.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich die Frameworks und Softwarebibliotheken an, die vom Local Agent gefunden wurden.	Sehen Sie sich die Frameworks und Softwarebibliotheken an, die von Ihren Anwendungen verwendet oder auf die verwiesen wird und die der Local Agent beim Codescan entdeckt hat. Sie können Elemente aus diesen Listen beibehalten oder ignorieren, indem Sie die entsprechende Umschalttaste wählen. Wählen Sie Abhängigkeiten bestätigen, um fortzufahren. **Important** Wenn ein Framework ausgeschaltet ist, ist es nicht im CAST Highlight-Portal aufgeführt oder an Ihre Anwendung angehängt.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Speichern Sie die Ergebnisse des Codescans.	Der Local Agent zeigt eine nach Technologie gruppiert e Zusammenfassung Ihrer Codescan-Ergebnisse an. Wählen Sie Speichern und geben Sie den Ordner an, in dem die Ergebnisse gespeiche rt werden sollen. Der Local Agent generiert pro Scan eine ZIP-Datei, die alle Analyseer gebnisse enthält. Abhängig von der Anzahl der unterschiedlichen Technolog ien und Stammquellordnern generiert der Local Agent automatisch eine oder mehrere .csv-Dateien mit der Benennungsstruktur FolderName.technology.date. csv.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Ergebnisse des Codescans in das CAST Highlight-Portal hoch.	Wählen Sie im CAST Highlight-Portal im Abschnitt Anwendungsscans die Anwendungen aus, die Sie analysiert haben. Wählen Sie Ergebnisse hochladen und wählen Sie die CSV-Dateien aus. Sie können die CSV-Dateien auch einzeln hochladen. Nachdem jede Datei hochgeladen wurde, erscheint eine Aufzeichnung des Uploads auf Ihrem Bildschirm.	N/A
Löschen Sie die Dateien mit den Analyseergebnissen, falls erforderlich.	(Optional) Eine Analyseergebnisdatei kann jederzeit während des Upload-Vorgangs gelöscht werden, indem Sie auf das Papierkorbsymbol klicken. **Important** Nur Benutzer mit Portfoliomanager-Rechten oder der Mitwirkende, der die Ergebnisse hochgeladen hat, können die Ergebnisse löschen.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beantworten Sie die Bewerbungsumfrage.	Bei Anwendungen, für die eine Umfrage erforderlich ist, wird eine Umfrage-Schaltfläche angezeigt. Wählen Sie „Umfrage“, beantworten Sie die Fragen für jeden Abschnitt der Umfrage und wählen Sie „Senden“, wenn Sie fertig sind. Der Fortschritt Ihrer Umfrage wird oben auf dem Bildschirm angezeigt. Sie können Ihre Ergebnisse einreichen, nachdem alle Pflichtangaben übermittelt wurden. Sie können die Daten in der CAST Highlight-Instanz Ihrer Organisation jedoch anreichern, indem Sie alle Fragen beantworten.	N/A
Senden Sie die Ergebnisse des Codescans.	Nachdem Sie alle CSV-Ergebnisdateien für die Anwendung hochgeladen und die Fragen zur Umfrage beantwortet haben, wählen Sie im Abschnitt Anwendungsscans die Option Senden aus. Dieser Schritt ist erforderlich, um den Vorgang abzuschließen und sicherzustellen, dass die Ergebnisse im CAST Highlight-Portal verfügbar sind.	N/A

Analyse der Ergebnisse

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Startseite des CAST Highlight-Portals anzeigen.	Die Startseite des CAST Highlight-Portals enthält Kacheln mit allgemeinen Informationen zu Ihrem Anwendungsportfolio, z. B. zum Zustand der Software CloudReady, und Open-Sour ce-Sicherheitsbewertungen für Ihr gesamtes Portfolio . Die Homepage enthält auch die Anzahl der integrier ten Anwendungen. Weitere Informationen zu den Definitio nen und der Messmethodik von CAST Highlight finden Sie unter CAST Highlight — Metriken und Methodik (PowerPoint Microsoft-Präsentation).	N/A
Sehen Sie sich das CloudReady Dashboard an.	Wählen Sie die CloudRead y Kachel aus, um das CloudReady Dashboard zu öffnen. Dies ist das wichtigste Dashboard auf Portfolioebene zur Bewertung der Cloud-Eig nung Ihrer Anwendungen. Es hilft Ihnen bei der Planung und Entwicklung einer Portfolio-Roadmap für Ihre Cloud-Mig ration	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich das Dashboard von Portfolio Advisor for Cloud an.	Das Dashboard von Portfolio Advisor for Cloud unterteilt Anwendungen automatisch in empfohlene Migrationskategorien. Die Segmentierung basiert auf den technischen Eigenschaften der einzelnen Anwendungen. Zu den Faktoren gehören die Quellcode-Analyse (Cloud-Bereitschaft, Software-Resilienz und mehr) und die Auswirkungen auf das Geschäft, die sich aus der Umfrage ergeben. Wählen Sie oben rechts Compute aus, um die ersten Segmentierungsempfehlungen zu generieren. Die Blasen in den Diagrammen oben im Dashboard stehen für jede Anwendung im Portfolio, geordnet nach der empfohlenen Segmentierung. Jede Anwendung ist außerdem in einer Datentabelle unter den Diagrammen aufgeführt, einschließlich relevanter Kennzahlen für jede Anwendung. Zu den möglichen Segmenten, die empfohlen werden, gehören:	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Rehost — Eine Empfehlung, die Infrastrukturkonfiguration der Anwendung zu ändern, um sie mithilfe einer Infrastructure-as-a-Service (IaaS) -Lösung in die Cloud zu verlagern. • Refactor — Eine Empfehlung, geringfügige Änderungen am Anwendungscode vorzunehmen, ohne die Architektur oder Funktionalität zu ändern, sodass er mithilfe einer Container-as-a-Service- (CaaS) - oder Platform-as-a-Service- (PaaS) -Lösung migriert werden kann. • Rearchitect — Eine Empfehlung, den Anwendungscode drastisch zu ändern, um den Zustand der Anwendung zu verbessern und sie mithilfe einer PaaS-Lösung auf die Migration vorzubereiten oder sie mithilfe einer Function-as-a-Service (FaaS) -Lösung als serverlose Anwendung bereitzustellen. • Rebuild — Eine Empfehlung, den Code der Anwendung zu verwerfen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und ihn mithilfe einer PaaS-Lösung erneut in der Cloud zu entwickeln oder ihn mithilfe einer FaaS-Lösung erneut als serverlose Anwendung zu entwickeln. • Außerbetriebnahme — Eine Empfehlung, die Anwendung ganz zu verwerfen oder sie möglicherweise durch eine kommerzielle SaaS-Alternative (Software as a Service) zu ersetzen.	
Ändern Sie die Segmentierungsempfehlungen.	In einigen Fällen können Sie sich dafür entscheiden, das von CAST Highlight empfohlene Segment zu ändern. Sie können dies tun, indem Sie in der Datentabelle nach der Anwendung suchen und in der Dropdownliste neben dem Anwendungsnamen ein anderes Segment auswählen. Wählen Sie dann oben rechts Speichern, um Ihre Änderungen zu speichern. Sie können diese Daten auch jederzeit exportieren, indem Sie oben rechts auf Exportieren klicken.	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie eine zu analysierende Anwendung aus.	Wählen Sie im Dashboard von Portfolio Advisor for Cloud eine Anwendungsblase aus, um diese Anwendung zu analysieren. Wählen Sie in der Tabelle hinter dem Blasendiagramm den Namen der Anwendung aus, um mit der eingehenderen Analyse zu beginnen. Für die Analyse einzelner Anwendungen stehen verschiedene Dashboards zur Verfügung, z. B. Code Insights (Softwarezustandsmuster), Trends und Software Composition (Open-Source-Risiken).	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie die CloudReady Ergebnisse einer einzelnen Anwendung.	Wählen Sie die CloudRead yRegisterkarte, auf der die CloudReady Gesamtpunktzahl der Anwendung angezeigt wird. Diese Punktzahl ist ein gewichteter Durchschn itt, der auf einer Kombinati on aus den Antworten der CloudReady Umfrage und dem CloudReady Codescan basiert. Die Antworten auf die Fragen der Umfrage werden in der Tabelle unter den Kacheln angezeigt. Wählen Sie CloudReady Codescan, um die Ergebniss e des Codescans anzuzeige n. Es gibt eine Liste von CloudReady Mustern, nach denen der Anwendungscode gescannt wurde. Diese Liste enthält die folgenden Spalten: • Cloud-Anforderung ist das spezifische Codemuster. • Technologie ist die Programmiersprache des Musters. „Auswirkung“ ist die Auswirkung des Musters auf die Anwendung (C = Code, F = Framework, A = Architektur). • Kritikalität gibt an, wie wichtig es ist, dieses	N/A

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Muster vor der Migration anzugehen. • Beitrag gibt an, wie dieses Muster zur CloudReady Gesamtpunktzahl beiträgt. Wenn das Muster grün ist, ist es ein Booster und erhöht die CloudRead y Punktzahl. Wenn das Muster rot ist, ist es ein Blocker und verringert die CloudReady Punktzahl. Wenn das Muster keine Farbe hat, handelt es sich um einen Blocker, der nicht erkannt wurde und die CloudReady Punktzahl erhöht. • Straßensperren sind die Anzahl der einzelnen Vorkommen eines Blockermusters. Wählen Sie die Roadblock-Nummer, um eine Liste der Quellcode dateien anzuzeigen, in denen das Muster erkannt wurde. • Est. Der Aufwand ist eine Schätzung der Anzahl der Tage, die benötigt werden, um die Hindernisse in jeder Reihe zu beseitigen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Exportieren Sie Daten nach Microsoft Excel.	(Optional) Wählen Sie Nach Excel exportieren, um die Daten zur weiteren Analyse zu exportieren. Die Ergebnisd aten der Anwendungsanalyse können verwendet werden, um die Cloud-Eignung einer Anwendung weiter zu analysieren und festzuste llen, welcher Code vor einer Migration aktualisiert werden muss.	N/A
Empfehlungen anzeigen.	Wählen Sie neben CloudRead y Codescan die Option Empfehlungen aus, um den Bildschirm mit den Empfehlun gen für Cloud-Services aufzurufen. Dadurch werden AWS-Services identifiziert, die die Anwendung aufgrund ihrer Eigenschaften übernehmen könnte. Wiederholen Sie diesen Schritt, um Empfehlungen für alle von Ihnen analysierten Anwendungen anzuzeigen.	N/A

Zugehörige Ressourcen

Kampagnenmanagement

- CAST Highlight Foundation-Zertifizierungsschulung, Abschnitt 3: Portfoliokonfiguration (Video)

Analyse des Quellcodes

- CAST Highlight Foundation-Zertifizierungsschulung, Abschnitt 4: Anwendungsanalyse (Video)

Sonstige Ressourcen

- CAST-Highlight im AWS Marketplace
- AWS und CAST: Beschleunigen Sie die Anwendungsmodernisierung
- CAST-Highlight — Dokumentation, Produkt-Tutorials und Tools von Drittanbietern
- CAST-Highlight — Cloud-Readiness-Produktdemo (Video)
- Modernisierung des Anwendungsportfolios mit CAST Highlight (AWS-Workshop)

Automatisches Archivieren von Elementen in Amazon S3 mithilfe von DynamoDB TTL

Erstellt von Tabby Ward (AWS)

Übersicht

Dieses Muster enthält Schritte zum Entfernen älterer Daten aus einer Amazon DynamoDB-Tabelle und zum Archivieren in einem Amazon Simple Storage Service (Amazon S3) -Bucket auf Amazon Web Services (AWS), ohne eine Serverflotte verwalten zu müssen.

Dieses Muster verwendet Amazon DynamoDB Time to Live (TTL), um alte Artikel automatisch zu löschen, und Amazon DynamoDB DynamoDB-Streams, um die TTL-abgelaufenen Artikel zu erfassen. Anschließend verbindet es DynamoDB Streams mit AWS Lambda, das den Code ausführt, ohne Server bereitzustellen oder zu verwalten.

Wenn dem DynamoDB-Stream neue Artikel hinzugefügt werden, wird die Lambda-Funktion initiiert und schreibt die Daten in einen Amazon Data Firehose-Lieferstream. Firehose bietet eine einfache, vollständig verwaltete Lösung zum Laden der Daten als Archiv in Amazon S3.

DynamoDB wird häufig zum Speichern von Zeitreihendaten verwendet, z. B. Click-Stream-Daten von Webseiten oder IoT-Daten (Internet of Things) von Sensoren und angeschlossenen Geräten. Anstatt Elemente zu löschen, auf die weniger häufig zugegriffen wird, möchten viele Kunden sie zu Prüfungszwecken archivieren. TTL vereinfacht diese Archivierung, indem Elemente auf der Grundlage des Timestamp-Attributs automatisch gelöscht werden.

Durch TTL gelöschte Elemente können in DynamoDB Streams identifiziert werden, wodurch eine zeitlich geordnete Abfolge von Änderungen auf Elementebene erfasst und die Reihenfolge bis zu 24 Stunden in einem Protokoll gespeichert wird. Diese Daten können von einer Lambda-Funktion genutzt und in einem Amazon S3 S3-Bucket archiviert werden, um die Speicherkosten zu senken. Um die Kosten weiter zu senken, können Amazon S3-Lebenszyklusregeln erstellt werden, um die Daten (sobald sie erstellt wurden) automatisch in kostengünstigste Speicherklassen wie S3 Glacier Instant Retrieval oder S3 Glacier Flexible Retrieval oder Amazon S3 Glacier Deep Archive für die Langzeitspeicherung zu übertragen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS Command Line Interface (AWS CLI) 1.7 oder höher, installiert und konfiguriert auf macOS, Linux oder Windows.
- Python 3.7 oder höher.
- Boto3, installiert und konfiguriert. Wenn Boto3 noch nicht installiert ist, führen Sie den `python -m pip install boto3` Befehl aus, um es zu installieren.

Architektur

Technologie-Stack

- Amazon-DynamoDB
- Amazon DynamoDB Streams
- Amazon Data Firehose
- AWS Lambda
- Amazon S3

1. Elemente werden per TTL gelöscht.
2. Der DynamoDB-Stream-Trigger ruft die Lambda-Stream-Prozessorfunktion auf.
3. Die Lambda-Funktion stellt Datensätze im Firehose-Lieferstream im Batch-Format bereit.
4. Datensätze werden im S3-Bucket archiviert.

Tools

- AWS CLI — Die AWS-Befehlszeilenschnittstelle (AWS CLI) ist ein einheitliches Tool zur Verwaltung Ihrer AWS-Services.
- Amazon DynamoDB — Amazon DynamoDB ist eine Schlüsselwert- und Dokumentendatenbank, die in jeder Größenordnung eine Leistung im einstelligen Millisekundenbereich bietet.
- Amazon DynamoDB Time to Live (TTL) — Amazon DynamoDB TTL unterstützt Sie bei der Definition eines Zeitstempels pro Artikel, um zu bestimmen, wann ein Artikel nicht mehr benötigt wird.

- Amazon DynamoDB Streams — Amazon DynamoDB Streams erfasst eine zeitlich geordnete Abfolge von Änderungen auf Elementebene in jeder DynamoDB-Tabelle und speichert diese Informationen bis zu 24 Stunden in einem Protokoll.
- Amazon Data Firehose — Amazon Data Firehose ist der einfachste Weg, Streaming-Daten zuverlässig in Data Lakes, Datenspeicher und Analysedienste zu laden.
- AWS Lambda — AWS Lambda führt Code aus, ohne dass Server bereitgestellt oder verwaltet werden müssen. Sie zahlen nur für die tatsächlich aufgewendete Zeit.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice, der branchenführende Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet.

Code

Der Code für dieses Muster ist im Repository GitHub Archivieren von Elementen in S3 mithilfe des DynamoDB-TTL-Repositorys verfügbar.

Epen

Richten Sie eine DynamoDB-Tabelle, TTL und einen DynamoDB-Stream ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine DynamoDB-Tabelle.	Verwenden Sie die AWS-CLI, um in DynamoDB eine Tabelle mit dem Namen zu erstellen. `Reservation` Wählen Sie Random Read Capacity Unit (RCU) und WCU (WCU) und geben Sie Ihrer Tabelle zwei Attribute: und. `ReservationID` `ReservationDate` `aws dynamodb create-table \ --table-name Reservation \ --attribute-definitions Attribute Name=ReservationID`	Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>,AttributeType=S
	 AttributeName=Rese
	rvationDate,Attrib
	uteType=N \
	--key-schema Attribute
	Name=ReservationID
	,KeyType=HASH
	 AttributeName=Rese
	rvationDate,KeyTyp
	e=RANGE \
	--provisioned-th
	roughput ReadCapac
	ityUnits=100,Write
	CapacityUnits=100</pre>
	`ReservationDate` ist ein Epochenzeitstempel, der verwendet wird, um TTL einzuschalten.	

Schalten Sie DynamoDB TTL ein.	Verwenden Sie die AWS-CLI, um DynamoDB-TTL für das Attribut zu aktivieren. `ReservationDate`
	<pre>aws dynamodb update-ti
	me-to-live \
	--table-name Reservati
	on\
	  --time-to-live-spe
	cification Enabled=t
	rue,AttributeName=
	ReservationDate</pre>
		Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schalten Sie einen DynamoDB-Stream ein.	Verwenden Sie die AWS-CLI, um mithilfe des Stream-Typs einen DynamoDB-Stream für die `Reservation` Tabelle zu aktivieren. `NEW_AND_OLD_IMAGES` `aws dynamodb update-table \ --table-name Reservation \ --stream-specification StreamEnabled=true,StreamViewType=NEW_AND_OLD_IMAGES` Dieser Stream enthält Datensätze für neue Elemente, aktualisierte Elemente, gelöschte Elemente und Elemente, die per TTL gelöscht wurden. Die Datensätze für Elemente, die per TTL gelöscht wurden, enthalten ein zusätzliches Metadatenattribut, um sie von manuell gelöschten Elementen zu unterscheiden. Das `userIdentity` Feld für TTL-Löschungen gibt an, dass der DynamoDB-Dienst die Löschaktion ausgeführt hat.	Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	In diesem Muster werden nur die durch TTL gelöschte n Elemente archiviert. Sie könnten aber auch nur die Datensätze archivieren, bei denen `eventName` ist `REMOVE` und was enthält. `userIdentity principalId dynamodb.amazonaws.com`	

Erstellen und konfigurieren Sie einen S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Verwenden Sie die AWS-CLI, um einen Ziel-S3-Bucket in Ihrer AWS-Region zu erstellen . `us-east-1` Ersetzen Sie ihn durch Ihre Region und amzn-s3- demo-destination-b ucket durch den Namen Ihres Buckets. `aws s3api create-bucket \ --bucket amzn-s3-demo-destination-bucket \ --region us-east-1` Stellen Sie sicher, dass der Name Ihres S3-Buckets weltweit eindeutig ist, da der Namespace von allen AWS-	Cloud-Architekt, App-Entwi ckler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Konten gemeinsam genutzt wird.	
Erstellen Sie eine 30-Tage-Lebenszyklusrichtlinie für den S3-Bucket.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon S3 S3-Konsole. 2. Wählen Sie den S3-Bucket aus, der die Daten von Firehose enthält. 3. Wählen Sie im S3-Bucket die Registerkarte Management und dann Lebenszyklusregel hinzufügen aus. 4. Geben Sie im Dialogfeld „Lebenszyklusregel“ einen Namen für Ihre Regel ein und konfigurieren Sie eine 30-Tage-Lebenszyklusregel für Ihren Bucket.	Cloud-Architekt, App-Entwickler

Erstellen Sie einen Firehose-Lieferstream

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und konfigurieren Sie einen Firehose-Lieferstream.	Laden Sie das `CreateFireHoseToS3.py` Codebeispiel aus dem GitHub Repository herunter und bearbeiten Sie es. Dieser Code ist in Python geschrieben und zeigt Ihnen,	Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wie Sie einen Firehose-Lieferstream und eine AWS Identity and Access Management (IAM) -Rolle erstellen. Die IAM-Rolle wird über eine Richtlinie verfügen, die von Firehose verwendet werden kann, um in den Ziel-S3-Bucket zu schreiben. Verwenden Sie den folgenden Befehl und die folgenden Befehlszeilenargumente, um das Skript auszuführen. Argument 1=<Your_S3_bucket_ARN> , das ist der Amazon-Ressourcenname (ARN) für den Bucket, den Sie zuvor erstellt haben Argument 2= Ihr Firehose-Name (Dieser Pilot verwendet `firehose_to_s3_stream` .) Argument 3= Ihr IAM-Rollenname (dieser Pilot verwendet `firehose_to_s3` .) `python CreateFirehoseToS3.py <Your_S3_Bucket_ARN> firehose_to_s3_stream firehose_to_s3`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wenn die angegebene IAM-Rolle nicht existiert, erstellt das Skript eine Rolle annehmen mit einer Richtlini e für vertrauenswürdige Beziehungen sowie eine Richtlinie, die ausreiche nde Amazon S3 S3-Berech tigungen gewährt. Beispiele für diese Richtlinien finden Sie im Abschnitt Zusätzliche Informationen.	
Überprüfen Sie den Firehose-Lieferstream.	Beschreiben Sie den Firehose-Lieferstream mithilfe der AWS-CLI, um zu überprüfen, ob der Lieferstr eam erfolgreich erstellt wurde. `aws firehose describe-delivery-stream --delivery-stream-name firehose_to_s3_str eam`	Cloud-Architekt, App-Entwi ckler

Erstellen Sie eine Lambda-Funktion zur Verarbeitung des Firehose-Lieferdatenstroms

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Vertrauen srichtlinie für die Lambda-Fu nktion.	Erstellen Sie eine Vertrauen srichtliniendatei mit den folgenden Informationen. `{`	Cloud-Architekt, App-Entwi ckler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, "Action": "sts:AssumeRole" }] }</pre> Dadurch erhält Ihre Funktion die Erlaubnis, auf AWS-Ressourcen zuzugreifen.	
Erstellen Sie eine Ausführungsrolle für die Lambda-Funktion.	Führen Sie den folgenden Code aus, um die Ausführungsrolle zu erstellen. <pre>aws iam create-role --role-name lambda-ex --assume-role-policy-document file://TrustPolicy.json</pre>	Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie der Rolle eine Berechtigung hinzu.	Verwenden Sie den `attach-policy-to-role` Befehl, um der Rolle eine Berechtigung hinzuzufügen.
	`aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	`aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole`
	`aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`
	`aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/IAMFullAccess`
		Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine Lambda-Funktion.	Komprimieren Sie die `LambdaStreamProcessor.py` Datei aus dem Code-Repository, indem Sie den folgenden Befehl ausführen.
	`zip function.zip LambdaStreamProcessor.py`
	Wenn Sie die Lambda-Funktion erstellen, benötigen Sie den ARN für die Lambda-Ausführungsrolle. Führen Sie den folgenden Code aus, um den ARN abzurufen.
	`aws iam get-role \ --role-name lambda-ex`
	Führen Sie den folgenden Code aus, um die Lambda-Funktion zu erstellen.
	`# Review the environment variables and replace them with your values.`
	`aws lambda create-function --function-name LambdaStreamProcessor \ --zip-file fileb://function.zip --handler LambdaStreamProces`
		Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`sor.handler --runtime python3.8 \ --role {Your Lamda Execution Role ARN}\ --environment Variables="{firehose_name=firehose_to_s3_stream,bucket_arn = <Your_S3_bucket_ARN>,iam_role_name = firehose_to_s3, batch_size=400}"`	
Konfigurieren Sie den Lambda-Funktionstrigger.	Verwenden Sie die AWS-CLI, um den Trigger (DynamoDB Streams) zu konfigurieren, der die Lambda-Funktion aufruft. Die Batchgröße von 400 soll verhindern, dass Lambda-Parallelitätsprobleme auftreten. `aws lambda create-event-source-mapping --function-name LambdaStreamProcessor \ --batch-size 400 --starting-position LATEST \ --event-source-arn <Your Latest Stream ARN From DynamoDB Console>`	Cloud-Architekt, App-Entwickler

Testen Sie die Funktionalität

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Artikel mit abgelaufenen Zeitstempeln zur Reservierungstabelle hinzu.	Um die Funktionalität zu testen, fügen Sie der Tabelle Artikel mit abgelaufenen Epochenzeitstempeln hinzu. `Reservation` TTL löscht automatisch Elemente auf der Grundlage des Zeitstempels. Die Lambda-Funktion wird bei DynamoDB-Stream-Aktivitäten ausgelöst und filtert das Ereignis, um `REMOVE` Aktivitäten oder gelöschte Elemente zu identifizieren. Anschließend werden Datensätze im Batch-Format in Firehose Firehose-Lieferstream eingefügt. Der Firehose-Lieferstream überträgt Artikel mit dem `firehosetos3example/year=current year/month=current month/day=current day/hour=current hour/` Präfix an einen S3-Ziel-Bucket. **Important** Um den Datenabruf zu optimieren, konfiguri eren Sie Amazon S3 mit den `Prefix` und`ErrorOutp`	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`utPrefix` , die im Abschnitt Zusätzliche Informationen detaillie rt beschrieben werden.	

Säubere die Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Alle Ressourcen löschen.	Löschen Sie alle Ressource n, um sicherzustellen, dass Ihnen keine Dienste in Rechnung gestellt werden, die Sie nicht nutzen.	Cloud-Architekt, App-Entwi ckler

Zugehörige Ressourcen

- Verwalten Ihres Speicher-Lebenszyklus
- Amazon S3 S3-Speicherklassen
- Dokumentation zum AWS-SDK SDK for Python (Boto3)

Zusätzliche Informationen

Einen Firehose-Lieferstream erstellen und konfigurieren — Richtlinienbeispiele

Beispieldokument Firehose Firehose-Richtlinie für vertrauenswürdige Beziehungen

```
firehose_assume_role = {
        'Version': '2012-10-17',
        'Statement': [
            {
                'Sid': '',
                'Effect': 'Allow',
                'Principal': {
```

```
                    'Service': 'firehose.amazonaws.com'
                },
                'Action': 'sts:AssumeRole'
            }
        ]
    }
```

Beispiel für eine S3-Berechtigungsrichtlinie

```
s3_access = {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "",
                "Effect": "Allow",
                "Action": [
                    "s3:AbortMultipartUpload",
                    "s3:GetBucketLocation",
                    "s3:GetObject",
                    "s3:ListBucket",
                    "s3:ListBucketMultipartUploads",
                    "s3:PutObject"
                ],
                "Resource": [
                    "{your s3_bucket ARN}/*",
                    "{Your s3 bucket ARN}"
                ]
            }
        ]
    }
```

Testen Sie die Funktionalität — Amazon S3 S3-Konfiguration

Die Amazon S3 S3-Konfiguration mit den folgenden Optionen `Prefix` wurde ausgewählt, um den Datenabruf zu optimieren. `ErrorOutputPrefix`

prefix

```
firehosetos3example/year=! {timestamp: yyyy}/month=! {timestamp:MM}/day=!
 {timestamp:dd}/hour=!{timestamp:HH}/
```

Firehose erstellt zunächst einen Basisordner, der `firehosetos3example` direkt unter dem S3-Bucket aufgerufen wird. Anschließend werden die Ausdrücke`!{timestamp:yyyy}`,`!{timestamp:MM}`, und `!{timestamp:HH}` nach Jahr`!{timestamp:dd}`, Monat, Tag und Stunde im DateTimeFormatterJava-Format ausgewertet.

Ein ungefährer Ankunftszeitstempel von 1604683577 in der Unix-Epochenzeit ergibt beispielsweise,, und. `year=2020` `month=11` `day=06` `hour=05` Daher wird der Standort in Amazon S3, an den die Datensätze geliefert werden, ausgewertet. `firehosetos3example/year=2020/month=11/day=06/hour=05/`

ErrorOutputPrefix

```
firehosetos3erroroutputbase/!{firehose:random-string}/!{firehose:error-output-type}/!{timestamp:yyyy/MM/dd}/
```

Die `ErrorOutputPrefix` Ergebnisse werden in einem Basisordner angezeigt, der `firehosetos3erroroutputbase` direkt unter dem S3-Bucket aufgerufen wird. Der Ausdruck `!{firehose:random-string}` ergibt eine zufällige 11-stellige Zeichenfolge wie. `ztWxkdg3Thg` Der Standort für ein Amazon S3 S3-Objekt, an das fehlerhafte Datensätze übermittelt werden, könnte ausgewertet werden`firehosetos3erroroutputbase/ztWxkdg3Thg/processing-failed/2020/11/06/`.

Erstellen Sie eine serverlose Architektur mit mehreren Mandanten in Amazon Service OpenSearch

Erstellt von Tabby Ward (AWS) und Nisha Gambhir (AWS)

Übersicht

Amazon OpenSearch Service ist ein verwalteter Service, der die Bereitstellung, den Betrieb und die Skalierung von Elasticsearch, einer beliebten Open-Source-Such- und Analyse-Engine, vereinfacht. OpenSearch Der Service bietet eine Freitextsuche sowie die Erfassung und das Dashboarding von Streaming-Daten wie Logs und Metriken nahezu in Echtzeit.

Anbieter von Software as a Service (SaaS) nutzen OpenSearch Service häufig, um eine Vielzahl von Anwendungsfällen abzudecken, z. B. um Kundeninformationen auf skalierbare und sichere Weise zu gewinnen und gleichzeitig Komplexität und Ausfallzeiten zu reduzieren.

Die Verwendung von OpenSearch Service in einer Umgebung mit mehreren Mandanten bringt eine Reihe von Überlegungen mit sich, die sich auf die Partitionierung, Isolierung, Bereitstellung und Verwaltung Ihrer SaaS-Lösung auswirken. SaaS-Anbieter müssen überlegen, wie sie ihre Elasticsearch-Cluster bei sich ständig ändernden Workloads effektiv skalieren können. Sie müssen auch berücksichtigen, wie sich Stufenbildung und laute Nachbarschaftsbedingungen auf ihr Partitionierungsmodell auswirken könnten.

In diesem Muster werden die Modelle untersucht, die zur Darstellung und Isolierung von Mandantendaten mit Elasticsearch-Konstrukten verwendet werden. Darüber hinaus konzentriert sich das Muster auf eine einfache serverlose Referenzarchitektur als Beispiel, um die Indizierung und Suche mithilfe von OpenSearch Service in einer Umgebung mit mehreren Mandanten zu demonstrieren. Es implementiert das Pool-Datenpartitionierungsmodell, das denselben Index für alle Mandanten verwendet und gleichzeitig die Datenisolierung eines Mandanten gewährleistet. Dieses Muster verwendet die folgenden AWS Dienste: Amazon API Gateway AWS Lambda, Amazon Simple Storage Service (Amazon S3) und OpenSearch Service.

Weitere Informationen zum Poolmodell und anderen Datenpartitionierungsmodellen finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- AWS Command Line Interface (AWS CLI) Version 2.x, installiert und konfiguriert auf macOS, Linux oder Windows
- Python-Version 3.9
- pip3 — Der Python-Quellcode wird als ZIP-Datei bereitgestellt, die in einer Lambda-Funktion bereitgestellt wird. Wenn Sie den Code lokal verwenden oder anpassen möchten, gehen Sie wie folgt vor, um den Quellcode zu entwickeln und neu zu kompilieren:
  1. Generieren Sie die `requirements.txt` Datei, indem Sie den folgenden Befehl im selben Verzeichnis wie die Python-Skripte ausführen: `pip3 freeze > requirements.txt`
  2. Installieren Sie die Abhängigkeiten: `pip3 install -r requirements.txt`

Einschränkungen

- Dieser Code läuft in Python und unterstützt derzeit keine anderen Programmiersprachen.
- Die Beispielanwendung bietet keine AWS regionsübergreifende Unterstützung oder Unterstützung für Disaster Recovery (DR).
- Dieses Muster dient nur zu Demonstrationszwecken. Es ist nicht für die Verwendung in einer Produktionsumgebung vorgesehen.

Architektur

Das folgende Diagramm veranschaulicht die allgemeine Architektur dieses Musters. Die Architektur umfasst Folgendes:

- Lambda zum Indizieren und Abfragen des Inhalts
- OpenSearch Dienst zur Durchführung der Suche
- API Gateway zur Bereitstellung einer API-Interaktion mit dem Benutzer
- Amazon S3 zum Speichern von Rohdaten (nicht indexiert)
- Amazon CloudWatch zur Überwachung von Protokollen
- AWS Identity and Access Management (IAM), um Mandantenrollen und Richtlinien zu erstellen

Automatisierung und Skalierung

Der Einfachheit halber wird das Muster für AWS CLI die Bereitstellung der Infrastruktur und für die Bereitstellung des Beispielcodes verwendet. Sie können eine AWS CloudFormation Vorlage oder AWS Cloud Development Kit (AWS CDK) Skripts erstellen, um das Muster zu automatisieren.

Tools

AWS-Services

- AWS CLIist ein einheitliches Tool zur Verwaltung AWS-Services von Ressourcen mithilfe von Befehlen in Ihrer Befehlszeilen-Shell.
- Lambda ist ein Rechendienst, mit dem Sie Code ausführen können, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- API Gateway dient AWS-Service zum Erstellen, Veröffentlichen, Verwalten, Überwachen und Sichern von REST, HTTP und WebSocket APIs in jeder Größenordnung.
- Amazon S3 ist ein Objektspeicherservice, mit dem Sie jederzeit und von überall im Internet eine beliebige Menge an Informationen speichern und abrufen können.
- OpenSearch Service ist ein vollständig verwalteter Service, der es Ihnen leicht macht, Elasticsearch kostengünstig und skalierbar bereitzustellen, zu sichern und auszuführen.

Code

Der Anhang enthält Beispieldateien für dieses Muster. Dazu zählen:

- `index_lambda_package.zip`— Die Lambda-Funktion für die Indizierung von Daten im OpenSearch Service mithilfe des Poolmodells.
- `search_lambda_package.zip`— Die Lambda-Funktion für die Suche nach Daten im OpenSearch Service.
- `Tenant-1-data`— Beispiel für Rohdaten (nicht indexiert) für Tenant-1.
- `Tenant-2-data`— Stichprobe von Rohdaten (nicht indexiert) für Tenant-2.

> **Important**
>
> Die Geschichten in diesem Muster enthalten AWS CLI Befehlsbeispiele, die für Unix, Linux und macOS formatiert sind. Ersetzen Sie unter Windows den umgekehrten Schrägstrich (\),

das Unix-Fortsetzungszeichen, am Ende jeder Zeile durch ein Caret-Zeichen oder Zirkumflex (^).

> **Note**
>
> Ersetzen Sie in AWS CLI Befehlen alle Werte in den spitzen Klammern (<>) durch korrekte Werte.

Epen

Erstellen und konfigurieren Sie einen S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie einen S3-Bucket.	Erstellen Sie einen S3-Bucket in Ihrem AWS-Region. Dieser Bucket enthält die nicht indizierten Mandantendaten für die Beispielanwendung. Stellen Sie sicher, dass der Name des S3-Bucket s global eindeutig ist, da der Namespace von allen gemeinsam genutzt wird. AWS-Konten
	
	Um einen S3-Bucket zu erstellen, können Sie den Befehl AWS CLI create-bucket wie folgt verwenden:
	
	`aws s3api create-bucket \`
	`  --bucket <tenantra wdata> \`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`  --region <your-AWS-Region>` wo `tenantrawdata` ist der Name des S3-Buckets. (Sie können jeden eindeutigen Namen verwenden, der den Richtlinien zur Benennung von Buckets entspricht.)	

Erstellen und konfigurieren Sie einen Elasticsearch-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine OpenSearch Dienstdomäne.	Führen Sie den AWS CLI create-elasticsearch-domainBefehl aus, um eine OpenSearch Dienstdomäne zu erstellen:
	
	`aws es create-elasticsearch-domain \`
	`  --domain-name vpc-cli-example \`
	`  --elasticsearch-version 7.10 \`
	`  --elasticsearch-cluster-config InstanceType=t3.medium.elasticsearch,InstanceCount=1 \`
	`  --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=10 \`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--domain-endpoint-options "{\"EnforceHTTPS\": true}" \ --encryption-at-rest-options "{\"Enabled\": true}" \ --node-to-node-encryption-options "{\"Enabled\": true}" \ --advanced-security-options "{\"Enabled\": true, \"InternalUserDatabaseEnabled\": true, \ \"MasterUserOptions\": {\"MasterUserName\": \"KibanaUser\", \ \"MasterUserPassword\": \"NewKibanaPassword@123\"}}" \ --vpc-options "{\"SubnetIds\": [\"<subnet-id>\"], \"SecurityGroupIds\": [\"<sg-id>\"]}" \ --access-policies "{\"Version\": \"2012-10-17\", \"Statement\": [{ \"Effect\": \"Allow\", \ \"Principal\": {\"AWS\": \"*\" }, \"Action\":\"es:*\", \ \"Resource\": \"arn:aws:es:<region>:<account-id>:domain\/vpc-cli-example\/*\" }] }"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Die Anzahl der Instanzen ist auf 1 gesetzt, da die Domäne zu Testzwecken dient. Sie müssen mithilfe des `advanced-security-options` Parameters eine differenzierte Zugriffskontrolle aktivieren, da die Details nach der Erstellung der Domäne nicht mehr geändert werden können. Dieser Befehl erstellt einen Master-Benutzernamen (`KibanaUser`) und ein Passwort, mit denen Sie sich bei der Kibana-Konsole anmelden können. Da die Domain Teil einer Virtual Private Cloud (VPC) ist, müssen Sie sicherstellen, dass Sie die Elasticsearch-Instanz erreichen können, indem Sie die zu verwendende Zugriffsrichtlinie angeben. Weitere Informationen finden Sie in der AWS Dokumenta tion unter Starten Ihrer Amazon OpenSearch Service-Domains innerhalb einer VPC.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie einen Bastion-Host ein.	Richten Sie eine Amazon Elastic Compute Cloud (Amazon EC2) Windows-Instance als Bastion-Host für den Zugriff auf die Kibana-Konsole ein. Die Elasticsearch-Sicherheitsgruppe muss Datenverkehr von der EC2 Amazon-Sicherheitsgruppe zulassen. Eine Anleitung finden Sie im Blogbeitrag Controlling Network Access to EC2 Instances Using a Bastion Server. Wenn der Bastion-Host eingerichtet wurde und Sie die Sicherheitsgruppe, die der Instance zugeordnet ist, verfügbar haben, verwenden Sie den AWS CLI authorize-security-group-ingressBefehl, um der Elasticsearch-Sicherheitsgruppe die Erlaubnis hinzuzufügen, Port 443 von der Amazon-Sicherheitsgruppe EC2 (Bastion Host) zuzulassen. `aws ec2 authorize-security-group-ingress \ --group-id <SecurityGroupIdfElasticSearch> \ --protocol tcp \`	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--port 443 \ --source-group <SecurityGroupIdfBashionHostEC2>`	

Erstellen und konfigurieren Sie die Lambda-Index-Funktion

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Lambda-Ausführungsrolle.	Führen Sie den Befehl AWS CLI create-role aus, um der Lambda-Indexfunktion Zugriff auf und Ressourcen zu AWS-Services gewähren:
	`aws iam create-role \ --role-name index-lambda-role \ --assume-role-policy-document file://lambda_assume_role.json`
	wo `lambda_assume_role.json` ist ein JSON-Dokument, das der Lambda-Funktion wie folgt `AssumeRole` Berechtigungen gewährt:
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": {`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Service": "lambda.amazonaws.com"
	},
	"Action": "sts:AssumeRole"
	}
	]
	}</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Hängen Sie verwaltete Richtlinien an die Lambda-Rolle an.	Führen Sie den AWS CLI attach-role-policyBefehl aus, um verwaltete Richtlinien an die im vorherigen Schritt erstellte Rolle anzuhängen. Diese beiden Richtlinien gewähren der Rolle Berechtigungen zum Erstellen einer elastic network interface und zum Schreiben von Protokollen in CloudWatch Logs.
	
	`aws iam attach-role-policy \`
	`  --role-name index-lambda-role \`
	`  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	
	`aws iam attach-role-policy \`
	`  --role-name index-lambda-role \`
	`  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine Richtlinie, um der Lambda-Indexfunktion die Berechtigung zum Lesen der S3-Objekte zu erteilen.	Führen Sie den Befehl AWS CLI create-policy aus, um der Lambda-Indexfunktion die `s3:GetObject` Erlaubnis zu erteilen, die Objekte im S3-Bucket zu lesen:
	`aws iam create-policy \ --policy-name s3-permission-policy \ --policy-document file://s3-policy.json`
	Bei der Datei `s3-policy.json` handelt es sich um ein unten gezeigtes JSON-Dokument, das `s3:GetObject` Berechtigungen für den Lesezugriff auf S3-Objekte gewährt. Wenn Sie bei der Erstellung des S3-Buckets s einen anderen Namen verwendet haben, geben Sie im `Resource` Abschnitt den richtigen Bucket-Namen an:
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject",`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Resource
	": "arn:aws:s3:::<ten
	antrawdata>/*"
	}
	]
	}</pre>	

Hängen Sie die Amazon S3 S3-Berechtigungsrichtlinie an die Lambda-Ausführungsrolle an.	Führen Sie den AWS CLI attach-role-policyBefehl aus, um die Amazon S3 S3-Berechtigungsrichtlinie, die Sie im vorherigen Schritt erstellt haben, an die Lambda-Ausführungsrolle anzuhängen:
	<pre>aws iam attach-role-policy \
	--role-name index-lambda-role \
	--policy-arn
	<PolicyARN></pre>
	wo `PolicyARN` ist der Amazon-Ressourcenname (ARN) der Amazon S3-Genehmigungsrichtlinie. Sie können diesen Wert aus der Ausgabe des vorherigen Befehls abrufen.
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Lambda-Index-Funktion.	Führen Sie den Befehl AWS CLI create-function aus, um die Lambda-Indexfunktion zu erstellen, die auf Service zugreift: OpenSearch `aws lambda create-function \ --function-name index-lambda-function \ --zip-file fileb://index_lambda_package.zip \ --handler lambda_index.lambda_handler \ --runtime python3.9 \ --role "arn:aws:iam::account-id:role/index-lambda-role" \ --timeout 30 \ --vpc-config "{\"SubnetIds\": [\"<subnet-id1\>", \"<subnet-id2>\"], \ \"SecurityGroupIds\": [\"<sg-1>\"]}"`	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erlauben Sie Amazon S3, die Lambda-Index-Funktion aufzurufen.	Führen Sie den Befehl AWS CLI add-permission aus, um Amazon S3 die Erlaubnis zu erteilen, die Lambda-Index-Funktion aufzurufen: `aws lambda add-permission \ --function-name index-lambda-function \ --statement-id s3-permissions \ --action lambda:InvokeFunction \ --principal s3.amazonaws.com \ --source-arn "arn:aws:s3:::<tenantrawdata>" \ --source-account "<account-id>"`	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie einen Lambda-Trigger für das Amazon S3 S3-Ereignis hinzu.	Führen Sie den AWS CLI put-bucket-notification-configuration Befehl aus, um Benachrichtigungen an die Lambda-Indexfunktion zu senden, wenn das Amazon S3 `ObjectCreated` S3-Ereignis erkannt wird. Die Indexfunktion wird immer dann ausgeführt, wenn ein Objekt in den S3-Bucket hochgeladen wird. `aws s3api put-bucket-notification-configuration \ --bucket <tenantrawdata> \ --notification-configuration file://s3-trigger.json` Die Datei `s3-trigger.json` ist ein JSON-Dokument im aktuellen Ordner, das die Ressourcenrichtlinie zur Lambda-Funktion hinzufügt, wenn das Amazon S3 `ObjectCreated` S3-Ereignis eintritt.	Cloud-Architekt, Cloud-Administrator

Lambda-Suchfunktion erstellen und konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die Lambda-Ausführungsrolle.	Führen Sie den Befehl AWS CLI create-role aus, um der Lambda-Suchfunktion Zugriff auf und Ressourcen zu AWS-Services gewähren:
	`aws iam create-role \ --role-name search-lambda-role \ --assume-role-policy-document file://lambda_assume_role.json`
	wo `lambda_assume_role.json` befindet sich ein JSON-Dokument im aktuellen Ordner, das der Lambda-Funktion wie folgt `AssumeRole` Berechtigungen gewährt:
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, "Action": "sts:AssumeRole" }`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>] }</pre>	

Hängen Sie verwaltete Richtlinien an die Lambda-Rolle an.	Führen Sie den AWS CLI attach-role-policyBefehl aus, um verwaltete Richtlinien an die im vorherigen Schritt erstellte Rolle anzuhängen. Diese beiden Richtlinien gewähren der Rolle Berechtigungen zum Erstellen einer elastic network interface und zum Schreiben von Protokollen in CloudWatch Logs.
	<pre>aws iam attach-role-policy \
	  --role-name search-lambda-role \
	  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
	
	aws iam attach-role-policy \
	  --role-name search-lambda-role \
	  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole</pre>
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Lambda-Suchfunktion.	Führen Sie den Befehl AWS CLI create-function aus, um die Lambda-Suchfunktion zu erstellen, die auf Service zugreift: OpenSearch `aws lambda create-function \ --function-name search-lambda-function \ --zip-file fileb://search_lambda_package.zip \ --handler lambda_search.lambda_handler \ --runtime python3.9 \ --role "arn:aws:iam::account-id:role/search-lambda-role" \ --timeout 30 \ --vpc-config "{\"SubnetIds\": [\"<subnet-id1\>", \"<subnet-id2>\"], \ \"SecurityGroupIds\": [\"<sg-1>\"]}"`	Cloud-Architekt, Cloud-Administrator

Mandantenrollen erstellen und konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Mandanten-IAM-Rollen.	Führen Sie den Befehl AWS CLI create-role aus, um zwei Mandantenrollen zu erstellen, die zum Testen der Suchfunktion verwendet werden:	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws iam create-role \ --role-name Tenant-1-role \ --assume-role-policy-document file://assume-role-policy.json`	
	`aws iam create-role \ --role-name Tenant-2-role \ --assume-role-policy-document file://assume-role-policy.json`	
	Die Datei `assume-role-policy.json` ist ein JSON-Dokument im aktuellen Ordner, das der Lambda-Ausführungsrolle `AssumeRole` Berechtigungen gewährt:	
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "<Lambda execution role for index function>", "AWS": "<Lambda execution role for search function>" }, "Action": "sts:AssumeRole"`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre> }] }</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine IAM-Richtlinie für Mandanten.	Führen Sie den Befehl AWS CLI create-policy aus, um eine Mandantenrichtlinie zu erstellen, die Zugriff auf Elasticsearch-Operationen gewährt:
	`aws iam create-policy \ --policy-name tenant-policy \ --policy-document file://policy.json`
	Die Datei `policy.json` ist ein JSON-Dokument im aktuellen Ordner, das Berechtigungen für Elasticsearch gewährt:
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "es:ESHttpDelete", "es:ESHttpGet", "es:ESHttpHead", "es:ESHttpPost", "es:ESHttpPut",`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"es:ESHttpPatch"
	            ],
	            "Resource":
	[
	                "<ARN of
	Elasticsearch domain
	created earlier>"
	            ]
	        }
	    ]
	}</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Hängen Sie die Mandanten -IAM-Richtlinie an die Mandantenrollen an.	Führen Sie den AWS CLI attach-role-policyBefehl aus, um die Mandanten-IAM-Rich tlinie an die beiden Mandanten rollen anzuhängen, die Sie im vorherigen Schritt erstellt haben:
	`aws iam attach-role-policy \ --policy-arn arn:aws:iam::accou nt-id:policy/tenant-policy \ --role-name Tenant-1-role`
	`aws iam attach-role-policy \ --policy-arn arn:aws:iam::accou nt-id:policy/tenant-policy \ --role-name Tenant-2-role`
	Der Richtlinien-ARN stammt aus der Ausgabe des vorherigen Schritts.
		Cloud-Architekt, Cloud-Adm inistrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine IAM-Richtlinie, um Lambda Berechtigungen zur Übernahme einer Rolle zu erteilen.	Führen Sie den Befehl AWS CLI create-policy aus, um eine Richtlinie zu erstellen, damit Lambda die Mandantenrolle übernimmt:
	`aws iam create-policy \ --policy-name assume-tenant-role-policy \ --policy-document file://lambda_policy.json`
	Die Datei `lambda_policy.json` ist ein JSON-Dokument im aktuellen Ordner, das Berechtigungen gewährt für: `AssumeRole`
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "<ARN of tenant role created earlier>" } ] }`
	Denn Sie können ein Platzhalterzeichen verwenden `Resource`, um zu vermeiden
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	, dass für jeden Mandanten eine neue Richtlinie erstellt wird.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine IAM-Richtlinie, um der Lambda-Indexrolle Zugriff auf Amazon S3 zu gewähren.	Führen Sie den Befehl AWS CLI create-policy aus, um der Lambda-Indexrolle die Erlaubnis zu erteilen, auf die Objekte im S3-Bucket zuzugreifen:
	`aws iam create-policy \ --policy-name s3-permission-policy \ --policy-document file://s3_lambda_policy.json`
	Bei der Datei `s3_lambda_policy.json` handelt es sich um das folgende JSON-Richtliniendokument im aktuellen Ordner:
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::tenantrawdata/*" } ] }`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Hängen Sie die Richtlinie an die Lambda-Ausführungsrolle an.	Führen Sie den AWS CLI attach-role-policyBefehl aus, um die im vorherigen Schritt erstellte Richtlinie an die zuvor erstellten Lambda-Index- und Suchausführungsrollen anzuhängen:
	
	`aws iam attach-role-policy \`
	`  --policy-arn arn:aws:iam::account-id:policy/assume-tenant-role-policy \`
	`  --role-name index-lambda-role`
	
	`aws iam attach-role-policy \`
	`  --policy-arn arn:aws:iam::account-id:policy/assume-tenant-role-policy \`
	`  --role-name search-lambda-role`
	
	`aws iam attach-role-policy \`
	`  --policy-arn arn:aws:iam::account-id:policy/s3-permission-policy \`
	`  --role-name index-lambda-role`
	
	Der Richtlinien-ARN stammt aus der Ausgabe des vorherigen Schritts.
		Cloud-Architekt, Cloud-Administrator

Erstellen und konfigurieren Sie eine Such-API

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine REST-API in API Gateway.	Führen Sie den AWS CLI create-rest-apiBefehl aus, um eine REST-API-Ressource zu erstellen: `aws apigateway create-rest-api \ --name Test-Api \ --endpoint-configu ration "{ \"types\": [\"REGIONAL\"] }"` Für den Endpunkt-Konfigura tionstyp können Sie angeben, `REGIONAL` dass `EDGE` anstelle eines bestimmten Kantensta ndorts verwendet werden soll AWS-Region. Notieren Sie sich den Wert des `id` Felds aus der Befehlsausgabe. Dies ist die API-ID, die Sie in nachfolge nden Befehlen verwenden werden.	Cloud-Architekt, Cloud-Adm inistrator
Erstellen Sie eine Ressource für die Such-API.	Die Such-API-Ressource startet die Lambda-Su chfunktion mit dem Ressource nnamen`search`. (Sie müssen keine API für die Lambda-Indexfunktion erstellen, da sie automatisch ausgeführt	Cloud-Architekt, Cloud-Adm inistrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	wird, wenn Objekte in den S3-Bucket hochgeladen werden.)
	
	1. Führen Sie den Befehl AWS CLI get-resources aus, um die übergeordnete ID für den Stammpfad abzurufen:
	
	`aws apigateway get-resources \ --rest-api-id <API-ID>`
	
	Notieren Sie sich den Wert des ID-Felds. Sie werden diese übergeordnete ID im nächsten Befehl verwenden .
	
	`{ "items": [ { "id": "zpsri964ck", "path": "/" } ] }`
	
	2. Führen Sie den Befehl AWS CLI create-resource aus, um eine Ressource für die Such-API zu erstellen. Geben Sie für `parent-id` die ID aus dem vorherigen Befehl an.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws apigateway create-resource \ --rest-api-id <API-ID> \ --parent-id <Parent-ID> \ --path-part search`	
Erstellen Sie eine GET-Methode für die Such-API.	Führen Sie den Befehl AWS CLI put-method aus, um eine `GET` Methode für die Such-API zu erstellen: `aws apigateway put-method \ --rest-api-id <API-ID> \ --resource-id <ID from the previous command output> \ --http-method GET \ --authorization-type "NONE" \ --no-api-key-required` Geben Sie für `resource-id` die ID aus der Ausgabe des `create-resource` Befehls an.	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Methodenantwort für die Such-API.	Führen Sie den AWS CLI put-method-responseBefehl aus, um eine Methodenantwort für die Such-API hinzuzufügen: `aws apigateway put-method-response \ --rest-api-id <API-ID> \ --resource-id <ID from the create-resource command output> \ --http-method GET \ --status-code 200 \ --response-models "{\"application/json\": \"Empty\"}"` Geben Sie für `resource-id` die ID aus der Ausgabe des vorherigen `create-resource` Befehls an.	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine Proxy-Lambda-Integration für die Such-API ein.	Führen Sie den Befehl AWS CLI put-integration aus, um eine Integration mit der Lambda-Suchfunktion einzurichten: `aws apigateway put-integration \ --rest-api-id <API-ID> \ --resource-id <ID from the create-resource command output> \ --http-method GET \ --type AWS_PROXY \ --integration-http-method GET \ --uri arn:aws:apigateway:region:lambda:path/2015-03-31/functions/arn:aws:lambda:<region>:<account-id>:function:<function-name>/invocations` Geben Sie für `resource-id` die ID aus dem vorherigen Befehl an. `create-resource`	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erteilen Sie API Gateway die Erlaubnis, die Lambda-Suchfunktion aufzurufen.	Führen Sie den Befehl AWS CLI add-permission aus, um API Gateway die Erlaubnis zu erteilen, die Suchfunktion zu verwenden: `aws lambda add-permission \ --function-name <function-name> \ --statement-id apigateway-get \ --action lambda:InvokeFunction \ --principal apigateway.amazonaws.com \ --source-arn "arn:aws:execute-api:<region>:<account-id>:api-id/*/GET/search"` Ändern Sie den `source-arn` Pfad, wenn Sie anstelle von `search` einen anderen API-Ressourcennamen verwendet haben.	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die Such-API bereit.	Führen Sie den Befehl AWS CLI create-deployment aus, um eine Staging-Ressource mit dem Namen zu erstellen: `dev`
	
	`aws apigateway create-deployment \`
	`  --rest-api-id <API-ID> \`
	`  --stage-name dev`
	
	Wenn Sie die API aktualisieren, können Sie sie mit demselben AWS CLI Befehl erneut in derselben Phase bereitstellen.
		Cloud-Architekt, Cloud-Administrator

Kibana-Rollen erstellen und konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Loggen Sie sich in die Kibana-Konsole ein.	1. Suchen Sie den Link zu Kibana in Ihrem Domain-Dashboard in der OpenSearch Service-Konsole. Die URL hat das Format:`<domain-endpoint>/_plugin/kibana/` . 2. Verwenden Sie den Bastion-Host, den Sie im ersten Epic konfiguriert haben, um auf die Kibana-Konsole zuzugreifen.	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Melden Sie sich bei der Kibana-Konsole an, indem Sie den Master-Benutzernamen und das Passwort aus dem vorherigen Schritt verwenden, als Sie die OpenSearch Service-Domain erstellt haben. 4. Wenn Sie aufgefordert werden, einen Mandanten auszuwählen, wählen Sie Privat.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und konfigurieren Sie Kibana-Rollen.	Um Daten zu isolieren und sicherzustellen, dass ein Mandant die Daten eines anderen Mandanten nicht abrufen kann, müssen Sie Document Security verwenden , sodass Mandanten nur auf Dokumente zugreifen können, die ihre Mandanten-ID enthalten. 1. Wählen Sie auf der Kibana-Konsole im Navigatio nsbereich Sicherheit, Rolle aus. 2. Erstellen Sie eine neue Mandantenrolle. 3. Legen Sie die Clusterbe rechtigungen auf festindices_all , wodurch die Berechtig ungen zum Erstellen, Lesen, Aktualisieren und Löschen (CRUD) für den OpenSearch Serviceindex erteilt werden. 4. Beschränken Sie die Indexberechtigungen auf den tenant-data Index. (Der Indexname sollte mit dem Namen in den Lambda-Such- und Indexfunktionen übereinst immen.)	Cloud-Architekt, Cloud-Adm inistrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Legen Sie die Indexberechtigungen auf fest`indices_all` , damit Benutzer alle indexbezogenen Operationen ausführen können. (Je nach Ihren Anforderungen können Sie die Vorgänge für einen detaillierteren Zugriff einschränken.) 6. Verwenden Sie aus Sicherheitsgründen auf Dokumentebene die folgende Richtlinie, um Dokumente nach Mandanten-ID zu filtern, um die Datenisolierung für Mandanten in einem gemeinsam genutzten Index zu gewährleisten: `{ "bool": { "must": { "match": { "TenantId": "Tenant-1" } } } }` Beim Indexnamen, den Eigenschaften und Werten wird zwischen Groß- und	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Kleinschreibung unterschieden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ordnen Sie Benutzer Rollen zu.	1. Wählen Sie die Registerkarte Zugeordnete Benutzer für die Rolle und wählen Sie dann Benutzer zuordnen aus. 2. Geben Sie im Abschnitt Backend-Rollen den ARN der IAM-Mandantenrolle an, die Sie zuvor erstellt haben, und wählen Sie dann Map aus. Dadurch wird die IAM-Mandantenrolle der Kibana-Rolle zugeordnet, sodass bei der mandantenspezifischen Suche nur Daten für diesen Mandanten zurückgegeben werden. Wenn der IAM-Rollenname für Tenant-1 beispielsweise lautet`Tenant-1-Role` , geben Sie den ARN für `Tenant-1-Role` (aus dem Epic Mandantenrollen erstellen und konfigurieren) im Feld Backend-Rollen für die Kibana-Rolle Tenant-1 an. 3. Wiederholen Sie die Schritte 1 und 2 für Tenant-2. Wir empfehlen Ihnen, die Erstellung der Mandanten- und Kibana-Rollen beim	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Onboarding des Mandanten zu automatisieren.	

Erstellen Sie den Mieterdatenindex.	Wählen Sie im Navigationsbereich unter Verwaltung die Option Dev Tools aus, und führen Sie dann den folgenden Befehl aus. Mit diesem Befehl wird der `tenant-data` Index erstellt, um die Zuordnung für die `TenantId` Eigenschaft zu definieren.
	`PUT /tenant-data`
	`{`
	`  "mappings": {`
	`  "properties": {`
	`  "TenantId":`
	`  { "type": "keyword"}`
	`  }`
	`  }`
	`}`
		Cloud-Architekt, Cloud-Administrator

VPC-Endpunkte für Amazon S3 erstellen und AWS STS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen VPC-Endpunkt für Amazon S3.	Führen Sie den AWS CLI create-vpc-endpointBefehl aus, um einen VPC-Endpunkt für Amazon S3 zu erstellen. Der Endpunkt ermöglicht der Lambda-Index-Funktion in der VPC den Zugriff auf Amazon S3.	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws ec2 create-vpc-endpoint \ --vpc-id <VPC-ID> \ --service-name com.amazonaws.us-east-1.s3 \ --route-table-ids <route-table-ID>` Geben Sie für `vpc-id` die VPC an, die Sie für die Lambda-Indexfunktion verwenden. Verwenden Sie für `service-name` die richtige URL für den Amazon S3 S3-Endpunkt. Geben Sie für `route-table-ids` die Routentabelle an, die dem VPC-Endpunkt zugeordnet ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie einen VPC-Endpunkt für AWS STS.	Führen Sie den AWS CLI create-vpc-endpointBefehl aus, um einen VPC-Endpunkt für AWS Security Token Service (AWS STS) zu erstellen. Der Endpunkt ermöglicht den Zugriff auf den Lambda-Index und die Suchfunktionen in der VPC. AWS STS Die Funktionen verwenden AWS STS , wenn sie die IAM-Rolle übernehmen.
	
	`aws ec2 create-vpc-endpoint \`
	`  --vpc-id <VPC-ID> \`
	`  --vpc-endpoint-type Interface \`
	`  --service-name com.amazonaws.us-east-1.sts \`
	`  --subnet-id <subnet-ID> \`
	`  --security-group-id <security-group-ID>`
	
	Geben Sie für `vpc-id` die VPC an, die Sie für den Lambda-Index und die Suchfunktionen verwenden. Geben Sie für das Subnetz an`subnet-id` , in dem dieser Endpunkt erstellt werden soll. Geben Sie für die Sicherheitsgruppe an`security-`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`group-id` , der dieser Endpunkt zugeordnet werden soll. (Es könnte dasselbe sein wie die Sicherheitsgruppe, die Lambda verwendet.)	

Testen Sie Mehrmandantenfähigkeit und Datenisolierung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Python-Dateien für die Index- und Suchfunktionen.	1. Bearbeiten Sie in der `index_lambda_package.zip` Datei die `lamba_index.py` Datei, um die AWS-Konto ID und die Elasticsearch-Endpunktinformationen zu aktualisieren. AWS-Region 2. Bearbeiten Sie in der `search_lambda_package.zip` Datei die `lambda_search.py` Datei, um die AWS-Konto ID und die Elasticsearch-Endpunktinformationen zu aktualisieren. AWS-Region Sie können den Elasticsearch-Endpunkt auf der Registerkarte „Übersicht“ der OpenSearch Service-Konsole abrufen. Er hat das Format<AWS-Regi	Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	on>.es.amazonaws.com .	

Aktualisieren Sie den Lambda-Code.	Verwenden Sie den AWS CLI update-function-codeBefehl, um den Lambda-Code mit den Änderungen zu aktualisieren, die Sie an den Python-Dateien vorgenommen haben:
	`aws lambda update-function-code \`
	`  --function-name index-lambda-function \`
	`  --zip-file fileb://index_lambda_package.zip`
	
	`aws lambda update-function-code \`
	`  --function-name search-lambda-function \`
	`  --zip-file fileb://search_lambda_package.zip`
		Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Laden Sie Rohdaten in den S3-Bucket hoch.	Verwenden Sie den Befehl AWS CLI cp, um Daten für die Objekte Tenant-1 und Tenant-2 in den `tenantrawdata` Bucket hochzuladen (geben Sie den Namen des S3-Buckets an, den Sie zu diesem Zweck erstellt haben):
	`aws s3 cp tenant-1-data s3://tenantrawdata`
	`aws s3 cp tenant-2-data s3://tenantrawdata`
	Der S3-Bucket ist so eingerichtet, dass er die Lambda-Indexfunktion jedes Mal ausführt, wenn Daten hochgeladen werden, sodass das Dokument in Elasticsearch indexiert wird.
		Cloud-Architekt, Cloud-Administrator

Suchen Sie Daten von der Kibana-Konsole aus.	Führen Sie auf der Kibana-Konsole die folgende Abfrage aus: `GET tenant-data/_search` Diese Abfrage zeigt alle in Elasticsearch indexierten Dokumente an. In diesem Fall sollten Sie zwei separate Dokumente für Tenant-1 und Tenant-2 sehen.	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Testen Sie die Such-API von API Gateway aus.	1. Öffnen Sie in der API Gateway Gateway-Konsole die Such-API, wählen Sie die `GET` Methode in der Suchressource aus und wählen Sie dann Test aus.
	2. Geben Sie im Testfenster die folgende Abfrageze ichenfolge (Groß- und Kleinschreibung beachten) für die Mandanten-ID ein und wählen Sie dann Test aus.
	`TenantId=Tenant-1`
	Die Lambda-Funktion sendet eine Abfrage an OpenSearch Service, die das Mandantendokument auf der Grundlage der Sicherheit auf Dokumente bene filtert. Die Methode gibt das Dokument zurück, das zu Tenant-1 gehört.
	3. Ändern Sie die Abfrageze ichenfolge in:
	`TenantId=Tenant-2`
	Diese Abfrage gibt das Dokument zurück, das zu Tenant-2 gehört.
		Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bildschirmdarstellungen finden Sie im Abschnitt Zusätzliche Informationen.	
Bereinigen von Ressourcen.	Bereinigen Sie alle Ressourcen, die Sie erstellt haben, um zusätzliche Gebühren für Ihr Konto zu vermeiden.	AWS DevOps, Cloud-Architekt, Cloud-Administrator

Zugehörige Ressourcen

- AWS SDK for Python (Boto)
- AWS Lambda Dokumentation
- API Gateway Gateway-Dokumentation
- Amazon S3 S3-Dokumentation
- Amazon OpenSearch Service-Dokumentation
  - Feinkörnige Zugriffskontrolle in Amazon Service OpenSearch
  - Eine Suchanwendung mit Amazon OpenSearch Service erstellen
  - Starten Ihrer Amazon OpenSearch Service-Domains innerhalb einer VPC

Zusätzliche Informationen

Modelle zur Datenpartitionierung

Es gibt drei gängige Datenpartitionierungsmodelle, die in Systemen mit mehreren Mandanten verwendet werden: Silo, Pool und Hybrid. Welches Modell Sie wählen, hängt von den Anforderungen Ihrer Umgebung in Bezug auf Compliance, Noisy Neighbor, Betrieb und Isolierung ab.

Silo-Modell

Im Silomodell werden die Daten jedes Mandanten in einem eigenen Speicherbereich gespeichert, in dem es nicht zu einer Vermischung von Mandantendaten kommt. Sie können zwei Ansätze verwenden, um das Silomodell mit OpenSearch Service zu implementieren: Domäne pro Mandant und Index pro Mandant.

- Domain pro Mandant — Sie können pro Mandant eine separate OpenSearch Service-Domain (gleichbedeutend mit einem Elasticsearch-Cluster) verwenden. Die Platzierung jedes Mandanten in einer eigenen Domain bietet alle Vorteile, die mit der Speicherung von Daten in einem eigenständigen Konstrukt verbunden sind. Dieser Ansatz bringt jedoch Herausforderungen in Bezug auf Management und Agilität mit sich. Aufgrund seines dezentralen Charakters ist es schwieriger, den betrieblichen Zustand und die Aktivität der Mieter zu aggregieren und zu bewerten. Dies ist eine kostspielige Option, bei der jede OpenSearch Dienstdomäne mindestens über drei Masterknoten und zwei Datenknoten für Produktionsworkloads verfügen muss.

- Index pro Mandant — Sie können Mandantendaten in separaten Indizes innerhalb eines Serviceclusters platzieren. OpenSearch Bei diesem Ansatz verwenden Sie bei der Erstellung und Benennung des Indexes eine Mandanten-ID, indem Sie die Mandanten-ID dem Indexnamen voranstellen. Der Ansatz „Index pro Mandant“ hilft Ihnen dabei, Ihre Siloziele zu erreichen, ohne für jeden Mandanten einen komplett separaten Cluster einzuführen. Es kann jedoch zu Speicherauslastung kommen, wenn die Anzahl der Indizes zunimmt, da für diesen Ansatz mehr Shards erforderlich sind und der Master-Knoten für mehr Zuweisung und Neuverteilung zuständig sein muss.

Isolierung im Silomodell — Im Silomodell verwenden Sie IAM-Richtlinien, um die Domänen oder Indizes zu isolieren, die die Daten der einzelnen Mandanten enthalten. Diese Richtlinien verhindern, dass ein Mandant auf die Daten eines anderen Mandanten zugreift. Um Ihr Silo-Isolationsmodell zu implementieren, können Sie eine ressourcenbasierte Richtlinie erstellen, die den Zugriff auf Ihre Mandantenressource steuert. Dabei handelt es sich häufig um eine Domain-Zugriffsrichtlinie, die festlegt, welche Aktionen ein Principal an den Unterressourcen der Domain durchführen kann, einschließlich Elasticsearch-Indizes und. APIs Mit identitätsbasierten IAM-Richtlinien können Sie zulässige oder verweigerte Aktionen für die Domain, Indizes oder innerhalb von Service angeben. APIs OpenSearch Das `Action` Element einer IAM-Richtlinie beschreibt die spezifischen Aktionen, die durch die Richtlinie zugelassen oder verweigert werden, und das `Principal` Element gibt die betroffenen Konten, Benutzer oder Rollen an.

Die folgende Beispielrichtlinie gewährt Tenant-1 vollen Zugriff (wie von angegeben`es:*`) nur auf die Unterressourcen in der Domäne. `tenant-1` Das nachstehende `/*` `Resource` Element weist darauf

hin, dass diese Richtlinie für die Unterressourcen der Domain gilt, nicht für die Domain selbst. Wenn diese Richtlinie in Kraft ist, dürfen Mandanten keine neue Domäne erstellen oder Einstellungen für eine bestehende Domäne ändern.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::<aws-account-id>:user/Tenant-1"
         },
         "Action": "es:*",
         "Resource": "arn:aws:es:<Region>:<account-id>:domain/tenant-1/*"
      }
   ]
}
```

Um das Silo-Modell „Mandant pro Index“ zu implementieren, müssten Sie diese Beispielrichtlinie ändern, um Tenant-1 weiter auf den angegebenen Index oder die angegebenen Indizes zu beschränken, indem Sie den Indexnamen angeben. Die folgende Beispielrichtlinie beschränkt Tenant-1 auf den Index. `tenant-index-1`

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/Tenant-1"
         },
         "Action": "es:*",
         "Resource": "arn:aws:es:<Region>:<account-id>:domain/test-domain/tenant-
index-1/*"
      }
   ]
}
```

Pool-Modell

Im Poolmodell werden alle Mandantendaten in einem Index innerhalb derselben Domäne gespeichert. Die Mandanten-ID ist in den Daten (Dokument) enthalten und wird als

Partitionsschlüssel verwendet, sodass Sie bestimmen können, welche Daten zu welchem Mandanten gehören. Dieses Modell reduziert den Verwaltungsaufwand. Der Betrieb und die Verwaltung des gepoolten Indexes sind einfacher und effizienter als die Verwaltung mehrerer Indizes. Da Mandantendaten jedoch innerhalb desselben Index zusammengefasst sind, verlieren Sie die natürliche Mandantenisolierung, die das Silomodell bietet. Dieser Ansatz kann aufgrund des Noisy-Neighbor-Effekts auch zu Leistungseinbußen führen.

Mandantenisolierung im Poolmodell — Im Allgemeinen ist es schwierig, die Mandantenisolierung im Poolmodell zu implementieren. Der im Silomodell verwendete IAM-Mechanismus ermöglicht es Ihnen nicht, die Isolierung anhand der in Ihrem Dokument gespeicherten Mandanten-ID zu beschreiben.

Ein alternativer Ansatz besteht darin, die FGAC-Unterstützung (Fine-Grained Access Control) zu verwenden, die von der Open Distro for Elasticsearch bereitgestellt wird. Mit FGAC können Sie Berechtigungen auf Index-, Dokument- oder Feldebene steuern. Bei jeder Anfrage wertet FGAC die Benutzeranmeldedaten aus und authentifiziert den Benutzer entweder oder verweigert den Zugriff. Wenn FGAC den Benutzer authentifiziert, ruft es alle Rollen ab, die diesem Benutzer zugeordnet sind, und verwendet den vollständigen Satz von Berechtigungen, um zu bestimmen, wie die Anfrage behandelt werden soll.

Um die erforderliche Isolierung im Poolmodell zu erreichen, können Sie die Sicherheit auf Dokumentebene verwenden, sodass Sie eine Rolle auf eine Teilmenge von Dokumenten in einem Index beschränken können. Die folgende Beispielrolle beschränkt Abfragen auf Tenant-1. Indem Sie diese Rolle auf Tenant-1 anwenden, können Sie die erforderliche Isolierung erreichen.

```
{
   "bool": {
     "must": {
       "match": {
         "tenantId": "Tenant-1"
       }
     }
   }
 }
```

Hybrides Modell

Das Hybridmodell verwendet eine Kombination der Silo- und Poolmodelle in derselben Umgebung, um jedem Mieter (z. B. kostenlose Tarife, Standard- und Premium-Tarife) einzigartige Erlebnisse zu bieten. Jede Stufe folgt demselben Sicherheitsprofil, das im Poolmodell verwendet wurde.

Mandantenisolierung im Hybridmodell — Im Hybridmodell verwenden Sie dasselbe Sicherheitsprofil wie im Poolmodell, wo die Verwendung des FGAC-Sicherheitsmodells auf Dokumentenebene die Mandantenisolierung ermöglichte. Diese Strategie vereinfacht zwar die Clusterverwaltung und bietet Flexibilität, verkompliziert aber andere Aspekte der Architektur. Ihr Code erfordert beispielsweise zusätzliche Komplexität, um zu bestimmen, welches Modell jedem Mandanten zugeordnet ist. Sie müssen außerdem sicherstellen, dass Abfragen für einzelne Mandanten nicht die gesamte Domäne überlasten und die Benutzererfahrung für andere Mandanten beeinträchtigen.

Testen im API Gateway

Testfenster für Tenant-1-Abfrage

Testfenster für Tenant-2-Abfrage

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Stellen Sie Anwendungen mit mehreren Stacks mithilfe von AWS CDK bereit mit TypeScript

Erstellt von Dr. Rahul Sharad Gaikwad (AWS)

Übersicht

Dieses Muster bietet einen step-by-step Ansatz für die Anwendungsbereitstellung auf Amazon Web Services (AWS) mithilfe des AWS Cloud Development Kit (AWS CDK) mit TypeScript. Das Muster stellt beispielsweise eine serverlose Echtzeit-Analyseanwendung bereit.

Das Muster erstellt und implementiert verschachtelte Stack-Anwendungen. Der übergeordnete CloudFormation AWS-Stack ruft die untergeordneten oder verschachtelten Stacks auf. Jeder untergeordnete Stack erstellt und stellt die AWS-Ressourcen bereit, die im CloudFormation Stack definiert sind. AWS CDK Toolkit, der Befehl Command Line Interface (CLI)`cdk`, ist die primäre Schnittstelle für die CloudFormation Stacks.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Bestehende virtuelle private Cloud (VPC) und Subnetze
- AWS CDK Toolkit installiert und konfiguriert
- Ein Benutzer mit Administratorrechten und einer Reihe von Zugriffsschlüsseln.
- Node.js
- AWS-Befehlszeilenschnittstelle (AWS Command Line Interface, AWS CLI)

Einschränkungen

- Da AWS CDK AWS verwendet CloudFormation, unterliegen AWS CDK-Anwendungen CloudFormation Service-Kontingenten. Weitere Informationen finden Sie unter CloudFormation AWS-Kontingente.

Produktversionen

Dieses Muster wurde mit den folgenden Tools und Versionen erstellt und getestet.

- AWS CDK-Toolkit 1.83.0
- Node.js 14,13.0
- npm 7.0.14

Das Muster sollte mit jeder Version von AWS CDK oder npm funktionieren. Beachten Sie, dass die Versionen 13.0.0 bis 13.6.0 von Node.js nicht mit dem AWS CDK kompatibel sind.

Architektur

Zieltechnologie-Stack

- AWS Amplify Amplify-Konsole
- Amazon API Gateway
- AWS-CDK
- Amazon CloudFront
- Amazon Cognito
- Amazon-DynamoDB
- Amazon Data Firehose
- Amazon Kinesis Data Streams
- AWS Lambda
- Amazon Simple Storage Service (Amazon-S3)

Zielarchitektur

Das folgende Diagramm zeigt die Bereitstellung mehrerer Stack-Anwendungen mithilfe von AWS CDK mit. TypeScript

Das folgende Diagramm zeigt die Architektur der beispielhaften serverlosen Echtzeitanwendung.

Tools

Tools

- Die AWS Amplify Console ist das Kontrollzentrum für Full-Stack-Bereitstellungen von Web- und Mobilanwendungen in AWS. Amplify Console Hosting bietet einen Git-basierten Workflow für das Hosten serverloser Full-Stack-Web-Apps mit kontinuierlicher Bereitstellung. Die Admin-Benutzeroberfläche ist eine visuelle Oberfläche für Frontend-Web- und Mobilentwickler, um App-Backends außerhalb der AWS-Konsole zu erstellen und zu verwalten.
- Amazon API Gateway ist ein AWS-Service für die Erstellung, Veröffentlichung, Wartung, Überwachung und Sicherung von REST, HTTP und WebSocket APIs in jeder Größenordnung.
- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS CDK Toolkit ist ein Befehlszeilen-Cloud-Entwicklungskit, das Sie bei der Interaktion mit Ihrer AWS-CDK-App unterstützt. Der `cdk` CLI-Befehl ist das wichtigste Tool für die Interaktion mit Ihrer AWS-CDK-App. Es führt Ihre App aus, fragt das von Ihnen definierte Anwendungsmodell ab und erstellt und stellt die vom AWS-CDK generierten CloudFormation AWS-Vorlagen bereit.
- Amazon CloudFront ist ein Webservice, der die Verteilung statischer und dynamischer Webinhalte wie .html-, .css-, .js- und Bilddateien beschleunigt. CloudFront stellt Ihre Inhalte über ein weltweites Netzwerk von Rechenzentren bereit, die als Edge-Standorte bezeichnet werden, um die Latenz zu verringern und die Leistung zu verbessern.
- Amazon Cognito bietet Authentifizierung, Autorisierung und Benutzerverwaltung für Ihre Web- und mobilen Apps. Ihre Benutzer können sich direkt oder über einen Drittanbieter anmelden.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der schnelle und vorhersehbare Leistung mit nahtloser Skalierbarkeit bietet.
- Amazon Data Firehose ist ein vollständig verwalteter Service für die Bereitstellung von Echtzeit-Streaming-Daten an Ziele wie Amazon S3, Amazon Redshift, Amazon OpenSearch Service, Splunk und alle benutzerdefinierten HTTP-Endpunkte oder HTTP-Endpunkte, die unterstützten Drittanbietern gehören.
- Amazon Kinesis Data Streams ist ein Service zum Sammeln und Verarbeiten großer Datenströme in Echtzeit.
- AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code

Der Code für dieses Muster ist angehängt.

Epen

Installieren Sie das AWS CDK Toolkit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie das AWS CDK Toolkit.	Führen Sie den folgenden Befehl aus, um AWS CDK Toolkit global zu installieren. `npm install -g aws-cdk`	DevOps
Überprüfen Sie die Version.	Führen Sie den folgenden Befehl aus, um die Version des AWS CDK Toolkit zu überprüfen. `cdk --version`	DevOps

AWS-Anmeldeinformationen einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie Anmeldein formationen ein.	Um Anmeldeinformationen einzurichten, führen Sie den `aws configure` Befehl aus und folgen Sie den Anweisung en.
	`$aws configure`
	`AWS Access Key ID [None]:`
	`AWS Secret Access Key [None]: your_secr et_access_key`
		DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`Default region name [None]:` `Default output format [None]:`	

Laden Sie den Projektcode herunter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den beigefügten Projektcode herunter.	Weitere Informationen zur Verzeichnis- und Dateistruktur finden Sie im Abschnitt Zusätzliche Informationen.	DevOps

Bootstrap für die AWS-CDK-Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bootstrap für die Umgebung.	Führen Sie den folgenden Befehl aus, um die CloudFormation AWS-Vorlage für das Konto und die AWS-Region bereitzustellen, die Sie verwenden möchten. `cdk bootstrap <account>/<Region>` Weitere Informationen finden Sie in der AWS-Dokumentation.	DevOps

Erstellen und implementieren Sie das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Projekt.	Führen Sie den `npm run build` Befehl aus, um den Projektcode zu erstellen.	DevOps
Stellen Sie das Projekt bereit.	Führen Sie den `cdk deploy` Befehl aus, um den Projektco de bereitzustellen.	

Überprüfen Sie die Ausgaben

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Stack-Ers tellung.	Wählen Sie in der AWS-Managementkonsole CloudFormation. Vergewiss ern Sie sich, dass in den Stacks für das Projekt ein übergeordneter Stack und zwei untergeordnete Stapel erstellt wurden.	DevOps

Testen der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie Daten an Kinesis Data Streams.	Konfigurieren Sie Ihr AWS-Konto so, dass Daten mithilfe von Amazon Kinesis Data Generator (KDG) an Kinesis Data Streams gesendet werden. Weitere Informati	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	onen finden Sie unter Amazon Kinesis Data Generator.	
Erstellen Sie einen Amazon Cognito Cognito-Benutzer.	Um einen Amazon Cognito Cognito-Benutzer zu erstellen, laden Sie die CloudFormation Vorlage cognito-setup.json aus dem Abschnitt Amazon Cognito Cognito-Benutzer erstellen auf der Kinesis Data Generator-Hilfeseite herunter. Initiieren Sie die Vorlage und geben Sie dann Ihren Amazon Cognito Cognito-Benutzerna men und Ihr Passwort ein. Auf der Registerkarte Ausgaben ist die Kinesis Data Generator-URL aufgeführt.	DevOps
Melden Sie sich bei Kinesis Data Generator an	Um sich bei KDG anzumelde n, verwenden Sie die von Ihnen angegebenen Amazon Cognito Cognito-Anmeldeinf ormationen und die Kinesis Data Generator-URL.	DevOps
Testen Sie die Anwendung.	Fügen Sie in KDG in Record template, Template 1, den Testcode aus dem Abschnitt Zusätzliche Informationen ein und wählen Sie Daten senden aus.	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie das API Gateway.	Nachdem die Daten aufgenommen wurden, testen Sie API Gateway, indem Sie die `GET` Methode zum Abrufen von Daten verwenden.	DevOps

Zugehörige Ressourcen

Referenzen

- AWS-Cloud-Entwicklungskit
- AWS CDK auf GitHub
- Arbeiten mit verschachtelten Stacks
- AWS-Beispielbeispiel — Serverlose Echtzeitanalysen

Zusätzliche Informationen

Verzeichnis- und Dateidetails

Dieses Muster erstellt die folgenden drei Stapel.

- `parent-cdk-stack.ts`— Dieser Stapel fungiert als übergeordneter Stapel und ruft die beiden untergeordneten Anwendungen als verschachtelte Stapel auf.
- `real-time-analytics-poc-stack.ts`— Dieser verschachtelte Stapel enthält die Infrastruktur und den Anwendungscode.
- `real-time-analytics-web-stack.ts`— Dieser verschachtelte Stapel enthält nur den statischen Webanwendungscode.

Wichtige Dateien und ihre Funktionalität

- `bin/real-time-analytics-poc.ts`— Einstiegspunkt der AWS-CDK-Anwendung. Es lädt alle Stacks, die unter definiert sind. `lib/`
- `lib/real-time-analytics-poc-stack.ts`— Definition des Stacks der AWS-CDK-Anwendung (`real-time-analytics-poc`).

- `lib/real-time-analytics-web-stack.ts`— Definition des Stacks der AWS-CDK-Anwendung (`real-time-analytics-web-stack`).
- `lib/parent-cdk-stack.ts`— Definition des Stacks der AWS-CDK-Anwendung (`parent-cdk`).
- `package.json`— Das NPM-Modulmanifest, das den Namen, die Version und die Abhängigkeiten der Anwendung enthält.
- `package-lock.json`— Wird von npm verwaltet.
- `cdk.json`— Toolkit zum Ausführen der Anwendung.
- `tsconfig.json`— Die TypeScript Konfiguration des Projekts.
- `.gitignore`— Liste der Dateien, die Git von der Quellcodeverwaltung ausschließen soll.
- `node_modules`— Wird von npm verwaltet; beinhaltet die Abhängigkeiten des Projekts.

Der folgende Codeabschnitt im übergeordneten Stack ruft untergeordnete Anwendungen als verschachtelte AWS-CDK-Stacks auf.

```
import * as cdk from '@aws-cdk/core';
import { Construct, Stack, StackProps } from '@aws-cdk/core';
import { RealTimeAnalyticsPocStack } from './real-time-analytics-poc-stack';
import { RealTimeAnalyticsWebStack } from './real-time-analytics-web-stack';


export class CdkParentStack extends Stack {
  constructor(scope: Construct, id: string, props?: StackProps) {
    super(scope, id, props);


    new RealTimeAnalyticsPocStack(this, 'RealTimeAnalyticsPocStack');
    new RealTimeAnalyticsWebStack(this, 'RealTimeAnalyticsWebStack');
  }
}
```

Code zum Testen

```
session={{date.now('YYYYMMDD')}}|sequence={{date.now('x')}}|
reception={{date.now('x')}}|instrument={{random.number(9)}}|
l={{random.number(20)}}|price_0={{random.number({"min":10000,
 "max":30000})}}|price_1={{random.number({"min":10000, "max":30000})}}|
price_2={{random.number({"min":10000, "max":30000})}}|
price_3={{random.number({"min":10000, "max":30000})}}|
```

```
price_4={{random.number({"min":10000, "max":30000})}}|
price_5={{random.number({"min":10000, "max":30000})}}|
price_6={{random.number({"min":10000, "max":30000})}}|
price_7={{random.number({"min":10000, "max":30000})}}|
price_8={{random.number({"min":10000, "max":30000})}}|
```

Testen des API Gateway

Testen Sie API Gateway auf der API Gateway Gateway-Konsole mithilfe der `GET` Methode.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Automatisieren Sie die Bereitstellung verschachtelter Anwendungen mit AWS SAM

Erstellt von Dr. Rahul Sharad Gaikwad (AWS), Dmitry Gulin (AWS), Ishwar Chauthaiwale (AWS) und Tabby Ward (AWS)

Übersicht

Auf Amazon Web Services (AWS) ist das AWS Serverless Application Model (AWS SAM) ein Open-Source-Framework, das Kurzsyntax zum Ausdrücken von Funktionen APIs, Datenbanken und Zuordnungen von Ereignisquellen bereitstellt. Mit nur wenigen Zeilen für jede Ressource können Sie die gewünschte Anwendung definieren und sie mithilfe von YAML modellieren. Während der Bereitstellung transformiert und erweitert SAM die SAM-Syntax in CloudFormation AWS-Syntax, mit der Sie serverlose Anwendungen schneller erstellen können.

AWS SAM vereinfacht die Entwicklung, Bereitstellung und Verwaltung serverloser Anwendungen auf der AWS-Plattform. Es bietet ein standardisiertes Framework, eine schnellere Bereitstellung, lokale Testfunktionen, Ressourcenmanagement, eine nahtlose Integration mit Entwicklungstools und eine unterstützende Community. Diese Funktionen machen es zu einem wertvollen Tool für die effiziente und effektive Erstellung serverloser Anwendungen.

Dieses Muster verwendet AWS-SAM-Vorlagen, um die Bereitstellung verschachtelter Anwendungen zu automatisieren. Eine verschachtelte Anwendung ist eine Anwendung innerhalb einer anderen Anwendung. Übergeordnete Anwendungen rufen ihre untergeordneten Anwendungen auf. Dabei handelt es sich um lose gekoppelte Komponenten einer serverlosen Architektur.

Mithilfe verschachtelter Anwendungen können Sie schnell hochentwickelte serverlose Architekturen erstellen, indem Sie Services oder Komponenten wiederverwenden, die unabhängig erstellt und verwaltet wurden, aber mithilfe von AWS SAM und dem Serverless Application Repository zusammengestellt wurden. Verschachtelte Anwendungen helfen Ihnen dabei, leistungsstärkere Anwendungen zu erstellen, Doppelarbeit zu vermeiden und Konsistenz und bewährte Verfahren in Ihren Teams und Organisationen sicherzustellen. Um verschachtelte Anwendungen zu demonstrieren, stellt das Muster eine serverlose AWS-Einkaufswagen-Beispielanwendung bereit.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

- Eine bestehende virtuelle private Cloud (VPC) und Subnetze
- Eine integrierte Entwicklungsumgebung wie Visual Studio Code (weitere Informationen finden Sie unter Tools to Build on AWS)
- Die Python-Wheel-Bibliothek wurde mit Pip Install Wheel installiert, falls sie noch nicht installiert ist

Einschränkungen

- Die maximale Anzahl von Anwendungen, die in einer serverlosen Anwendung verschachtelt werden können, beträgt 200.
- Die maximale Anzahl von Parametern für eine verschachtelte Anwendung kann 60 betragen.

Produktversionen

- Diese Lösung basiert auf der AWS SAM-Befehlszeilenschnittstelle (AWS SAM CLI) Version 1.21.1, aber diese Architektur sollte mit späteren AWS SAM CLI-Versionen funktionieren.

Architektur

Zieltechnologie-Stack

- Amazon API Gateway
- AWS SAM
- Amazon Cognito
- Amazon-DynamoDB
- AWS Lambda
- Amazon Simple Queue Service-Warteschlange (Amazon SQS)

Zielarchitektur

Das folgende Diagramm zeigt, wie Benutzeranfragen per Anruf an die Einkaufsdienste gestellt werden APIs. Die Anfrage des Benutzers, einschließlich aller erforderlichen Informationen, wird an Amazon API Gateway und den Amazon Cognito Authorizer gesendet, der Authentifizierungs- und Autorisierungsmechanismen für die durchführt. APIs

Wenn ein Element in DynamoDB hinzugefügt, gelöscht oder aktualisiert wird, wird ein Ereignis in DynamoDB Streams abgelegt, wodurch wiederum eine Lambda-Funktion ausgelöst wird. Um zu

verhindern, dass alte Elemente im Rahmen eines synchronen Workflows sofort gelöscht werden, werden Nachrichten in eine SQS-Warteschlange gestellt, wodurch eine Worker-Funktion zum Löschen der Nachrichten ausgelöst wird.

In diesem Lösungs-Setup dient AWS SAM CLI als Schnittstelle für CloudFormation AWS-Stacks. AWS-SAM-Vorlagen stellen automatisch verschachtelte Anwendungen bereit. Die übergeordnete SAM-Vorlage ruft die untergeordneten Vorlagen auf, und der übergeordnete CloudFormation Stack stellt die untergeordneten Stacks bereit. Jeder untergeordnete Stack erstellt die AWS-Ressourcen, die in den CloudFormation AWS-SAM-Vorlagen definiert sind.

1. Erstellen und implementieren Sie die Stacks.
2. Der CloudFormation Auth-Stack enthält Amazon Cognito.
3. Der CloudFormation Produkt-Stack enthält eine Lambda-Funktion und Amazon API Gateway
4. Der CloudFormation Shopping-Stack enthält eine Lambda-Funktion, Amazon API Gateway, die SQS-Warteschlange und die Amazon DynamoDB DynamoDB-Datenbank.

Tools

Tools

- Amazon API Gateway unterstützt Sie bei der Erstellung, Veröffentlichung, Wartung, Überwachung und Sicherung von REST, HTTP und WebSocket APIs in jeder Größenordnung.
- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.
- Amazon Cognito bietet Authentifizierung, Autorisierung und Benutzerverwaltung für Web- und mobile Apps.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Das AWS Serverless Application Model (AWS SAM) ist ein Open-Source-Framework, mit dem Sie serverlose Anwendungen in der AWS-Cloud erstellen können.

- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.

Code

Der Code für dieses Muster ist im GitHub AWS SAM Nested Stack Sample Repository verfügbar.

Epen

Installieren Sie AWS SAM CLI

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie AWS SAM CLI.	Informationen zur Installation von AWS SAM CLI finden Sie in der AWS SAM-Dokumentation.	DevOps Ingenieur

Richten Sie AWS-Anmeldeinformationen ein.	Um AWS-Anmeldeinformationen so einzurichten, dass die AWS SAM CLI in Ihrem Namen AWS-Services aufrufen kann, führen Sie den `aws configure` Befehl aus und folgen Sie den Anweisungen.
	`$aws configure`
	`AWS Access Key ID [None]: <your_access_key_id>`
	`AWS Secret Access Key [None]: your_secret_access_key`
	`Default region name [None]:`
	`Default output format [None]:`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen zur Einrichtung Ihrer Anmeldein formationen finden Sie unter Authentifizierungs- und Zugangsdaten.	

Initialisieren Sie das AWS-SAM-Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Klonen Sie das AWS-SAM-C ode-Repository.	1. Klonen Sie das AWS Sam Nested Stack-Beispiel-Rep ository für dieses Muster, indem Sie den folgenden Befehl eingeben.
	`git clone https://g ithub.com/aws-samp les/aws-sam-nested- stack-sample.git`
	2. Navigieren Sie in das geklonte Verzeichnis, indem Sie den folgenden Befehl eingeben.
	`cd aws-sam-nested-sta ck-sample`
		DevOps Ingenieur

Stellen Sie Vorlagen bereit, um das Projekt zu initialis ieren.	Führen Sie den Befehl aus, um das Projekt zu initialis ieren. `SAM init` Wenn Sie aufgefordert werden, eine Vorlagenquelle auszuwähl	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en, wählen Sie`Custom Template Location`.	

Kompilieren und erstellen Sie den SAM-Vorlagencode

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich die AWS-SAM-Anwendungsvorlagen an.	Überprüfen Sie die Vorlagen für die verschachtelten Anwendungen. In diesem Beispiel werden die folgenden verschachtelten Anwendung svorlagen verwendet: • `auth.yaml` — Diese Vorlage richtet authentif izierungsbezogene Ressourcen wie Amazon Cognito und AWS Systems Manager Parameter Store ein. • `product-mock.yaml` — Diese Vorlage stellt produktbezogene Ressourcen wie Lambda-Fu nktionen und Amazon API Gateway bereit. • `shoppingcart-servi ce.yaml` — Diese Vorlage richtet Ressourcen für Einkaufswagen ein, z. B. AWS Identity and Access Management (IAM),	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	DynamoDB-Tabellen und Lambda-Funktionen.	
Überprüfen Sie die übergeordnete Vorlage.	Prüfen Sie die Vorlage, mit der die verschachtelten Anwendungsvorlagen aufgerufen werden. In diesem Beispiel ist die übergeordnete Vorlage. `template.yml` Alle separaten Anwendungen sind in der einzigen übergeordneten Vorlage `template.yml` verschachtelt.	DevOps Ingenieur
Kompilieren und erstellen Sie den AWS-SAM-Vorlagencode.	Führen Sie mit der AWS SAM CLI den folgenden Befehl aus. `sam build`	DevOps Ingenieur

Stellen Sie die AWS-SAM-Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Anwendungen bereit.	Führen Sie den folgenden Befehl aus, um den SAM-Vorlagencode zu starten, der die verschachtelten CloudFormation Anwendungsstapel erstellt und Code in der AWS-Umgebung bereitstellt. `sam deploy --guided --stack-name shopping-cart-nested-stack --`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`capabilities CAPABILIT Y_IAM CAPABILIT Y_AUTO_EXPAND` Der Befehl wird Sie mit einigen Fragen auffordern. Beantwort en Sie alle Fragen mity.	

Überprüfen der Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfe die Stapel.	Gehen Sie wie folgt vor, um die CloudFormation AWS-Stacks und AWS-Ressourcen zu überprüfen, die in den AWS-SAM-Vorlagen definiert wurden: 1. Melden Sie sich bei der AWS-Managementkonsole an und navigieren Sie zur CloudFormationKonsole. 2. Stellen Sie sicher, dass die übergeordneten und untergeordneten Stacks aufgeführt sind. In diesem Beispiel `sam-shopping-cart` ist es der übergeordnete Stack, der die verschach telten Auth-, Product- und Shopping-Stacks aufruft.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Der Produkt-Stack gibt den Produkt-API-Gateway-URL-Link als Ausgabe aus.	

Zugehörige Ressourcen

Referenzen

- Serverloses AWS-Anwendungsmodell (AWS SAM)
- AWS SAM auf GitHub
- Serverloser Einkaufswagen-Microservice (AWS-Beispielanwendung)

Tutorials und Videos

- Erstellen Sie eine serverlose App
- AWS Online Tech Talks: Serverlose Anwendungsentwicklung und -bereitstellung mit AWS SAM

Zusätzliche Informationen

Nachdem der gesamte Code vorhanden ist, hat das Beispiel die folgende Verzeichnisstruktur:

- sam_stacks — Dieser Ordner enthält die Ebene. `shared.py` Eine Ebene ist ein Dateiarchiv, das Bibliotheken, eine benutzerdefinierte Runtime oder andere Abhängigkeiten enthält. Mit Ebenen können Sie Bibliotheken in Ihrer Funktion verwenden, ohne sie in ein Bereitstellungspaket aufnehmen zu müssen.
- product-mock-service— Dieser Ordner enthält alle produktbezogenen Lambda-Funktionen und -Dateien.
- shopping-cart-service— Dieser Ordner enthält alle Lambda-Funktionen und -Dateien zum Einkaufen.

Implementieren Sie die SaaS-Mandantenisolierung für Amazon S3 mithilfe eines AWS Lambda Lambda-Token-Verkaufsautomaten

Erstellt von Tabby Ward (AWS), Sravan Periyathambi (AWS) und Thomas Davis (AWS)

Übersicht

Mehrmandantenfähige SaaS-Anwendungen müssen Systeme implementieren, um sicherzustellen, dass die Mandantenisolierung aufrechterhalten wird. Wenn Sie Mandantendaten auf derselben Amazon Web Services (AWS) -Ressource speichern, z. B. wenn mehrere Mandanten Daten in demselben Amazon Simple Storage Service (Amazon S3) -Bucket speichern, müssen Sie sicherstellen, dass kein mandantenübergreifender Zugriff möglich ist. Token-Verkaufsautomaten (TVMs) sind eine Möglichkeit, die Daten von Mietern zu isolieren. Diese Maschinen bieten einen Mechanismus zum Abrufen von Token und abstrahieren gleichzeitig die Komplexität der Token-Generierung. Entwickler können ein TVM verwenden, ohne detaillierte Kenntnisse darüber zu haben, wie es Token produziert.

Dieses Muster implementiert ein TVM mithilfe von AWS Lambda. Das TVM generiert ein Token, das aus temporären STS-Anmeldeinformationen (Security Token Service) besteht, die den Zugriff auf die Daten eines einzelnen SaaS-Mandanten in einem S3-Bucket einschränken.

TVMs, und der Code, der mit diesem Muster bereitgestellt wird, werden in der Regel mit Ansprüchen verwendet, die von JSON Web Tokens (JWTs) abgeleitet werden, um Anfragen nach AWS-Ressourcen mit einer mandantenbezogenen AWS Identity and Access Management (IAM) -Richtlinie zu verknüpfen. Sie können den Code in diesem Muster als Grundlage für die Implementierung einer SaaS-Anwendung verwenden, die temporäre STS-Anmeldeinformationen mit Gültigkeitsbereich auf der Grundlage der in einem JWT-Token bereitgestellten Ansprüche generiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 1.19.0 oder höher, installiert und konfiguriert auf macOS, Linux oder Windows. Alternativ können Sie AWS CLI Version 2.1 oder höher verwenden.

Einschränkungen

- Dieser Code läuft in Java und unterstützt derzeit keine anderen Programmiersprachen.

- Die Beispielanwendung beinhaltet keinen regionsübergreifenden AWS-Support oder Disaster Recovery (DR) Support.
- Dieses Muster zeigt, wie ein Lambda-TVM für eine SaaS-Anwendung begrenzten Mandantenzugriff bereitstellen kann. Es ist nicht für den Einsatz in Produktionsumgebungen vorgesehen.

Architektur

Zieltechnologie-Stack

- AWS Lambda
- Amazon S3
- IAM
- AWS Security Token Service (AWS STS)

Zielarchitektur

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Security Token Service (AWS STS) hilft Ihnen dabei, temporäre Anmeldeinformationen mit eingeschränkten Rechten für Benutzer anzufordern.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code

Der Quellcode für dieses Muster ist als Anhang verfügbar und umfasst die folgenden Dateien:

- `s3UploadSample.jar`stellt den Quellcode für eine Lambda-Funktion bereit, die ein JSON-Dokument in einen S3-Bucket hochlädt.
- `tvm-layer.zip`stellt eine wiederverwendbare Java-Bibliothek bereit, die ein Token (temporäre STS-Anmeldeinformationen) für die Lambda-Funktion bereitstellt, um auf den S3-Bucket zuzugreifen und das JSON-Dokument hochzuladen.
- `token-vending-machine-sample-app.zip`stellt den Quellcode bereit, der zur Erstellung dieser Artefakte und Kompilierungsanweisungen verwendet wurde.

Folgen Sie den Anweisungen im nächsten Abschnitt, um diese Dateien zu verwenden.

Epen

Ermitteln Sie Variablenwerte

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie Variablenwerte.	Die Implementierung dieses Musters umfasst mehrere Variablennamen, die konsistent verwendet werden müssen. Ermitteln Sie die Werte, die für jede Variable verwendet werden sollen, und geben Sie diesen Wert an, wenn Sie in den nachfolgenden Schritten dazu aufgefordert werden. – <AWS Account ID>Die 12-stellige Konto-ID, die dem AWS-Konto zugeordnet ist, in dem Sie dieses Muster implementieren. Informationen dazu, wie Sie Ihre AWS-Konto-ID finden, finden Sie in der IAM-Dokumentation unter	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ihre AWS-Konto-ID und deren Alias. – <AWS Region>Die AWS-Region, in der Sie dieses Muster implementieren. Weitere Informationen zu AWS-Regionen finden Sie unter Regionen und Availability Zones auf der AWS-Website. < sample-tenant-name > – Der Name eines Mandanten, der in der Anwendung verwendet werden soll. Der Einfachheit halber empfehlen wir, in diesem Wert nur alphanumerische Zeichen zu verwenden. Sie können jedoch jeden gültigen Namen für einen S3-Objektschlüssel verwenden. < sample-tvm-role-name > – Der Name der IAM-Rolle, die der Lambda-Funktion zugeordnet ist, die das TVM und die Beispielanwendung ausführt. Der Rollenname ist eine Zeichenfolge, die aus alphanumerischen Groß- und Kleinbuchstaben ohne Leerzeichen besteht. Sie können auch eines der folgenden Zeichen verwenden: Unterstrich (_), Pluszeich	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en (+), Gleichheitszeichen (=), Komma (,), Punkt (.), At-Zeichen (@) und Bindestri ch (-). Der Rollenname muss innerhalb des Kontos eindeutig sein. **< sample-app-role-name >** – Der Name der IAM-Rolle, der von der Lambda-Funktion angenommen wird, wenn sie temporäre STS-Anmel deinformationen mit Gültigkei tsbereich generiert. Der Rollenname ist eine Zeichenfo lge, die aus alphanume rischen Groß- und Kleinbuch staben ohne Leerzeichen besteht. Sie können auch eines der folgenden Zeichen verwenden: Unterstrich (_), Pluszeichen (+), Gleichhei tszeichen (=), Komma (,), Punkt (.), At-Zeichen (@) und Bindestrich (-). Der Rollennam e muss innerhalb des Kontos eindeutig sein. **< sample-app-function-name > –** Der Name der Lambda-Fu nktion. Dies ist eine Zeichenfo lge mit einer Länge von bis zu 64 Zeichen. **< sample-app-bucket-name >** – Der Name eines S3-Bucket	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	s, auf den mit Berechtigungen zugegriffen werden muss, die auf einen bestimmten Mandanten beschränkt sind. S3-Bucket-Namen: • Muss zwischen 3 und 63 Zeichen lang sein. • Darf nur aus Kleinbuch staben, Zahlen, Punkten (.) und Bindestrichen (-) bestehen. • Muss mit einem Buchstabe n oder einer Zahl beginnen und enden. • Darf nicht als IP-Adresse (z. B. 192.168.5.4) formatier t sein. • Muss innerhalb einer Partition eindeutig sein. Eine Partition ist eine Gruppe von Regionen. AWS hat derzeit drei Partitionen: `aws` (Standardregionen), `aws-cn` (Regionen China) und `aws-us-gov` (AWS-Regionen GovCloud [USA]).	

Erstellen eines S3-Buckets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket für die Beispielanwendung.	Verwenden Sie den folgenden AWS-CLI-Befehl, um einen	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	S3-Bucket zu erstellen. Geben Sie den Wert **<** sample-app-bucket-name **>** im Codeausschnitt an: `aws s3api create-bucket --bucket <sample-app-bucket-name>` Die Lambda-Beispielanwendung lädt JSON-Dateien in diesen Bucket hoch.	

Erstellen Sie die IAM-TVM-Rolle und -Richtlinie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine TVM-Rolle.	Verwenden Sie einen der folgenden AWS-CLI-Befehle, um eine IAM-Rolle zu erstellen. Geben Sie den Wert **<** sample-tvm-role-name **>** im Befehl ein. Für macOS- oder Linux-Shells: `aws iam create-role \ --role-name <sample-tvm-role-name> \ --assume-role-policy-document '{ "Version": "2012-10-17", "Statement": [ {`	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Effect":
	"Allow",
	"Principa
	l": {
	
	"Service": "lambda.a
	mazonaws.com"
	},
	"Action":
	"sts:AssumeRole"
	}
	]}'</pre>
	Für die Windows-Befehlszeile:
	<pre>aws iam create-role ^
	--role-name <sample-t
	vm-role-name> ^
	--assume-role-policy-
	document "{\"Versi
	on\": \"2012-10
	-17\", \"Statement
	\": [{\"Effect\":
	\"Allow\", \"Princip
	al\": {\"Service\":
	\"lambda.amazonaws
	.com\"}, \"Action\":
	\"sts:AssumeRole\"
	}]}"</pre>
	Die Lambda-Beispielanw endung übernimmt diese Rolle, wenn die Anwendung aufgerufen wird. Durch die Möglichkeit, die Anwendung srolle mit einer bereichsb ezogenen Richtlinie zu übernehmen, erhält der Code umfassendere Zugriffsb	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	erechtigungen auf den S3-Bucket.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine Inline-TVM-Rollenrichtlinie.	Verwenden Sie einen der folgenden AWS-CLI-Befehle, um eine IAM-Richtlinie zu erstellen. Geben Sie die <AWS Account ID>Werte < sample-tvm-role-name >, und < sample-app-role-name > im Befehl ein.
	
	Für macOS- oder Linux-Shells:
	
	`aws iam put-role-policy \ --role-name <sample-tvm-role-name> \ --policy-name assume-app-role \ --policy-document '{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "arn:aws:iam::<AWS Account ID>:role/<sample-app-role-name>" } ]}'`
	
	Für die Windows-Befehlszeile:
	
	`aws iam put-role-policy ^`
		Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--role-name <sample-tvm-role-name> ^ --policy-name assume-app-role ^ --policy-document "{\"Version\": \"2012-10-17\", \"Statement\": [{\"Effect\": \"Allow\", \"Action\": \"sts:AssumeRole\", \"Resource\": \"arn:aws:iam::<AWS Account ID>:role/<sample-app-role-name>\"}]}"` Diese Richtlinie ist der TVM-Rolle zugeordnet. Sie gibt dem Code die Möglichkeit, die Anwendungsrolle zu übernehmen, die über umfassendere Berechtigungen für den Zugriff auf den S3-Bucket verfügt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Hängen Sie die verwaltete Lambda-Richtlinie an.	Verwenden Sie den folgenden AWS-CLI-Befehl, um die `AWSLambdaBasicExecutionRole` IAM-Richtlinie anzuhängen. Geben Sie den Wert **<** sample-tvm-role-name **>** im Befehl ein:
	`aws iam attach-role-policy \ --role-name <sample-tvm-role-name> \ --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	Für die Windows-Befehlszeile:
	`aws iam attach-role-policy ^ --role-name <sample-tvm-role-name> ^ --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	Diese verwaltete Richtlinie ist der TVM-Rolle zugeordnet, damit Lambda Protokolle an Amazon senden kann. CloudWatch
		Cloud-Administrator

Erstellen Sie die IAM-Anwendungsrolle und -Richtlinie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Anwendungsrolle.	Verwenden Sie einen der folgenden AWS-CLI-Befehle, um eine IAM-Rolle zu erstellen. Geben Sie die **<**AWS Account ID**>**Werte **<** sample-app-role-name **>**, und **<** sample-tvm-role-name **>** im Befehl ein. Für macOS- oder Linux-Shells: `aws iam create-role \ --role-name <sample-app-role-name> \ --assume-role-policy-document '{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::<AWS Account ID>:role/<sample-tvm-role-name>" }, "Action": "sts:AssumeRole" } ]}'` Für die Windows-Befehlszeile:	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`aws iam create-role ^ --role-name <sample-app-role-name> ^ --assume-role-policy-document "{\"Version\": \"2012-10-17\", \"Statement\": [{\"Effect\": \"Allow\",\"Principal\": {\"AWS\": \"arn:aws:iam::<AWS Account ID>:role/<sample-tvm-role-name>\"},\"Action\": \"sts:AssumeRole\" }]}"` Die Lambda-Beispielanwendung übernimmt diese Rolle mit einer bereichsbezogenen Richtlinie, um mandanten basierten Zugriff auf einen S3-Bucket zu erhalten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Inline-Rollenrichtlinie für Anwendungen.	Verwenden Sie einen der folgenden AWS-CLI-Befehle, um eine IAM-Richtlinie zu erstellen. Geben Sie die Werte **<** sample-app-role-name **>** und **<** sample-app-bucket-name **>** im Befehl ein. Für macOS- oder Linux-Shells: `aws iam put-role-policy \ --role-name <sample-app-role-name> \ --policy-name s3-bucket-access \ --policy-document '{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"], "Resource": "arn:aws:s3:::<sample-app-bucket-name>/*" }, { "Effect": "Allow",`	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Action":
	["s3:ListBucket"],
	"Resource
	": "arn:aws:s3:::<sam
	ple-app-bucket-name>"
	}
	]}'</pre>
	Für die Windows-Befehlszeile:
	<pre>aws iam put-role-policy
	^
	--role-name <sample-a
	pp-role-name> ^
	--policy-name s3-bucket
	-access ^
	--policy-documen
	t "{\"Version\":
	\"2012-10-17\",
	\"Statement\":
	[{\"Effect\": \"Allow
	\", \"Action\":
	[\"s3:PutObject\",
	\"s3:GetObject\",
	\"s3:DeleteObject\
	"], \"Resource\":
	\"arn:aws:s3:::<sa
	mple-app-bucket-na
	me>/*\"}, {\"Effect\":
	\"Allow\", \"Action\
	": [\"s3:ListBucket
	\"], \"Resource\":
	\"arn:aws:s3:::<sa
	mple-app-bucket-name>
	\"}]}"</pre>
	Diese Richtlinie ist der Anwendungsrolle zugeordnet. Sie bietet umfassenden Zugriff auf Objekte im S3-Bucket.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wenn die Beispielanwendung die Rolle übernimmt, werden diese Berechtigungen anhand der dynamisch generiert en Richtlinie des TVM auf einen bestimmten Mandanten beschränkt.	

Erstellen Sie die Lambda-Beispielanwendung mit TVM

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die kompilierten Quelldateien herunter.	Laden Sie die `tvm-layer.zip` Dateien `s3UploadSample.jar` und herunter, die als Anlagen enthalten sind. Den Quellcode, der zur Erstellung dieser Artefakte verwendet wurde, sowie Anweisungen zur Kompilierung finden Sie unter. `token-vending-machine-sample-app.zip`	Cloud-Administrator
Erstellen Sie die Lambda-Schicht.	Verwenden Sie den folgenden AWS-CLI-Befehl, um eine Lambda-Schicht zu erstellen, die das TVM für Lambda zugänglich macht. **Note** Wenn Sie diesen Befehl nicht von dem Speicherort	Cloud-Administrator, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	aus ausführen, den Sie heruntergeladen haben `tvm-layer.zip` , geben Sie `tvm-layer.zip` im Parameter den richtigen Pfad zu an. `--zip-file`
	
	`aws lambda publish-layer-version \ --layer-name sample-token-vending-machine \ --compatible-runtimes java11 \ --zip-file fileb://tvm-layer.zip`
	
	Für die Windows-Befehlszeile:
	
	`aws lambda publish-layer-version ^ --layer-name sample-token-vending-machine ^ --compatible-runtimes java11 ^ --zip-file fileb://tvm-layer.zip`
	
	Dieser Befehl erstellt eine Lambda-Schicht, die die wiederverwendbare TVM-Bibliothek enthält.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

So erstellen Sie die Lambda-Funktion:	Verwenden Sie den folgenden AWS-CLI-Befehl, um eine Lambda-Funktion zu erstellen . Geben Sie die Werte < sample-app-function-name >,,, < sample-app-bucket-name >, < > und < sample-app-role-name > im Befehl ein. sample-tvm-role-name <AWS Account ID><AWS Region>
	
	Note
	Wenn Sie diesen Befehl nicht von dem Speicherort aus ausführen, den Sie heruntergeladen habens`3UploadSample.jar` , geben Sie `s3UploadSample.jar` im `--zip-file` Parameter den richtigen Pfad zu an.
	
	`aws lambda create-function \`
	`--function-name <sample-app-function-name> \`
	`--timeout 30 \`
	`--memory-size 256 \`
	`--runtime java11 \`
		Cloud-Administrator, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
--role arn:aws:i
am::<AWS Account
 ID>:role/<sample-tvm-
role-name> \
--handler com.amazo
n.aws.s3UploadSamp
le.App \
--zip-file fileb://s
3UploadSample.jar \
--layers arn:aws:l
ambda:<AWS Region>:<
AWS Account ID>:layer
:sample-token-vend
ing-machine:1 \
--environment "Variable
s={S3_BUCKET=<sample-
app-bucket-name>,
ROLE=arn:aws:iam::<AWS
 Account ID>:role/
<sample-app-role-n
ame>}"
```

Für die Windows-Befehlszeile:

```
aws lambda create-fu
nction ^
--function-name
 <sample-app-function-
name>  ^
--timeout 30 ^
--memory-size 256 ^
--runtime java11 ^
--role arn:aws:i
am::<AWS Account
 ID>:role/<sample-tvm-
role-name> ^
--handler com.amazo
n.aws.s3UploadSamp
le.App ^
--zip-file fileb://s
3UploadSample.jar ^
```

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--layers arn:aws:lambda:<AWS Region>:<AWS Account ID>:layer:sample-token-vending-machine:1 ^ --environment "Variables={S3_BUCKET=<sample-app-bucket-name>,ROLE=arn:aws:iam::<AWS Account ID>:role/<sample-app-role-name>}"` Dieser Befehl erstellt eine Lambda-Funktion mit dem Beispielanwendungscode und der angehängten TVM-Schicht. Außerdem werden zwei Umgebungsvariablen festgelegt: `S3_BUCKET` und. `ROLE` Die Beispielanwendung verwendet diese Variablen, um die zu übernehmende Rolle und den S3-Bucket zu bestimmen, in den JSON-Dokumente hochgeladen werden sollen.	

Testen Sie die Beispielanwendung und TVM

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie die Lambda-Beispielanwendung auf.	Verwenden Sie einen der folgenden AWS-CLI-Befehle, um die Lambda-Beispielanwendung mit der erwarteten	Cloud-Administrator, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Nutzlast zu starten. Geben Sie die Werte **<** sample-app-function-name **>** und **<** sample-tenant-name **>** im Befehl ein.
	
	Für macOS- und Linux-Shells:
	
	`aws lambda invoke \ --function <sample-app-function-name> \ --invocation-type RequestResponse \ --payload '{"tenant": "<sample-tenant-name>"}' \ --cli-binary-format raw-in-base64-out response.json`
	
	Für die Windows-Befehlszeile:
	
	`aws lambda invoke ^ --function <sample-app-function-name> ^ --invocation-type RequestResponse ^ --payload "{\"tenant\": \"<sample-tenant-name>\"}" ^ --cli-binary-format raw-in-base64-out response.json`
	
	Dieser Befehl ruft die Lambda-Funktion auf und gibt das Ergebnis in einem `response.json` Dokument zurück.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Auf vielen UNIX-basierten Systemen können Sie `response.json` zu ändern, `/dev/stdout` um die Ergebnisse direkt in Ihrer Shell auszugeben, ohne eine weitere Datei zu erstellen. **Note** Wenn Sie den Wert **<** sample-tenant-name **>** in nachfolgenden Aufrufen dieser Lambda-Funktion ändern, werden der Speicherort des JSON-Dokuments und die vom Token bereitgestellten Berechtigungen geändert.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich den S3-Bucket an, um die erstellten Objekte zu sehen.	Navigieren Sie zu dem S3-Bucket (< sample-app-bucket-name >), den Sie zuvor erstellt haben. Dieser Bucket enthält ein S3-Objektpräfix mit dem Wert < sample-tenant-name >. Unter diesem Präfix finden Sie ein JSON-Dokument, das mit einer UUID benannt ist. Wenn Sie die Beispielanwendung mehrmals aufrufen, werden weitere JSON-Dokumente hinzugefügt.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich die Cloudwatch-Protokolle für die Beispielanwendung an.	Sehen Sie sich die Cloudwatch-Protokolle an, die der Lambda-Funktion mit dem Namen < > sample-app-function-name zugeordnet sind. Anweisungen finden Sie unter Zugreifen auf CloudWatch Amazon-Protokolle für AWS Lambda in der AWS Lambda Lambda-Dokumentation. In diesen Protokollen können Sie die vom TVM generierte Richtlinie für Mandanten einsehen. Diese mandantenbezogene Richtlinie gewährt Amazon S3,, und Berechtigungen für die Beispielanwendung PutObjectGetObject, DeleteObjectjedoch nur für das Objektpräfix ListBucket APIs, das mit < > verknüpft ist. sample-tenant-name Wenn Sie bei nachfolgenden Aufrufen der Beispielanwendung den Wert < sample-tenant-name > ändern, aktualisiert der TVM die Bereichsrichtlinie so, dass sie dem Mandanten entspricht, der in der Aufruf-Payload angegeben ist. Diese dynamisch generierte Richtlinie zeigt, wie der mandanten	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bezogene Zugriff mit einem TVM in SaaS-Anwendungen aufrechterhalten werden kann. Die TVM-Funktionalität wird in einer Lambda-Schicht bereitgestellt, sodass sie an andere Lambda-Funktionen angehängt werden kann, die von einer Anwendung verwendet werden, ohne dass der Code repliziert werden muss. Eine Veranschaulichung der dynamisch generierten Richtlinie finden Sie im Abschnitt Zusätzliche Informationen.	

Zugehörige Ressourcen

- Isolieren von Mandanten mit dynamisch generierten IAM-Richtlinien (Blogbeitrag)
- Anwendung dynamisch generierter Isolationsrichtlinien in einer SaaS-Umgebung (Blogbeitrag)
- AWS SaaS Boost (eine Open-Source-Referenzumgebung, mit der Sie Ihr SaaS-Angebot auf AWS migrieren können)

Zusätzliche Informationen

Das folgende Amazon Cloudwatch-Protokoll zeigt die dynamisch generierte Richtlinie, die durch den TVM-Code in diesem Muster erzeugt wird. In diesem Screenshot ist < sample-app-bucket-name > `DOC-EXAMPLE-BUCKET` und < sample-tenant-name > ist. `test-tenant-1` Die von dieser bereichsbezogenen Richtlinie zurückgegebenen STS-Anmeldeinformationen können keine Aktionen

für Objekte im S3-Bucket ausführen, mit Ausnahme von Objekten, die dem Objektschlüsselpräfix zugeordnet sind. `test-tenant-1`

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Implementieren Sie das serverlose Saga-Muster mithilfe von AWS Step Functions

Erstellt von Tabby Ward (AWS), Joe Kern (AWS) und Rohan Mehta (AWS)

Übersicht

In einer Microservices-Architektur besteht das Hauptziel darin, entkoppelte und unabhängige Komponenten zu erstellen, um Agilität, Flexibilität und eine schnellere Markteinführung Ihrer Anwendungen zu fördern. Durch die Entkopplung verfügt jede Microservice-Komponente über eine eigene Datenpersistenzschicht. In einer verteilten Architektur können sich Geschäftstransaktionen über mehrere Microservices erstrecken. Da diese Microservices keine einzige ACID-Transaktion (Atomicity, Consistency, Isolation, Durability) verwenden können, kann es am Ende zu Teiltransaktionen kommen. In diesem Fall ist eine gewisse Kontrolllogik erforderlich, um die bereits verarbeiteten Transaktionen rückgängig zu machen. Zu diesem Zweck wird in der Regel das verteilte Saga-Muster verwendet.

Das Saga-Muster ist ein Fehlermanagement-Muster, das dazu beiträgt, Konsistenz in verteilten Anwendungen herzustellen und Transaktionen zwischen mehreren Microservices zu koordinieren, um die Datenkonsistenz aufrechtzuerhalten. Wenn Sie das Saga-Muster verwenden, veröffentlicht jeder Dienst, der eine Transaktion ausführt, ein Ereignis, das nachfolgende Dienste veranlasst, die nächste Transaktion in der Kette auszuführen. Dies wird fortgesetzt, bis die letzte Transaktion in der Kette abgeschlossen ist. Wenn eine Geschäftstransaktion fehlschlägt, orchestriert Saga eine Reihe von Ausgleichstransaktionen, die die Änderungen rückgängig machen, die durch die vorherigen Transaktionen vorgenommen wurden.

Dieses Muster zeigt, wie die Einrichtung und Bereitstellung einer Beispielanwendung (die Reisereservierungen bearbeitet) mit serverlosen Technologien wie AWS Step Functions, AWS Lambda und Amazon DynamoDB automatisiert werden kann. Die Beispielanwendung verwendet auch Amazon API Gateway und Amazon Simple Notification Service (Amazon SNS), um einen Saga-Ausführungskoordinator zu implementieren. Das Muster kann mit einem Infrastructure as Code (IaC) -Framework wie dem AWS Cloud Development Kit (AWS CDK), dem AWS Serverless Application Model (AWS SAM) oder Terraform bereitgestellt werden.

Weitere Informationen zum Saga-Muster und anderen Datenpersistenzmustern finden Sie im Leitfaden Enabling data persistence in microservices auf der AWS Prescriptive Guidance Guidance-Website.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Berechtigungen zum Erstellen eines CloudFormation AWS-Stacks. Weitere Informationen finden Sie in der CloudFormation Dokumentation unter Zugriffskontrolle.
- IaC-Framework Ihrer Wahl (AWS CDK, AWS SAM oder Terraform), das mit Ihrem AWS-Konto konfiguriert ist, sodass Sie die Framework-CLI zur Bereitstellung der Anwendung verwenden können.
- NodeJS, wird verwendet, um die Anwendung zu erstellen und lokal auszuführen.
- Ein Code-Editor Ihrer Wahl (wie Visual Studio Code, Sublime oder Atom).

Produktversionen

- NodeJS Version 14
- AWS CDK versie 2.37.1
- AWS SAM versie 1.71.0
- Terraform versie 1.3.7

Einschränkungen

Event Sourcing ist eine natürliche Methode, um das Saga-Orchestrierungsmuster in einer Microservices-Architektur zu implementieren, in der alle Komponenten lose miteinander verknüpft sind und keine direkte Kenntnis voneinander haben. Wenn Ihre Transaktion eine kleine Anzahl von Schritten (drei bis fünf) umfasst, ist das Saga-Muster möglicherweise hervorragend geeignet. Die Komplexität nimmt jedoch mit der Anzahl der Microservices und der Anzahl der Schritte zu.

Das Testen und Debuggen kann schwierig werden, wenn Sie dieses Design verwenden, da alle Dienste ausgeführt werden müssen, um das Transaktionsmuster zu simulieren.

Architektur

Zielarchitektur

Die vorgeschlagene Architektur verwendet AWS Step Functions, um ein Saga-Muster zu erstellen, um Flüge zu buchen, Mietwagen zu buchen und Zahlungen für einen Urlaub zu verarbeiten.

Das folgende Workflow-Diagramm veranschaulicht den typischen Ablauf des Reisebuchungssystems. Der Workflow besteht aus der Reservierung von Flugreisen („ReserveFlight“), der Reservierung eines Autos („ReserveCarRental“), der Bearbeitung von Zahlungen („ProcessPayment“), der Bestätigung von Flugreservierungen („ConfirmFlight“) und der Bestätigung von Mietwagen („ConfirmCarRental“), gefolgt von einer Erfolgsmeldung, wenn diese Schritte abgeschlossen sind. Wenn das System jedoch bei der Ausführung einer dieser Transaktionen auf Fehler stößt, schlägt es rückwärts fehl. Beispielsweise löst ein Fehler bei der Zahlungsabwicklung („ProcessPayment“) eine Rückerstattung („RefundPayment“) aus, wodurch der Mietwagen und der Flug („CancelRentalReservation“ und „CancelFlightReservation“) storniert werden, wodurch die gesamte Transaktion mit einer Fehlermeldung beendet wird.

Dieses Muster stellt separate Lambda-Funktionen für jede im Diagramm hervorgehobene Aufgabe sowie drei DynamoDB-Tabellen für Flüge, Mietwagen und Zahlungen bereit. Jede Lambda-Funktion erstellt, aktualisiert oder löscht die Zeilen in den jeweiligen DynamoDB-Tabellen, je nachdem, ob eine Transaktion bestätigt oder zurückgesetzt wurde. Das Muster verwendet Amazon SNS, um Textnachrichten (SMS) an Abonnenten zu senden und sie über fehlgeschlagene oder erfolgreiche Transaktionen zu informieren.

Automatisierung und Skalierung

Sie können die Konfiguration für diese Architektur mithilfe eines der IaC-Frameworks erstellen. Verwenden Sie einen der folgenden Links für Ihre bevorzugte IaC.

- Mit AWS CDK bereitstellen
- Mit AWS SAM bereitstellen
- Mit Terraform bereitstellen

Tools

AWS-Services

- AWS Step Functions ist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen. In der grafischen Konsole von Step Functions sehen Sie den Arbeitsablauf Ihrer Anwendung als eine Reihe von ereignisgesteuerten Schritten.

- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der schnelle und vorhersehbare Leistung mit nahtloser Skalierbarkeit bietet. Sie können mit DynamoDB eine Datenbanktabelle erstellen, mit der eine beliebige Datenmenge gespeichert und abgerufen werden kann und der Anforderungsdatenverkehr verarbeitet werden kann.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon API Gateway ist ein AWS-Service für die Erstellung, Veröffentlichung, Wartung, Überwachung und Sicherung von REST, HTTP und WebSocket APIs in jeder Größenordnung.
- Amazon Simple Notification Service (Amazon SNS) ist ein verwalteter Service, der die Nachrichtenzustellung von Verlagen an Abonnenten ermöglicht.
- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungsframework zur Definition Ihrer Cloud-Anwendungsressourcen mithilfe vertrauter Programmiersprachen wie TypeScript,, Python JavaScript, Java und C#/.Net.
- Das AWS Serverless Application Model (AWS SAM) ist ein Open-Source-Framework für die Erstellung serverloser Anwendungen. Es bietet Kurzsyntax zum Ausdrücken von Funktionen APIs, Datenbanken und Zuordnungen von Ereignisquellen.

Code

Den Code für eine Beispielanwendung, die das Saga-Muster demonstriert, einschließlich der IaC-Vorlage (AWS CDK, AWS SAM oder Terraform), der Lambda-Funktionen und der DynamoDB-Tabellen, finden Sie unter den folgenden Links. Folgen Sie den Anweisungen im ersten Epos, um diese zu installieren.

- Mit AWS CDK bereitstellen
- Mit AWS SAM bereitstellen
- Mit Terraform bereitstellen

Epen

Pakete installieren, kompilieren und bauen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie die NPM-Pakete.	Erstellen Sie ein neues Verzeichnis, navigieren Sie in einem Terminal zu diesem Verzeichnis und klonen Sie das GitHub Repository Ihrer Wahl aus dem Codeabschnitt weiter oben in diesem Muster. Führen Sie im Stammordner, der die `package.json` Datei enthält, den folgenden Befehl aus, um alle Node Package Manager (NPM) - Pakete herunterzuladen und zu installieren: `npm install`	Entwickler, Cloud-Architekt
Kompilieren Sie Skripte.	Führen Sie im Stammordner den folgenden Befehl aus, um den TypeScript Transpiler anzuweisen, alle erforderlichen JavaScript Dateien zu erstellen: `npm run build`	Entwickler, Cloud-Architekt
Achten Sie auf Änderungen und kompilieren Sie sie neu.	Führen Sie im Stammordner den folgenden Befehl in einem separaten Terminalfenster aus, um nach Codeänder	Entwickler, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ungen zu suchen, und kompilieren Sie den Code, wenn eine Änderung erkannt wird: `npm run watch`	
Führen Sie Komponententests durch (nur AWS CDK).	Wenn Sie das AWS-CDK verwenden, führen Sie im Stammordner den folgenden Befehl aus, um die Jest-Komponententests durchzuführen: `npm run test`	Entwickler, Cloud-Architekt

Ressourcen für das AWS-Zielkonto bereitstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Demo-Stack auf AWS bereit.	**Important** Die Anwendung ist von der AWS-Region unabhängig. Wenn Sie ein Profil verwenden, müssen Sie die Region explizit entweder im AWS-Befehlszeilenschnittstellen-Profil (AWS CLI) oder über AWS CLI-Umgebungsvariablen deklarieren.	Entwickler, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Führen Sie im Stammordner den folgenden Befehl aus, um eine Bereitstellungsassembly zu erstellen und sie für das AWS-Standardkonto und die AWS-Region bereitzustellen.
	
	AWS-CDK:
	
	`cdk bootstrap`
	`cdk deploy`
	
	AWS-BETRUG:
	
	`sam build`
	`sam deploy --guided`
	
	Terraform:
	
	`terraform init`
	`terraform apply`
	
	Dieser Schritt kann mehrere Minuten dauern. Dieser Befehl verwendet die Standarda nmeldedaten, die für die AWS-CLI konfiguriert wurden.
	
	Notieren Sie sich die API Gateway Gateway-URL, die nach Abschluss der Bereitstellung auf der Konsole angezeigt wird. Sie benötigen diese Informationen, um den Saga-Ausführungsablauf zu testen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Vergleichen Sie den bereitgestellten Stack mit dem aktuellen Status.	Führen Sie im Stammordner den folgenden Befehl aus, um den bereitgestellten Stack mit dem aktuellen Status zu vergleichen, nachdem Sie Änderungen am Quellcode vorgenommen haben:
	AWS-CDK:
	`cdk diff`
	AWS-BETRUG:
	`sam deploy`
	Terraform:
	`terraform plan`
		Entwickler, Cloud-Architekt

Testen Sie den Ausführungsablauf

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie den Ausführungsablauf der Saga.	Navigieren Sie zu der API-Gateway-URL, die Sie im vorherigen Schritt bei der Bereitstellung des Stacks notiert haben. Diese URL löst den Start der Zustandsmaschine aus. Weitere Informationen darüber, wie Sie den Fluss der Zustandsmaschine manipulieren können, indem	Entwickler, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie verschiedene URL-Parameter übergeben, finden Sie im Abschnitt Zusätzliche Informationen. Um die Ergebnisse anzusehen, melden Sie sich bei der AWS-Managementkonsole an und navigieren Sie zur Step Functions Functions -Konsole. Hier können Sie jeden Schritt der Saga State Machine sehen. Sie können auch die DynamoDB-Tabelle anzeigen, um die eingefügten, aktualisierten oder gelöschten Datensätze zu sehen. Wenn Sie den Bildschirm häufig aktualisieren, können Sie beobachten, wie sich der Transaktionsstatus von `pending` zu `confirmed` ändert. Sie können das SNS-Thema abonnieren, indem Sie den Code in der `stateMachine.ts` Datei mit Ihrer Handynummer aktualisieren, um SMS-Nachrichten bei erfolgreichen oder fehlgeschlagenen Reservierungen zu erhalten. Weitere Informationen finden Sie unter Amazon	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SNS im Abschnitt Zusätzliche Informationen.	

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bereinigen von Ressourcen.	Um die für diese Anwendung bereitgestellten Ressourcen zu bereinigen, können Sie einen der folgenden Befehle verwenden.
	AWS-CDK:
	`cdk destroy`
	AWS-BETRUG:
	`sam delete`
	Terraform:
	`terraform destroy`
		App-Entwickler, Cloud-Architekt

Zugehörige Ressourcen

Technische Dokumente

- Implementierung von Microservices auf AWS
- Linse für serverlose Anwendungen
- Aktivierung der Datenpersistenz in Microservices

AWS-Servicedokumentation

- Erste Schritte mit dem AWS CDK
- Erste Schritte mit AWS SAM
- AWS Step Functions
- Amazon-DynamoDB
- AWS Lambda
- Amazon API Gateway
- Amazon SNS

Tutorials

- Praktische Workshops zum Thema Serverless Computing

Zusätzliche Informationen

Code

Zu Testzwecken stellt dieses Muster API Gateway und eine Test-Lambda-Funktion bereit, die die Step Functions Functions-Zustandsmaschine auslöst. Mit Step Functions können Sie die Funktionalität des Reisereservierungssystems steuern, indem Sie einen `run_type` Parameter übergeben, um Fehler in „ReserveFlight," „ReserveCarRental," „ProcessPayment," und „ConfirmFlight" nachzuahmenConfirmCarRental.

Die `saga` Lambda-Funktion (`sagaLambda.ts`) nimmt Eingaben aus den Abfrageparametern in der API-Gateway-URL entgegen, erstellt das folgende JSON-Objekt und übergibt es zur Ausführung an Step Functions:

```
let input = {
"trip_id": tripID, //  value taken from query parameter, default is AWS request ID
"depart_city": "Detroit",
"depart_time": "2021-07-07T06:00:00.000Z",
"arrive_city": "Frankfurt",
"arrive_time": "2021-07-09T08:00:00.000Z",
"rental": "BMW",
"rental_from": "2021-07-09T00:00:00.000Z",
"rental_to": "2021-07-17T00:00:00.000Z",
"run_type": runType // value taken from query parameter, default is "success"
};
```

Sie können mit verschiedenen Abläufen der Step Functions Functions-Zustandsmaschine experimentieren, indem Sie die folgenden URL-Parameter übergeben:

- Erfolgreiche Ausführung – https://{api gateway url}
- Flug reservieren gescheitert – https://{api Gateway-URL}? Ausführungstyp = failFlightsReservation
- Flugfehler bestätigen – https://{api Gateway-URL}? Ausführungstyp = failFlightsConfirmation
- Mietwagen-Reservierung ist fehlgeschlagen – https://{api Gateway-URL}? runType= Reservierung failCarRental
- Bestätigen Sie, dass die Autovermietung fehlgeschlagen ist – https://{api Gateway-URL}? runType= Bestätigung failCarRental
- Zahlungsvorgang fehlgeschlagen – https://{api Gateway-URL}? runType=Zahlung fehlschlagen
- Eine Reise-ID weitergeben – https://{api Gateway-URL}? TripId= {Standardmäßig ist die Reise-ID die AWS-Anfrage-ID}

IaC-Vorlagen

Die verknüpften Repositorien enthalten IaC-Vorlagen, mit denen Sie den gesamten Musterantrag für Reisereservierungen erstellen können.

- Mit AWS CDK bereitstellen
- Mit AWS SAM bereitstellen
- Mit Terraform bereitstellen

DynamoDB-Tabellen

Hier sind die Datenmodelle für die Tabellen mit Flügen, Mietwagen und Zahlungen.

```
Flight Data Model:
 var params = {
      TableName: process.env.TABLE_NAME,
      Item: {
        'pk' : {S: event.trip_id},
        'sk' : {S: flightReservationID},
        'trip_id' : {S: event.trip_id},
        'id': {S: flightReservationID},
        'depart_city' : {S: event.depart_city},
        'depart_time': {S: event.depart_time},
```

```
        'arrive_city': {S: event.arrive_city},
        'arrive_time': {S: event.arrive_time},
        'transaction_status': {S: 'pending'}
      }
    };

Car Rental Data Model:
var params = {
      TableName: process.env.TABLE_NAME,
      Item: {
        'pk' : {S: event.trip_id},
        'sk' : {S: carRentalReservationID},
        'trip_id' : {S: event.trip_id},
        'id': {S: carRentalReservationID},
        'rental': {S: event.rental},
        'rental_from': {S: event.rental_from},
        'rental_to': {S: event.rental_to},
        'transaction_status': {S: 'pending'}
      }
    };

Payment Data Model:
var params = {
      TableName: process.env.TABLE_NAME,
      Item: {
        'pk' : {S: event.trip_id},
        'sk' : {S: paymentID},
        'trip_id' : {S: event.trip_id},
        'id': {S: paymentID},
        'amount': {S: "750.00"}, // hard coded for simplicity as implementing any
 monetary transaction functionality is beyond the scope of this pattern
        'currency': {S: "USD"},
        'transaction_status': {S: "confirmed"}
      }
    };
```

Lambda-Funktionen

Die folgenden Funktionen werden erstellt, um den Zustandsmaschinenfluss und die Ausführung in Step Functions zu unterstützen:

- Flüge reservieren: Fügt einen Datensatz mit einem `transaction_status` of in die DynamoDB-Flugtabelle ein`pending`, um einen Flug zu buchen.

- Flug bestätigen: Aktualisiert den Datensatz in der DynamoDB-Flugtabelle, um ihn auf einzustellen`confirmed`, `transaction_status` um den Flug zu bestätigen.
- Flugreservierung stornieren: Löscht den Datensatz aus der DynamoDB-Flugtabelle, um den ausstehenden Flug zu stornieren.
- Mietwagen reservieren: Fügt einen Datensatz mit einem `transaction_status` of in die CarRentals DynamoDB-Tabelle ein`pending`, um eine Autovermietung zu buchen.
- Autovermietungen bestätigen: Aktualisiert den Datensatz in der CarRentals DynamoDB-Tabelle, um ihn auf zu setzen`confirmed`, `transaction_status` um die Autovermietung zu bestätigen.
- Mietwagenreservierung stornieren: Löscht den Datensatz aus der CarRentals DynamoDB-Tabelle, um die ausstehende Autovermietung zu stornieren.
- Zahlung verarbeiten: Fügt einen Datensatz für die Zahlung in die DynamoDB-Zahlungstabelle ein.
- Zahlung stornieren: Löscht den Datensatz für die Zahlung aus der DynamoDB-Zahlungstabelle.

Amazon SNS

Die Beispielanwendung erstellt das folgende Thema und Abonnement für den Versand von SMS-Nachrichten und die Benachrichtigung des Kunden über erfolgreiche oder fehlgeschlagene Reservierungen. Wenn Sie beim Testen der Beispielanwendung Textnachrichten empfangen möchten, aktualisieren Sie das SMS-Abonnement mit Ihrer gültigen Telefonnummer in der State-Machine-Definitionsdatei.

AWS-CDK-Snippet (fügen Sie die Telefonnummer in der zweiten Zeile des folgenden Codes hinzu):

```
const topic = new  sns.Topic(this, 'Topic');
topic.addSubscription(new subscriptions.SmsSubscription('+11111111111'));
const snsNotificationFailure = new tasks.SnsPublish(this ,'SendingSMSFailure', {
topic:topic,
integrationPattern: sfn.IntegrationPattern.REQUEST_RESPONSE,
message: sfn.TaskInput.fromText('Your Travel Reservation Failed'),
});

const snsNotificationSuccess = new tasks.SnsPublish(this ,'SendingSMSSuccess', {
topic:topic,
integrationPattern: sfn.IntegrationPattern.REQUEST_RESPONSE,
message: sfn.TaskInput.fromText('Your Travel Reservation is Successful'),
});
```

AWS SAM-Snippet (ersetzen Sie die +1111111111 Zeichenketten durch Ihre gültige Telefonnummer):

```
  StateMachineTopic11111111111:
    Type: 'AWS::SNS::Subscription'
    Properties:
      Protocol: sms
      TopicArn:
        Ref: StateMachineTopic
      Endpoint: '+11111111111'
    Metadata:
      'aws:sam:path': SamServerlessSagaStack/StateMachine/Topic/+11111111111/Resource
```

Terraform-Snippet (ersetzen Sie die +111111111 Zeichenfolge durch Ihre gültige Telefonnummer):

```
resource "aws_sns_topic_subscription" "sms-target" {
  topic_arn = aws_sns_topic.topic.arn
  protocol  = "sms"
  endpoint  = "+11111111111"
}
```

Erfolgreiche Reservierungen

Der folgende Ablauf veranschaulicht eine erfolgreiche Reservierung mit „ReserveFlight," „ReserveCarRental," und „ProcessPayment", gefolgt von „ConfirmFlight" und „"ConfirmCarRental. Der Kunde wird durch SMS-Nachrichten, die an den Abonnenten des SNS-Themas gesendet werden, über die erfolgreiche Buchung informiert.

Fehlgeschlagene Reservierungen

Dieser Ablauf ist ein Beispiel für einen Fehler im Saga-Muster. Wenn „ProcessPayment" nach der Buchung von Flügen und Mietwagen fehlschlägt, werden die Schritte in umgekehrter Reihenfolge storniert. Die Reservierungen werden freigegeben und der Kunde wird über SMS-Nachrichten, die an den Abonnenten des SNS-Themas gesendet werden, über den Fehler informiert.

Verwalten Sie lokale Containeranwendungen, indem Sie Amazon ECS Anywhere mit dem AWS CDK einrichten

Erstellt von Dr. Rahul Sharad Gaikwad (AWS)

Übersicht

Amazon ECS Anywhere ist eine Erweiterung des Amazon Elastic Container Service (Amazon ECS). Sie können ECS Anywhere verwenden, um native Amazon ECS-Aufgaben in einer lokalen oder vom Kunden verwalteten Umgebung bereitzustellen. Diese Funktion trägt dazu bei, Kosten zu senken und komplexe lokale Container-Orchestrierung und Betriebsabläufe zu vereinfachen. Sie können ECS Anywhere verwenden, um Containeranwendungen sowohl in lokalen als auch in Cloud-Umgebungen bereitzustellen und auszuführen. Dadurch entfällt für Ihr Team die Notwendigkeit, mehrere Bereiche und Fähigkeiten zu erlernen oder komplexe Software eigenständig zu verwalten.

Dieses Muster veranschaulicht die Schritte zur Einrichtung von ECS Anywhere mithilfe von AWS Cloud Development Kit (AWS CDK) -Stacks.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert. (Weitere Informationen finden Sie unter Installation, Aktualisierung und Deinstallation der AWS-CLI in der AWS-CLI-Dokumentation.)
- AWS CDK Toolkit, installiert und konfiguriert. (Sehen Sie sich das AWS CDK Toolkit in der AWS CDK-Dokumentation an und folgen Sie den Anweisungen, um Version 2 global zu installieren.)
- Node Package Manager (npm), installiert und konfiguriert für das AWS-CDK in. TypeScript (Weitere Informationen finden Sie unter Node.js und npm herunterladen und installieren in der npm-Dokumentation.)

Einschränkungen

- Einschränkungen und Überlegungen finden Sie unter Externe Instances (Amazon ECS Anywhere) in der Amazon ECS-Dokumentation.

Produktversionen

- AWS CDK Toolkit, Version 2
- npm Version 7.20.3 oder höher
- Node.js Version 16.6.1 oder höher

Architektur

Zieltechnologie-Stack

- AWS CloudFormation
- AWS-CDK
- Amazon ECS Anywhere
- AWS Identity and Access Management (IAM)

Zielarchitektur

Das folgende Diagramm zeigt eine allgemeine Systemarchitektur des ECS Anywhere-Setups unter Verwendung des AWS CDK mit TypeScript, wie in diesem Muster implementiert.

1. Wenn Sie den AWS-CDK-Stack bereitstellen, erstellt er einen CloudFormation Stack auf AWS.
2. Der CloudFormation Stack stellt einen Amazon ECS-Cluster und zugehörige AWS-Ressourcen bereit.
3. Um eine externe Instance bei einem Amazon ECS-Cluster zu registrieren, müssen Sie den AWS Systems Manager Agent (SSM Agent) auf Ihrer virtuellen Maschine (VM) installieren und die VM als von AWS Systems Manager verwaltete Instanz registrieren.
4. Sie müssen auch den Amazon ECS-Container-Agenten und Docker auf Ihrer VM installieren, um sie als externe Instance beim Amazon ECS-Cluster zu registrieren.
5. Wenn die externe Instance registriert und mit dem Amazon ECS-Cluster konfiguriert ist, kann sie mehrere Container auf Ihrer VM ausführen, die als externe Instance registriert ist.

Automatisierung und Skalierung

Das mit diesem Muster bereitgestellte GitHub Repository verwendet das AWS-CDK als Infrastructure-as-Code-Tool (IaC), um die Konfiguration für diese Architektur zu erstellen. AWS CDK hilft Ihnen bei der Orchestrierung von Ressourcen und der Einrichtung von ECS Anywhere.

Tools

- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

Code

Der Quellcode für dieses Muster ist im Amazon ECS Anywhere CDK Samples-Repository verfügbar. GitHub Folgen Sie den Anweisungen im nächsten Abschnitt, um das Repository zu klonen und zu verwenden.

Epen

Überprüfen Sie die AWS-CDK-Konfiguration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die AWS-CDK-Version.	Überprüfen Sie die Version des AWS CDK Toolkit, indem Sie den folgenden Befehl ausführen: `cdk --version` Für dieses Muster ist AWS CDK Version 2 erforderlich. Wenn Sie eine frühere Version von AWS CDK haben, folgen Sie den Anweisungen in der AWS CDK-Dokumentation, um sie zu aktualisieren.	DevOps Ingenieur
Richten Sie AWS-Anmeldeinformationen ein.	Um Anmeldeinformationen einzurichten, führen Sie den `aws configure` Befehl aus	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	und folgen Sie den Anweisungen:
	
	`$aws configure`
	`AWS Access Key ID [None]: <your-access-key-ID>`
	`AWS Secret Access Key [None]: <your-secret-access-key>`
	`Default region name [None]: <your-Region-name>`
	`Default output format [None]:`	

Bootstrap für die AWS-CDK-Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das AWS-CDK-Code-Repository.	Klonen Sie das GitHub Code-Repository für dieses Muster mit dem folgenden Befehl: `git clone https://github.com/aws-samples/amazon-ecs-anywhere-cdk-samples.git`	DevOps Ingenieur
Bootstrapping für die Umwelt.	Führen Sie den folgenden Befehl aus, um die CloudFormation AWS-Vorlage für das Konto und die AWS-Region bereitzustellen, die Sie verwenden möchten:	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cdk bootstrap <account-number>/<Region>` Weitere Informationen finden Sie unter Bootstrapping in der AWS CDK-Dokumentation.	

Erstellen und implementieren Sie das Projekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie Paketabhängigkeiten und kompilieren Sie TypeScript Dateien.	Installieren Sie die Paketabhängigkeiten und kompilieren Sie die TypeScript Dateien, indem Sie die folgenden Befehle ausführen:
	
	`$cd amazon-ecs-anywhere-cdk-samples`
	`$npm install`
	`$npm fund`
	
	Mit diesen Befehlen werden alle Pakete aus dem Beispiel-Repository installiert.
	
	⚠ Important
	Wenn Sie eine Fehlermeldung über fehlende Pakete erhalten, verwenden Sie einen der folgenden Befehle:
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`$npm ci`
	
	–oder–
	
	`$npm install -g @aws-cdk/<package_name>`
	
	Weitere Informationen finden Sie unter npm ci und npm install in der npm-Dokum entation.	

Erstellen Sie das Projekt.	Führen Sie den folgenden Befehl aus, um den Projektco de zu erstellen: `npm run build` Weitere Informationen zum Erstellen und Bereitstellen des Projekts finden Sie unter Ihre erste AWS-CDK-App in der AWS-CDK-Dokumentation.	DevOps Ingenieur
Stellen Sie das Projekt bereit.	Führen Sie den folgenden Befehl aus, um den Projektco de bereitzustellen: `cdk deploy`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Erstellung und Ausgabe des Stacks.	Öffnen Sie die CloudFormation AWS-Konsole unter https://console.aws.amazon.com/cloudformation und wählen Sie den `EcsAnywhereStack` Stack aus. Auf der Registerkarte Ausgaben werden die Befehle angezeigt, die auf Ihrer externen VM ausgeführt werden sollen.	DevOps Ingenieur

Richten Sie einen lokalen Computer ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Ihre VM mithilfe von Vagrant ein.	Zu Demonstrationszwecken können Sie HashiCorp Vagrant verwenden, um eine VM zu erstellen. Vagrant ist ein Open-Source-Hilfsprogramm für den Aufbau und die Wartung portabler virtueller Softwareentwicklungsumgebungen. Erstellen Sie eine Vagrant-VM, indem Sie den `vagrant up` Befehl im Stammverzeichnis ausführen, in dem Vagrantfile gespeichert ist. Weitere Informationen finden Sie in der Vagrant-Dokumentation.	DevOps Ingenieur
Registrieren Sie Ihre VM als externe Instanz.	1. Melden Sie sich mit dem `vagrant ssh` Befehl bei	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	der Vagrant-VM an. Weitere Informationen finden Sie in der Vagrant-Dokumentation.
	
	2. Erstellen Sie einen Aktivierungscode und eine ID, mit denen Sie Ihre VM bei AWS Systems Manager registrieren und Ihre externe Instanz aktivieren können. Die Ausgabe dieses Befehls umfasst `ActivationId` und `ActivationCode` Werte:
	
	`aws ssm create-activation --iam-role EcsAnywhereInstanceRole | tee ssm-activation.json`
	
	3. Exportieren Sie die Aktivierungs-ID und die Codewerte:
	
	`export ACTIVATION_ID=<activation-ID>`
	`export ACTIVATION_CODE=<activation-code>`
	
	4. Laden Sie das Installationsskript auf Ihren lokalen Server oder Ihre VM herunter:
	
	`curl -o "ecs-anywhere-install.sh" "https://amazon-ecs-agent.s3.amazonaws.com/ec`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`s-anywhere-install -latest.sh" && sudo chmod +x ecs-anywhere-install.sh`
	
	5. Führen Sie das Installationsskript auf Ihrem lokalen Server oder Ihrer VM aus:
	
	`sudo ./ecs-anywhere-install.sh \ --cluster test-ecs-anywhere \ --activation-id $ACTIVATION_ID \ --activation-code $ACTIVATION_CODE \ --region <Region>`
	
	Weitere Informationen zum Einrichten und Registrieren Ihrer VM finden Sie unter Registrierung einer externen Instance in einem Cluster in der Amazon ECS-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie den Status von ECS Anywhere und der externen VM.	Verwenden Sie die folgenden Befehle, um zu überprüfen, ob Ihre virtuelle Box mit der Amazon ECS-Steuerebene verbunden ist und läuft:
	`aws ssm describe-instance-information`
	`aws ecs list-container-instances --cluster $CLUSTER_NAME`
		DevOps Ingenieur

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ressourcen bereinigen und löschen.	Nachdem Sie dieses Muster durchgegangen sind, sollten Sie die Ressourcen, die Sie erstellt haben, entfernen, um weitere Kosten zu vermeiden . Führen Sie zum Aufräumen den folgenden Befehl aus: `cdk destroy`	DevOps Ingenieur

Zugehörige Ressourcen

- Dokumentation zu Amazon ECS Anywhere
- Amazon ECS Anywhere Anywhere-Demo
- Beispiele Amazon ECS Anywhere Anywhere-Workshops

Modernisieren Sie ASP.NET Web Forms-Anwendungen auf AWS

Erstellt von Vijai Anand Ramalingam (AWS) und Sreelaxmi Pai (AWS)

Übersicht

Dieses Muster beschreibt die Schritte zur Modernisierung einer älteren, monolithischen ASP.NET Web Forms-Anwendung durch Portierung auf ASP.NET Core auf AWS.

Durch die Portierung von ASP.NET Web Forms-Anwendungen auf ASP.NET Core können Sie die Leistung, die Kosteneinsparungen und das robuste Ökosystem von Linux nutzen. Dies kann jedoch ein erheblicher manueller Aufwand sein. In diesem Muster wird die Legacy-Anwendung schrittweise mithilfe eines schrittweisen Ansatzes modernisiert und anschließend in der AWS-Cloud containerisiert.

Stellen Sie sich eine ältere, monolithische Anwendung für einen Einkaufswagen vor. Nehmen wir an, dass sie als ASP.NET-Webforms-Anwendung erstellt wurde und aus ASPX-Seiten mit einer Code-Behind () -Datei besteht. `aspx.cs` Der Modernisierungsprozess besteht aus den folgenden Schritten:

1. Teilen Sie den Monolith in Microservices auf, indem Sie die entsprechenden Zerlegungsmuster verwenden. Weitere Informationen finden Sie im Leitfaden Decomposing monoliths into microservices auf der AWS Prescriptive Guidance Guidance-Website.
2. Portieren Sie Ihre ältere ASP.NET Web Forms (.NET Framework) -Anwendung auf ASP.NET Core in .NET 5 oder höher. In diesem Muster verwenden Sie den Portierungsassistenten für .NET, um Ihre ASP.NET Web Forms-Anwendung zu scannen und Inkompatibilitäten mit ASP.NET Core zu identifizieren. Dadurch wird der manuelle Portierungsaufwand reduziert.
3. Entwickeln Sie die Web Forms-Benutzeroberflächenebene mithilfe von React neu. Dieses Muster deckt die Neuentwicklung der Benutzeroberfläche nicht ab. Anweisungen finden Sie unter Neue React-App erstellen in der React-Dokumentation.
4. Entwickeln Sie die Web Forms-Codebehind-Datei (Geschäftsschnittstelle) als ASP.NET Core-Web-API neu. Dieses Muster verwendet NDepend Berichte, um benötigte Dateien und Abhängigkeiten zu identifizieren.
5. Aktualisieren Sie gemeinsam genutzte oder häufig genutzte Projekte wie Business Logic und Data Access in Ihrer Legacy-Anwendung auf .NET 5 oder höher, indem Sie den Portierungsassistenten für .NET verwenden.
6. Fügen Sie AWS-Services hinzu, um Ihre Anwendung zu ergänzen. Sie können beispielsweise Amazon CloudWatch Logs verwenden, um die Protokolle Ihrer Anwendung

zu überwachen, zu speichern und darauf zuzugreifen, und AWS Systems Manager, um Ihre Anwendungseinstellungen zu speichern.

7. Containerisieren Sie die modernisierte ASP.NET Core-Anwendung. Dieses Muster erstellt eine Docker-Datei, die auf Linux in Visual Studio abzielt und Docker Desktop verwendet, um sie lokal zu testen. In diesem Schritt wird davon ausgegangen, dass Ihre Legacy-Anwendung bereits auf einer lokalen Windows-Instance oder einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance ausgeführt wird. Weitere Informationen finden Sie im Muster Einen ASP.NET Core-Web-API-Docker-Container auf einer Amazon EC2 Linux-Instance ausführen.
8. Stellen Sie die modernisierte ASP.NET-Kernanwendung auf Amazon Elastic Container Service (Amazon ECS) bereit. Dieses Muster deckt den Bereitstellungsschritt nicht ab. Anweisungen finden Sie im Amazon ECS-Workshop.

> **Note**
>
> Dieses Muster deckt keine Schritte zur Entwicklung der Benutzeroberfläche, zur Datenbankmodernisierung oder zur Container-Bereitstellung ab.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Visual Studio oder Visual Studio Code, heruntergeladen und installiert.
- Zugriff auf ein AWS-Konto über die AWS-Managementkonsole und die AWS-Befehlszeilenschnittstelle (AWS CLI) Version 2. (Weitere Informationen finden Sie in den Anweisungen zur Konfiguration der AWS-CLI.)
- Das AWS Toolkit for Visual Studio (siehe Anweisungen zur Einrichtung).
- Docker Desktop, heruntergeladen und installiert.
- .NET SDK, heruntergeladen und installiert.
- NDepend Tool, heruntergeladen und installiert. Um die NDepend Erweiterung für Visual Studio zu installieren, führen Sie den `NDepend.VisualStudioExtension.Installer` Befehl aus (siehe Anweisungen). Sie können je nach Ihren Anforderungen Visual Studio 2019 oder 2022 auswählen.
- Portierungsassistent für .NET, heruntergeladen und installiert.

Architektur

Modernisierung der Warenkorb-Anwendung

Das folgende Diagramm veranschaulicht den Modernisierungsprozess für eine ältere ASP.NET-Einkaufswagenanwendung.

Zielarchitektur

Das folgende Diagramm veranschaulicht die Architektur der modernisierten Einkaufswagen-Anwendung auf AWS. ASP.NET Core-Web APIs werden in einem Amazon ECS-Cluster bereitgestellt. Protokollierungs- und Konfigurationsservices werden von Amazon CloudWatch Logs und AWS Systems Manager bereitgestellt.

Tools

AWS-Services

- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service zum Ausführen, Stoppen und Verwalten von Containern in einem Cluster. Sie können Ihre Aufgaben und Services auf einer serverlosen Infrastruktur ausführen, die von AWS Fargate verwaltet wird. Um mehr Kontrolle über Ihre Infrastruktur zu erhalten, können Sie Ihre Aufgaben und Dienste alternativ auf einem Cluster von EC2 Instances ausführen, die Sie verwalten.
- Amazon CloudWatch Logs — Amazon CloudWatch Logs zentralisiert die Protokolle all Ihrer Systeme, Anwendungen und AWS-Services, die Sie verwenden. Sie können die Protokolle anzeigen und überwachen, sie nach bestimmten Fehlercodes oder Mustern durchsuchen, sie nach bestimmten Feldern filtern oder sie für future Analysen sicher archivieren.
- AWS Systems Manager – AWS Systems Manager ist ein AWS-Service, mit dem Sie Ihre Infrastruktur auf AWS anzeigen und steuern können. Mithilfe der Systems Manager Manager-Konsole können Sie Betriebsdaten von mehreren AWS-Services anzeigen und betriebliche Aufgaben in Ihren AWS-Ressourcen automatisieren. Systems Manager unterstützt Sie bei der Aufrechterhaltung von Sicherheit und Compliance, indem es Ihre verwalteten Instanzen scannt und festgestellte Richtlinienverstöße meldet (oder Korrekturmaßnahmen ergreift).

Tools

- Visual Studio oder Visual Studio Code — Tools zum Erstellen von.NET-Anwendungen APIs, Web- und anderen Programmen.
- AWS Toolkit for Visual Studio — Eine Erweiterung für Visual Studio, die beim Entwickeln, Debuggen und Bereitstellen von.NET-Anwendungen hilft, die AWS-Services verwenden.
- Docker Desktop — Ein Tool, das die Erstellung und Bereitstellung containerisierter Anwendungen vereinfacht.
- NDepend— Ein Analysator, der .NET-Code auf Abhängigkeiten, Qualitätsprobleme und Codeänderungen überwacht.
- Portierungsassistent für .NET — Ein Analysetool, das .NET-Code scannt, um Inkompatibilitäten mit .NET Core zu identifizieren und den Migrationsaufwand abzuschätzen.

Epen

Portieren Sie Ihre Legacy-Anwendung auf .NET 5 oder eine neuere Version

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie Ihre.NET Framework-Legacy-Anwendung auf .NET 5.	Sie können den Portierungsassistenten für .NET verwenden, um Ihre ältere ASP.NET Web Forms-Anwendung auf .NET 5 oder höher zu konvertieren. Folgen Sie den Anweisungen in der Dokumentation zu Porting Assistant for .NET.	App-Developer
Generieren Sie NDepend Berichte.	Wenn Sie Ihre ASP.NET Web Forms-Anwendung modernisieren, indem Sie sie in Microservices zerlegen, benötigen Sie möglicherweise nicht alle .cs-Dateien aus der Legacy-Anwendung. Sie können NDepend damit einen Bericht für jede Code-Behi	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	nd (.cs) -Datei generieren, um alle Anrufer und Anrufer abzurufen. Dieser Bericht hilft Ihnen dabei, nur die erforderlichen Dateien in Ihren Microservices zu identifizieren und zu verwenden. Öffnen Sie nach der Installat ion NDepend (siehe Abschnitt Voraussetzungen) die Lösung (.sln-Datei) für Ihre Legacy-An wendung in Visual Studio und gehen Sie wie folgt vor: 1. Erstellen Sie die Legacy-An wendung in Visual Studio. 2. Wählen Sie NDepend in der Visual Studio-Menüleiste die Option Neues NDepend Projekt an aktuelle VS-Lösung anhängen. 3. Wählen Sie .NET-Asse mblys analysieren. 4. Wenn die Analyse abgeschlossen ist, navigieren Sie im Solution Explorer zu dem Projekt. Klicken Sie mit der rechten Maustaste auf eine beliebige Codebehind-Datei (z. B.`listprodu cts.aspx.cs`), für die Sie den Bericht erstellen möchten, und wählen Sie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dann Im Abhängigkeitsdiagramm anzeigen aus. 5. Wählen Sie in der Navigationsleiste Anrufer und Anrufer und anschließend Codeabfrage bearbeiten aus. 6. Wählen Sie im Bereich Abfragen und Regeln bearbeiten den Download-Pfeil und dann Nach Excel exportieren aus. Dieser Vorgang generiert einen Bericht für die Code-Behind-Datei, in der alle Anrufer und Anrufer aufgeführt sind. Weitere Informationen zum Abhängigkeitsdiagramm finden Sie in der Dokumentation. NDepend	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine neue.NET 5-Lösung.	So erstellen Sie eine neue.NET 5-Struktur (oder höher) für Ihr modernisiertes ASP.NET Core-Web: APIs 1. Öffnen Sie Visual Studio. 2. Erstellen Sie eine neue, leere Lösung. 3. Erstellen Sie neue Projekte, die auf .NET 5 (oder höher) abzielen und auf Ihrer Legacy-Anwendung basieren. Beispiele für ältere und neue Projekte für eine Einkaufswagen-Anwendung finden Sie im Abschnitt Zusätzliche Informationen. 4. Verwenden Sie den NDepend Bericht aus dem vorherigen Schritt, um alle erforderlichen Dateien zu identifizieren. Kopieren Sie diese Dateien aus der Anwendung, die Sie zuvor aktualisiert haben, und fügen Sie sie der neuen Lösung hinzu. 5. Erstellen Sie die Lösung und beheben Sie alle Probleme. Weitere Informationen zum Erstellen von Projekten und	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Lösungen finden Sie in der Visual Studio-Dokumentation. **Note** Beim Erstellen der Lösung und beim Überprüfen der Funktionalität können Sie zusätzlich zu den NDepend identifizierten Dateien mehrere zusätzliche Dateien identifizieren, die der Lösung hinzugefügt werden sollen.	

Aktualisieren Sie Ihren Anwendungscode

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Implementieren Sie das Web APIs mit ASP.NET Core.	Nehmen wir an, dass es sich bei einem der Microservices, die Sie in Ihrer alten Monolith-Einkaufswagen-Anwendung identifiziert haben, um Produkte handelt. Sie haben im vorherigen Epos ein neues ASP.NET Core-Web-API-Projekt für Produkte erstellt. In diesem Schritt identifizieren und modernisieren Sie alle Webformulare	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(.aspx-Seiten), die sich auf Produkte beziehen. Gehen wir davon aus, dass Produkte aus vier Webformularen bestehen, wie weiter oben im Abschnitt Architektur dargestellt: • Produkte auflisten • Produkt ansehen • Produkt hinzufügen/bearbeiten • Produkt löschen Sie sollten jedes Webformular analysieren, alle Anfragen identifizieren, die an die Datenbank gesendet werden, um eine gewisse Logik auszuführen, und Antworten erhalten. Sie können jede Anfrage als Web-API-Endpunkt implementieren. Aufgrund ihrer Webformulare können Produkte die folgenden möglichen Endpunkte haben: • `/api/products` • `/api/products/{id}` • `/api/products/add` • `/api/products/update/{id}` • `/api/products/delete/{id}`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wie bereits erwähnt, können Sie auch alle anderen Projekte, die Sie auf .NET 5 aktualisiert haben, wiederver wenden, einschließlich Business Logic, Data Access und gemeinsam genutzte/ gemeinsame Projekte.	
Konfigurieren Sie Amazon CloudWatch Logs.	Sie können Amazon CloudWatch Logs verwenden , um die Protokolle Ihrer Anwendung zu überwache n, zu speichern und darauf zuzugreifen. Sie können Daten mithilfe eines AWS-SDK in Amazon CloudWatch Logs protokollieren. Sie können auch.NET-Anwendungen in CloudWatch Logs integrier en, indem Sie gängige .NET-Logging-Frameworks wie NLogLog4Net und das ASP.NET Core-Logging-Framework verwenden. Weitere Informationen zu diesem Schritt finden Sie im Blogbeitrag Amazon CloudWatch Logs and.NET Logging Frameworks.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den AWS Systems Manager Parameter Store.	Sie können den AWS Systems Manager Parameter Store verwenden, um Anwendungseinstellungen wie Verbindungszeichenfolgen getrennt vom Code Ihrer Anwendung zu speichern. Das NuGet Paket Amazon.Extensions.Configuration.SystemsManager vereinfacht, wie Ihre Anwendung diese Einstellungen aus dem AWS Systems Manager Parameter Store in das .NET Core-Konfigurationssystem lädt. Weitere Informationen zu diesem Schritt finden Sie im Blogbeitrag .NET Core-Konfigurationsanbieter für AWS Systems Manager.	App-Developer

Fügen Sie Authentifizierung und Autorisierung hinzu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie ein geteiltes Cookie zur Authentifizierung.	Die Modernisierung einer älteren Monolith-Anwendung ist ein iterativer Prozess, bei dem der Monolith und seine modernisierte Version nebeneinander existieren müssen. Sie können ein geteiltes Cookie verwenden	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	, um eine nahtlose Authentif izierung zwischen den beiden Versionen zu erreichen . Die ältere ASP.NET-A nwendung validiert weiterhin die Benutzeranmeldeinf ormationen und gibt das Cookie aus, während die modernisierte ASP.NET Core-Anwendung das Cookie validiert. Anweisungen und Beispielc ode finden Sie im Beispielp rojekt. GitHub	

Erstellen Sie den Container und führen Sie ihn lokal aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Docker-Im age mit Visual Studio.	In diesem Schritt erstellen Sie eine Docker-Datei mithilfe der Visual Studio for .NET Core-Web-API. 1. Öffnen Sie Visual Studio. 2. Wählen Sie im Solution Explorer im Kontextmenü (Rechtsklick) Ihres Projekts die Optionen Hinzufügen, Docker-Unterstützung aus. 3. Wählen Sie Linux als Zielbetriebssystem aus.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Visual Studio erstellt eine Docker-Datei für Ihr Projekt. Eine Docker-Beispieldatei finden Sie unter Visual Studio Container Tools for Docker auf der Microsoft-Website.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den Container mit Docker Desktop und führen Sie ihn aus.	Jetzt können Sie den Container in Docker Desktop erstellen, erstellen und ausführen.
	1. Öffnen Sie ein Befehlszeilenfenster. Navigieren Sie zu dem Lösungsordner, in dem sich die Docker-Datei befindet. Führen Sie den folgenden Befehl aus, um das Docker-Image zu erstellen:
	`docker build -t aspnetcorewebapiimage -f Dockerfile .`
	2. Führen Sie den folgenden Befehl aus, um alle Docker-Images anzuzeigen:
	`docker images`
	3. Führen Sie den folgenden Befehl aus, um einen Container zu erstellen und auszuführen:
	`docker run -d -p 8080:80 --name aspnetcorewebapicontainer aspnetcorewebapiimage`
	4. Öffnen Sie Docker Desktop und wählen Sie dann
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Containers/Apps. Sie können einen neuen Container mit dem Namen running sehen. `aspnetcoreewebapicontainer`	

Zugehörige Ressourcen

- Einen ASP.NET Core-Web-API-Docker-Container auf einer Amazon EC2 Linux-Instance ausführen (AWS Prescriptive Guidance)
- Amazon ECS-Workshop
- Führen Sie ECS Blue/Green-Bereitstellungen CodeDeploy mithilfe von AWS durch CloudFormation (AWS-Dokumentation) CloudFormation
- Erste Schritte mit NDepend (Dokumentation) NDepend
- Portierungsassistent für .NET

Zusätzliche Informationen

Die folgenden Tabellen enthalten Beispiele für Beispielprojekte für eine ältere Warenkorbanwendung und die entsprechenden Projekte in Ihrer modernisierten ASP.NET Core-Anwendung.

Legacy-Lösung:

Project name	Vorlage für ein Projekt	Target framework
Geschäftsschnittstelle	Klassenbibliothek	.NET Framework.
BusinessLogic	Klassenbibliothek	.NET Framework.
WebApplication	ASP.NET Framework-Webanwendung	.NET Framework.
UnitTests	NUnit Projekt testen	.NET Framework.
Geteilt -> Allgemein	Klassenbibliothek	.NET Framework.

Geteilt -> Framework	Klassenbibliothek	.NET Framework.

Neue Lösung:

Project name	Vorlage für ein Projekt	Target framework
BusinessLogic	Klassenbibliothek	.NET 5.0
<WebAPI>	ASP.NET-Core-Web-API	.NET 5.0
<WebAPI>. UnitTests	NUnit 3 Testprojekt	.NET 5.0
Geteilt -> Allgemein	Klassenbibliothek	.NET 5.0
Geteilt -> Framework	Klassenbibliothek	.NET 5.0

Führen Sie ereignisgesteuerte und geplante Workloads in großem Umfang mit AWS Fargate aus

Erstellt von HARI OHM PRASATH RAJAGOPAL (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Dieses Muster beschreibt, wie geplante und ereignisgesteuerte Workloads mithilfe von AWS Fargate in großem Umfang in der Amazon Web Services (AWS) -Cloud ausgeführt werden.

In dem Anwendungsfall, den dieses Muster einrichtet, wird der Code immer dann nach sensiblen AWS-Informationen wie der AWS-Kontonummer und den Anmeldeinformationen durchsucht, wenn eine Pull-Anfrage eingereicht wird. Die Pull-Anfrage initiiert eine Lambda-Funktion. Die Lambda-Funktion ruft eine Fargate-Aufgabe auf, die sich um den Codescan kümmert. Lambda wird immer dann initiiert, wenn eine neue Pull-Anfrage gestellt wird. Wenn beim Scan vertrauliche Informationen gefunden werden, sendet Amazon Simple Notification Service (Amazon SNS) die Scanergebnisse in einer E-Mail-Nachricht.

Dieses Muster ist in den folgenden Geschäftsanwendungsfällen hilfreich:

- Wenn Ihr Unternehmen viele geplante und ereignisgesteuerte Workloads ausführen muss, die aufgrund von Einschränkungen in Bezug auf Laufzeit (15-Minuten-Limit) oder Arbeitsspeicher nicht von AWS Lambda ausgeführt werden können
- Wenn Sie möchten, dass AWS die für diese Workloads bereitgestellten Instances verwaltet

Wenn Sie dieses Muster verwenden, haben Sie die Möglichkeit, eine neue Virtual Private Cloud (VPC) zu erstellen. Dieses Muster verwendet AWS CodeCommit auch.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS CodeCommit für das Hosten der Codebasis und das Erstellen von Pull-Requests
- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 1.7 oder höher, installiert und konfiguriert auf macOS, Linux oder Windows

- Workloads, die in Containern ausgeführt werden
- Ausführbare Apache Maven-Datei, die im Klassenpfad eingerichtet ist

Architektur

Der gesamte Ablauf umfasst die folgenden Schritte.

1. Immer wenn eine neue Pull-Anfrage eingereicht wird CodeCommit, wird eine Lambda-Funktion initiiert. Die Lambda-Funktion überwacht das `CodeCommit Pull Request State Change` Ereignis über Amazon. EventBridge
2. Die Lambda-Funktion sendet eine neue Fargate-Aufgabe mit den folgenden Umgebungsparametern zum Auschecken und Scannen des Codes.

   ```
   RUNNER # <<TaskARN>>
   SNS_TOPIC # <<SNSTopicARN>>
   SUBNET # <<Subnet in which Fargate task gets launched>>
   ```

   Findet der Scan vertrauliche Informationen im Code, leitet Fargate eine neue Nachricht an das Amazon SNS SNS-Thema weiter.
3. Ein SNS-Abonnent liest die Nachricht aus dem Thema und sendet eine E-Mail-Nachricht.

Technologie

- AWS CodeCommit
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)
- Amazon EventBridge
- AWS Fargate
- AWS Lambda
- Amazon SNS
- Docker

Tools

Tools

- AWS CLI — Die AWS-Befehlszeilenschnittstelle (CLI) ist ein einheitliches Tool zur Verwaltung Ihrer AWS-Services.
- AWS CodeCommit — AWS CodeCommit ist ein vollständig verwalteter Quellcodeverwaltungsservice, der sichere Git-basierte Repositorys hostet. Auf diese CodeCommit Weise können Teams in einer sicheren und hochgradig skalierbaren Umgebung gemeinsam an Code arbeiten.
- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) ist eine vollständig verwaltete Registry, die Entwickler zum Speichern, Verwalten und Bereitstellen von Docker-Container-Images verwenden können.
- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service. Sie können Amazon ECS verwenden, um Container in einem Cluster auszuführen, zu stoppen und zu verwalten.
- AWS Fargate — AWS Fargate ist eine Technologie, die Sie mit Amazon ECS verwenden können, um Container auszuführen, ohne Server oder Cluster von EC2 Amazon-Instances verwalten zu müssen.
- AWS Lambda — AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) ist ein verwalteter Service, der die Nachrichtenzustellung von Verlagen an Abonnenten (auch bekannt als Produzenten und Verbraucher) ermöglicht. Herausgeber kommunizieren asynchron mit Abonnenten, indem sie eine Nachricht erstellen und an ein Thema senden, bei dem es sich um einen logischen Zugriffspunkt und Kommunikationskanal handelt. Kunden, die das SNS-Thema abonnieren, erhalten veröffentlichte Nachrichten über ein unterstütztes Protokoll wie Lambda, E-Mail, mobile Push-Benachrichtigungen und mobile Textnachrichten (SMS).
- Docker — Docker unterstützt Sie beim Erstellen, Testen und Bereitstellen von Anwendungen in Paketen, die als Container bezeichnet werden.
- Git-Client — Befehlszeilen- oder Desktop-Tool zum Auschecken der benötigten Artefakte
- Maven — Apache Maven ist ein Projektmanagement-Tool zur zentralen Verwaltung des Builds, der Berichterstattung und der Dokumentation eines Projekts.

Epen

Richten Sie das lokale Repository ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Code herunter.	Laden Sie im Bereich Anlagen die ZIP-Datei herunter und extrahieren Sie die Dateien.	Entwickler, AWS-Systemadministrator
Richten Sie das Repo ein.	Führen Sie es `mvn clean install` im Stammordner aus.	Entwickler, AWS-Systemadministrator

Erstellen Sie ein Amazon ECR-Image und übertragen Sie das Image

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon ECR-Repository und melden Sie sich an.	Öffnen Sie die Amazon ECR-Konsole. Wählen Sie im Navigationsbereich Repositories und dann Create repository aus. Hilfe zu dieser und anderen Geschichten finden Sie im Abschnitt Verwandte Ressourcen.	Entwickler, AWS-Systemadministrator
Pushen Sie Ihr Container-Image.	Öffnen Sie das Repository, wählen Sie Push-Befehle anzeigen und melden Sie sich bei Docker an. Nachdem Sie angemeldet sind, führen Sie die Befehle mit den erforderlichen Ersetzungen aus, die sich unter Push the container image im Abschnitt Zusätzliche Informationen befinden.	Entwickler, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dadurch wird das Docker-Container-Image hochgeladen, das zum Scannen von Code verwendet wird. Nachdem der Upload abgeschlossen ist, kopieren Sie die URL des neuesten Builds in das Amazon ECR-Repository.	

Erstellen Sie das CodeCommit Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das CodeCommit Repository.	Um ein neues CodeCommit AWS-Repository zu erstellen, führen Sie den Befehl unter CodeCommit Repository erstellen im Abschnitt Zusätzliche Informationen aus.	Entwickler, AWS-Systemadministrator

Erstellen Sie die VPC (optional)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC.	Wenn Sie eine neue VPC anstelle einer vorhandenen verwenden möchten, führen Sie die Befehle unter VPC erstellen im Abschnitt Zusätzliche Informationen aus. Das AWS Cloud Development Kit (AWS CDK) -Skript gibt die	Entwickler, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Daten IDs der erstellten VPC und des Subnetzes aus.	

Erstellen Sie den Amazon ECS-Cluster und die Fargate-Aufgabe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Cluster und die Aufgabe.	Um einen Amazon ECS-Cluster und eine Fargate-Aufgabendefinition zu erstellen, führen Sie die Befehle unter Cluster und Aufgabe erstellen im Abschnitt Zusätzliche Informationen aus. Stellen Sie sicher, dass bei der Ausführung des Shell-Skripts die richtige VPC-ID und der Amazon ECR-Repo-URI als Parameter übergeben werden. Das Skript erstellt eine Fargate-Aufgabendefinition, die auf das Docker-Image (verantwortlich für das Scannen) verweist. Das Skript erstellt dann einen Job und eine zugehörige Ausführungsrolle.	Entwickler, AWS-Systemadministrator
Überprüfen Sie den Amazon ECS-Cluster.	Öffnen Sie die Amazon-ECS-Konsole. Wählen Sie im Navigationsbereich Clusters und dann den neu erstellten Amazon ECS-Cluster mit dem Namen Fargate-Job-Cluster aus. Wählen Sie anschließend im Navigationsbereich	Entwickler, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Aufgabendefinition aus und vergewissern Sie sich, dass es eine neue Aufgabend efinition mit dem Präfix gibt. `awscdkfargateecsTa skDef`	

Erstellen Sie das SNS-Thema und den Abonnenten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein SNS-Thema.	Um ein SNS-Thema zu erstellen, führen Sie den Befehl unter SNS-Thema erstellen im Abschnitt Zusätzliche Informationen aus. Notieren Sie sich nach erfolgreicher Erstellung den`SNS ARN`, der im nächsten Schritt verwendet wird.	Entwickler, AWS-Syste madministrator
Erstellen Sie den SNS-Abonn enten.	Um einen E-Mail-Abonnenten für das SNS-Thema zu erstellen, führen Sie den Befehl unter SNS-Abonn ent erstellen im Abschnitt Zusätzliche Informationen aus. Stellen Sie sicher, dass Sie den Befehl ersetzen `TopicARN` und `Email address` im CLI-Befehl verwenden. Um E-Mail-Be nachrichtigungen zu erhalten, stellen Sie sicher, dass Sie die	Entwickler, AWS-Syste madministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	E-Mail-Adresse bestätigen, die als Abonnent verwendet wird.	

Lambda-Funktion erstellen und auslösen CodeCommit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Funktion und den Auslöser.	Um eine Lambda-Funktion mit einem CodeCommit Trigger zu erstellen, führen Sie den Befehl unter Lambda-Funktion und CodeCommit Trigger im Abschnitt Zusätzliche Informationen aus. Stellen Sie sicher, dass Sie die Parameter durch die entsprechenden Werte ersetzen, bevor Sie den Befehl ausführen. Das Skript erstellt die Lambda-Funktion und konfiguriert sie so, dass sie aufgerufen wird, wenn eine neue Pull-Anfrage gestellt wird.	Entwickler, AWS-Systemadministrator

Testen der Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Anwendung.	Wenn Sie vertrauliche AWS-Informationen in das CodeCommit Repo einchecken, sollte die Lambda-Funktion initiiert werden. Die Lambda-Funktion initiiert die Fargate-A	Entwickler, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ufgabe, die den Code scannt und die Scanergebnisse in einer E-Mail-Benachrichtigung sendet.	

Zugehörige Ressourcen

- Erstellen eines Amazon ECR-Repositorys
- Docker-Images auf Amazon ECR übertragen

Zusätzliche Informationen

Übertragen Sie das Container-Image

```
> cd 1-ecr-image-push
> ./run.sh <<ecr-repository>>
```

Erstellen Sie das CodeCommit Repository

```
aws codecommit create-repository --repository-name test-repo --repository-description
 "My Test repository"
```

Erstellen einer VPC

```
> cd 2-create-vpc
> ./run.sh
```

Ausgabe

```
aws-batch-cdk-vpc-efs-launch-template.privatesubnet = subnet-<<id>>
aws-batch-cdk-vpc-efs-launch-template.publicsubnet = subnet-<<id>>
aws-batch-cdk-vpc-efs-launch-template.vpcid = vpc-<<id>>
```

Erstellen Sie den Cluster und die Aufgabe

```
> export CDK_DEFAULT_ACCOUNT = <<aws_account_id>>
> export CDK_DEFAULT_REGION = <<aws_region>>
> cd 3-create-ecs-task
> ./run.sh <<vpc-id>> <<ecr-repo-uri>>
```

Ausgabe

```
aws-cdk-fargate-ecs.CLUSTERNAME = Fargate-Job-Cluster
aws-cdk-fargate-ecs.ClusterARN = <<cluster_arn>>
aws-cdk-fargate-ecs.ContainerARN = Fargate-Container
aws-cdk-fargate-ecs.TaskARN = <<task_arn>>
aws-cdk-fargate-ecs.TaskExecutionRole = <<execution_role_arn>>
aws-cdk-fargate-ecs.TaskRole = <<task_role_arn>>
```

Erstellen Sie das SNS-Thema

```
aws sns create-topic --name code-commit-topic
```

Erstellen Sie den SNS-Abonnenten

```
aws sns subscribe \
    --topic-arn <<topic_arn>> \
    --protocol email \
    --notification-endpoint <<email_address>>
```

Lambda-Funktion und Trigger CodeCommit

```
> export CDK_DEFAULT_ACCOUNT = <<aws_account_id>>
> export CDK_DEFAULT_REGION = <<aws_region>>
> cd 5-Lambda-CodeCommit-Trigger
> ./run.sh <<taskarn>> <<snstopicarn>> subnet-<<id>> <<codecommitarn>>
```

Ausgabe

```
aws-cdk-fargate-lambda-event.Cloudwatchrule = <<cloudwatchrule>>
aws-cdk-fargate-lambda-event.CodeCommitLambda = AWS-Code-Scanner-Function
aws-cdk-fargate-lambda-event.LambdaRole = <<lambdaiamrole>>
```

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Mandanten-Onboarding in der SaaS-Architektur für das Silomodell mit C# und AWS CDK

Erstellt von Tabby Ward (AWS), Susmitha Reddy Gankidi (AWS) und Vijai Anand Ramalingam (AWS)

Übersicht

Software-as-a-Service (SaaS) -Anwendungen können mit einer Vielzahl unterschiedlicher Architekturmodelle erstellt werden. Das Silomodell bezieht sich auf eine Architektur, in der Mandanten dedizierte Ressourcen zur Verfügung gestellt werden.

SaaS-Anwendungen basieren auf einem reibungslosen Modell für die Einführung neuer Mandanten in ihre Umgebung. Dies erfordert häufig die Orchestrierung einer Reihe von Komponenten, um alle Elemente, die für die Erstellung eines neuen Mandanten erforderlich sind, erfolgreich bereitzustellen und zu konfigurieren. Dieser Prozess wird in der SaaS-Architektur als Mandanten-Onboarding bezeichnet. Das Onboarding sollte für jede SaaS-Umgebung vollständig automatisiert werden, indem Infrastruktur als Code in Ihrem Onboarding-Prozess verwendet wird.

Dieses Muster führt Sie durch ein Beispiel für die Erstellung eines Mandanten und die Bereitstellung einer Basisinfrastruktur für den Mandanten auf Amazon Web Services (AWS). Das Muster verwendet C# und das AWS Cloud Development Kit (AWS CDK).

Da dieses Muster einen Fakturierungsalarm auslöst, empfehlen wir, den Stack in der AWS-Region USA Ost (Nord-Virginia) oder US-East-1 bereitzustellen. Weitere Informationen finden Sie in der AWS-Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein AWS Identity and Access Management (IAM) -Principal mit ausreichendem IAM-Zugriff, um AWS-Ressourcen für dieses Muster zu erstellen. Weitere Informationen finden Sie unter IAM-Rollen.
- Installieren Sie Amazon Command Line Interface (AWS CLI) und konfigurieren Sie AWS CLI für die AWS-CDK-Bereitstellung.
- Visual Studio 2022 wurde heruntergeladen und installiert oder Visual Studio Code wurde heruntergeladen und installiert.

- Einrichtung von AWS Toolkit for Visual Studio.
- .NET Core 3.1 oder höher (erforderlich für C# AWS CDK-Anwendungen)
- Amazon.Lambda.Tools installiert.

Einschränkungen

- AWS CDK verwendet AWS CloudFormation, sodass AWS-CDK-Anwendungen CloudFormation Service-Kontingenten unterliegen. Weitere Informationen finden Sie unter CloudFormation AWS-Kontingente.
- Der CloudFormation Mandanten-Stack wird mit einer CloudFormation Servicerolle `infra-cloudformation-role` mit Platzhalterzeichen für Aktionen (`sns*` und`sqs*`) erstellt, wobei die Ressourcen jedoch auf das `tenant-cluster` Präfix beschränkt sind. Evaluieren Sie diese Einstellung für einen Produktionsanwendungsfall und gewähren Sie nur den erforderlichen Zugriff auf diese Servicerolle. Die `InfrastructureProvision` Lambda-Funktion verwendet auch ein Platzhalterzeichen (`cloudformation*`), um den CloudFormation Stack bereitzustellen, wobei die Ressourcen jedoch auf das `tenant-cluster` Präfix beschränkt sind.
- Der Docker-Build dieses Beispielcodes verwendet`--platform=linux/amd64`, um `linux/amd64` basierte Images zu erzwingen. Dadurch soll sichergestellt werden, dass die endgültigen Bildartefakte für Lambda geeignet sind, das standardmäßig die x86-64-Architektur verwendet. Wenn Sie die Lambda-Zielarchitektur ändern müssen, stellen Sie sicher, dass Sie sowohl die Dockerfiles als auch die AWS-CDK-Codes ändern. Weitere Informationen finden Sie im Blogbeitrag Migration von AWS Lambda Lambda-Funktionen auf ARM-basierte AWS Graviton2-Prozessoren.
- Beim Löschen des Stacks werden keine vom Stack generierten CloudWatch Protokolle (Protokollgruppen und Protokolle) bereinigt. Sie müssen die Protokolle manuell über die AWS-Managementkonsole, die CloudWatch Amazon-Konsole oder die API bereinigen.

Dieses Muster dient als Beispiel. Evaluieren Sie für den Einsatz in der Produktion die folgenden Konfigurationen und nehmen Sie je nach Ihren Geschäftsanforderungen Änderungen vor:

- Für den Bucket AWS Simple Storage Service (Amazon S3) ist in diesem Beispiel der Einfachheit halber die Versionierung nicht aktiviert. Evaluieren und aktualisieren Sie das Setup nach Bedarf.
- In diesem Beispiel werden der Einfachheit halber Amazon API Gateway REST-API-Endpunkte ohne Authentifizierung, Autorisierung oder Drosselung eingerichtet. Für den Produktionseinsatz empfehlen wir, das System in die Sicherheitsinfrastruktur des Unternehmens

zu integrieren. Bewerten Sie diese Einstellung und fügen Sie bei Bedarf die erforderlichen Sicherheitseinstellungen hinzu.

- Für dieses Beispiel mit einer Mandanteninfrastruktur haben Amazon Simple Notification Service (Amazon SNS) und Amazon Simple Queue Service (Amazon SQS) nur Mindestkonfigurationen. Der AWS Key Management Service (AWS KMS) für jeden Mandanten wird für Amazon CloudWatch - und Amazon SNS SNS-Services im Konto geöffnet, um sie auf der Grundlage der AWS KMS KMS-Schlüsselrichtlinie zu nutzen. Das Setup ist nur ein Beispiel für einen Platzhalter. Passen Sie die Setups je nach Bedarf an Ihren geschäftlichen Anwendungsfall an.
- Das gesamte Setup, das unter anderem API-Endpunkte und die Bereitstellung und Löschung von Backend-Mandanten mithilfe von AWS umfasst CloudFormation, deckt nur den grundlegenden Happy-Path-Fall ab. Evaluieren und aktualisieren Sie das Setup mit der erforderlichen Wiederholungslogik, zusätzlicher Fehlerbehandlungslogik und Sicherheitslogik auf der Grundlage Ihrer Geschäftsanforderungen.
- Der Beispielcode wurde mit up-to-date cdk-nag getestet, um zu überprüfen, ob es zum Zeitpunkt der Erstellung dieses Artikels Richtlinien gibt. In future könnten neue Richtlinien durchgesetzt werden. Diese neuen Richtlinien erfordern möglicherweise, dass Sie den Stack anhand der Empfehlungen manuell ändern müssen, bevor der Stack bereitgestellt werden kann. Überprüfen Sie den vorhandenen Code, um sicherzustellen, dass er Ihren Geschäftsanforderungen entspricht.
- Der Code verwendet das AWS-CDK, um ein zufälliges Suffix zu generieren, anstatt sich auf statisch zugewiesene physische Namen für die meisten erstellten Ressourcen zu verlassen. Dieses Setup soll sicherstellen, dass diese Ressourcen einzigartig sind und nicht mit anderen Stacks in Konflikt geraten. Weitere Informationen finden Sie in der AWS-CDK-Dokumentation. Passen Sie dies an Ihre Geschäftsanforderungen an.
- Dieser Beispielcode packt .NET Lambda-Artefakte in Docker-basierte Images und wird mit der von Lambda bereitgestellten Container-Image-Laufzeit ausgeführt. Die Container-Image-Laufzeit bietet Vorteile für standardmäßige Übertragungs- und Speichermechanismen (Container-Registries) und genauere lokale Testumgebungen (über das Container-Image). Sie können das Projekt so umstellen, dass es die von Lambda bereitgestellten .NET-Laufzeiten verwendet, um die Erstellungszeit der Docker-Images zu reduzieren. Dann müssen Sie jedoch Übertragungs- und Speichermechanismen einrichten und sicherstellen, dass das lokale Setup mit dem Lambda-Setup übereinstimmt. Passen Sie den Code an die Geschäftsanforderungen der Benutzer an.

Produktversionen

- AWS CDK Version 2.45.0 oder höher

- Visual Studio 2022

Architektur

Technologie-Stack

- Amazon API Gateway
- AWS CloudFormation
- Amazon CloudWatch
- Amazon-DynamoDB
- AWS Identity and Access Management (IAM)
- AWS KMS
- AWS Lambda
- Amazon S3
- Amazon SNS
- Amazon SQS

Architektur

Das folgende Diagramm zeigt den Ablauf der Erstellung von Mandanten-Stacks. Weitere Informationen zu den Technologie-Stacks für Steuerungsebene und Mandanten finden Sie im Abschnitt Zusätzliche Informationen.

Ablauf zur Erstellung eines Mandanten-Stacks

1. Der Benutzer sendet eine POST-API-Anfrage mit neuer Mandanten-Payload (Mandantenname, Mandantenbeschreibung) in JSON an eine von Amazon API Gateway gehostete REST-API. Das API Gateway verarbeitet die Anfrage und leitet sie an die Lambda Tenant Onboarding-Funktion im Backend weiter. In diesem Beispiel gibt es keine Autorisierung oder Authentifizierung. In einer Produktionsumgebung sollte diese API in das Sicherheitssystem der SaaS-Infrastruktur integriert werden.
2. Die Tenant Onboarding-Funktion verifiziert die Anfrage. Anschließend wird versucht, den Mandantendatensatz, der den Namen des Mandanten, die generierte allgemeine eindeutige Kennung (UUID) und die Mandantenbeschreibung enthält, in der Amazon DynamoDB Tenant Onboarding-Tabelle zu speichern.

3. Nachdem DynamoDB den Datensatz gespeichert hat, initiiert ein DynamoDB-Stream die nachgeschaltete Lambda Tenant Infrastructure-Funktion.
4. Die Lambda-Funktion Tenant Infrastructure agiert auf der Grundlage des empfangenen DynamoDB-Streams. Wenn der Stream für das INSERT-Ereignis bestimmt ist, verwendet die Funktion den NewImage Abschnitt des Streams (letzter Aktualisierungsdatensatz, Feld Mandantenname), um mithilfe der Vorlage, die im S3-Bucket gespeichert ist, eine neue Mandanteninfrastruktur aufzurufen CloudFormation . Für die CloudFormation Vorlage ist der Parameter Tenant Name erforderlich.
5. AWS CloudFormation erstellt die Mandanteninfrastruktur auf der Grundlage der CloudFormation Vorlage und der Eingabeparameter.
6. Jede Einrichtung der Mandanteninfrastruktur verfügt über einen CloudWatch Alarm, einen Abrechnungsalarm und ein Alarmereignis.
7. Das Alarmereignis wird zu einer Nachricht an ein SNS-Thema, die mit dem AWS-KMS-Schlüssel des Mandanten verschlüsselt wird.
8. Das SNS-Thema leitet die empfangene Alarmmeldung an die SQS-Warteschlange weiter, die mit dem AWS-KMS-Verschlüsselungsschlüssel des Mandanten verschlüsselt wird.

Andere Systeme können in Amazon SQS integriert werden, um Aktionen auf der Grundlage von Nachrichten in der Warteschlange durchzuführen. In diesem Beispiel bleiben eingehende Nachrichten in der Warteschlange und müssen manuell gelöscht werden, um den Code generisch zu halten.

Ablauf beim Löschen von Mandantenstapeln

1. Der Benutzer sendet eine DELETE-API-Anfrage mit neuer Mandanten-Payload (Mandantenname, Mandantenbeschreibung) in JSON an die von Amazon API Gateway gehostete REST-API, die die Anfrage verarbeitet und an die Tenant-Onboarding-Funktion weiterleitet. In diesem Beispiel gibt es keine Autorisierung oder Authentifizierung. In einem Produktionssetup wird diese API in das Sicherheitssystem der SaaS-Infrastruktur integriert.
2. Die Tenant-Onboarding-Funktion überprüft die Anfrage und versucht dann, den Mandantendatensatz (Mandantenname) aus der Tenant-Onboarding-Tabelle zu löschen.
3. Nachdem DynamoDB den Datensatz erfolgreich gelöscht hat (der Datensatz ist in der Tabelle vorhanden und wird gelöscht), initiiert ein DynamoDB-Stream die Downstream-Funktion Lambda Tenant Infrastructure.

4. Die Lambda-Funktion Tenant Infrastructure handelt auf der Grundlage des empfangenen DynamoDB-Stream-Datensatzes. Wenn der Stream für das REMOVE-Ereignis bestimmt ist, verwendet die Funktion den OldImage Abschnitt des Datensatzes (Datensatzinformationen und Feld Mandantenname vor der letzten Änderung, d. h. Löschen), um das Löschen eines vorhandenen Stacks auf der Grundlage dieser Datensatzinformationen zu initiieren.
5. AWS CloudFormation löscht den Zielmandanten-Stack entsprechend der Eingabe.

Tools

AWS-Services

- Amazon API Gateway unterstützt Sie bei der Erstellung, Veröffentlichung, Wartung, Überwachung und Sicherung von REST, HTTP und WebSocket APIs in jeder Größenordnung.
- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS CDK Toolkit ist ein Befehlszeilen-Cloud-Entwicklungskit, mit dem Sie mit Ihrer AWS Cloud Development Kit (AWS CDK) -App interagieren können.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.
- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Key Management Service (AWS KMS) unterstützt Sie bei der Erstellung und Kontrolle kryptografischer Schlüssel, um Ihre Daten zu schützen.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.
- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.
- AWS Toolkit for Visual Studio ist ein Plugin für die integrierte Entwicklungsumgebung (IDE) von Visual Studio. Das Toolkit for Visual Studio unterstützt die Entwicklung, das Debuggen und die Bereitstellung von.NET-Anwendungen, die AWS-Services verwenden.

Andere Tools

- Visual Studio ist eine IDE, die Compiler, Tools zur Codevervollständigung, Grafikdesigner und andere Funktionen zur Unterstützung der Softwareentwicklung enthält.

Code

Der Code für dieses Muster befindet sich im APG-Beispiel-Repository Tenant Onboarding in SaaS Architecture for Silo Model.

Epen

AWS CDK einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Installation von Node.js.	Führen Sie den folgenden Befehl aus, um zu überprüfen, ob Node.js auf Ihrem lokalen Computer installiert ist. `node --version`	AWS-Administrator, AWS DevOps
Installieren Sie das AWS CDK Toolkit.	Führen Sie den folgenden Befehl aus, um AWS CDK Toolkit auf Ihrem lokalen Computer zu installieren.	AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`npm install -g aws-cdk` Wenn npm nicht installiert ist, können Sie es von der Website Node.js aus installieren.	
Überprüfen Sie die Version des AWS CDK Toolkit.	Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die Version des AWS CDK Toolkit korrekt auf Ihrem Computer installiert ist. `cdk --version`	AWS-Administrator, AWS DevOps

Überprüfen Sie den Code für die Onboarding-Kontrollebene des Mandanten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Klonen Sie das Repository und navigieren Sie zu dem `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example` Ordner. Öffnen Sie die `\src\TenantOnboardingInfra.sln` Lösung in Visual Studio 2022. Öffnen Sie die `TenantOnboardingInfraStack.cs` Datei und überprüfen Sie den Code.	AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Die folgenden Ressourcen werden als Teil dieses Stacks erstellt: • DynamoDB-Tabelle • S3-Bucket (Laden Sie die CloudFormation Vorlage in den S3-Bucket hoch.) • Lambda-Ausführungsrolle • Lambda-Funktion • API-Gateway-API • Ereignisquelle zur Lambda-Funktion	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die CloudFormation Vorlage.	Öffnen `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\template infra.yaml` Sie im Ordner die CloudFormation Vorlage und überprüfen Sie sie. Diese Vorlage wird mit dem Mandantennamen, der aus der DynamoDB-Tabelle zum Onboarding des Mandanten abgerufen wurde, hydratisiert. Die Vorlage stellt die mandantenspezifische Infrastruktur bereit. In diesem Beispiel werden der AWS-KMS-Schlüssel, Amazon SNS, Amazon SQS und der CloudWatch Alarm bereitgestellt.	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich die Onboarding-Funktion für Mandanten an.	Öffnen `Function.cs` und überprüfen Sie den Code für die Mandanten-Onboarding-Funktion, die mit der Visual Studio AWS Lambda Lambda-Projektvorlage (.NET Core-C#) mit dem.NET 6-Blueprint (Container Image) erstellt wurde. Öffnen Sie die `Dockerfile` und überprüfen Sie den Code. Das `Dockerfile` ist eine Textdatei, die Anweisungen zum Erstellen des Lambda-Container-Images enthält. Beachten Sie, dass die folgenden NuGet Pakete dem `TenantOnboardingFunction` Projekt als Abhängigkeiten hinzugefügt werden: • `Amazon.Lambda.APIGatewayEvents` • `AWSSDK.DynamoDBv2` • `Newtonsoft.Json`	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die InfraProvisioning Mandantenfunktion.	Navigieren Sie zu `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\src\InfraProvisioningFunction` . Öffnen `Function.cs` und überprüfen Sie den Code für die Funktion zur Bereitstellung der Mandanteninfrastruktur, die mit der Vorlage Visual Studio AWS Lambda Project (.NET Core — C#) mit dem.NET 6-Blueprint (Container Image) erstellt wurde. Öffnen Sie die `Dockerfile` und überprüfen Sie den Code. Beachten Sie, dass die folgenden NuGet Pakete dem `InfraProvisioningFunction` Projekt als Abhängigkeiten hinzugefügt werden: • `Amazon.Lambda.DynamoDBEvents` • `AWSSDK.DynamoDBv2` • `AWSSDK.Cloudformation`	App-Entwickler, AWS DevOps

Stellen Sie die AWS-Ressourcen bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Lösung.	Gehen Sie wie folgt vor, um die Lösung zu erstellen: 1. Öffnen Sie die `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\src\TenantOnboardingInfra.sln` Lösung in Visual Studio 2022. 2. Öffnen Sie das Kontextmenü (mit der rechten Maustaste) für die Lösung und wählen Sie Lösung erstellen aus. **Note** Stellen Sie sicher, dass Sie das `Amazon.CDK.Lib` `NuGet` Paket auf die neueste Version im `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\src\TenantOnboardingInfra`	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Projekt aktualisieren, bevor Sie die Lösung erstellen.	

Bootstrap der AWS-CDK-Umgebung.	Öffnen Sie die Windows-Befehlszeile und navigieren Sie zum Stammordner der AWS CDK-App, in dem die `cdk.json` Datei verfügbar ist (`\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example`). Führen Sie den folgenden Befehl für das Bootstrapping aus.
	`cdk bootstrap`
	Wenn Sie ein AWS-Profil für die Anmeldeinformationen erstellt haben, verwenden Sie den Befehl mit Ihrem Profil.
	`cdk bootstrap --profile <profile name>`
		AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Listet die AWS-CDK-Stacks auf.	Führen Sie den folgenden Befehl aus, um alle Stacks aufzulisten, die im Rahmen dieses Projekts erstellt werden sollen.
	`cdk ls`
	`cdk ls --profile <profile name>`
	Wenn Sie ein AWS-Profil für die Anmeldeinformationen erstellt haben, verwenden Sie den Befehl mit Ihrem Profil.
	`cdk ls --profile <profile name>`
		AWS-Administrator, AWS DevOps

Prüfen Sie, welche AWS-Ressourcen erstellt werden.	Führen Sie den folgenden Befehl aus, um alle AWS-Ressourcen zu überprüfen, die im Rahmen dieses Projekts erstellt werden.
	`cdk diff`
	Wenn Sie ein AWS-Profil für die Anmeldeinformationen erstellt haben, verwenden Sie den Befehl mit Ihrem Profil.
	`cdk diff --profile <profile name>`
		AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie alle AWS-Ressourcen mithilfe von AWS CDK bereit.	Führen Sie den folgenden Befehl aus, um alle AWS-Ressourcen bereitzustellen.
	`cdk deploy --all --require-approval never`
	Wenn Sie ein AWS-Profil für die Anmeldeinformationen erstellt haben, verwenden Sie den Befehl mit Ihrem Profil.
	`cdk deploy --all --require-approval never --profile <profile name>`
	Kopieren Sie nach Abschluss der Bereitstellung die API-URL aus dem Ausgabebereich in der Befehlszeile, wie im folgenden Beispiel gezeigt.
	`Outputs: TenantOnboardingInfraStack.TenantOnboardingAPIEndpoint42E526D7 = https://j2qmp8ds21i1i.execute-api.us-west-2.amazonaws.com/prod/`
		AWS-Administrator, AWS DevOps

Überprüfen Sie die Funktionalität

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie einen neuen Mandanten.	Um den neuen Mandanten zu erstellen, senden Sie die folgende Curl-Anfrage.
	`curl -X POST <TenantOnboardingAPIEndpoint* from CDK Output>tenant -d '{"Name":"Tenant123", "Description":"Stack for Tenant123"}'`
	Ändern Sie den Platzhalter `<TenantOnboardingAPIEndpoint* from CDK Output>` auf den tatsächlichen Wert von AWS CDK, wie im folgenden Beispiel gezeigt.
	`curl -X POST https://j2qmp8ds21i1i.execute-api.us-west-2.amazonaws.com/prod/tenant -d '{"Name": "Tenant123", "Description":"test12"}'`
	Das folgende Beispiel zeigt die Ausgabe.
	`{"message": "A new tenant added - 5/4/2022 7:11:30 AM"}`
		App-Entwickler, AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die neu erstellten Mandantendetails in DynamoDB.	Gehen Sie wie folgt vor, um die neu erstellten Mandanten details in DynamoDB zu überprüfen. 1. Öffnen Sie die AWS-Managementkonsole und navigieren Sie zum Amazon DynamoDB-Service. 2. Wählen Sie in der linken Navigationsleiste Elemente erkunden und wählen Sie die `TenantOnboarding` Tabelle aus. **Note** Dem Namen des Mandanten wird Folgendes vorangestellt. `tenantcluster-` Weitere Informati onen finden Sie im Abschnitt Zusätzlic he Informationen. 3. Stellen Sie sicher, dass ein neues Element mit den Mandantendetails erstellt wurde.	App-Entwickler, AWS-Admin istrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Stack-Erstellung für den neuen Mandanten.	Stellen Sie sicher, dass der neue Stack erfolgreich erstellt und mit der Infrastruktur für den neu erstellten Mandanten gemäß der CloudFormation Vorlage ausgestattet wurde. 1. Öffnen Sie die CloudFormation Konsole. 2. Wählen Sie in der linken Navigationsleiste Stacks aus und vergewissern Sie sich, dass ein Stack mit dem Mandantennamen erfolgreich erstellt wurde. 3. Wählen Sie den neu erstellten Mandanten-Stack und dann die Registerkarte Ressourcen aus. Notieren Sie sich die Alarm-Ressource und die Amazon SQS SQS-Ressource. 4. Öffnen Sie ein neues Terminal mit konfigurierten AWS-Anmeldeinformationen und zeigen Sie auf die richtige Region. Um einen Testalarm auszulösen, geben Sie den folgenden Code ein und `<alarm resource name>` ersetzen Sie ihn durch den in Schritt 3	App-Entwickler, AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	angegebenen Namen der Alarm-Ressource.
	
	`aws cloudwatch set-alarm-state --alarm-name <alarm resource name> --state-value ALARM --state-reason 'Test setup'`
	
	Das folgende Beispiel zeigt den Code mit einem Alarm-Ressourcennamen.
	
	`aws cloudwatch set-alarm-state --alarm-name tenantcluster-tenant123-alarm --state-value ALARM --state-reason 'Test setup'`
	
	5. Öffnen Sie die Konsole und navigieren Sie zur Amazon SQS SQS-Konsole. Wählen Sie den in Schritt 3 identifizierten Amazon SQS SQS-Ressourcennamen aus. Folgen Sie den Anweisungen in der AWS-Dokumentation, um die Testnachricht zu empfangen und aus dem in Schritt 4 ausgelösten Alarm zu löschen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Löschen Sie den Mandanten-Stack.	Um den Tenant-Stack zu löschen, senden Sie die folgende Curl-Anfrage.
	`curl -X DELETE <TenantOnboardingAPIEndpoint* from CDK Output>tenant/<Tenant Name from previous step>`
	Ändern Sie den Platzhalter `<TenantOnboardingAPIEndpoint* from CDK Output>` auf den tatsächlichen Wert aus AWS CDK und ändern Sie ihn `<Tenant Name from previous step>` auf den tatsächlichen Wert aus dem vorherigen Schritt zur Mandantenerstellung, wie im folgenden Beispiel gezeigt.
	`curl -X DELETE https://j2qmp8ds21i1i.execute-api.us-west-2.amazonaws.com/prod/tenant/Tenant123`
	Das folgende Beispiel zeigt die Ausgabe.
	`{"message": "Tenant destroyed - 5/4/2022 7:14:48 AM"}`
		App-Entwickler, AWS DevOps, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie, ob der Stack für den vorhandenen Mandanten gelöscht wurde.	Gehen Sie wie folgt vor, um zu überprüfen, ob der vorhandene Mandanten-Stack gelöscht wurde: 1. Öffnen Sie die Konsole und navigieren Sie zur CloudFormation Konsole. 2. Vergewissern Sie sich im linken Navigationsbereich, dass sich der vorhandene Stack mit dem Mandantennamen nicht mehr in der CloudFormation Konsole befindet (wenn die Konsole so eingerichtet ist, dass sie nur aktive Stacks anzeigt) oder gerade gelöscht wird. Wenn sich der Stack nicht mehr in der CloudFormation Konsole befindet, ändern Sie mithilfe der Dropdownliste die Einstellung der Konsole von Aktiv auf Gelöscht, um den gelöschten Stack zu sehen und zu überprüfen, ob der Stack erfolgreich gelöscht wurde.	App-Entwickler, AWS-Administrator, AWS DevOps

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Zerstöre die Umwelt.	Stellen Sie vor dem Aufräumen des Stacks Folgendes sicher: • Alle Datensätze in DynamoDB werden entweder durch den vorherigen Mandanten löschvorgang oder über die DynamoDB-Konsole oder -API entfernt. Bei jeder Löschung von Mandanten datensätzen wird die Säuberung des entsprech enden CloudFormation AWS-Pendants eingeleitet. • Alle mandantenbasierten CloudFormation AWS-Stack s werden auf der AWS-Konsole bereinigt (falls die DynamoDB-Trigger-B ereinigungslogik fehlschlä gt). CloudFormation Nach Abschluss der Tests kann AWS CDK verwendet werden, um alle Stacks und zugehörigen Ressourcen zu löschen, indem Sie den folgenden Befehl ausführen. `cdk destroy --all;`	AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wenn Sie ein AWS-Profil für die Anmeldeinformationen erstellt haben, verwenden Sie das Profil. Bestätigen Sie die Aufforder ung zum Löschen des Stacks, um den Stack zu löschen.	
Bereinigen Sie Amazon CloudWatch Logs.	Beim Löschen des Stacks werden keine CloudWatch Protokolle (Protokollgruppen und Protokolle) bereinigt, die vom Stack generiert wurden. Bereinigen Sie die CloudWatc h Ressourcen manuell mithilfe der CloudWatch Konsole oder der API.	App-Entwickler, AWS DevOps, AWS-Administrator

Zugehörige Ressourcen

- AWS CDK .NET-Workshop
- Arbeiten mit dem AWS-CDK in C#
- CDK.NET-Referenz

Zusätzliche Informationen

Technologie-Stack auf Steuerungsebene

Der in .NET geschriebene CDK-Code wird verwendet, um die Infrastruktur der Steuerungsebene bereitzustellen, die aus den folgenden Ressourcen besteht:

1. API Gateway

   Dient als REST-API-Einstiegspunkt für den Kontrollebenen-Stack.

2. Lambda-Funktion zum Onboarding von Mandanten

   Diese Lambda-Funktion wird von API Gateway mit der Methode m initiiert.

   Eine API-Anfrage der POST-Methode führt dazu, dass (`tenant name`,`tenant description`) in die DynamoDB-Tabelle `Tenant Onboarding` eingefügt wird.

   In diesem Codebeispiel wird der Mandantenname auch als Teil des Mandanten-Stack-Namens und der Namen der Ressourcen innerhalb dieses Stacks verwendet. Dies soll die Identifizierung dieser Ressourcen erleichtern. Dieser Mandantenname muss im gesamten Setup eindeutig sein, um Konflikte oder Fehler zu vermeiden. Eine detaillierte Einrichtung der Eingabevalidierung wird in der Dokumentation zu den IAM-Rollen und im Abschnitt Einschränkungen erläutert.

   Der Persistenzprozess für die DynamoDB-Tabelle ist nur erfolgreich, wenn der Mandantenname in keinem anderen Datensatz in der Tabelle verwendet wird.

   Der Mandantenname ist in diesem Fall der Partitionsschlüssel für diese Tabelle, da nur der Partitionsschlüssel als Bedingungsausdruck verwendet werden kann. `PutItem`

   Wenn der Mandantenname noch nie zuvor aufgezeichnet wurde, wird der Datensatz erfolgreich in der Tabelle gespeichert.

   Wenn der Mandantenname jedoch bereits von einem vorhandenen Datensatz in der Tabelle verwendet wird, schlägt der Vorgang fehl und löst eine DynamoDB-Ausnahme `ConditionalCheckFailedException` aus. Die Ausnahme wird verwendet, um eine Fehlermeldung (`HTTP BadRequest`) zurückzugeben, die angibt, dass der Mandantenname bereits existiert.

   Eine `DELETE` Methoden-API-Anfrage entfernt den Datensatz für einen bestimmten Mandantennamen aus der `Tenant Onboardin` G-Tabelle.

   Das Löschen von DynamoDB-Datensätzen in diesem Beispiel ist erfolgreich, auch wenn der Datensatz nicht existiert.

   Wenn der Zieldatensatz existiert und gelöscht wird, wird ein DynamoDB-Stream-Datensatz erstellt. Andernfalls wird kein Downstream-Datensatz erstellt.

3. Einbindung von Mandanten in DynamoDB mit aktivierten Amazon DynamoDB DynamoDB-Streams

Dadurch werden die Metadateninformationen des Mandanten aufgezeichnet, und bei jedem Speichern oder Löschen von Datensätzen wird ein Stream flussabwärts an die `Tenant Infrastructure` Lambda-Funktion gesendet.

4. Lambda-Funktion für Mandanteninfrastruktur

   Diese Lambda-Funktion wird durch den DynamoDB-Stream-Datensatz aus dem vorherigen Schritt initiiert. Wenn sich der Datensatz auf ein `INSERT` Ereignis bezieht, ruft er AWS CloudFormation auf, um eine neue Mandanteninfrastruktur mit der CloudFormation Vorlage zu erstellen, die in einem S3-Bucket gespeichert ist. Wenn der Datensatz für ist`REMOVE`, initiiert er das Löschen eines vorhandenen Stacks auf der Grundlage des Felds `Tenant Name` des Stream-Datensatzes.

5. S3 bucket

   Dies dient zum Speichern der CloudFormation Vorlage.

6. IAM-Rollen für jede Lambda-Funktion und eine Servicerolle für CloudFormation

   Jede Lambda-Funktion hat ihre eigene IAM-Rolle mit den geringsten Rechten, um ihre Aufgabe zu erfüllen. Die `Tenant On-boarding` Lambda-Funktion hat beispielsweise Lese-/Schreibzugriff auf DynamoDB, und die `Tenant Infrastructure` Lambda-Funktion kann nur den DynamoDB-Stream lesen.

   Eine benutzerdefinierte CloudFormation Servicerolle wird für die Bereitstellung von Mandanten-Stacks erstellt. Diese Servicerolle enthält zusätzliche Berechtigungen für die CloudFormation Stack-Bereitstellung (z. B. den AWS-KMS-Schlüssel). Dadurch werden Rollen zwischen Lambda aufgeteilt und alle Berechtigungen CloudFormation für eine einzelne Rolle (Infrastructure Lambda-Rolle) vermieden.

   Berechtigungen, die leistungsstarke Aktionen (wie das Erstellen und Löschen von CloudFormation Stacks) ermöglichen, sind gesperrt und nur für Ressourcen zulässig, die mit beginnen. `tenantcluster-` Die Ausnahme ist AWS KMS aufgrund seiner Benennungskonvention für Ressourcen. Dem aus der API aufgenommenen Mandantennamen werden `tenantcluster-` zusammen mit anderen Validierungsprüfungen vorangestellt (nur alphanumerisch mit Bindestrich und begrenzt auf weniger als 30 Zeichen, sodass er in die meisten AWS-Ressourcenbenennungen passt). Dadurch wird sichergestellt, dass der Mandantenname nicht versehentlich zu einer Störung der Stacks oder Ressourcen der Kerninfrastruktur führt.

Technologie-Stack für Mandanten

Eine CloudFormation Vorlage wird im S3-Bucket gespeichert. Die Vorlage stellt den mandantenspezifischen AWS-KMS-Schlüssel, einen CloudWatch Alarm, ein SNS-Thema, eine SQS-Warteschlange und eine SQS-Richtlinie bereit.

Der AWS-KMS-Schlüssel wird von Amazon SNS und Amazon SQS für die Datenverschlüsselung ihrer Nachrichten verwendet. Die Sicherheitspraktiken für AwsSolutions— SNS2 und AwsSolutions — SQS2 empfehlen, dass Sie Amazon SNS und Amazon SQS mit Verschlüsselung einrichten. CloudWatch Alarme funktionieren jedoch nicht mit Amazon SNS, wenn Sie einen von AWS verwalteten Schlüssel verwenden. Daher müssen Sie in diesem Fall einen vom Kunden verwalteten Schlüssel verwenden. Weitere Informationen finden Sie im AWS Knowledge Center.

Die SQS-Richtlinie wird in der Amazon SQS SQS-Warteschlange verwendet, damit das erstellte SNS-Thema die Nachricht an die Warteschlange übermitteln kann. Ohne die SQS-Richtlinie wird der Zugriff verweigert. Weitere Informationen finden Sie in der Amazon SNS SNS-Dokumentation.

Zerlegen Sie Monolithen mithilfe von CQRS und Event Sourcing in Microservices

Erstellt von Rodolfo Jr. Cerrada (AWS), Dmitry Gulin (AWS) und Tabby Ward (AWS)

Übersicht

Dieses Muster kombiniert zwei Muster und verwendet sowohl das Command Query Responsibility Separation (CQRS) -Muster als auch das Event Sourcing-Muster. Das CQRS-Muster trennt die Zuständigkeiten der Befehls- und Abfragemodelle. Das Eventsourcing-Muster nutzt die Vorteile der asynchronen ereignisgesteuerten Kommunikation, um die allgemeine Benutzererfahrung zu verbessern.

Sie können CQRS- und Amazon Web Services (AWS) -Services verwenden, um jedes Datenmodell unabhängig zu verwalten und zu skalieren und gleichzeitig Ihre Monolith-Anwendung in eine Microservices-Architektur umzustrukturieren. Anschließend können Sie das Event Sourcing Pattern verwenden, um Daten aus der Befehlsdatenbank mit der Abfragedatenbank zu synchronisieren.

Dieses Muster verwendet Beispielcode, der eine Lösungsdatei (*.sln) enthält, die Sie mit der neuesten Version von Visual Studio öffnen können. Das Beispiel enthält Reward-API-Code, der zeigt, wie CQRS und Event Sourcing in serverlosen und traditionellen oder lokalen AWS-Anwendungen funktionieren.

Weitere Informationen zu CQRS und Event Sourcing finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Amazon CloudWatch
- Amazon-DynamoDB-Tabellen
- Amazon DynamoDB Streams
- Zugriffsschlüssel und geheimer Schlüssel für AWS Identity and Access Management (IAM); weitere Informationen finden Sie im Video im Abschnitt Verwandte Ressourcen
- AWS Lambda
- Vertrautheit mit Visual Studio

- Vertrautheit mit AWS Toolkit for Visual Studio; weitere Informationen finden Sie im Demo-Video zu AWS Toolkit for Visual Studio im Abschnitt Verwandte Ressourcen

Produktversionen

- Visual Studio 2019 Community-Ausgabe.
- AWS Toolkit for Visual Studio 2019.
- .NET Core 3.1. Diese Komponente ist eine Option in der Visual Studio-Installation. Um .NET Core bei der Installation einzubeziehen, wählen Sie plattformübergreifende Entwicklung mit NET Core aus.

Einschränkungen

- Der Beispielcode für eine herkömmliche lokale Anwendung (ASP.NET Core-Web-API und Datenzugriffsobjekte) ist nicht im Lieferumfang einer Datenbank enthalten. Er wird jedoch mit dem `CustomerData` In-Memory-Objekt geliefert, das als Scheindatenbank fungiert. Der bereitgestellte Code reicht aus, um das Muster zu testen.

Architektur

Quelltechnologie-Stack

- ASP.NET Core-Web-API-Projekt
- IIS-Webserver
- Datenzugriffsobjekt
- CRUD-Modell

Quellarchitektur

In der Quellarchitektur enthält das CRUD-Modell sowohl Befehls- als auch Abfrageschnittstellen in einer Anwendung. Beispielcode finden Sie unter `CustomerDA0.cs` (angehängt).

Zieltechnologie-Stack

- Amazon-DynamoDB

- Amazon DynamoDB Streams
- AWS Lambda
- (Fakultativ) Amazon API Gateway
- (Optional) Amazon Simple Notification Service (Amazon SNS)

Zielarchitektur

In der Zielarchitektur sind die Befehls- und Abfrageschnittstellen getrennt. Die in der folgenden Abbildung gezeigte Architektur kann mit API Gateway und Amazon SNS erweitert werden. Weitere Informationen finden Sie im Abschnitt Zusätzliche Informationen.

1. Befehls-Lambda-Funktionen führen Schreiboperationen wie Erstellen, Aktualisieren oder Löschen in der Datenbank durch.
2. Lambda-Abfragefunktionen führen Lesevorgänge wie Get oder Select in der Datenbank durch.
3. Diese Lambda-Funktion verarbeitet die DynamoDB-Streams aus der Befehlsdatenbank und aktualisiert die Query-Datenbank für die Änderungen.

Tools

Tools

- Amazon DynamoDB — Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der schnelle und vorhersehbare Leistung mit nahtloser Skalierbarkeit bietet.
- Amazon DynamoDB Streams — DynamoDB Streams erfasst eine zeitlich geordnete Abfolge von Änderungen auf Elementebene in jeder DynamoDB-Tabelle. Anschließend werden diese Informationen bis zu 24 Stunden lang in einem Protokoll gespeichert. Die Verschlüsselung ruhender Daten verschlüsselt die Daten in DynamoDB Streams.
- AWS Lambda — AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.
- AWS-Managementkonsole — Die AWS-Managementkonsole ist eine Webanwendung, die eine breite Sammlung von Servicekonsolen für die Verwaltung von AWS-Services umfasst.

- Visual Studio 2019 Community Edition — Visual Studio 2019 ist eine integrierte Entwicklungsumgebung (IDE). Die Community Edition ist für Open-Source-Mitwirkende kostenlos. In diesem Muster verwenden Sie Visual Studio 2019 Community Edition, um Beispielcode zu öffnen, zu kompilieren und auszuführen. Nur zur Anzeige können Sie einen beliebigen Texteditor oder Visual Studio Code verwenden.
- AWS Toolkit für Visual Studio — Das AWS Toolkit for Visual Studio ist ein Plugin für die Visual Studio-IDE. Das AWS Toolkit for Visual Studio erleichtert Ihnen das Entwickeln, Debuggen und Bereitstellen von.NET-Anwendungen, die AWS-Services verwenden.

Code

Der Beispielcode ist angehängt. Anweisungen zur Bereitstellung des Beispielcodes finden Sie im Abschnitt Epics.

Epen

Öffnen und erstellen Sie die Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Öffnen Sie die Lösung.	1. Laden Sie den Beispielquellcode (`CQRS-ES Code.zip`) aus dem Bereich Anlagen herunter und extrahieren Sie die Dateien. 2. Wählen Sie in der Visual Studio-IDE Datei, Öffnen, Projektlösung und navigieren Sie zu dem Ordner, in den Sie den Quellcode extrahiert haben. 3. Wählen Sie aws.apg.cqrses.sln und wählen Sie dann Öffnen. Die gesamte Lösung wird in Visual Studio geladen.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Lösung.	Öffnen Sie das Kontextmenü (mit der rechten Maustaste) für die Lösung und wählen Sie dann Lösung erstellen aus. Dadurch werden alle Projekte in der Lösung erstellt und kompiliert. Es sollte erfolgreich kompiliert werden. Visual Studio Solution Explorer sollte die Verzeichn isstruktur anzeigen. • `CQRS On-Premises Code Sample`enthält ein Beispiel für die lokale Verwendung von CQRS. • `CQRS AWS Serverles s` enthält den gesamten CQRS- und Eventsourcing-Beispielcode mit serverlos en AWS-Services.	App-Developer

Erstellen Sie die DynamoDB-Tabellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie die Anmeldein formationen an.	Wenn Sie noch keinen Zugriffsschlüssel haben, sehen Sie sich das Video im Abschnitt Verwandte Ressourcen an. 1. Erweitern Sie im Solution Explorer CQRS AWS	App-Entwickler, Dateninge nieur, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Serverless und dann den Ordner Build solution. 2. Erweitern Sie das Projekt aws.apg.cqrses.Build und zeigen Sie die Datei an. `Program.cs` 3. Scrollen Sie nach oben und suchen Sie nach. `Program.cs Program()` 4. `YOUR ACCESS KEY`Ersetzen Sie es durch Ihren Kontozugriffsschlüssel und `YOUR SECRET KEY` ersetzen Sie es durch Ihren geheimen Kontoschlüssel. Beachten Sie, dass Sie in einer Produktionsumgebung Ihre Schlüssel nicht fest codieren würden. Stattdessen könnten Sie AWS Secrets Manager verwenden, um die Anmeldeinformationen zu speichern und abzurufen.	
Erstellen Sie das Projekt.	Um das Projekt zu erstellen, öffnen Sie das Kontextmenü (Rechtsklick) für das Projekt aws.apg.cqrses.Build und wählen Sie dann Build aus.	App-Entwickler, Dateningenieur, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und füllen Sie die Tabellen.	Um die Tabellen zu erstellen und sie mit Ausgangsdaten zu füllen, öffnen Sie das Kontextmenü (mit der rechten Maustaste) für das Projekt aws.apg.cqrses.Build und wählen Sie dann Debug, Start New Instance aus.	App-Entwickler, Dateninge nieur, DBA
Überprüfen Sie die Tabellenk onstruktion und die Daten.	Gehen Sie zur Überprüfung zu AWS Explorer und erweitern Sie Amazon DynamoDB. Es sollte die Tabellen anzeigen. Öffnen Sie jede Tabelle, um die Beispieldaten anzuzeigen.	App-Entwickler, Dateninge nieur, DBA

Führen Sie lokale Tests durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das CQRS-Proj ekt.	1. Öffnen Sie die Lösung und navigieren Sie zum CQRS Services/CQRS/Test s AWS-Lösungsordner. 2. In der Datei AWS.APG.C QRSES. CQRSLambd a.Tests-Projekt, öffnen Sie BaseFunctionTest.cs und ersetzen Sie AccessKeyund SecretKeydurch die IAM-Schlüssel, die Sie erstellt haben. 3. Speichern Sie die Änderungen.	App-Entwickler, Testingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Um das Testprojekt zu kompilieren und zu erstellen, öffnen Sie das Kontextmenü (mit der rechten Maustaste) für das Projekt und wählen Sie dann Build.	
Erstellen Sie das Eventsourcing-Projekt.	1. Navigieren Sie zum CQRS Services/Event Source/Tests AWS-Lösungsordner. 2. Im Ordner AWS.APG.CQRSES. EventSourceLambda.Tests-Projekt, öffnen Sie BaseFunctionTest.cs und ersetzen Sie AccessKeyund SecretKey durch die IAM-Schlüssel, die Sie erstellt haben. 3. Speichern Sie die Änderungen. 4. Um das Testprojekt zu kompilieren und zu erstellen, öffnen Sie das Kontextmenü (mit der rechten Maustaste) für das Projekt und wählen Sie dann Build.	App-Entwickler, Testingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Tests aus.	Um alle Tests auszuführen, wählen Sie Ansicht, Test Explorer und dann Alle Tests in Ansicht ausführen aus. Alle Tests sollten erfolgreich sein, was durch ein grünes Häkchen gekennzeichnet ist.	App-Entwickler, Testingenieur

Veröffentlichen Sie die CQRS Lambda-Funktionen in AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Veröffentlichen Sie die erste Lambda-Funktion.	1. Öffnen Sie im Solution Explorer das Kontextmenü (Rechtsklick) für AWS.APG.CQRSES.CommandCreateLambda project und wählen Sie dann Publish to AWS Lambda. 2. Wählen Sie das Profil aus, das Sie verwenden möchten, und die AWS-Region, in der Sie die Lambda-Funktion bereitstellen möchten, sowie den Funktionsnamen. 3. Behalten Sie für die übrigen Felder die Standardwerte bei und wählen Sie Weiter. 4. Wählen Sie in der Dropdownliste Rollennam	App-Entwickler, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	e die Option aus AWSLambdaFullAccess. 5. Um Ihre Kontoschlüssel anzugeben, wählen Sie Hinzufügen und geben Sie `AcessKey` als Variable und Ihren Zugriffsschlüssel als Wert ein. Wählen Sie dann erneut Hinzufügen, geben Sie `SecretKey` als Variable und Ihren geheimen Schlüssel als Wert ein. 6. Behalten Sie für die übrigen Felder die Standardw erte bei und wählen Sie Hochladen. Nachdem die Lambda-Testfunktion hochgeladen wurde, wird sie automatisch in Visual Studio angezeigt. 7. Wiederholen Sie die Schritte 1—6 für die folgenden Projekte: • AWS.APG.CQRSES. CommandDeleteLambda • AWS.APG.CSES. CommandUpdateLambda • AWS.APG.CSES. CommandAddRewardLa mbda	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• AWS.APG.CSES.CommandRedeemRewardLambda • AWS.APG.CSES.QueryCustomerListLambda • AWS.APG.CSES.QueryRewqardLambda	
Überprüfen Sie den Funktions-Upload.	(Optional) Sie können überprüfen, ob die Funktion erfolgreich geladen wurde, indem Sie zu AWS Explorer navigieren und AWS Lambda erweitern. Um das Testfenster zu öffnen, wählen Sie die Lambda-Funktion (Doppelklick).	App-Entwickler, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Lambda-Funktion.	1. Geben Sie die Anforderungsdaten ein, oder kopieren Sie ein Beispiel für Anforderungsdaten aus den Testdaten im Abschnitt Zusätzliche Informationen. Stellen Sie sicher, dass Sie Daten auswählen, die für die Funktion bestimmt sind, die Sie testen. 2. Um den Test durchzuführen, wählen Sie Invoke (Aufrufen) aus. Die Antwort und etwaige Fehler werden im Textfeld Antwort angezeigt, und Protokolle werden im Textfeld Protokolle oder in CloudWatch Protokollen angezeigt. 3. Um die Daten zu überprüfen, wählen Sie im AWS Explorer die DynamoDB-Tabelle aus (Doppelklicken). Alle CQRS Lambda-Projekte befinden sich in den Ordnern `CQRS AWS Serverless\CQRS\Command Microservice` und `CQRS AWS Serverless\CQRS\Command Microservice` Solution.	App-Entwickler, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Das Lösungsverzeichnis und die Projekte finden Sie unter Quellcodeverzeichnis im Abschnitt Zusätzliche Informationen.	
Veröffentlichen Sie die verbleibenden Funktionen.	Wiederholen Sie die vorherigen Schritte für die folgenden Projekte: • AWS.APG.CQRSES.CommandDeleteLambda • AWS.APG.CSES.CommandUpdateLambda • AWS.APG.CSES.CommandAddRewardLambda • AWS.APG.CSES.CommandRedeemRewardLambda • AWS.APG.CSES.QueryCustomerListLambda • AWS.APG.CSES.QueryRewqardLambda	App-Entwickler, DevOps Ingenieur

Richten Sie die Lambda-Funktion als Event-Listener ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Veröffentlichen Sie die Lambda-Event-Handler „Customer“ und „Reward“.	Um die einzelnen Event-Handler zu veröffentlichen, folgen Sie den Schritten im vorherigen Abschnitt.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Die Projekte befinden sich in den Ordnern `CQRS AWS Serverless\Event Source\Customer Event` und `CQRS AWS Serverless\Event Source\Reward Event` Solution. Weitere Informationen finden Sie unter Quellcode-Verzeichnis im Abschnitt Zusätzliche Informationen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Hängen Sie den Lambda-Event-Listener an, der das Ereignis ausgibt.	1. Melden Sie sich bei der AWS-Managementkonsole mit demselben Konto an, das Sie bei der Veröffent lichung der Lambda-Pr ojekte verwenden. 2. Wählen Sie für die Region US East 1 oder die Region aus, in der Sie die Lambda-Funktionen im vorherigen Epic bereitgestellt haben. 3. Navigieren Sie zum Lambda-Service. 4. Wählen Sie die `EventSour ceCustomer` Lambda-Funktion aus. 5. Wählen Sie Trigger hinzufügen. 6. Wählen Sie in der Dropdownliste Trigger-Konfiguration die Option DynamoDB aus. 7. Wählen Sie in der Dropdownliste DynamoDB-Tabelle die Option aus. cqrses-customer-cmd 8. Wählen Sie in der Dropdownliste Startposi tion die Option Horizont abschneiden aus. Trim Horizon bedeutet, dass der DynamoDB-Trigger mit dem Lesen beim letzten	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(ungetrimmten) Stream-Datensatz beginnt, der der älteste Datensatz im Shard ist. 9. Aktivieren Sie das Kontrollkästchen Trigger aktivieren. 10. Behalten Sie für die übrigen Felder die Standardwerte bei und wählen Sie Hinzufügen. Nachdem der Listener erfolgreich an die DynamoDB-Tabelle angehängt wurde, wird er auf der Lambda-Designer-Seite angezeigt.	
Veröffentlichen Sie die EventSourceReward Lambda-Funktion und hängen Sie sie an.	Um die `EventSourceReward` Lambda-Funktion zu veröffentlichen und anzuhängen, wiederholen Sie die Schritte in den beiden vorherigen Storys und wählen Sie cqrses-reward-cmdaus der Dropdownliste der DynamoDB-Tabelle aus.	App-Developer

Testen und validieren Sie die DynamoDB-Streams und den Lambda-Trigger

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie den Stream und den Lambda-Trigger.	1. Navigieren Sie in Visual Studio zu AWS Explorer.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Erweitern Sie AWS Lambda und wählen Sie die CommandRe deemRewardFunktion aus (Doppelklicken). In dem sich öffnenden Funktions fenster können Sie die Funktion testen. 3. Geben Sie im Textfeld „Anfrage“ die Anforderu ngsdaten im Format JavaScript Object Notation (JSON) ein. Eine Beispiela nforderung finden Sie unter Testdaten im Abschnitt Zusätzliche Informationen. 4. Wählen Sie aufrufen aus.	
Überprüfen Sie, indem Sie die DynamoDDB-Belohnun gsabfragetabelle verwenden.	1. Öffnen Sie die Tabelle. cqrses-reward-query 2. Überprüfe die Punkte des Kunden, der die Prämie eingelöst hat. Die eingelöst en Punkte sollten von der Gesamtpunktzahl des Kunden abgezogen werden.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie mithilfe von Protokollen. CloudWatch	1. Navigieren Sie zu Protokollgruppen CloudWatch und wählen Sie diese aus. 2. Die aws/lambda/EventSourceReward Protokollgruppe/enthält die Protokolle für den `EventSourceReward` Trigger. Alle Lambda-Aufrufe werden protokolliert, einschließlich der Nachrichten, die Sie in `context.Logger.LogLine` und `Console.WriteLine` im Lambda-Code eingegeben haben.	App-Developer
Validieren Sie den Trigger EventSourceCustomer .	Um den `EventSourceCustomer` Trigger zu validieren, wiederholen Sie die Schritte in diesem Epic und verwenden Sie dabei die entsprechende Kundentabelle und die CloudWatch Logs des `EventSourceCustomer` Triggers.	App-Developer

Zugehörige Ressourcen

Referenzen

- Visual Studio 2019 Community Edition wird heruntergeladen
- AWS Toolkit for Visual Studio herunterladen
- AWS Toolkit for Visual Studio — Benutzerhandbuch
- Serverlos auf AWS

- DynamoDB-Anwendungsfälle und Entwurfsmuster
- Martin Fowler CQRS
- Martin Fowler Beschaffung von Veranstaltungen

Videos

- Demo zu AWS Toolkit for Visual Studio
- Wie erstelle ich eine Zugriffsschlüssel-ID für einen neuen IAM-Benutzer?

Zusätzliche Informationen

CQRS und Eventsourcing

CQRS

Das CQRS-Muster unterteilt ein einzelnes konzeptionelles Betriebsmodell, z. B. ein einzelnes CRUD-Modell (Create, Read, Update, Delete) für Datenzugriffsobjekte, in Befehls- und Abfrageoperationsmodelle. Das Befehlsmodell bezieht sich auf jede Operation, z. B. Erstellen, Aktualisieren oder Löschen, die den Status ändert. Das Abfragemodell bezieht sich auf jede Operation, die einen Wert zurückgibt.

1. Das Kunden-CRUD-Modell umfasst die folgenden Schnittstellen:
   - `Create Customer()`
   - `UpdateCustomer()`
   - `DeleteCustomer()`
   - `AddPoints()`
   - `RedeemPoints()`
   - `GetVIPCustomers()`
   - `GetCustomerList()`
   - `GetCustomerPoints()`

Wenn Ihre Anforderungen immer komplexer werden, können Sie von diesem Einzelmodellansatz abrücken. CQRS verwendet ein Befehlsmodell und ein Abfragemodell, um die Verantwortung für das Schreiben und Lesen von Daten zu trennen. Auf diese Weise können die Daten unabhängig

voneinander verwaltet und verwaltet werden. Bei einer klaren Trennung der Zuständigkeiten wirken sich Verbesserungen an den einzelnen Modellen nicht auf das andere aus. Diese Trennung verbessert Wartung und Leistung und reduziert die Komplexität der Anwendung, wenn sie wächst.

1. Schnittstellen im Customer Command-Modell:
   - `Create Customer()`
   - `UpdateCustomer()`
   - `DeleteCustomer()`
   - `AddPoints()`
   - `RedeemPoints()`
2. Schnittstellen im Modell Customer Query:
   - `GetVIPCustomers()`
   - `GetCustomerList()`
   - `GetCustomerPoints()`
   - `GetMonthlyStatement()`

Beispielcode finden Sie unter Quellcode-Verzeichnis.

Das CQRS-Muster entkoppelt dann die Datenbank. Diese Entkopplung führt zur vollständigen Unabhängigkeit der einzelnen Dienste, was der Hauptbestandteil der Microservice-Architektur ist.

Mit CQRS in der AWS-Cloud können Sie jeden Service weiter optimieren. Sie können beispielsweise verschiedene Recheneinstellungen festlegen oder zwischen einem serverlosen oder einem containerbasierten Microservice wählen. Sie können Ihr lokales Caching durch Amazon ersetzen. ElastiCache Wenn Sie ein lokales Veröffentlichungs-/Abonnement-Messaging haben, können Sie es durch Amazon Simple Notification Service (Amazon SNS) ersetzen. Darüber hinaus können Sie die pay-as-you-go Preisgestaltung und das breite Spektrum an AWS-Services nutzen, bei denen Sie nur für das bezahlen, was Sie tatsächlich nutzen.

CQRS bietet die folgenden Vorteile:

- Unabhängige Skalierung — Für jedes Modell kann die Skalierungsstrategie an die Anforderungen und die Nachfrage des Dienstes angepasst werden. Ähnlich wie bei Hochleistungsanwendungen

ermöglicht die Trennung von Lese- und Schreibvorgängen, dass das Modell unabhängig skaliert werden kann, um jeder Anforderung gerecht zu werden. Sie können auch Rechenressourcen hinzufügen oder reduzieren, um den Skalierbarkeitsanforderungen eines Modells gerecht zu werden, ohne dass sich dies auf das andere Modell auswirkt.

- Unabhängige Wartung — Die Trennung von Abfrage- und Befehlsmodellen verbessert die Wartbarkeit der Modelle. Sie können Codeänderungen und Erweiterungen an einem Modell vornehmen, ohne dass sich dies auf das andere auswirkt.
- Sicherheit — Es ist einfacher, die Berechtigungen und Richtlinien auf separate Modelle zum Lesen und Schreiben anzuwenden.
- Optimierte Lesevorgänge — Sie können ein Schema definieren, das für Abfragen optimiert ist. Sie können beispielsweise ein Schema für die aggregierten Daten und ein separates Schema für die Faktentabellen definieren.
- Integration — CQRS passt gut zu ereignisbasierten Programmiermodellen.
- Verwaltete Komplexität — Die Trennung in Abfrage- und Befehlsmodelle eignet sich für komplexe Domänen.

Beachten Sie bei der Verwendung von CQRS die folgenden Vorbehalte:

- Das CQRS-Muster gilt nur für einen bestimmten Teil einer Anwendung und nicht für die gesamte Anwendung. Wenn es in einer Domäne implementiert wird, die nicht dem Muster entspricht, kann es die Produktivität verringern, das Risiko erhöhen und zu Komplexität führen.
- Das Muster eignet sich am besten für häufig verwendete Modelle mit einem Ungleichgewicht zwischen Lese- und Schreibvorgängen.
- Für leseintensive Anwendungen, wie z. B. große Berichte, deren Verarbeitung einige Zeit in Anspruch nimmt, bietet Ihnen CQRS die Möglichkeit, die richtige Datenbank auszuwählen und ein Schema zum Speichern Ihrer aggregierten Daten zu erstellen. Dadurch wird die Reaktionszeit beim Lesen und Anzeigen des Berichts verbessert, da die Berichtsdaten nur einmal verarbeitet und in der aggregierten Tabelle abgelegt werden.
- Für schreibintensive Anwendungen können Sie die Datenbank für Schreibvorgänge konfigurieren und dem Befehls-Microservice ermöglichen, unabhängig zu skalieren, wenn der Schreibbedarf steigt. Beispiele finden Sie unter den `AWS.APG.CQRSES.CommandRedeemRewardLambda` Microservices und. `AWS.APG.CQRSES.CommandAddRewardLambda`

Ereignis-Sourcing

Der nächste Schritt besteht darin, die Abfragedatenbank mithilfe von Event Sourcing zu synchronisieren, wenn ein Befehl ausgeführt wird. Betrachten Sie beispielsweise die folgenden Ereignisse:

- Ein Kundenprämienpunkt wird hinzugefügt, sodass die Gesamtzahl oder die aggregierten Prämienpunkte des Kunden in der Abfragedatenbank aktualisiert werden müssen.
- Der Nachname eines Kunden wird in der Befehlsdatenbank aktualisiert, weshalb die Ersatzkundeninformationen in der Abfragedatenbank aktualisiert werden müssen.

Im herkömmlichen CRUD-Modell stellen Sie die Konsistenz der Daten sicher, indem Sie die Daten sperren, bis eine Transaktion abgeschlossen ist. Beim Event Sourcing werden die Daten synchronisiert, indem eine Reihe von Ereignissen veröffentlicht wird, die dann von einem Abonnenten genutzt werden, um seine jeweiligen Daten zu aktualisieren.

Das Muster der Ereignisbeschaffung gewährleistet und zeichnet eine vollständige Reihe von Aktionen auf, die an den Daten vorgenommen wurden, und veröffentlicht sie in einer Abfolge von Ereignissen. Diese Ereignisse stellen eine Reihe von Änderungen an den Daten dar, die Abonnenten dieses Ereignisses verarbeiten müssen, um ihre Aufzeichnungen auf dem neuesten Stand zu halten. Diese Ereignisse werden vom Abonnenten verarbeitet, wodurch die Daten in der Datenbank des Abonnenten synchronisiert werden. In diesem Fall ist das die Abfragedatenbank.

Das folgende Diagramm zeigt Event Sourcing, das mit CQRS auf AWS verwendet wird.

1. Befehls-Lambda-Funktionen führen Schreiboperationen wie Erstellen, Aktualisieren oder Löschen in der Datenbank durch.
2. Lambda-Abfragefunktionen führen Lesevorgänge wie Get oder Select in der Datenbank durch.
3. Diese Lambda-Funktion verarbeitet die DynamoDB-Streams aus der Befehlsdatenbank und aktualisiert die Query-Datenbank für die Änderungen. Sie können diese Funktion auch verwenden, um eine Nachricht an Amazon SNS zu veröffentlichen, damit die Abonnenten die Daten verarbeiten können.
4. (Optional) Der Lambda-Event-Abonnent verarbeitet die von Amazon SNS veröffentlichte Nachricht und aktualisiert die Query-Datenbank.
5. (Optional) Amazon SNS sendet eine E-Mail-Benachrichtigung über den Schreibvorgang.

Auf AWS kann die Abfragedatenbank mit DynamoDB Streams synchronisiert werden. DynamoDB erfasst eine zeitlich geordnete Abfolge von Änderungen auf Elementebene in einer DynamoBDB-Tabelle nahezu in Echtzeit und speichert die Informationen dauerhaft innerhalb von 24 Stunden.

Durch die Aktivierung von DynamoDB Streams kann die Datenbank eine Sequenz von Ereignissen veröffentlichen, die das Eventsourcing-Muster ermöglicht. Das Event-Sourcing-Muster fügt den Event-Abonnenten hinzu. Die Anwendung für Event-Abonnenten verarbeitet das Ereignis und verarbeitet es je nach Verantwortung des Abonnenten. Im vorherigen Diagramm überträgt der Ereignisabonnent die Änderungen an die Query DynamoDB-Datenbank, um die Daten synchron zu halten. Durch die Verwendung von Amazon SNS, dem Message Broker und der Event-Abonnentenanwendung bleibt die Architektur entkoppelt.

Event Sourcing bietet die folgenden Vorteile:

- Konsistenz für Transaktionsdaten
- Ein zuverlässiger Prüfpfad und eine Historie der Maßnahmen, anhand derer die anhand der Daten ergriffenen Maßnahmen überwacht werden können
- Ermöglicht verteilten Anwendungen wie Microservices, ihre Daten in der gesamten Umgebung zu synchronisieren
- Zuverlässige Veröffentlichung von Ereignissen, wann immer sich der Status ändert
- Rekonstruktion oder Wiederholung vergangener Staaten
- Lose gekoppelte Entitäten, die Ereignisse austauschen, um von einer monolithischen Anwendung zu Microservices zu migrieren
- Reduzierung von Konflikten, die durch gleichzeitige Aktualisierungen verursacht werden; durch die Ereignisbeschaffung entfällt die Notwendigkeit, Objekte direkt im Datenspeicher zu aktualisieren
- Flexibilität und Erweiterbarkeit durch die Entkopplung von Aufgabe und Ereignis
- Updates für externe Systeme
- Verwaltung mehrerer Aufgaben in einem einzigen Ereignis

Beachten Sie bei der Verwendung von Event Sourcing die folgenden Vorbehalte:

- Da es bei der Aktualisierung von Daten zwischen den Quell-Abonnentendatenbanken zu Verzögerungen kommt, besteht die einzige Möglichkeit, eine Änderung rückgängig zu machen, darin, dem Ereignisspeicher ein kompensierendes Ereignis hinzuzufügen.
- Die Implementierung von Event Sourcing ist aufgrund des unterschiedlichen Programmierstils mit einer gewissen Lernkurve verbunden.

Daten testen

Verwenden Sie die folgenden Testdaten, um die Lambda-Funktion nach erfolgreicher Bereitstellung zu testen.

CommandCreate Kunde

```
{  "Id":1501,  "Firstname":"John",  "Lastname":"Done",  "CompanyName":"AnyCompany",
 "Address": "USA",  "VIP":true }
```

CommandUpdate Kunde

```
{  "Id":1501,  "Firstname":"John",  "Lastname":"Doe",  "CompanyName":"Example Corp.",
 "Address": "Seattle, USA",  "VIP":true }
```

CommandDelete Kunde

Geben Sie die Kunden-ID als Anfragedaten ein. Wenn die Kunden-ID beispielsweise 151 ist, geben Sie 151 als Anforderungsdaten ein.

```
151
```

QueryCustomerList

Das ist leer. Wenn es aufgerufen wird, werden alle Kunden zurückgegeben.

CommandAddReward

Dadurch werden dem Kunden mit der ID 1 (Richard) 40 Punkte gutgeschrieben.

```
{
  "Id":10101,
  "CustomerId":1,
  "Points":40
}
```

CommandRedeemReward

Dem Kunden mit der ID 1 (Richard) werden dadurch 15 Punkte abgezogen.

```
{
```

```
  "Id":10110,
  "CustomerId":1,
  "Points":15
}
```

QueryReward

Geben Sie die ID des Kunden ein. Geben Sie beispielsweise 1 für Richard, 2 für Arnav und 3 für Shirley ein.

```
2
```

Quellcode-Verzeichnis

Verwenden Sie die folgende Tabelle als Leitfaden für die Verzeichnisstruktur der Visual Studio-Lösung.

Lösungsverzeichnis mit lokalen CQRS-Codebeispielen

CRUD-Modell für Kunden

Lokales CQRS-Codebeispiel\ CRUD-Modell\ AWS.APG.CQRSES.DAL-Projekt

CQRS-Version des Kunden-CRUD-Modells

- Kundenbefehl: Projekt `CQRS On-Premises Code Sample\CQRS Model\Command Microservice\AWS.APG.CQRSES.Command`
- Kundenanfrage: `CQRS On-Premises Code Sample\CQRS Model\Query Microservice \AWS.APG.CQRSES.Query` Projekt

Microservices für Befehle und Abfragen

Der Command-Mikroservice befindet sich im Lösungsordner: `CQRS On-Premises Code Sample \CQRS Model\Command Microservice`

- `AWS.APG.CQRSES.CommandMicroservice`Das ASP.NET Core API-Projekt dient als Einstiegspunkt, über den Verbraucher mit dem Dienst interagieren.
- `AWS.APG.CQRSES.Command`.NET Core-Projekt ist ein Objekt, das befehlsbezogene Objekte und Schnittstellen hostet.

Der Abfrage-Microservice befindet sich im Lösungsordner: `CQRS On-Premises Code Sample \CQRS Model\Query Microservice`

- `AWS.APG.CQRSES.QueryMicroservice`Das ASP.NET Core API-Projekt dient als Einstiegspunkt, über den Verbraucher mit dem Dienst interagieren.
- `AWS.APG.CQRSES.Query`.NET Core-Projekt ist ein Objekt, das abfragebezogene Objekte und Schnittstellen hostet.

Verzeichnis der CQRS AWS-Serverless-Codelösungen

Dieser Code ist die AWS-Version des lokalen Codes, der serverlose AWS-Services verwendet.

In C#.NET Core wird jede Lambda-Funktion durch ein .NET Core-Projekt repräsentiert. Im Beispielcode dieses Musters gibt es für jede Schnittstelle im Befehls- und Abfragemodell ein eigenes Projekt.

CQRS verwendet AWS-Services

Sie finden das Stammlösungsverzeichnis für CQRS, das AWS-Serverless-Services verwendet, im `CQRS AWS Serverless\CQRS` Ordner. Das Beispiel umfasst zwei Modelle: Customer und Reward.

Die Befehle Lambda-Funktionen für Customer und Reward befinden sich in den `CQRS\Command Microservice\Reward` Ordnern `CQRS\Command Microservice\Customer` und. Sie enthalten die folgenden Lambda-Projekte:

- Kundenbefehl: `CommandCreateLambdaCommandDeleteLambda`, und `CommandUpdateLambda`
- Belohnungsbefehl: `CommandAddRewardLambda` und `CommandRedeemRewardLambda`

Die Lambda-Abfragefunktionen für Customer und Reward befinden sich in den `CQRS \QueryMicroservice\Reward` Ordnern `CQRS\Query Microservice\Customer` und. Sie enthalten die Projekte `QueryCustomerListLambda` und `QueryRewardLambda` Lambda.

CQRS-Testprojekt

Das Testprojekt befindet sich unter dem `CQRS\Tests` Ordner. Dieses Projekt enthält ein Testskript zur Automatisierung des Testens der CQRS-Lambda-Funktionen.

Beschaffung von Veranstaltungen mithilfe von AWS-Services

Die folgenden Lambda-Event-Handler werden von den DynamoDB-Streams Customer und Reward initiiert, um die Daten in Abfragetabellen zu verarbeiten und zu synchronisieren.

- Die `EventSourceCustomer` Lambda-Funktion ist dem DynamoDB-Stream Customer table (`cqrses-customer-cmd`) zugeordnet.
- Die `EventSourceReward` Lambda-Funktion ist dem DynamoDB-Stream Reward table (`cqrses-reward-cmd`) zugeordnet.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Mehr Muster

- Greifen Sie mit AWS PrivateLink und einem Network Load Balancer privat auf Container-Anwendungen auf Amazon EKS zu
- Automatisieren Sie das Hinzufügen oder Aktualisieren von Windows-Registrierungseinträgen mit AWS Systems Manager
- Automatisieren Sie regionsübergreifendes Failover und Failback mithilfe des DR Orchestrator Framework
- Automatisches Erstellen und Bereitstellen einer Java-Anwendung auf Amazon EKS mithilfe einer CI/CD-Pipeline
- Automatisches Erstellen von CI/CD-Pipelines und Amazon ECS-Clustern für Microservices mithilfe von AWS CDK
- Mainframe-Daten mithilfe von BMC AMI Cloud Data auf Amazon S3 sichern und archivieren
- Erstellen Sie ein Micro Focus Enterprise Server PAC mit Amazon EC2 Auto Scaling und Systems Manager
- Bauen Sie mit Amazon ein Datennetz für Unternehmen auf DataZone AWS CDK, und AWS CloudFormation
- Verketten Sie AWS-Services mithilfe eines serverlosen Ansatzes
- Containerisieren Sie Mainframe-Workloads, die von Blu Age modernisiert wurden
- Kontinuierliche Bereitstellung einer modernen AWS Amplify Amplify-Webanwendung aus einem AWS-Repository CodeCommit
- EBCDIC-Daten mithilfe von Python in ASCII auf AWS konvertieren und entpacken
- Konvertieren Sie Mainframe-Datendateien mit komplexen Datensatzlayouts mit Micro Focus
- Erstellen Sie eine Pipeline und ein AMI mit CodePipeline und HashiCorp Packer
- Erstellen Sie eine Pipeline und stellen Sie Artefaktaktualisierungen für lokale Instanzen EC2 bereit mit CodePipeline
- Erstellen Sie ein Portal für Mikro-Frontends mithilfe AWS Amplify von Angular und Module Federation
- Bereitstellen und Debuggen von Amazon EKS-Clustern
- Container mithilfe von Elastic Beanstalk bereitstellen
- Emulieren Sie Oracle DR mithilfe einer PostgreSQL-kompatiblen globalen Aurora-Datenbank
- Generieren Sie Dateneinblicke mithilfe von AWS Mainframe Modernization und Amazon Q in QuickSight

- Generieren Sie Einblicke in Db2 z/OS-Daten mithilfe von Amazon AWS Mainframe Modernization Q in QuickSight
- Automatische Identifizierung doppelter Container-Images bei der Migration zu einem Amazon ECR-Repository
- Implementieren Sie eine pfadbasierte API-Versionierung mithilfe benutzerdefinierter Domains in Amazon API Gateway
- Schrittweise Migration von Amazon RDS for Oracle zu Amazon RDS for PostgreSQL mithilfe von Oracle SQL Developer und AWS SCT
- Integrieren Sie den Stonebranch Universal Controller in die AWS-Mainframe-Modernisierung
- AWS Service Catalog-Produkte in mehreren AWS-Konten und AWS-Regionen verwalten
- Migrieren Sie ein AWS-Mitgliedskonto von AWS Organizations zu AWS Control Tower
- Migrieren und replizieren Sie VSAM-Dateien mit Connect von Precisely zu Amazon RDS oder Amazon MSK
- Migrieren Sie mithilfe von AWS DMS von SAP ASE zu Amazon RDS for SQL Server
- Migrieren Sie externe Oracle-Tabellen zu Amazon Aurora PostgreSQL-kompatibel
- Modernisieren Sie die CardDemo Mainframe-Anwendung mithilfe von AWS Transform
- Modernisieren Sie Mainframe-Batchdruck-Workloads mithilfe AWS von Rocket Enterprise Server und LRS VPSX/MFI
- Modernisieren Sie Mainframe-Online-Druck-Workloads auf AWS mithilfe von Micro Focus Enterprise Server und LRS VPSX/MFI
- Modernisieren Sie das Mainframe-Output-Management mithilfe AWS von Rocket Enterprise Server und LRS X PageCenter
- Verschieben Sie Mainframe-Dateien mit Transfer Family direkt nach Amazon S3
- Optimieren Sie die von AWS App2Container generierten Docker-Images
- Optimieren Sie serverlose Bereitstellungen mit mehreren Konten mithilfe der AWS CDK Workflows und Aktionen GitHub
- Automatisieren Sie blaue/grüne Bereitstellungen globaler Amazon Aurora Aurora-Datenbanken mithilfe von IaC-Prinzipien
- Replizieren Sie Mainframe-Datenbanken mithilfe von Precisely Connect nach AWS
- Führen Sie Amazon ECS-Aufgaben auf Amazon WorkSpaces mit Amazon ECS Anywhere aus
- Senden Sie Telemetriedaten von AWS Lambda zu OpenSearch für Analysen und Visualisierungen in Echtzeit

- Richten Sie ein Helm v3-Chart-Repository in Amazon S3 ein
- Richten Sie die AWS CloudFormation Drifterkennung in einer Organisation mit mehreren Regionen und mehreren Konten ein
- Strukturieren Sie ein Python-Projekt in hexagonaler Architektur mit AWS Lambda
- Testen Sie die AWS Infrastruktur mithilfe LocalStack von Terraform-Tests
- Aktualisieren Sie SAP Pacemaker-Cluster von ENSA1 auf ENSA2
- Verwenden Sie Amazon Q Developer als Programmierassistenten, um Ihre Produktivität zu steigern
- Validieren Sie den Account Factory for Terraform (AFT) -Code lokal

Großrechner

Themen

- Zugriff AWS-Services von IBM z/OS aus durch Installation des AWS CLI
- Mainframe-Daten mithilfe von BMC AMI Cloud Data auf Amazon S3 sichern und archivieren
- Erstellen Sie COBOL Db2-Programme mit und AWS Mainframe ModernizationAWS CodeBuild
- Erstellen Sie ein Micro Focus Enterprise Server PAC mit Amazon EC2 Auto Scaling und Systems Manager
- Erstellen Sie einen fortschrittlichen Mainframe-Dateiviewer in der AWS-Cloud
- Containerisieren Sie Mainframe-Workloads, die von Blu Age modernisiert wurden
- EBCDIC-Daten mithilfe von Python in ASCII auf AWS konvertieren und entpacken
- Konvertieren Sie Mainframe-Dateien mithilfe von AWS Lambda vom EBCDIC-Format in das durch Zeichen getrennte ASCII-Format in Amazon S3
- Konvertieren Sie Mainframe-Datendateien mit komplexen Datensatzlayouts mit Micro Focus
- Stellen Sie mithilfe von Terraform eine Umgebung für containerisierte Blu Age-Anwendungen bereit
- Generieren Sie Einblicke in Db2 z/OS-Daten mithilfe von Amazon AWS Mainframe Modernization Q in QuickSight
- Generieren Sie Dateneinblicke mithilfe von AWS Mainframe Modernization und Amazon Q in QuickSight
- Integrieren Sie den Stonebranch Universal Controller in die AWS-Mainframe-Modernisierung
- Migrieren und replizieren Sie VSAM-Dateien mit Connect von Precisely zu Amazon RDS oder Amazon MSK
- Modernisieren Sie das Mainframe-Output-Management mithilfe AWS von Rocket Enterprise Server und LRS X PageCenter
- Modernisieren Sie die CardDemo Mainframe-Anwendung mithilfe von AWS Transform
- Modernisieren Sie Mainframe-Batchdruck-Workloads mithilfe AWS von Rocket Enterprise Server und LRS VPSX/MFI
- Mainframe-Modernisierung: DevOps Weiter AWS mit Rocket Software Enterprise Suite
- Modernisieren Sie Mainframe-Online-Druck-Workloads auf AWS mithilfe von Micro Focus Enterprise Server und LRS VPSX/MFI
- Verschieben Sie Mainframe-Dateien mit Transfer Family direkt nach Amazon S3

- Sicherer und optimierter Benutzerzugriff in einer Db2-Verbunddatenbank auf AWS mithilfe vertrauenswürdiger Kontexte
- Übertragung umfangreicher Db2 z/OS-Daten in CSV-Dateien nach Amazon S3
- Mehr Muster

Zugriff AWS-Services von IBM z/OS aus durch Installation des AWS CLI

Erstellt von Souma Ghosh (AWS), Phil de Valence (AWS) und Paulo Vitor Pereira (AWS)

Übersicht

The AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool zur Verwaltung mehrerer AWS Dienste mithilfe von Befehlen in einer Befehlszeilen-Shell. Mit minimaler Konfiguration können Sie Befehle von Befehlszeilensitzungen wie der Befehlszeile, dem Terminal und der Bash-Shell aus ausführen, um Funktionen zu implementieren, die der browserbasierten AWS Management Console Version entsprechen.

Alle Administrations-, Management- und Zugriffsfunktionen von AWS Infrastructure as a Service (IaaS) in der AWS Management Console sind in der AWS API und AWS CLI verfügbar. Sie können den AWS CLI auf einem IBM z/OS-Mainframe installieren, um von z/OS aus direkt darauf zuzugreifen, ihn zu verwalten und mit AWS-Services ihm zu interagieren. Das AWS CLI ermöglicht es Benutzern und Anwendungen, verschiedene Aufgaben auszuführen, wie z. B.:

- Übertragung von Dateien oder Datensätzen zwischen z/OS und dem Objektspeicher von Amazon Simple Storage Service (Amazon S3) und Anzeigen des Inhalts von Buckets
- Starten und Stoppen verschiedener AWS Ressourcen, z. B. Starten eines Batch-Jobs in einer Umgebung AWS Mainframe Modernization
- Aufruf einer AWS Lambda Funktion zur Implementierung allgemeiner Geschäftslogik
- Integration mit Diensten für künstliche Intelligenz und maschinelles Lernen (AI/ML) sowie Analysedienste

Dieses Muster beschreibt, wie Sie das AWS CLI auf z/OS installieren, konfigurieren und verwenden. Sie können es global installieren, sodass es für alle z/OS-Benutzer verfügbar ist, oder auf Benutzerebene. Das Muster beschreibt auch, wie der AWS CLI in einer interaktiven Befehlszeilensitzung von z/OS Unix System Services (USS) oder als Batch-Job verwendet wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Netzwerkkommunikation von z/OS zu AWS

  Standardmäßig AWS CLI sendet der Anfragen unter Verwendung AWS-Services von HTTPS an TCP-Port 443. Um das AWS CLI erfolgreich verwenden zu können, müssen Sie in der Lage

sein, ausgehende Verbindungen über den TCP-Port 443 herzustellen. Sie können jeden der folgenden z/OS USS-Befehle (einige davon sind möglicherweise nicht in Ihrer Umgebung installiert) verwenden, um die Netzwerkkonnektivität von z/OS zu testen: AWS

```
ping amazonaws.com
dig amazonaws.com
traceroute amazonaws.com
curl -k https://docs.aws.amazon.com/cli/v1/userguide/cli-chap-welcome.html
```

- AWS Anmeldedaten

  Um mit AWS Cloud Services von z/OS kommunizieren zu können, AWS CLI müssen Sie einige Anmeldeinformationen mit Zugriffsrechten auf das Ziel konfigurieren. AWS-Konto Für programmatische Befehle können Sie Zugriffsschlüssel verwenden, die aus einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel bestehen. AWS Wenn Sie noch keine Zugriffsschlüssel besitzen, können Sie diese über die AWS Management Console erstellen. Es hat sich bewährt, die Zugriffsschlüssel für den AWS-Konto Root-Benutzer für keine Aufgabe zu verwenden, es sei denn, der Root-Benutzer ist erforderlich. Erstellen Sie stattdessen einen neuen Administrator-IAM-Benutzer und bereiten Sie sich auf die Berechtigungen mit den geringsten Rechten vor, um den Benutzer mit Zugriffsschlüsseln einzurichten. Nachdem Sie den Benutzer erstellt haben, können Sie eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel für diesen Benutzer erstellen.

  > **Warning**
  >
  > AWS Identity and Access Management (IAM) -Benutzer verfügen über langfristige Anmeldeinformationen, die ein Sicherheitsrisiko darstellen. Um dieses Risiko zu minimieren, empfehlen wir, diesen Benutzern nur die Berechtigungen zu gewähren, die sie für die Ausführung der Aufgabe benötigen, und diese Benutzer zu entfernen, wenn sie nicht mehr benötigt werden.

- IBM Python für z/OS

  Das AWS CLI erfordert Python 3.8 oder höher. IBM hat Python mit IBM Open Enterprise Python for z/OS für die Ausführung auf z/OS aktiviert. IBM Open Enterprise Python ist kostenlos über Shopz SMP/E erhältlich, oder Sie können die PAX-Datei von der IBM-Website herunterladen. Anweisungen finden Sie in der Installations- und Konfigurationsdokumentation für IBM Open Enterprise Python for z/OS.

Einschränkungen

- Die in diesem Muster enthaltenen Installationsanweisungen gelten nur für AWS CLI Version 1. Die neueste Version von AWS CLI ist Version 2. Dieses Muster verwendet jedoch die ältere Version, da die Installationsmethoden für Version 2 unterschiedlich sind und die für Version 2 verfügbaren binären ausführbaren Dateien nicht mit dem z/OS-System kompatibel sind.

Produktversionen

- AWS CLI Version 1
- Python 3.8 oder höher

Architektur

Technologie-Stack

- Mainframe, auf dem z/OS ausgeführt wird
- Mainframe z/OS UNIX-Systemdienste (USS)
- Mainframe Open MVS (OMVS) — Befehlsschnittstelle für die z/OS UNIX-Shell-Umgebung
- Mainframe-Festplatte, z. B. ein Direct-Access-Speichergerät (DASD)
- AWS CLI

Zielarchitektur

Das folgende Diagramm zeigt eine AWS CLI Bereitstellung auf IBM z/OS. Sie können die AWS CLI in einer interaktiven Benutzersitzung wie SSH- und Telnet-Sitzungen aufrufen. Sie können ihn auch von einem Batch-Job aus aufrufen, indem Sie die Job Control Language (JCL) verwenden, oder von einem beliebigen Programm aus, das einen z/OS Unix-Shell-Befehl aufrufen kann.

Der AWS CLI kommuniziert mit AWS-Service Endpunkten über ein TCP/IP-Netzwerk. Diese Netzwerkverbindung kann über das Internet oder über eine private AWS Direct Connect Verbindung vom Kundenrechenzentrum zu den Rechenzentren erfolgen. AWS Cloud Die Kommunikation wird mit AWS Anmeldeinformationen authentifiziert und verschlüsselt.

Automatisierung und Skalierung

Sie können die Funktionen von und AWS-Service mit dem erkunden AWS CLI und USS-Shell-Skripte entwickeln, um Ihre AWS Ressourcen von z/OS aus zu verwalten. Sie können auch AWS CLI Befehle und Shell-Skripte in der z/OS-Batch-Umgebung ausführen und durch die Integration mit Mainframe-Schedulern Batch-Jobs automatisieren, sodass sie nach einem bestimmten Zeitplan ausgeführt werden. AWS CLI Befehle oder Skripten können innerhalb von Parametern (PARMs) und Prozeduren (PROCs) codiert und skaliert werden, indem man dem Standardansatz folgt, den PARM oder PROC von verschiedenen Batch-Jobs mit unterschiedlichen Parametern aus aufzurufen.

Tools

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie AWS-Services über Befehle in Ihrer Befehlszeilen-Shell interagieren können.

Bewährte Methoden

- Beschränken Sie aus Sicherheitsgründen die Zugriffsberechtigungen auf das USS-Verzeichnis, in dem die AWS Zugangsschlüsseldetails gespeichert sind. Erlauben Sie den Zugriff nur Benutzern oder Programmen, die den verwenden AWS CLI.
- Verwenden Sie die AWS-Konto Root-Benutzerzugriffstasten für keine Aufgabe. Erstellen Sie stattdessen einen neuen Administrator-IAM-Benutzer für sich selbst und richten Sie ihn mit Zugriffsschlüsseln ein.

> **Warning**
>
> IAM-Benutzer verfügen über langfristige Anmeldeinformationen, die ein Sicherheitsrisiko darstellen. Um dieses Risiko zu minimieren, empfehlen wir, diesen Benutzern nur die Berechtigungen zu gewähren, die sie für die Ausführung der Aufgabe benötigen, und diese Benutzer zu entfernen, wenn sie nicht mehr benötigt werden.

Epen

Installieren Sie AWS CLI Version 1 auf z/OS USS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Python 3.8 oder höher.	1. Melden Sie sich mit einer der folgenden Methoden bei der z/OS USS-Befeh lszeilenschnittstelle an: • Verwenden Sie einen OMVS-Befehl (Time Sharing Option) (TSO) im Bereich Interactive System Productivity Facility (ISPF), oder • Verwenden Sie SSH oder Telnet, um eine Verbindung zur IP der logischen Mainframe -Partition (LPAR) herzustellen. Bei diesem Muster wird davon ausgegang en, dass `cliuser` es sich um die Benutzer-ID handelt, die für die Anmeldung in der USS-Umgebung verwendet wird, und dass es sich um das Home-Verzeichnis für den Benutzer `/u/cliuser/` handelt. Sie können das Benutzer-Home-Verzeichnis in Ihrer z/OS-Umgebung	Mainframe-z/OS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	je nach Ihren Installat ionsanforderungen unterschiedlich einrichte n. 2. Folgen Sie der Installat ionsanleitung für IBM Open Enterprise Python for z/OS, um Python 3.8 oder höher zu installieren, falls es noch nicht installiert ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Legen Sie USS-Umgebungsvariablen fest.	Fügen Sie dem Profil Umgebungsvariablen hinzu. Sie können diese entweder der `/u/cliuser/.profile` Datei für einen einzelnen Benutzer (`cliuser`) oder der `/etc/profile` Datei für alle Benutzer hinzufügen.
	
	Note
	Dieses Muster geht davon aus, dass Python im `/u/awscli/python` Verzeichnis installiert wurde. Wenn Ihr Installationsverzeichnis anders ist, aktualisieren Sie den Code entsprechend.
	
	`# Python configuration`
	`export BPXKAUTOCVT='ON'`
	`export CEERUNOPTS='FILETAG(AUTOCVT,AUTOTAG) POSIX(ON)'`
	`export TAGREDIR_ERR=txt`
	`export TAGREDIR_IN=txt`
	`export TAGREDIR_OUT=txt`
	
	`# AWS CLI configuration`
		Mainframe-z/OS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`export PATH=/u/cliuser/python/bin:$PATH` `export PYTHONPATH=/u/cliuser/python:$PYTHONPATH`	
Testen Sie die Python-Installation.	Führen Sie den Python-Befehl aus: `python --version` Die Ausgabe sollte bestätigen, dass Sie Python 3.8 oder höher korrekt installiert haben.	Mainframe-z/OS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen oder installieren Sie Pip.	1. Der Befehl pip wird normalerweise automatisch installiert, wenn Sie Python von der IBM-Website installieren. Führen Sie zur Überprüfung den folgenden Befehl aus:
	`pip —-version`
	Wenn pip installiert ist, sollte dieser Befehl die installierte Version anzeigen.
	2. Wenn der Befehl pip nicht gefunden wird, installieren Sie pip, indem Sie den folgenden Befehl ausführen:
	`python -m ensurepip --upgrade`
	Weitere Installationsoptionen finden Sie in der Pip-Dokumentation.
		Mainframe-z/OS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie AWS CLI Version 1.	1. Um das zu installieren AWS CLI, führen Sie den folgenden Befehl aus:
	`python -m pip install awscli`
	Die Ausgabe sollte folgendermaßen oder ähnlich aussehen.
	`Successfully installed PyYAML-6.0.1 awscli-1.32.23 botocore-1.34.23 colorama-0.4.4 docutils-0.16 jmespath-1.0.1 pyasn1-0.5.1 python-dateutil-2.8.2 rsa-4.7.2 s3transfer-0.10.0 urllib3-2.0.7`
	2. Ändern Sie die Berechtigungen der ausführbaren AWS-Datei, indem Sie den folgenden Befehl ausführen. Stellen Sie sicher, dass Sie das Platzhalterverzeichnis `<python_installation_dir>` mit Ihrem Python-Installationspfad aktualisieren.
		Mainframe-z/OS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`chmod 744 <python_installation_dir>/bin/aws`
	3. Führen Sie den folgenden Befehl aus, um die AWS CLI Installation zu testen:
	`aws --version`
	Die Ausgabe sollte die Versionen von Python und Botocore zeigen, ähnlich wie im Folgenden. AWS CLI
	`aws-cli/1.32.3 Python/3.9.5 OS/390/27.00 botocore/1.34.3`	

Konfigurieren Sie den AWS CLI Zugriff von z/OS aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die AWS Zugriffstasten, die Standardregion und die Ausgabe.	In der AWS CLI Dokumentation werden verschiedene Optionen für die Einrichtung des AWS Zugriffs beschrieben. Sie können eine Konfiguration wählen, die den Standards Ihrer Organisation entspricht. In diesem Beispiel wird die Konfiguration	AWS-Administrator, Mainframe z/OS-Administrator, Mainframe z/OS-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	mit kurzfristigen Anmeldein formationen verwendet.
	
	1. Konfigurieren Sie das AWS CLI mit dem folgenden Befehl:
	
	`aws configure`
	
	2. Geben Sie die Details für die folgenden Elemente ein, wenn Sie dazu aufgeford ert werden. Die Werte für die Zugriffsschlüssel-ID und den geheimen Zugriffss chlüssel stammen aus den Schlüsseln, die Sie erhalten haben, als Sie die AWS Anmeldeinformationen in den Schritten „Vorausset zungen“ festgelegt haben.
	
	`AWS Access Key ID [None]: ASIAIOSFO DNN7EXAMPLE`
	`AWS Secret Access Key [None]: wJalrXUtn FEMI/K7MDENG/bPxRf iCYEXAMPLEKEY`
	`Default region name [None]: us-east-1`
	`Default output format [None]:`
	`aws configure set aws_session_token IQoJb3JpZ2luX2IQoJ b3JpZ2luX2IQoJb3Jp Z2luX2IQoJb3JpZ2lu`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`X2IQoJb3JpZVERYLON GSTRINGEXAMPLE` Diese Konfiguration, einschließlich der Zugriffsschlüssel, wird in dem `/u/cliuser/.aws` Ordner gespeichert. Beschränken Sie diesen Ordner aus Sicherheitsgründen so, dass nur Benutzer oder Programme darauf zugreifen können, die den verwenden AWS CLI.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie das. AWS CLI	1. Führen Sie den folgenden Befehl an der Eingabeaufforderung aus, um das AWS CLI mit einem einfachen Befehl zu testen: `aws s3 ls` Die Ausgabe sollte alle S3-Buckets für die Konfiguration AWS-Konto ohne Fehler auflisten. 2. Folgen Sie den Anweisungen in den nächsten beiden Epen, um Daten von USS nach Amazon S3 zu übertragen. Sie können eine dieser beiden Optionen wählen: • Option 1 (nächstes Epic): Interaktiv eine EBCDIC-Datei mit kommagetrennten Werten (CSV) nach Amazon S3 übertragen und die Datei von Amazon Athena abfragen. • Option 2: Übertragen Sie einen EBCDIC-Datensatz mit fester Länge als Batch-Job an Amazon S3.	Mainframe z/OS-Administrator, Mainframe z/OS-Entwickler

Option 1 – Daten interaktiv aus einer USS-Sitzung von USS zu Amazon S3 übertragen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die CSV-Beispieldatei herunter und übertragen Sie sie.	1. Laden Sie sie `sales-records.csv` aus dem Bereich Anlagen herunter. Diese Datei enthält eine CSV-Beispieldatei mit Verkaufsdatensätzen. 2. Übertragen Sie die Datei nach z/OS USS. 3. Stellen Sie sicher, dass die `/u/cliuser/sales-records.csv` Datei in USS im EBCDIC-Format lesbar ist, indem Sie einen Texteditor Ihrer Wahl verwenden.	App-Entwickler, Mainframe z/OS-Entwickler

Erstellen Sie einen S3-Bucket und laden Sie die CSV-Datei hoch.	1. Erstellen Sie einen S3-Bucket zum Speichern der CSV-Datei.
	`aws s3 mb s3://<s3_bucket_name>`
	wo `<s3_bucket_name>` ist der eindeutige Name für einen Bucket; zum Beispiel:
	`aws s3 mb s3://DOC-EXAMPLE-BUCKET1`
	2. Laden Sie die CSV-Datei von z/OS USS in den S3-Bucket hoch:
		App-Entwickler, Mainframe z/OS-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`aws s3 cp <csv_file _path> s3://<s3_ bucket_name>`
	
	Zum Beispiel:
	
	`aws s3 cp /u/cliuser/ sales-records.csv s3://DOC-EXAMPLE-B UCKET1`
	
	3. Listen Sie den Inhalt des S3-Buckets auf und vergewissern Sie sich, dass er die hochgeladene Datei enthält:
	
	`aws s3 ls s3://<s3_ bucket_name>`
	
	Zum Beispiel:
	
	`aws s3 ls s3://DOC-EXAMPLE-BUCKET1`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich den S3-Bucket und die hochgeladene Datei an.	1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon S3 S3-Konsole. 2. Navigieren Sie, um den neuen S3-Bucket und das hochgeladene Objekt zu sehen. Weitere Informationen zum Hochladen von Objekten finden Sie unter Erste Schritte mit Amazon S3 in der Amazon S3 S3-Dokumentation.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Führen Sie eine SQL-Abfrage für eine Amazon Athena Athena-Tabelle aus.	1. Öffnen Sie die Amazon-Athena-Konsole.
	2. Erstellen Sie eine neue Tabelle (z. B. `DOC-EXAMPLE-BUCKET`) mithilfe der CSV-Daten von Amazon S3. Weitere Informationen finden Sie unter Abfragen von Amazon S3 S3-Inventar mit Amazon Athena in der Amazon S3 S3-Dokumentation.
	3. Führen Sie die `SELECT` Abfrage anhand der Tabelle aus, um die Daten anzuzeigen.
	`SELECT * FROM <table_name>;`
	Zum Beispiel:
	`SELECT * FROM DOC-EXAMPLE-BUCKET;`
	In der Ausgabe der SQL-Abfrage wird der Inhalt Ihrer CSV-Datei angezeigt.
		Allgemein AWS, App-Entwickler

Option 2 – Daten mithilfe von Batch-JCL von USS nach Amazon S3 übertragen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Beispieldatei hoch.	1. Laden Sie sie `sales-records-fixed.txt` aus dem Bereich Anlagen herunter. Dies ist eine Beispieldatei mit Verkaufsaufzeichnungen. Benennen Sie die Textdatei um, z. B. in `USER.DATA.FIXED` . 2. Übertragen Sie die Datei als festblockierten (FB) Datensatz mit 256 Datensätzen (LRECL) und physikalischer sequentieller Datenmenge (PS) nach z/OS. 3. Verwenden Sie das Programm zur Datensatzliste, um zu überprüfen, ob der `USER.DATA.FIXED` Datensatz unter ISPF-Option 3.4 im EBCDIC-Format lesbar ist. Ein Beispiel für die Ausgabe finden Sie im Abschnitt Zusätzliche Informationen.	Mainframe z/OS-Entwickler
Erstellen Sie eine Batch-JCL.	Codieren Sie die Batch-JCL wie folgt, um den Ziel-S3-Bucket zu erstellen, den Datensatz hochzuladen und den Bucket-Inhalt aufzulisten. Stellen Sie sicher, dass Sie	Mainframe-z/OS-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	den Verzeichnisnamen, die Dateinamen und den Bucket-Namen durch Ihre eigenen Werte ersetzen.
	
	`//AWSCLICP JOB`
	` ACTINFO1,'IBMUSER'`
	`,CLASS=A,MSGCLASS=`
	`H,MSGLEVEL=(1,1),`
	`// NOTIFY=&SYSUID,TIM`
	`E=1440`
	`//*--------------`
	`------------------`
	`------------------`
	`-------`
	`//* Sample job for AWS`
	` CLI`
	`//*--------------`
	`------------------`
	`------------------`
	`-------`
	`//USSCMD EXEC PGM=BPXBA`
	`TCH`
	`//STDERR  DD SYSOUT=*`
	`//STDOUT  DD SYSOUT=*`
	`//STDENV  DD *`
	` export PATH=/u/c`
	`liuser/python/bin:`
	`$PATH`
	`//STDPARM DD *`
	`SH`
	` export _BPXK_AUT`
	`OCVT=ON;`
	` aws s3 mb s3://DOC-`
	`EXAMPLE-BUCKET2;`
	` cp "//'USER.DATA.FIXE`
	`D'" /tmp/tmpfile;`
	` aws s3 cp /tmp/tmpf`
	`ile s3://DOC-EXAMPLE-`
	`BUCKET2/USER.DATA.F`
	`IXED;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`rm /tmp/tmpfile; aws s3 ls s3://DOC-EXAMPLE-BUCKET2; /*`	
Reichen Sie den Batch-JCL-Job ein.	1. Reichen Sie den JCL-Job ein, den Sie im vorherigen Schritt codiert haben. 2. Überprüfen Sie den Status des Jobs in der System Display and Search Facility (SDSF). Bei Erfolg sollte der Job mit dem Rückgabecode 0 enden. 3. Die Standardausgabe (STDOUT) aus dem Job-Log zeigt die erfolgreiche Bucket-Erstellung, den Upload des Datensatzes und die Liste der Bucket-Inhalte. Ein Beispiel für eine Bildschirmdarstellung finden Sie im Abschnitt Zusätzliche Informationen.	Mainframe z/OS-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich den Datensatz an, der in den S3-Bucket hochgeladen wurde.	1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon S3 S3-Konsole. 2. Navigieren Sie, um die hochgeladene Datei im Test-Bucket zu sehen. 3. Sie können die `USER.DATA.FIXED` Datei weiter verarbeiten oder mithilfe von Analysediensten wie Amazon Redshift analysieren.	Allgemeines AWS

Zugehörige Ressourcen

- AWS CLI Dokumentation zu Version 1
- AWS Mainframe Modernization CLI-Befehlsreferenz
- AWS Mainframe Modernization

Zusätzliche Informationen

USER.DATA.FIXED in der ISPF-Option 3.4 (Hilfsprogramm zur Datensatzliste)

SYSOUT des übermittelten Batch-Jobs

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Mainframe-Daten mithilfe von BMC AMI Cloud Data auf Amazon S3 sichern und archivieren

Erstellt von Santosh Kumar Singh (AWS), Mikhael Liberman (Model9 Mainframe Software), Gilberto Biondo (AWS) und Maggie Li (AWS)

Übersicht

Dieses Muster zeigt, wie Mainframe-Daten direkt in Amazon Simple Storage Service (Amazon S3) gesichert und archiviert werden. Anschließend werden diese Daten mithilfe von BMC AMI Cloud Data (früher bekannt als Model9 Manager) abgerufen und auf dem Mainframe wiederhergestellt. Wenn Sie nach einer Möglichkeit suchen, Ihre Sicherungs- und Archivierungslösung im Rahmen eines Mainframe-Modernisierungsprojekts zu modernisieren oder um Compliance-Anforderungen zu erfüllen, kann dieses Muster Ihnen helfen, diese Ziele zu erreichen.

In der Regel verwenden Unternehmen, die wichtige Geschäftsanwendungen auf Mainframes ausführen, eine virtuelle Bandbibliothek (VTL), um Datenspeicher wie Dateien und Protokolle zu sichern. Diese Methode kann teuer sein, da sie gebührenpflichtiges MIPS verbraucht und auf die auf Bändern außerhalb des Mainframes gespeicherten Daten nicht zugegriffen werden kann. Um diese Probleme zu vermeiden, können Sie BMC AMI Cloud Data verwenden, um betriebliche und historische Mainframe-Daten schnell und kostengünstig direkt zu Amazon S3 zu übertragen. Sie können BMC AMI Cloud Data verwenden, um Daten über TCP/IP zu sichern und zu archivieren und AWS gleichzeitig die Vorteile der IBM z Integrated Information Processor (zIIP) -Engines zu nutzen, um Kosten, Parallelität und Übertragungszeiten zu reduzieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- BMC AMI Cloud Data mit einem gültigen Lizenzschlüssel
- TCP/IP-Konnektivität zwischen dem Mainframe und AWS
- Eine AWS Identity and Access Management (IAM-) Rolle für den Lese-/Schreibzugriff auf einen S3-Bucket
- Zugriff auf das Mainframe-Sicherheitsprodukt (RACF) zur Ausführung von BMC AMI Cloud-Prozessen vorhanden

- Ein BMC AMI Cloud z/OS-Agent (Java Version 8 64-Bit SR5 FP16 oder höher) mit verfügbaren Netzwerkports, Firewallregeln, die den Zugriff auf S3-Buckets ermöglichen, und einem dedizierten z/FS-Dateisystem
- Die Anforderungen für den BMC AMI Cloud-Verwaltungsserver wurden erfüllt

Einschränkungen

- BMC AMI Cloud Data speichert seine Betriebsdaten in einer PostgreSQL-Datenbank, die als Docker-Container auf derselben Amazon Elastic Compute Cloud (Amazon EC2) -Instance wie der Management-Server ausgeführt wird. Amazon Relational Database Service (Amazon RDS) wird derzeit nicht als Backend für BMC AMI Cloud Data unterstützt. Weitere Informationen zu den neuesten Produktupdates finden Sie unter Was ist neu? in der BMC-Dokumentation.
- Mit diesem Muster werden nur z/OS-Mainframe-Daten gesichert und archiviert. BMC AMI Cloud Data sichert und archiviert nur Mainframe-Dateien.
- Dieses Muster konvertiert keine Daten in offene Standardformate wie JSON oder CSV. Verwenden Sie einen zusätzlichen Transformationsdienst wie BMC AMI Cloud Analytics (früher bekannt als Model9 Gravity), um die Daten in offene Standardformate zu konvertieren. Cloud-native Anwendungen und Datenanalysetools können auf die Daten zugreifen, nachdem sie in die Cloud geschrieben wurden.

Produktversionen

- BMC AMI Cloud-Daten Version 2.x

Architektur

Quelltechnologie-Stack

- Mainframe, auf dem z/OS ausgeführt wird
- Mainframe-Dateien wie Datensätze und z/OS UNIX System Services (USS) -Dateien
- Mainframe-Festplatte, z. B. ein Direct-Access-Speichergerät (DASD)
- Mainframe-Band (virtuelle oder physische Bandbibliothek)

Zieltechnologie-Stack

- Amazon S3

- EC2 Amazon-Instanz in einer virtuellen privaten Cloud (VPC)
- AWS Direct Connect
- Amazon Elastic File System (Amazon EFS)

Zielarchitektur

Das folgende Diagramm zeigt eine Referenzarchitektur, in der BMC AMI Cloud Data-Softwareagenten auf einem Mainframe die älteren Datensicherungs- und Archivierungsprozesse ausführen, die die Daten in Amazon S3 speichern.

Das Diagramm zeigt den folgenden Workflow:

1. BMC AMI Cloud Data-Softwareagenten werden auf logischen Mainframe-Partitionen () LPARs ausgeführt. Die Softwareagenten lesen und schreiben Mainframe-Daten von DASD oder Band direkt über TCP/IP in Amazon S3.
2. AWS Direct Connect richtet eine physische, isolierte Verbindung zwischen dem lokalen Netzwerk und ein. AWS Führen Sie zur Erhöhung der Sicherheit zusätzlich ein site-to-site VPN aus, um Daten während der Übertragung AWS Direct Connect zu verschlüsseln.
3. Der S3-Bucket speichert Mainframe-Dateien als Objektspeicherdaten, und BMC AMI Cloud Data-Agents kommunizieren direkt mit den S3-Buckets. Zertifikate werden für die HTTPS-Verschlüsselung der gesamten Kommunikation zwischen dem Agenten und Amazon S3 verwendet. Die Amazon S3 S3-Datenverschlüsselung wird verwendet, um die Daten im Ruhezustand zu verschlüsseln und zu schützen.
4. BMC AMI Cloud Data Management Server werden als Docker-Container auf EC2 Instanzen ausgeführt. Die Instances kommunizieren mit Agenten, die auf Mainframe LPARs - und S3-Buckets laufen.
5. Amazon EFS wird sowohl auf aktiven als auch auf passiven EC2 Instances bereitgestellt, um den NFS-Speicher (Network File System) gemeinsam zu nutzen. Dadurch wird sichergestellt, dass Metadaten, die sich auf eine auf dem Management-Server erstellte Richtlinie beziehen, im Falle eines Failovers nicht verloren gehen. Im Falle eines Failovers durch den aktiven Server kann ohne Datenverlust auf den passiven Server zugegriffen werden. Wenn der passive Server ausfällt, kann ohne Datenverlust auf den aktiven Server zugegriffen werden.

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Elastic File System (Amazon EFS) hilft Ihnen bei der Erstellung und Konfiguration gemeinsam genutzter Dateisysteme in der AWS Cloud.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, mit dem Sie nahezu jede Datenmenge speichern, schützen und abrufen können.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk bereitzustellen. Dieses virtuelle Netzwerk entspricht einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben würden, mit den Vorteilen der Verwendung der skalierbaren Infrastruktur von AWS.
- AWS Direct Connectverbindet Ihr internes Netzwerk über ein Standard-Ethernet-Glasfaserkabel mit einem AWS Direct Connect Standort. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt zu öffentlichen AWS Diensten einrichten und gleichzeitig Internetdienstanbieter in Ihrem Netzwerkpfad umgehen.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.

BMC-Tools

- Der BMC AMI Cloud Management Server ist eine GUI-Anwendung, die als Docker-Container auf einem Amazon Linux Amazon Machine Image (AMI) für Amazon läuft. EC2 Der Management-Server bietet Funktionen zur Verwaltung von BMC AMI Cloud-Aktivitäten wie Berichten, Erstellen und Verwalten von Richtlinien, Ausführen von Archiven und Durchführen von Backups, Rückrufen und Wiederherstellungen.
- Der BMC AMI Cloud-Agent wird auf einem lokalen Mainframe-LPAR ausgeführt, der Dateien mithilfe von TCP/IP direkt in den Objektspeicher liest und schreibt. Eine gestartete Aufgabe wird auf einem Mainframe-LPAR ausgeführt und ist für das Lesen und Schreiben von Sicherungs- und Archivdaten in und von Amazon S3 verantwortlich.

- Das BMC AMI Cloud Mainframe Command Line Interface (M9CLI) bietet Ihnen eine Reihe von Befehlen, mit denen Sie BMC AMI Cloud-Aktionen direkt von TSO/E oder in Batch-Vorgängen ausführen können, ohne vom Verwaltungsserver abhängig zu sein.

Epen

Erstellen Sie einen S3-Bucket und eine IAM-Richtlinie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Erstellen Sie einen S3-Bucket, um die Dateien und Volumes zu speichern, die Sie aus Ihrer Mainframe-Umgebung sichern und archivieren möchten.	Allgemeines AWS
Erstellen Sie eine IAM-Richtlinie.	Alle BMC AMI Cloud-Verwaltungsserver und -Agenten benötigen Zugriff auf den S3-Bucket, den Sie im vorherigen Schritt erstellt haben. Um den erforderlichen Zugriff zu gewähren, erstellen Sie die folgende IAM-Richtlinie: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "Listfolder", "Action": [ "s3:ListBucket", "s3:GetBucketLocation",`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	"s3:ListBucketVersions"
	],
	"Effect": "Allow",
	"Resource": [
	"arn:aws:s3:::<BucketName>"
	]
	},
	{
	"Sid": "Objectaccess",
	"Effect": "Allow",
	"Action": [
	"s3:PutObject",
	"s3:GetObjectAcl",
	"s3:GetObject",
	"s3:DeleteObjectVersion",
	"s3:DeleteObject",
	"s3:PutObjectAcl",
	"s3:GetObjectVersion"
	],
	"Resource": [
	"arn:aws:s3:::<BucketName>/*"
	]
	}	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>] }</pre>	

Holen Sie sich die BMC AMI Cloud-Softwarelizenz und laden Sie die Software herunter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Besorgen Sie sich eine BMC AMI Cloud-Softwarelizenz.	Um einen Softwarelizenzschlüssel zu erhalten, wenden Sie sich an das BMC AMI Cloud-Team. Die Ausgabe des `D M=CPU` z/OS-Befehls ist für die Generierung einer Lizenz erforderlich.	Bauen Sie einen Vorsprung auf
Laden Sie die BMC AMI Cloud-Software und den Lizenzschlüssel herunter.	Besorgen Sie sich die Installationsdateien und den Lizenzschlüssel, indem Sie den Anweisungen in der BMC-Dokumentation folgen.	Administrator der Mainframe-Infrastruktur

Installieren Sie den BMC AMI Cloud-Softwareagenten auf dem Mainframe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den BMC AMI Cloud-Softwareagent.	1. Bevor Sie mit der Installation beginnen, stellen Sie sicher, dass die Mindestanforderungen an Software und Hardware für den Agenten erfüllt sind. 2. Folgen Sie den Anweisungen in der BMC-Dokum	Administrator der Mainframe-Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	entation, um den Agenten zu installieren. 3. Nachdem der Agent auf dem Mainframe-LPAR gestartet wurde, suchen Sie im Spool nach der `ZM91000I MODEL9 BACKUP AGENT INITIALIZED` Meldung. Stellen Sie sicher, dass die Konnektivität zwischen dem Agenten und dem S3-Bucket erfolgreich hergestellt wurde, indem Sie im STDOUT des Agenten nach der `Object store connectivity has been established successfully` Nachricht suchen.	

Richten Sie einen BMC AMI Cloud-Verwaltungsserver auf einer Instanz ein EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Amazon EC2 Linux 2-Instances.	Starten Sie zwei Amazon EC2 Linux 2-Instances in verschiedenen Availability Zones, indem Sie den Anweisungen in Schritt 1: Starten einer Instance in der EC2 Amazon-Dokumentation folgen.	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Die Instance muss die folgenden empfohlenen Hardware- und Softwarea nforderungen erfüllen: • CPU — Mindestens 4 Kerne • RAM — Mindestens 8 GB • Laufwerk — 40 GB • Empfohlene EC2 Instanz — C5.xlarge • Betriebssystem — Linux • Software — Docker, entpacken, VI/Vim • Netzwerkbandbreite — mindestens 1 GB Weitere Informationen finden Sie in der BMC-Dokum entation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Amazon EFS-Dateisystem.	Erstellen Sie ein Amazon EFS-Dateisystem, indem Sie den Anweisungen unter Schritt 1: Erstellen Sie Ihr Amazon EFS-Dateisystem in der Amazon EFS-Dokumentation folgen. Gehen Sie beim Erstellen des Dateisystems wie folgt vor: • Wählen Sie die Standard-Speicherklasse. • Wählen Sie dieselbe VPC aus, mit der Sie Ihre EC2 Instances gestartet haben.	Cloud-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie Docker und konfigurieren Sie den Management-Server.	Connect zu Ihren EC2 Instances her:
	
	Stellen Sie eine Verbindung zu Ihren EC2 Instances her, indem Sie den Anweisungen unter Connect to your Linux Instance in der EC2 Amazon-Dokumentation folgen.
	
	Konfigurieren Sie Ihre EC2 Instances:
	
	Gehen Sie für jede EC2 Instanz wie folgt vor:
	
	1. Führen Sie den folgenden Befehl aus, um Docker zu installieren:
	
	`sudo yum install docker`
	
	2. Um Docker zu starten, führen Sie den folgenden Befehl aus:
	
	`sudo service docker start`
	
	3. Führen Sie den folgenden Befehl aus, um den Status von Docker zu überprüfen:
	
	`sudo service docker status`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	4. Ändern `/etc/selinux` Sie die `config` Datei im Ordner in`SELINUX=permissive` .
	5. Laden Sie die `VerificationScripts.zip` Dateien `model9-v2.x.y_build_build-id-server.zip` und (die Sie zuvor heruntergeladen haben) in einen temporären Ordner in einer der EC2 Instanzen hoch (z. B. in den `/var/tmp` Ordner in Ihrer Instanz).
	6. Um zu dem `tmp` Ordner zu wechseln, führen Sie den folgenden Befehl aus:
	`cd/var/tmp`
	7. Führen Sie den folgenden Befehl aus, um das Überprüfungsskript zu entpacken:
	`unzip VerificationScripts.zip`
	8. Um das Verzeichnis zu ändern, führen Sie den folgenden Befehl aus:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`cd /var/tmp/sysutils/PrereqsScripts`
	9. Führen Sie den folgenden Befehl aus, um das Überprüfungsskript auszuführen:
	`./M9VerifyPrereqs.sh`
	10. Nachdem das Überprüfungsskript zur Eingabe aufgefordert hat, geben Sie die Amazon S3 S3-URL und die Portnummer ein. Geben Sie dann die z/OS-IP/DNS und die Portnummer ein.
	Note
	Das Skript überprüft, ob die EC2 Instance eine Verbindung mit dem S3-Bucket und dem Agenten herstellen kann, die auf dem Mainframe ausgeführt werden. Wenn eine Verbindung hergestellt wurde,	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wird eine Erfolgsmeldung angezeigt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie die Management-Server-Software.	1. Erstellen Sie einen Ordner und einen Unterordner im Stammverzeichnis (z. B. `/data/model9`) in der EC2 Instanz, die Sie zum aktiven Server machen möchten.
	2. Führen Sie die folgenden Befehle aus, um das `amazon-efs-utils` Paket zu installieren und das zuvor erstellte Amazon EFS-Dateisystem zu mounten:
	`sudo yum install -y amazon-efs-utils`
	`sudo mount -t efs -o tls <File System ID>:/ /data/model9`
	3. Um die EC2 `/etc/fstab` Instance-Datei mit einem Eintrag für das Amazon EFS-Datei system zu aktualisieren (sodass Amazon EFS beim EC2 Neustart von Amazon automatisch erneut bereitgestellt wird), führen Sie den folgenden Befehl aus:
	`<Amazon-EFS-file-system-id>:/ /data/`
		Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`model9 efs defaults, _netdev 0 0`
	4. Um den Pfad zu den BMC AMI Cloud-Installation sdateien und den Zielinsta llationsort zu definieren, führen Sie die folgenden Befehle aus, um Variablen zu exportieren:
	`export MODEL9_HOME=/data/model9`
	`export M9INSTALL=/var/tmp`
	Note
	Wir empfehlen , dass Sie diese EXPORT-Befehle zu Ihrem `.bashrc` Skript hinzufügen.
	5. Um das Verzeichnis zu ändern, führen Sie den `cd $MODEL9_HOME` Befehl aus und erstellen Sie dann ein weiteres Unterverzeichnis, indem Sie den `mkdir diag` Befehl ausführen.
	6. Führen Sie den folgenden Befehl aus, um die Installat ionsdatei zu entpacken:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`unzip $M9INSTALL/model9-<v2.x.y>_build_<build-id>-server.zip`
	
	Note
	Ersetze `x.y` (die Version) und `build-id` durch deine Werte.
	
	7. Führen Sie die folgenden Befehle aus, um die Anwendung bereitzustellen:
	
	`docker load -i $MODEL9_HOME/model9-<v2.x.y>_build_<build-id>.docker`
	`docker load -i $MODEL9_HOME/postgres-12.10-x86.docker.gz`
	
	Note
	Ersetzen Sie `v2.x.y` (die Version) und `build-id` durch Ihre Werte.
	
	8. Aktualisieren `$MODEL9_HOME/conf` Sie die	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`model9-local.yml` Datei im Ordner.
	
	Note
	Einige der Parameter haben Standardwerte, andere können bei Bedarf aktualisiert werden. Weitere Informationen finden Sie in den Anweisungen in der `model9-local.yml` Datei.
	
	9. Erstellen Sie eine Datei mit dem Namen **`$MODEL9_HOME/conf`** , und fügen Sie der Datei dann die folgenden Parameter hinzu:
	
	`TZ=America/New_York`
	`EXTRA_JVM_ARGS=-Xmx2048m`
	
	10. Führen Sie den folgenden Befehl aus, um eine Docker-Netzwerkbrücke zu erstellen:
	
	`docker network create -d bridge model9network`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	11. Führen Sie den folgenden Befehl aus, um den PostgreSQL-Datenbankcontainer für BMC AMI Cloud zu starten:
	
	`docker run -p 127.0.0.1:5432:5432 \ -v $MODEL9_HOME/db/data:/var/lib/postgresql/data:z \ --name model9db --restart unless-stopped \ --network model9network \ -e POSTGRES_PASSWORD=model9 -e POSTGRES_DB=model9 -d postgres:12.10`
	
	12. Nachdem der PostgreSQL-Container gestartet wurde, führen Sie den folgenden Befehl aus, um den Anwendungsserver zu starten:
	
	`docker run -d -p 0.0.0.0:443:443 -p 0.0.0.0:80:80 \ --sysctl net.ipv4.tcp_keepalive_time=600 \ --sysctl net.ipv4.tcp_keepalive_intvl=30 \`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`--sysctl net.ipv4.tcp_keepalive_probes=10 \`
	`-v $MODEL9_HOME:/model9:z -h $(hostname)`
	` --restart unless-stopped \`
	`--env-file $MODEL9_HOME/conf/model9.env`
	` \`
	`--network model9network \`
	`--name model9-v2.x.y`
	` model9:<v2.x.y>.<build-id>`	

	Note Ersetzen Sie `v2.x.y` (die Version) und `build-id` durch Ihre Werte.	
	13. Führen Sie den folgenden Befehl aus, um den Integritätsstatus beider Container zu überprüfen: `docker ps -a`	
	14. Um einen Management-Server auf den passiven EC2 Instances zu installieren, wiederholen Sie die Schritte 1—4, 7 und 10—13.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Um Probleme zu beheben, gehen Sie zu den Protokollen, die im Ordner gespeicherte sind. `/data/model9/logs/` Weitere Informationen finden Sie in der BMC-Dokumentation.	

Fügen Sie einen Agenten hinzu und definieren Sie eine Sicherungs- oder Archivierungsrichtlinie auf dem BMC AMI Cloud-Verwaltungsserver

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie einen neuen Agenten hinzu.	Bevor Sie einen neuen Agenten hinzufügen, bestätigen Sie Folgendes: • Ein BMC AMI Cloud-Agent läuft auf dem Mainframe-LPAR und wurde vollständig initialisiert. Identifizieren Sie den Agenten, indem Sie im Spool nach der `ZM91000I MODEL9 BACKUP AGENT INITIALIZED` Initialisierungsnachricht suchen. • Ein Docker-Container für den Management-Server ist vollständig initialisiert und läuft.	Mainframe-Speicheradministrator oder Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie müssen einen Agenten auf dem Management-Server erstellen, bevor Sie Sicherungs- und Archivierungsrichtlinien definieren. Gehen Sie wie folgt vor, um den Agenten zu erstellen: 1. Verwenden Sie einen Webbrowser, um auf den Management-Server zuzugreifen, der auf Ihrem EC2 Amazon-Computer bereitgestellt ist, und melden Sie sich dann mit Ihren Mainframe-Anmeldeinformationen an. 2. Wählen Sie die Registerkarte AGENTEN und dann NEUEN AGENTEN HINZUFÜGEN. 3. Geben Sie unter Name den Namen des Agenten ein. 4. Geben Sie für Hostname/IP-Adresse den Hostnamen oder die IP-Adresse Ihres Mainframes ein. 5. Geben Sie für Port Ihre Portnummer ein. 6. Wählen Sie VERBINDUNG TESTEN. Wenn die Verbindung erfolgreich hergestellt wurde, wird eine Erfolgsmeldung angezeigt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Wählen Sie CREATE (Erstellen) aus. Nachdem der Agent erstellt wurde, wird in einem neuen Fenster, das in der Tabelle angezeigt wird, der Verbindungsstatus für den Objektspeicher und den Mainframe-Agenten angezeigt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Sicherungs- oder Archivierungsrichtlinie.	1. Wählen Sie RICHTLINIEN. 2. Wählen Sie RICHTLINIE ERSTELLEN. 3. Geben Sie auf der Seite NEUE RICHTLINIE ERSTELLEN Ihre Richtlinienspezifikationen ein. **Note** Weitere Informationen zu den verfügbaren Spezifikationen finden Sie in der BMC-Dokumentation unter Neue Richtlinie erstellen. 4. Wählen Sie Finish (Abschließen). 5. Die neue Richtlinie ist jetzt als Tabelle aufgeführt. Um diese Tabelle zu sehen, wählen Sie die Registerkarte RICHTLINIEN.	Mainframe-Speicheradministrator oder Entwickler

Führen Sie die Sicherungs- oder Archivierungsrichtlinie vom Management-Server aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Sicherungs- oder Archivierungsrichtlinie aus.	Führen Sie die Datensicherungs- oder Archivierungsrichtlinie, die Sie zuvor	Mainframe-Speicheradministrator oder Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	auf dem Management-Server erstellt haben, entweder manuell oder automatisch (nach einem Zeitplan) aus. Gehen Sie wie folgt vor, um die Richtlinie manuell auszuführen: 1. Wählen Sie im Navigatio nsmenü die Registerkarte RICHTLINIEN. 2. Wählen Sie auf der rechten Seite der Tabelle für die Richtlinie, die Sie ausführen möchten, das Dreipunkt menü aus. 3. Wählen Sie Jetzt ausführen aus. 4. Wählen Sie im Popup-Bestätigungsfenster JA, RICHTLINIE JETZT AUSFÜHREN aus. 5. Nachdem die Richtlini e ausgeführt wurde, überprüfen Sie den Ausführungsstatus im Abschnitt Richtlinienaktivit ät. 6. Wählen Sie für die Richtlini e, die ausgeführt wurde, das Dreipunktmenü und dann Ausführungsprotoko ll anzeigen aus, um die Protokolle anzuzeigen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Um zu überprüfen, ob das Backup erstellt wurde, überprüfen Sie den S3-Bucket.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Sicherungs- oder Archivierungsrichtlinie wieder her.	1. Wählen Sie im Navigationsmenü die Registerkarte RICHTLINIEN aus. 2. Wählen Sie die Richtlinie aus, auf der Ihr Wiederherstellungsprozess ausgeführt werden soll. Dadurch werden alle Sicherungs- oder Archivierungsaktivitäten aufgelistet, die in der Vergangenheit für diese bestimmte Richtlinie ausgeführt wurden. 3. Um die Backups auszuwählen, die Sie wiederherstellen möchten, wählen Sie die Spalte Datum/Uhrzeit aus. Der `file/Volume/Storage` Gruppenname zeigt die Ausführungsdetails der Richtlinie. 4. Wählen Sie auf der rechten Seite der Tabelle das Dreipunktmenü und dann RESTORE aus. 5. Geben Sie im Popup-Fenster Ihren Zielnamen, Ihr Volume und Ihre Speichergruppe ein und wählen Sie dann WIEDERHERSTELLEN. 6. Geben Sie Ihre Mainframe-Anmeldeinformationen ein	Mainframe-Speicheradministrator oder Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und wählen Sie dann erneut WIEDERHERSTELLEN. 7. Um zu überprüfen, ob die Wiederherstellung erfolgrei ch war, überprüfen Sie die Protokolle oder den Mainframe.	

Führen Sie die Sicherungs- oder Archivierungsrichtlinie vom Mainframe aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Sicherungs- oder Archivierungsrichtlinie mithilfe von M9CLI aus.	Verwenden Sie die M9CLI, um Sicherungs- und Wiederher stellungsprozesse von TSO/E, REXX oder so aus durchzufü hren, JCLs ohne Regeln auf dem BMC AMI Cloud-Ver waltungsserver einzurichten. Verwenden von TSO/E: Wenn Sie TSO/E verwenden , stellen Sie sicher, dass dies mit verknüpft ist. `M9CLI REXX TSO` Verwenden Sie den Befehl, um einen Datensatz über TSO/E zu sichern. `TSO M9CLI BACKDSN <DSNAME>` **Note** Weitere Informationen zu M9CLI-Befehlen finden Sie in der CLI-	Mainframe-Speicheradministr ator oder Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Referenz in der BMC-Dokumentation.
	
	JCLsVerwenden von:
	
	Um die Sicherungs- und Archivierungsrichtlinie mithilfe auszuführen JCLs, führen Sie den `M9CLI` Befehl aus.
	
	Verwenden von Batch-Operationen:
	
	Das folgende Beispiel zeigt Ihnen, wie Sie einen Datensatz archivieren, indem Sie den `M9CLI` Befehl im Batch ausführen:
	
	`//JOBNAME JOB …`
	`//M9CLI EXEC PGM=IKJEFT01`
	`//STEPLIB DD DISP=SHR, DSN=<MODEL9 LOADLIB>`
	`//SYSEXEC DD DISP=SHR, DSN=<MODEL9 EXEC LIB>`
	`//SYSTSPRT DD SYSOUT=*`
	`//SYSPRINT DD SYSOUT=*`
	`//SYSTSIN DD TSO M9CLI`
	` ARCHIVE`
	` M9CLI ARCHIVE <DSNNAME`
	` OR DSN PATTERN>`
	`/`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Sicherungs- oder Archivierungsrichtlinie im JCL-Batch aus.	BMC AMI Cloud bietet eine JCL-Beispielroutine namens M9SAPIJ. Sie können M9SAPIJ so anpassen, dass eine bestimmte Richtlinie ausgeführt wird, die auf dem Management-Server mit einer JCL erstellt wurde. Dieser Job kann auch Teil eines Batch-Schedulers sein, mit dem Sicherungs- und Wiederherstellungsprozesse automatisch ausgeführt werden. Der Batch-Job erwartet die folgenden obligatorischen Werte: • IP-Adresse/Hostname des Verwaltungsservers • Port-Nummer • Richtlinien-ID oder Richtlinienname (der auf dem Management-Server erstellt wird) **Note** Sie können auch andere Werte ändern, indem Sie den Anweisungen im Beispieljob folgen.	Mainframe-Speicheradministrator oder Entwickler

Zugehörige Ressourcen

- Mainframe-Modernisierung mit AWS (AWS-Dokumentation)
- Wie Cloud Backup für Mainframes mit Model9 und AWS Kosten senkt (AWS-Partnernetzwerk-Blog)
- So aktivieren Sie Mainframe-Datenanalysen auf AWS mithilfe von Model9 (AWS-Partnernetzwerk-Blog)
- Empfehlungen zur Ausfallsicherheit von AWS Direct Connect (AWS-Dokumentation)
- BMC AMI Cloud-Dokumentation (BMC-Webseite)

Erstellen Sie COBOL Db2-Programme mit und AWS Mainframe ModernizationAWS CodeBuild

Erstellt von Luis Gustavo Dantas (AWS) und Eduardo Zimelewicz (AWS)

Übersicht

Dieses Muster erklärt, wie ein einfaches AWS CodeBuild Projekt zum Vorkompilieren und Binden von COBOL Db2-Programmen mithilfe der Replatform-Tools erstellt wird. AWS Mainframe Modernization Dies ermöglicht die Bereitstellung und Ausführung dieser Programme in der Replatform-Laufzeitumgebung. AWS Mainframe Modernization

COBOL, eine geschäftsorientierte Programmiersprache, unterstützt aufgrund ihrer Zuverlässigkeit und Lesbarkeit viele kritische Anwendungen. IBM Db2, ein relationales Datenbankmanagementsystem, verwaltet große Datenmengen effizient und lässt sich über SQL in COBOL-Programme integrieren. Zusammen bilden COBOL und Db2 trotz des Aufkommens neuerer Technologien das Rückgrat geschäftskritischer Abläufe in Branchen wie Finanzen und Behörden.

Die Migration von COBOL- und Db2-Komponenten aus der Mainframe-Umgebung auf andere Plattformen führt zu Herausforderungen wie Plattformkompatibilität, Integrationskomplexität, Datenmigration und Leistungsoptimierung. Die Migration dieser kritischen Komponenten erfordert sorgfältige Planung, technisches Fachwissen und Ressourcen, um eine reibungslose Migration zu gewährleisten und gleichzeitig Zuverlässigkeit und Funktionalität zu gewährleisten.

Der AWS Mainframe Modernization Service bietet Tools und Ressourcen zur Neuplattformierung von Mainframe-Anwendungen und Datenbanken, sodass sie auf AWS Infrastrukturen wie Amazon Elastic Compute Cloud (Amazon EC2) -Instances ausgeführt werden können. Dies beinhaltet die Verlagerung von Mainframe-Workloads in die Cloud ohne größere Codeänderungen.

Der Db2-Vorkompilierungs- und Bindungsprozess ist für die Optimierung der Leistung und Zuverlässigkeit von Datenbankanwendungen unerlässlich. Durch die Vorkompilierung werden eingebettete SQL-Anweisungen in ausführbaren Code umgewandelt, wodurch der Laufzeitaufwand reduziert und die Effizienz gesteigert wird. Der Bind-Prozess verknüpft den vorkompilierten Code mit Datenbankstrukturen und erleichtert so die Zugriffspfade und die Abfrageoptimierung. Dieser Prozess gewährleistet die Datenintegrität, verbessert die Reaktionsfähigkeit von Anwendungen und schützt vor Sicherheitslücken. Ordnungsgemäß vorkompilierte und gebundene Anwendungen minimieren den Ressourcenverbrauch, verbessern die Skalierbarkeit und verringern die Risiken von SQL-Injection-Angriffen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein AWS-Konto Konsolenzugriff auf Administrationsebene.
- Ein IBM Db2-Datenbanksystem, wie IBM Db2 für z/OS oder Db2 für Linux, Unix und Windows (LUW).
- Die IBM Data Server Client-Software, die von der IBM-Website heruntergeladen werden kann. Weitere Informationen finden Sie unter IBM Data Server Client- und Data Server-Treibertypen.
- Ein COBOL Db2-Programm, das kompiliert und gebunden werden soll. Alternativ bietet dieses Muster ein grundlegendes Beispielprogramm, das Sie verwenden können.
- Eine virtuelle private Cloud (VPC) AWS mit einem privaten Netzwerk. Informationen zum Erstellen einer VPC finden Sie in der Dokumentation zu Amazon Virtual Private Cloud (Amazon VPC).
- Ein Quellcodeverwaltungs-Repository wie GitHub oder. GitLab

Einschränkungen

- AWS CodeBuild Kontingente finden Sie unter Kontingente für AWS CodeBuild.
- Einige AWS-Services sind nicht in allen verfügbar AWS-Regionen. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie auf der Seite Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Architektur

Quelltechnologie-Stack

Der Quellstapel umfasst:

- COBOL-Programme, die eine Db2-Datenbank zum Speichern von Daten verwenden
- IBM COBOL-Compiler und Db2 für z/OS-Precompiler
- Andere Teile des Mainframe-Setups, wie das Dateisystem, der Transaktionsmanager und der Spool

Zieltechnologie-Stack

Der Ansatz dieses Musters funktioniert bei zwei Optionen: beim Verschieben von Daten von Db2 für z/OS nach Db2 für LUW oder beim Verbleiben auf Db2 for z/OS. Die Zielarchitektur umfasst:

- COBOL-Programme, die eine Db2-Datenbank zum Speichern von Daten verwenden
- AWS Mainframe Modernization Kompilierungstools auf eine neue Plattform
- AWS CodeBuild als Infrastruktur für die Erstellung der Anwendung
- Andere AWS Cloud Ressourcen wie Amazon Linux

Zielarchitektur

Das Diagramm veranschaulicht folgende Vorgänge:

1. Der Benutzer lädt seinen Code in ein Quellcodeverwaltungs-Repository wie oder hoch. GitHub GitLab
2. AWS CodePipeline bemerkt die Änderung und ruft den Code aus dem Repository ab.
3. CodePipeline startet AWS CodeBuild und sendet den Code.
4. CodeBuild folgt den Anweisungen in der `buildspec.yml` Vorlage (im Abschnitt Zusätzliche Informationen), um:
   a. Holen Sie sich den IBM Data Server Client aus einem Amazon Simple Storage Service (Amazon S3) -Bucket.
   b. Installieren und richten Sie den IBM Data Server Client ein.
   c. Rufen Sie die Db2-Anmeldeinformationen von ab AWS Secrets Manager.
   d. Connect zum Db2-Server her.
   e. Das COBOL-Programm vorkompilieren, kompilieren und binden.
   f. Speichern Sie die fertigen Produkte zur AWS CodeDeploy Verwendung in einem S3-Bucket.
5. CodePipeline beginnt CodeDeploy.
6. CodeDeploy koordiniert seine Agenten, die bereits in den Laufzeitumgebungen installiert sind. Die Agenten rufen die Anwendung von Amazon S3 ab und installieren sie gemäß den Anweisungen in`appspec.yml`.

Um die Dinge einfach zu halten und sich auf den Build zu konzentrieren, decken die Anweisungen in diesem Muster die Schritte 1 bis 4 ab, beinhalten jedoch nicht die Bereitstellung des COBOL Db2-Programms.

Automatisierung und Skalierung

Der Einfachheit halber beschreibt dieses Muster, wie Ressourcen manuell bereitgestellt werden. Es stehen jedoch zahlreiche Automatisierungsoptionen wie, und HashiCorp Terraform zur Verfügung AWS CloudFormation AWS Cloud Development Kit (AWS CDK), mit denen diese Aufgaben automatisiert werden können. Weitere Informationen finden Sie in der Dokumentation AWS CloudFormationund AWS CDK.

Tools

AWS-Services

- AWS CodeBuildist ein vollständig verwalteter Build-Service, der Sie beim Kompilieren von Quellcode, beim Ausführen von Komponententests und beim Erstellen von Artefakten unterstützt, die sofort einsatzbereit sind.
- AWS CodeDeployautomatisiert Bereitstellungen für Amazon EC2 - oder lokale Instances, AWS Lambda Funktionen oder Amazon Elastic Container Service (Amazon ECS) -Services.
- AWS CodePipelinehilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.
- AWS Mainframe Modernizationstellt Tools und Ressourcen bereit, die Sie bei der Planung und Implementierung der Migration und Modernisierung von Mainframes zu AWS verwalteten Runtime-Umgebungen unterstützen.

Andere Tools

- Amazon ECR-Image für AWS Mainframe Modernization Replatform-Tools. Um eine COBOL-Anwendung zu kompilieren, müssen Sie sie CodeBuild mithilfe eines Amazon Elastic Container Registry (Amazon ECR) -Images initiieren, das die AWS Mainframe Modernization Replatform-Tools enthält:

  ```
  673918848628.dkr.ecr.<your-region>.amazonaws.com/m2-enterprise-build-tools:9.0.7.R1
  ```

  Weitere Informationen zum verfügbaren ECR-Image finden Sie im Tutorial im Benutzerhandbuch.AWS Mainframe Modernization

- Die IBM Data Server Client-Software ist für die Vorkompilierung und Einbindung von COBOL Db2-Programmen unverzichtbar. CodeBuild Sie fungiert als Brücke zwischen dem COBOL-Compiler und Db2.

Bewährte Methoden

- Nicht jedes COBOL-Programm stützt sich auf Db2 als Datenpersistenzschicht. Stellen Sie sicher, dass Kompilierungsanweisungen für den Zugriff auf Db2 nur auf COBOL-Programme angewendet werden, die speziell für die Interaktion mit Db2 entwickelt wurden. Implementieren Sie eine Logik zur Unterscheidung zwischen COBOL-Db2-Programmen und COBOL-Programmen, die Db2 nicht verwenden.
- Es wird empfohlen, das Kompilieren von Programmen zu vermeiden, die nicht geändert wurden. Implementieren Sie einen Prozess, um zu ermitteln, welche Programme kompiliert werden müssen.

Epen

Erstellen Sie die Cloud-Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket, um den IBM Data Server Client und die Pipeline-Artefakte zu hosten.	Sie müssen einen S3-Bucket einrichten, um (a) den IBM Data Server Client hochzuladen, (b) Ihren Code aus dem Repository zu speichern und (c) die Ergebnisse des Build-Prozesses zu speichern. 1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon S3 S3-Konsole. 2. Wählen Sie einen vorhandenen S3-Bucket oder erstellen Sie einen neuen Bucket. Notieren	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie sich den Amazon-Ressourcennamen (ARN) des Buckets für die future Verwendung. Informationen zum Erstellen eines S3-Buckets finden Sie in der Amazon S3 S3-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den IBM Data Server Client in den S3-Bucket hoch.	1. Wählen Sie auf der Amazon S3 S3-Konsole den Bucket aus, um ihn zu öffnen. 2. Wählen Sie Ordner erstellen, geben Sie seinen Namen als Client an und wählen Sie dann Ordner erstellen. 3. Öffnen Sie den Client-Ordner und wählen Sie Hochladen, Dateien hinzufügen. 4. Wählen Sie die IBM Data Server Client-Datei aus, die Sie zuvor von der IBM Website in Ihr lokales Dateisystem heruntergeladen haben. Der Dateiname sollte `v11.5.8_linuxx64_client.tar.gz` oder ähnelnv`11.5.9_linuxx64_client.tar.gz` . 5. Wählen Sie Öffnen, Hochladen und warten Sie, bis der Upload abgeschlossen ist. 6. Wählen Sie auf der Registerkarte Dateien und Ordner den Data Server	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Client aus und notieren Sie sich dessen S3-URI.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein AWS Secrets Manager Geheimnis für Ihre Db2-Anmeldeinformationen.	Um ein Geheimnis zu erstellen, um Ihre DB2 Anmeldeinformationen sicher zu speichern: 1. Wählen Sie in der Secrets Manager Manager-Konsole die Option Neues Geheimnis speichern aus. 2. Wählen Sie im Bereich Geheimtyp auswählen die Optionen Anderer Geheimtyp und Klartext aus. 3. Geben Sie in das Feld Klartext Ihre Db2-Anmeldeinformationen ein, indem Sie die folgende JSON-Struktur verwenden. `{ "username": "<your-db2-user-name>", "password": "<your-db2-password>", "db2node": "db2dev", "db2host": "<your-db2-hostname-or-IP>", "db2port": <your-db2-port>, "db2name": "<your-db2-location>",`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"qualifier": "<your-db2-qualifier>"
	}</pre>
	4. Wählen Sie Weiter und geben Sie dem Geheimnis einen Namen wie. `dev-db2-cred`
	5. Wählen Sie Weiter, Weiter und Speichern.
	
	Weitere Informationen zum Erstellen von Geheimnissen finden Sie in der Secrets Manager Manager-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass auf Db2 vom VPC-Subnetz aus zugegriffen werden kann.	AWS CodeBuild benötigt eine Verbindung zum Db2-Server, damit der Data Server Client Vorkompilierungs- und Bindungsvorgänge durchführ en kann. Stellen Sie sicher, dass der Db2-Server über eine sichere Verbindung erreicht werden CodeBuild kann. 1. Öffnen Sie die Amazon VPC-Konsole. 2. Wählen Sie im Navigatio nsbereich Subnetze aus und notieren Sie sich die IDs und IPv4 CIDRsdie privaten Subnetze, in denen sie CodeBuild funktionieren sollen. 3. Aktualisieren Sie die aktuellen Einstellungen für die Netzwerkzugriffsko ntrolle für Ihr Db2-System, indem Sie eine Regel für eingehenden Datenverk ehr einführen. Diese Regel sollte den benutzerd efinierten TCP-Zugriff auf den Db2-Port ausschlie ßlich von dem Subnetz aus ermöglichen CIDRs , das Ihrem Projekt zugeordnet ist. CodeBuild	Netzwerkadministrator, General AWS

Erstellen Sie die Anwendungsartefakte

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das COBOL Db2-Asset.	1. Wenn Sie ein einfaches COBOL Db2-Beispiel verwenden möchten, speichern Sie den folgenden Quellcode unter. `CDB2SMP.cbl` Sie können dieses Beispiel auch durch ein Programm ersetzen, das Sie bereits besitzen. `IDENTIFICATION DIVISION. PROGRAM-ID. CDB2SMP. DATA DIVISION. WORKING-STORAGE SECTION. 01 WS-NAME PIC X(100). PROCEDURE DIVISION. EXEC SQL SELECT NAME INTO :WS-NAME FROM SYSIBM.SYSTABLES END-EXEC GOBACK.` 2. Übernehmen Sie die Änderungen und übertragen Sie die Datei in Ihr Repository.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Datei `buildspec.yml` .	1. Generieren Sie die `buildspec.yml` Datei anhand des Beispiels, das im Abschnitt Zusätzliche Informationen bereitgestellt wird. 2. Übernehmen Sie die Änderungen und übertragen Sie die Datei in Ihr Repository.	AWS DevOps
Connect dein Repository mit CodePipeline.	1. Öffnen Sie die AWS Developer Tools-Konsole. 2. Wählen Sie im Navigationsbereich Einstellungen, Verbindungen aus. 3. Folgen Sie den Anweisungen in der Dokumentation der Developer Tools-Konsole für den Quellanbieter Ihrer Wahl. Sie benötigen den Amazon-Ressourcennamen (ARN) für die Verbindung, wenn Sie CodePipeline in einem späteren Schritt die AWS Identity and Access Management (IAM) -Richtlinie für erstellen.	AWS DevOps

Konfigurieren von Berechtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Richtlinie für CodeBuild.	Das CodeBuild Projekt benötigt Zugriff auf einige Ressourcen, darunter Secrets Manager und Amazon S3. So richten Sie die erforderlichen Berechtigungen ein: 1. Öffnen Sie die IAM-Konsole. 2. Wählen Sie im Navigationsbereich Policies, Create Policy und dann den CodeBuild Service aus. 3. Wechseln Sie zur Formatierung von Visual zu JSON und kopieren Sie die CodeBuild Richtlinie, die im Abschnitt Zusätzliche Informationen bereitgestellt wird, in das Feld Richtlinien-Editor. 4. Benennen Sie diese Richtlinie und speichern Sie sie, future Sie im nächsten Schritt später darauf zurückgreifen können. Weitere Informationen zum Erstellen von IAM-Richtlinien finden Sie in der IAM-Dokumentation.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle für CodeBuild.	Um die Sicherheitsrichtlinien für verfügbar zu machen CodeBuild, müssen Sie eine IAM-Rolle konfigurieren. Um diese Rolle zu erstellen: 1. Wählen Sie in der IAM-Konsole im Navigatio nsbereich Rollen, Rolle erstellen aus. 3. Behalten Sie für den Entitätstyp Vertrauenswürdig die AWS-ServiceStandarde instellung bei. 4. Wählen Sie unter Anwendungsfall den CodeBuild Dienst aus und klicken Sie dann auf Weiter. 4. Suchen Sie in der Liste der verfügbaren IAM-Richt linien nach der Richtlinie, für die Sie sie erstellt haben CodeBuild, und klicken Sie dann auf Weiter, um sie der Rolle hinzuzufügen. 5. Geben Sie einen Namen für die Rolle an und wählen Sie Rolle erstellen aus, um sie zur future in zu speichern CodeBuild.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen zum Erstellen einer IAM-Rolle für eine AWS-Service finden Sie in der IAM-Dokumentation.	
Erstellen Sie eine IAM-Richtlinie für CodePipeline.	Die AWS CodePipeline Pipeline benötigt Zugriff auf einige Ressourcen, einschließlich Ihres Code-Repositorys und Amazon S3. Wiederholen Sie die zuvor beschriebenen Schritte CodeBuild , um eine IAM-Richtlinie für zu erstellen CodePipeline (wählen Sie in Schritt 2 CodePipelinestatt CodeBuild).	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine IAM-Rolle für CodePipeline.	Um die Sicherheitsrichtlinien für verfügbar zu machen CodePipeline, müssen Sie eine IAM-Rolle konfigurieren.
	
	Um diese Rolle zu erstellen:
	
	1. Wählen Sie in der IAM-Konsole Rollen, Rolle erstellen aus.
	2. Für Trusted entity type (Vertrauenstyp der Entität), wählen Sie Custom trust policy (Benutzerdefinierte Vertrauensrichtlinie).
	
	Eine Richtlinie mit einem leeren `Principal` Element wird angezeigt.
	3. Fügen Sie in der `Principal` Zeile zwischen den geschweiften Klammern Folgendes hinzu:
	
	`"Service": "codepipeline.amazonaws.com"`
	
	Die Vertrauensrichtlinie wird wie folgt aussehen:
	
	`{ "Version": "2012-10-17", "Statement": [ {`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"Sid": "Statement1", "Effect": "Allow", "Principal": { "Service": "codepipeline.amazonaws.com" }, "Action": "sts:AssumeRole" }] }</pre> 4. Wählen Sie Weiter aus. 5. Suchen Sie in der Liste der verfügbaren IAM-Richtlinien nach der Richtlinie, für die Sie sie erstellt haben CodePipeline, und klicken Sie dann auf Weiter, um sie der Rolle hinzuzufügen. 6. Geben Sie einen Namen für die Rolle an und wählen Sie Rolle erstellen aus, um sie zur future in zu speichern CodePipeline.	

Kompilieren und binden Sie das COBOL Db2-Programm

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CodePipeline Pipeline und ein CodeBuild Projekt.	So erstellen Sie eine CodePipeline Pipeline und das CodeBuild Projekt, das	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	das COBOL Db2-Programm kompiliert und bindet: 1. Öffnen Sie die CodePipeline Konsole und wählen Sie „Pipeline erstellen“, „Benutzerdefinierte Pipeline erstellen“. 2. Geben Sie einen Namen für die Pipeline an. 3. Wählen Sie für Service role die Option Existing service role und geben Sie den ARN für die IAM-Rolle an, für CodePipeline die Sie erstellt haben. 4. Erweitern Sie Erweiterte Einstellungen, wählen Sie Benutzerdefinierter Speicherort, wählen Sie den S3-Bucket aus, den Sie zuvor erstellt haben, und klicken Sie dann auf Weiter. 5. Wählen Sie unter Quellanbieter Ihren externen Quellanbieter aus und geben Sie die relevanten Informationen für den Anbieter ein:. a. Wählen Sie unter Verbindung die Verbindung aus, die für den Quellanbieter erstellt wurde.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	b. Wählen Sie unter Repository-Name Ihr Repository aus. c. Wählen Sie unter Standardzweig den Zweig aus, in dem Ihr COBOL-Pro gramm gespeichert ist, und `buildspec.yml` . d. Wählen Sie Weiter aus. 6. Wählen Sie für Buildanbi eter die Option Andere Buildanbieter, AWS CodeBuildaus. 7. Wählen Sie als Projektna me die Option Projekt erstellen aus. In der Konsole wird ein CodeBuild Fenster angezeigt, in dem Sie ein Build-Projekt erstellen können. In diesem Fenster: a. Geben Sie einen Namen für das Projekt ein. b. Wählen Sie unter Environment image (Umgebungsabbild) die Option Custom image (Benutzerdefiniertes Abbild) aus. c. Wählen Sie als Umgebungstyp die	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Option Linux Container aus. d. Wählen Sie für ECR-Konto die Option Anderes ECR-Konto aus. e. Geben Sie für den Amazon ECR-Repository-URI Folgendes ein:`673918848628.dkr.ecr.<your-region>.amazonaws.com/m2-enterprise-build-tools:8.0.9.R1` . f. Wählen Sie für Servicerolle die Option Bestehende Servicerolle und wählen Sie die Rolle aus, für CodeBuild die Sie erstellt haben. g. Erweitern Sie den Abschnitt Zusätzliche Konfiguration und wählen Sie dann die VPC, die privaten Subnetze und die Sicherheitsgruppe für dieses Projekt aus. h. Wählen Sie im Abschnitt Buildspec die Option Use a buildspec-Datei aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	i. Wählen Sie am Ende des Fensters Weiter zu. CodePipeline Das CodeBuild Fenster wird geschlossen, sodass Sie zur CodePipeline Konsole zurückkehren können. 8. Zurück in der CodePipeline Konsole wählen Sie Weiter. 9. Wählen Sie im Bereich Bereitstellungsphase hinzufügen die Option Bereitstellungsphase überspringen aus und bestätigen Sie. 10. Überprüfen Sie die Pipeline-Parameter und wählen Sie dann Pipeline erstellen aus.	
Überprüfen Sie die Ausgabe.	Überprüfen Sie den Erfolg des Builds, indem Sie die CodePipeline Build-Logs überprüfen.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Ergebnisse in Db2.	Überprüfen Sie die Paketversion in der SYSPLAN-Tabelle.
	`select CAST(NAME AS VARCHAR(10)) as name, VALIDATE, LAST_BIND_TIME, LASTUSED, CAST(PKGVERSION AS VARCHAR(10)) as PKGVERSION from SYSIBM.SYSPLAN where NAME = 'CDB2SMP' order by LAST_BIND_TIME desc`
	Die Version muss mit der CodeBuild Build-ID übereinstimmen, die `CDB2SMP` in unserem Beispiel lautet:
	`NAME VALIDATE LAST_BIND_TIME LASTUSED PKGVERSION ---------- -------- ------------------ -------- ---------- ---------- CDB2SMP B 2024-05-18-11.53.11.503738 01/01/0001 19`	

Fehlerbehebung

Problem	Lösung
Gelegentlich wechselt die AWS Konsole zwischen Regionen, wenn Sie zwischen Diensten wechseln.	Stellen Sie sicher, dass Sie bei AWS-Region jedem Wechsel zwischen Diensten die Auswahl überprüfen. Der AWS-Region Selektor befindet sich in der oberen rechten Ecke des Konsolenfensters.
Es kann schwierig sein, Db2-Konnektivitäts probleme anhand von zu identifizieren. CodeBuild	Um Verbindungsprobleme zu beheben, fügen Sie der `buildspec.yml` Datei den folgenden DB2 Verbindungsbefehl hinzu. Dieser Zusatz hilft Ihnen beim Debuggen und Beheben von Verbindungsproblemen. `db2 connect to $DB_NAME user $DB2USER using $DB2PASS`
Gelegentlich wird im Rollenbereich der IAM-Konsole die von Ihnen erstellte IAM-Richtlinie nicht sofort angezeigt.	Wenn Sie auf eine Verzögerung stoßen, aktualisieren Sie den Bildschirm, um die neuesten Informationen anzuzeigen.

Zugehörige Ressourcen

IBM-Dokumentation

- IBM Data Server Client- und Treibertypen
- Laden Sie IBM Data Server Client und Treibertypen herunter

AWS Dokumentation

- Amazon S3 S3-Benutzerhandbuch
- AWS CodeBuild Benutzerhandbuch
- AWS Mainframe Modernization Benutzerhandbuch

- AWS Secrets Manager Benutzerhandbuch
- AWS CodePipeline Benutzerhandbuch
- AWS CodeDeploy Benutzerhandbuch

Zusätzliche Informationen

CodeBuild Richtlinie

Ersetzen Sie die Platzhalter <RegionID><AccountID>,, <SubnetARN><BucketARN>, und <DB2CredSecretARN> durch Ihre Werte.

```
{"Version": "2012-10-17",
    "Statement": [
        {"Action": "ecr:GetAuthorizationToken", "Effect": "Allow", "Resource": "*" },
        {"Action": ["ecr:GetDownloadUrlForLayer", "ecr:BatchGetImage",
                    "ecr:BatchCheckLayerAvailability"],
         "Effect": "Allow",
         "Resource": "arn:aws:ecr:*:673918848628:repository/m2-enterprise-build-
tools"},
        {"Action": "s3:PutObject", "Effect": "Allow", "Resource": "arn:aws:s3:::aws-m2-
repo-*/*"},
        {"Action": ["logs:PutLogEvents", "logs:CreateLogStream",
 "logs:CreateLogGroup"],
         "Effect": "Allow", "Resource": "arn:aws:logs:<RegionId>:<AccountId>:*"},
        {"Action": ["ec2:DescribeVpcs", "ec2:DescribeSubnets",
                    "ec2:DescribeSecurityGroups", "ec2:DescribeNetworkInterfaces",
                    "ec2:DescribeDhcpOptions", "ec2:DeleteNetworkInterface",
                    "ec2:CreateNetworkInterface"],
         "Effect": "Allow", "Resource": "*"},
        {"Action": "ec2:CreateNetworkInterfacePermission",
         "Effect": "Allow", "Resource": ["<SubnetARN>"]},
        {"Action": "s3:*", "Effect": "Allow", "Resource": ["<BucketARN>/
*","<BucketARN>"]},
        {"Action": "secretsmanager:GetSecretValue",
         "Effect": "Allow", "Resource": "<DB2CredSecretARN>"}
    ]
}
```

CodePipeline Richtlinie

Ersetzen Sie die Platzhalter <BucketARN> und <ConnectionARN> durch Ihre Werte.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {"Action": ["s3:List*", "s3:GetObjectVersion", "s3:GetObject",
 "s3:GetBucketVersioning" ],
        "Effect": "Allow",
        "Resource": ["<BucketARN>/*", "<BucketARN>"]},
        {"Action": ["codebuild:StartBuild", "codebuild:BatchGetBuilds"],
         "Effect": "Allow", "Resource": "*"},
        {"Action": ["codestar-connections:UseConnection"],
         "Effect": "Allow", "Resource": "<ConnectionARN>"}
        ]
}
```

buildspec.yml

Ersetzen Sie den <your-bucket-name> Platzhalter durch Ihren tatsächlichen S3-Bucket-Namen.

```
version: 0.2
phases:
  pre_build:
    commands:
      - /var/microfocuslicensing/bin/mfcesd -no > /var/microfocuslicensing/logs/
mfcesd_startup.log 2>&1 &
      - |
        mkdir $CODEBUILD_SRC_DIR/db2client
        aws s3 cp s3://<your-bucket-name>/v11.5.8_linuxx64_client.tar.gz
 $CODEBUILD_SRC_DIR/db2client/ >> /dev/null 2>&1
        tar -xf $CODEBUILD_SRC_DIR/db2client/v11.5.8_linuxx64_client.tar.gz -C
 $CODEBUILD_SRC_DIR/db2client/
        cd $CODEBUILD_SRC_DIR/db2client/
        ./client/db2_install -f sysreq -y -b /opt/ibm/db2/V11.5 >> /dev/null 2>&1

        useradd db2cli
        /opt/ibm/db2/V11.5/instance/db2icrt -s client -u db2cli db2cli
        DB2CRED=$(aws secretsmanager get-secret-value --secret-id dev-db2-cred | jq -r
 '.SecretString | fromjson')
        read -r DB2USER DB2PASS DB_NODE DB_HOST DB_PORT DB_NAME DB_QUAL <<<$(echo
 $DB2CRED | jq -r
 '.username, .password, .db2node, .db2host, .db2port, .db2name, .qualifier')
        . /home/db2cli/sqllib/db2profile
        db2 catalog tcpip node $DB_NODE remote $DB_HOST server $DB_PORT
        db2 catalog db $DB_NAME as $DB_NAME at node $DB_NODE authentication server
```

```
  build:
    commands:
      - |
        revision=$CODEBUILD_SRC_DIR/loadlib
        mkdir -p $revision; cd $revision
        . /opt/microfocus/EnterpriseDeveloper/bin/cobsetenv
        cob -zU $CODEBUILD_SRC_DIR/CDB2SMP.cbl -C "DB2(DB==${DB_NAME} PASS==${DB2USER}.
${DB2PASS} VERSION==${CODEBUILD_BUILD_NUMBER} COLLECTION==DB2AWSDB"
artifacts:
  files:
    - "**/*"
  base-directory: $revision
```

Erstellen Sie ein Micro Focus Enterprise Server PAC mit Amazon EC2 Auto Scaling und Systems Manager

Erstellt von Kevin Yung (AWS), Peter Woods, Abraham Rondon (Micro Focus) und Krithika Palani Selvam (AWS)

Übersicht

Dieses Muster führt eine skalierbare Architektur für Mainframe-Anwendungen ein, die Micro Focus Enterprise Server im Scale-Out Performance and Availability Cluster (PAC) und eine Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppe auf Amazon Web Services () verwenden.AWS Die Lösung ist vollständig automatisiert AWS Systems Manager und verfügt über Lifecycle-Hooks von Amazon EC2 Auto Scaling. Mithilfe dieses Musters können Sie Ihre Mainframe-Online- und Batch-Anwendungen so einrichten, dass sie durch automatische Ein- und Ausskalierung auf der Grundlage Ihrer Kapazitätsanforderungen eine hohe Ausfallsicherheit erreichen.

> **Note**
>
> Dieses Muster wurde mit Micro Focus Enterprise Server Version 6.0 getestet. Informationen zu Version 8 finden Sie unter Micro Focus Runtime einrichten (bei Amazon EC2).

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Micro Focus Enterprise Server-Software und -Lizenz. Weitere Informationen erhalten Sie vom Micro Focus-Vertrieb.
- Ein Verständnis des Konzepts der Neuerstellung und Bereitstellung einer Mainframe-Anwendung zur Ausführung auf Micro Focus Enterprise Server. Einen allgemeinen Überblick finden Sie im Micro Focus Enterprise Server-Datenblatt.
- Ein Verständnis der Konzepte im Micro Focus Enterprise Server Scale-out Performance and Availability Cluster. Weitere Informationen finden Sie in der Micro Focus Enterprise Server-Dokumentation.

- Ein Verständnis des Gesamtkonzepts einer Mainframe-Anwendung DevOps mit kontinuierlicher Integration (CI). Ein von AWS und Micro Focus entwickeltes AWS Prescriptive Guidance-Muster finden Sie unter Mainframe-Modernisierung: DevOps weiter AWS mit Micro Focus.

> **Note**
>
> Dieses Muster wurde mit Micro Focus Enterprise Server Version 6 getestet. Informationen zu Version 8 finden Sie unter Micro Focus Runtime einrichten (bei Amazon EC2).

Einschränkungen

- Eine Liste der Plattformen, die von Micro Focus Enterprise Server unterstützt werden, finden Sie im Micro Focus Enterprise Server-Datenblatt.
- Die in diesem Muster verwendeten Skripts und Tests basieren auf Amazon EC2 Windows Server 2019; andere Windows Server-Versionen und Betriebssysteme wurden nicht auf dieses Muster getestet.
- Das Muster basiert auf Micro Focus Enterprise Server 6.0 für Windows. Frühere oder spätere Versionen wurden bei der Entwicklung dieses Musters nicht getestet.

Produktversionen

- Micro Focus Enterprise Server 6.0
- Windows Server 2019

Architektur

In der herkömmlichen Mainframe-Umgebung müssen Sie Hardware bereitstellen, um Ihre Anwendungen und Unternehmensdaten zu hosten. Um den saisonalen, monatlichen, vierteljährlichen oder sogar beispiellosen oder unerwarteten Bedarfsspitzen gerecht zu werden und diese zu bewältigen, müssen Mainframe-Benutzer skalieren, indem sie zusätzliche Speicher- und Rechenkapazität erwerben. Durch die Erhöhung der Anzahl der Speicher- und Rechenkapazitätsressourcen wird die Gesamtleistung verbessert, die Skalierung erfolgt jedoch nicht linear.

Dies ist nicht der Fall, wenn Sie mit der Einführung eines On-Demand-Nutzungsmodells auf AWS beginnen, indem Sie Amazon EC2 Auto Scaling und Micro Focus Enterprise Server verwenden. In den folgenden Abschnitten wird detailliert beschrieben, wie Sie mithilfe des Micro Focus Enterprise Server Scale-Out Performance and Availability Clusters (PAC) mit einer Amazon EC2 Auto Scaling-Gruppe eine vollautomatische, skalierbare Mainframe-Anwendungsarchitektur aufbauen.

Die automatische Skalierungsarchitektur von Micro Focus Enterprise Server

Zunächst ist es wichtig, die grundlegenden Konzepte von Micro Focus Enterprise Server zu verstehen. Diese Umgebung bietet eine Mainframe-kompatible x86-Bereitstellungsumgebung für Anwendungen, die traditionell auf dem IBM Mainframe ausgeführt wurden. Sie bietet sowohl Online- als auch Batchläufe sowie eine Transaktionsumgebung, die Folgendes unterstützt:

- IBM COBOL
- IBM PL/I
- IBM JCL-Batchaufträge
- IBM CICS- und IMS TM-Transaktionen
- Web-Services
- Gängige Batch-Dienstprogramme, einschließlich SORT

Micro Focus Enterprise Server ermöglicht die Ausführung von Mainframe-Anwendungen mit minimalen Änderungen. Bestehende Mainframe-Workloads können auf x86-Plattformen verlagert und modernisiert werden, um die Vorteile der nativen AWS-Cloud-Erweiterungen für eine schnelle Expansion in neue Märkte oder Regionen zu nutzen.

Das AWS Prescriptive Guidance Guidance-Muster Mainframe-Modernisierung: DevOps auf AWS mit Micro Focus wurde die Architektur eingeführt, um die Entwicklung und das Testen von Mainframe-Anwendungen auf AWS mithilfe von Micro Focus Enterprise Developer und Enterprise Test Server mit AWS und AWS zu beschleunigen. CodePipeline CodeBuild Dieses Muster konzentriert sich auf die Bereitstellung von Mainframe-Anwendungen in der AWS-Produktionsumgebung, um eine hohe Verfügbarkeit und Ausfallsicherheit zu erreichen.

In einer Mainframe-Produktionsumgebung haben Sie möglicherweise IBM Parallel Sysplex auf dem Mainframe eingerichtet, um eine hohe Leistung und hohe Verfügbarkeit zu erreichen. Um eine Scale-Out-Architektur zu schaffen, die Sysplex ähnelt, hat Micro Focus den Performance and Availability Cluster (PAC) in Enterprise Server eingeführt. PACs unterstützt die Bereitstellung von Mainframe-Anwendungen auf mehreren Enterprise Server-Regionen, die als einzelnes Image

verwaltet und in EC2 Amazon-Instances skaliert werden. PACs unterstützt außerdem vorhersehbare Anwendungsleistung und Systemdurchsatz bei Bedarf.

In einem PAC arbeiten mehrere Enterprise Server-Instanzen als eine einzige logische Einheit zusammen. Der Ausfall einer Enterprise Server-Instance beeinträchtigt daher nicht die Geschäftskontinuität, da die Kapazität mit anderen Regionen geteilt wird, während neue Instances automatisch mit Industriestandardfunktionen wie einer Amazon EC2 Auto Scaling Scaling-Gruppe gestartet werden. Dadurch werden einzelne Fehlerquellen beseitigt und die Widerstandsfähigkeit gegenüber Hardware-, Netzwerk- und Anwendungsproblemen verbessert. Skalierte Enterprise Server-Instanzen können mithilfe der Enterprise Server Common Web Administration (ESCWA) betrieben und verwaltet werden APIs, was die betriebliche Wartung und Wartungsfreundlichkeit von Enterprise Servern vereinfacht.

> **Note**
>
> Micro Focus empfiehlt, dass der Performance and Availability Cluster (PAC) aus mindestens drei Enterprise Server-Regionen bestehen sollte, damit die Verfügbarkeit nicht beeinträchtigt wird, falls eine Enterprise Server-Region ausfällt oder gewartet werden muss.

Für die PAC-Konfiguration ist ein unterstützter relationaler Datenbankverwaltungsdienst (RDBMS) zur Verwaltung der Regionsdatenbank, einer regionsübergreifenden Datenbank und optionaler Datenspeicherdatenbanken erforderlich. Für die Verwaltung von VSAM-Dateien (Virtual Storage Access Method) mithilfe der Micro Focus Database File Handler-Unterstützung sollte eine Datenspeicher-Datenbank verwendet werden, um die Verfügbarkeit und Skalierbarkeit zu verbessern. RDBMSs Zu den unterstützten Produkten gehören:

- Microsoft SQL Server 2009 R2 und höher
- PostgreSQL 10.x, einschließlich Amazon Aurora PostgreSQL-kompatibler Edition
- DB2 10.4 und höher

Einzelheiten zu den unterstützten RDBMS- und PAC-Anforderungen finden Sie unter Micro Focus Enterprise Server — Voraussetzungen und Micro Focus Enterprise Server — Empfohlene PAC-Konfiguration.

Das folgende Diagramm zeigt ein typisches AWS-Architektur-Setup für ein Micro Focus PAC.

	Komponente	Beschreibung
1	Automatische Skalierung der Enterprise Server-Instanzen (Gruppe)	Richten Sie eine automatische Skalierungsgruppe ein, die mit Enterprise Server-Instanzen in einem PAC bereitgestellt wird. Die Anzahl der Instances kann durch CloudWatch Amazon-Alarme mithilfe von CloudWatch Metriken nach oben oder unten skaliert werden.
2	Automatische Skalierung der ESCWA-Instanzen von Enterprise Server	Richten Sie eine automatische Skalierungsgruppe ein, die mit Enterprise Server Common Web Administration (ESCWA) bereitgestellt wird. ESCWA bietet Clusterverwaltung. APIs Die ESCWA-Server dienen als Steuerungsebene zum Hinzufügen oder Entfernen von Enterprise Servern und zum Starten oder Stoppen von Enterprise Server-Regionen in der PAC während der automatischen Skalierungsereignisse der Enterprise Server-Instanz. Da die ESCWA-Instanz nur für das PAC-Management verwendet wird, ist ihr Datenverkehrsmuster vorhersehbar, und die gewünschte Kapazitätsanforderung für die automatische Skalierung kann auf 1 gesetzt werden.

3	Amazon Aurora Aurora-Instance in einem Multi-AZ-Setup	Richten Sie ein relationales Datenbankmanagementsystem (RDBMS) ein, um sowohl Benutzer- als auch Systemdatendateien zu hosten, die von den Enterprise Server-Instances gemeinsam genutzt werden sollen.
4	Amazon-Instanz ElastiCache (Redis OSS) und Replikat	Richten Sie eine primäre Instance ElastiCache (Redis OSS) und mindestens ein Replikat ein, um Benutzerdaten zu hosten und als Scale-Out-Repository (SOR) für die Enterprise Server-Instances zu fungieren. Sie können ein oder mehrere Scale-Out-Repositorys konfigurieren, um bestimmte Arten von Benutzerdaten zu speichern. Enterprise Server verwendet eine Redis NoSQL-Datenbank als SOR, eine Voraussetzung für die Aufrechterhaltung der PAC-Integrität.

5	Network Load Balancer	Richten Sie einen Load Balancer ein, der einen Hostnamen für Anwendungen bereitstellt, um eine Verbindung zu den von Enterprise Server-Instanzen bereitgestellten Diensten herzustellen (z. B. für den Zugriff auf die Anwendung über einen 3270-Emulator).

Diese Komponenten bilden die Mindestanforderung für einen Micro Focus Enterprise Server PAC-Cluster. Der nächste Abschnitt befasst sich mit der Automatisierung der Clusterverwaltung.

Verwenden von AWS Systems Manager Automation für die Skalierung

Nachdem der PAC-Cluster auf AWS bereitgestellt wurde, wird der PAC über die Enterprise Server Common Web Administration (ESCWA) APIs verwaltet.

Um die Clusterverwaltungsaufgaben bei automatischen Skalierungsereignissen zu automatisieren, können Sie Systems Manager Automation-Runbooks und Amazon EC2 Auto Scaling mit Amazon EventBridge verwenden. Die Architektur dieser Automatisierungen ist in der folgenden Abbildung dargestellt.

	Komponente	Beschreibung
1	Automatischer Skalierungslebenszyklus-Hook	Richten Sie automatische Skalierungs-Lifecycle-Hooks ein und senden Sie Benachrichtigungen an Amazon, EventBridge wenn neue Instances gestartet und bestehende Instances in der automatischen Skalierungsgruppe beendet werden.

2	Amazon EventBridge	Richten Sie eine EventBridge Amazon-Regel ein, um automatische Skalierungsereignisse an Systems Manager Automation-Runbook-Ziele weiterzuleiten.
3	Runbooks für die Automatisierung	Richten Sie Systems Manager Automation-Runbooks ein, um PowerShell Windows-Skripts auszuführen, und rufen Sie ESCWA auf, um das PAC APIs zu verwalten. Beispiele finden Sie im Abschnitt Zusätzliche Informationen.
4	Enterprise Server ESCWA-Instanz in einer automatischen Skalierungsgruppe	Richten Sie eine Enterprise Server ESCWA-Instanz in einer automatischen Skalierungsgruppe ein. Die ESCWA-Instanz ermöglicht APIs die Verwaltung des PAC.

Tools

- Micro Focus Enterprise Server — Micro Focus Enterprise Server bietet die Ausführungsumgebung für Anwendungen, die mit einer beliebigen IDE-Variante (Integrated Development Environment) von Enterprise Developer erstellt wurden.
- Amazon EC2 Auto Scaling — Amazon EC2 Auto Scaling hilft Ihnen sicherzustellen, dass Ihnen die richtige Anzahl von EC2 Amazon-Instances zur Verfügung steht, um die Last für Ihre Anwendung zu bewältigen. Sie erstellen Sammlungen von EC2 Instances, sogenannte Auto Scaling Scaling-Gruppen, und geben die Mindest- und Höchstanzahl von Instances an.
- Amazon ElastiCache (Redis OSS) — Amazon ElastiCache ist ein Webservice zum Einrichten, Verwalten und Skalieren einer verteilten In-Memory-Datenspeicher- oder Cache-Umgebung in der Cloud. Es handelt sich um eine leistungsstarke, skalierbare und kostengünstige Caching-Lösung.

- Amazon RDS — Amazon Relational Database Service (Amazon RDS) ist ein Webservice, der die Einrichtung, den Betrieb und die Skalierung einer relationalen Datenbank in der AWS-Cloud erleichtert. Er bietet kosteneffiziente, anpassbare Kapazität für eine relationale Datenbank und verwaltet allgemeine Datenbankverwaltungsaufgaben.
- AWS Systems Manager — AWS Systems Manager ist ein AWS-Service, mit dem Sie Ihre Infrastruktur auf AWS anzeigen und steuern können. Mithilfe der Systems Manager Manager-Konsole können Sie Betriebsdaten von mehreren AWS-Services anzeigen und betriebliche Aufgaben in Ihren AWS-Ressourcen automatisieren. Systems Manager unterstützt Sie bei der Aufrechterhaltung von Sicherheit und Compliance, indem er Ihre verwalteten Instances scannt und über festgestellte Richtlinienverstöße (oder Abhilfemaßnahmen ergreifen) berichtet.

Epen

Eine Amazon Aurora Aurora-Instance erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CloudFormation AWS-Vorlage für eine Amazon Aurora Aurora-Instance.	Verwenden Sie den AWS-Beispielcodeausschnitt, um eine CloudFormation Vorlage zu erstellen, mit der eine Amazon Aurora PostgreSQL-kompatible Edition-Instance erstellt wird.	Cloud-Architekt
Stellen Sie einen CloudFormation Stack bereit, um die Amazon Aurora Aurora-Instance zu erstellen.	Verwenden Sie die CloudFormation Vorlage, um eine Aurora PostgreSQL-kompatible Instance zu erstellen, für die Multi-AZ-Replikation für Produktions-Workloads aktiviert ist.	Cloud-Architekt
Konfigurieren Sie die Datenbankverbindungseinstellungen für Enterprise Server.	Folgen Sie den Anweisungen in der Micro Focus-Dokumentation, um die Verbindungszeichenfolgen und die	Dateningenieur, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Datenbankkonfiguration für Micro Focus Enterprise Server vorzubereiten.	

Erstellen Sie einen ElastiCache Amazon-Cluster für die Redis-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CloudFormation Vorlage für den ElastiCache Amazon-Cluster für die Redis-Instance.	Verwenden Sie den AWS-Beispielcodeausschnitt, um eine CloudFormation Vorlage zu erstellen, die einen ElastiCache Amazon-Cluster für die Redis-Instance erstellt.	Cloud-Architekt
Stellen Sie den CloudFormation Stack bereit, um einen ElastiCache Amazon-Cluster für die Redis-Instance zu erstellen.	Erstellen Sie den ElastiCache Amazon-Cluster für die Redis-Instance, für die Multi-AZ-Replikation für Produktions-Workloads aktiviert ist.	Cloud-Architekt
Konfigurieren Sie die PSOR-Verbindungseinstellungen für Enterprise Server.	Folgen Sie den Anweisungen in der Micro Focus-Dokumentation, um die Verbindungskonfiguration des PAC Scale-Out Repository (PSOR) für Micro Focus Enterprise Server PAC vorzubereiten.	DevOps Ingenieur

Erstellen Sie eine automatische ESCWA-Skalierungsgruppe für Micro Focus Enterprise Server

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Micro Focus Enterprise Server-AMI.	Erstellen Sie eine Amazon EC2 Windows Server-In stance und installieren Sie die Micro Focus Enterprise Server-Binärdatei in der EC2 Instance. Erstellen Sie ein Amazon Machine Image (AMI) der EC2 Instance. Weitere Informationen finden Sie in der Enterprise Server-Installatio nsdokumentation.	Cloud-Architekt
Erstellen Sie eine CloudForm ation Vorlage für Enterprise Server ESCWA.	Verwenden Sie den AWS-Beispielcodeausschnitt, um eine Vorlage für die Erstellun g eines benutzerdefinierten Stacks von Enterprise Server ESCWA in einer automatis chen Skalierungsgruppe zu erstellen.	Cloud-Architekt
Stellen Sie den CloudForm ation Stack bereit, um eine EC2 Amazon-Skalierungs gruppe für Enterprise Server ESCWA zu erstellen.	Verwenden Sie die CloudForm ation Vorlage, um die automatische Skalierun gsgruppe mit dem Micro Focus Enterprise Server ESCWA-AMI bereitzus tellen, das in der vorherigen Geschichte erstellt wurde.	Cloud-Architekt

Erstellen Sie ein AWS Systems Manager Automation Automation-Runbook

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CloudFormation Vorlage für ein Systems Manager Automation-Runbook.	Verwenden Sie die Beispielcodefragmente im Abschnitt Zusätzliche Informationen, um eine CloudFormation Vorlage zu erstellen, mit der ein Systems Manager Automation-Runbook zur Automatisierung der PAC-Erstellung, Enterprise Server Scale In und Enterprise Server Scale Out erstellt wird.	Cloud-Architekt
Stellen Sie den CloudFormation Stack bereit, der das Systems Manager Automation-Runbook enthält.	Verwenden Sie die CloudFormation Vorlage, um einen Stack bereitzustellen, der das Automation-Runbook für die PAC-Erstellung, Enterprise Server Scale In und Enterprise Server Scale Out enthält.	Cloud-Architekt

Erstellen Sie eine automatische Skalierungsgruppe für Micro Focus Enterprise Server

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CloudFormation Vorlage für die Einrichtung einer automatischen Skalierungsgruppe für Micro Focus Enterprise Server.	Verwenden Sie den AWS-Beispielcodeausschnitt, um eine CloudFormation Vorlage zu erstellen, die eine automatische Skalierungsgruppe erstellt. Diese Vorlage verwendet dasselbe AMI, das für die Micro Focus	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Enterprise Server ESCWA-Instanz erstellt wurde. Verwenden Sie dann einen AWS-Beispielcodeausschnitt, um das automatische Skalierungslebenszykluserei gnis zu erstellen, und richten Sie Amazon so ein, dass in derselben EventBridge Vorlage nach Scale-Out- und Scale-In-Ereignissen gefiltert wird. CloudFormation	
Stellen Sie den CloudFormation Stack für die automatische Skalierungsgruppe für Micro Focus Enterprise Server bereit.	Stellen Sie den CloudFormation Stack bereit, der die automatische Skalierungsgruppe für Micro Focus Enterprise Server enthält.	Cloud-Architekt

Zugehörige Ressourcen

- Micro Focus Enterprise Server Leistungs- und Verfügbarkeitscluster (PAC)
- Lebenszyklus-Hooks von Amazon EC2 Auto Scaling
- Ausführen von Automatisierungen mit Triggern unter Verwendung von EventBridge

Zusätzliche Informationen

Die folgenden Szenarien müssen für die Ein- oder Ausskalierung der PAC-Cluster automatisiert werden.

Automatisierung für den Start oder die Neuerstellung eines PAC

Beim Start eines PAC-Clusters verlangt Enterprise Server, dass ESCWA aufgerufen wird, um eine APIs PAC-Konfiguration zu erstellen. Dadurch werden Enterprise Server-Regionen gestartet und dem PAC hinzugefügt. Gehen Sie wie folgt vor, um eine PAC zu erstellen oder neu zu erstellen:

1. Konfigurieren Sie ein PAC Scale-Out Repository (PSOR) in ESCWA mit einem bestimmten Namen.

```
POST /server/v1/config/groups/sors
```

2. Erstellen Sie ein PAC mit einem bestimmten Namen und hängen Sie den PSOR daran an.

```
POST /server/v1/config/groups/pacs
```

3. Konfigurieren Sie die Regionsdatenbank und die regionsübergreifende Datenbank, wenn Sie zum ersten Mal eine PAC einrichten.

> **Note**
>
> In diesem Schritt werden SQL-Abfragen und das Befehlszeilentool dbhfhadmin der Micro Focus Enterprise Suite verwendet, um die Datenbank zu erstellen und die ersten Daten zu importieren.

4. Installieren Sie die PAC-Definition in den Enterprise Server-Regionen.

```
POST /server/v1/config/mfds
POST /native/v1/config/groups/pacs/${pac_uid}/install
```

5. Starten Sie die Enterprise Server-Regionen in der PAC.

```
POST /native/v1/regions/${host_ip}/${port}/${region_name}/start
```

Die vorherigen Schritte können mithilfe eines PowerShell Windows-Skripts implementiert werden.

In den folgenden Schritten wird erklärt, wie Sie mithilfe des PowerShell Windows-Skripts eine Automatisierung für die Erstellung einer PAC erstellen.

1. Erstellen Sie eine EC2 Amazon-Startvorlage, die das PowerShell Windows-Skript als Teil des Bootstrap-Prozesses herunterlädt oder erstellt. Sie können beispielsweise EC2 Benutzerdaten

verwenden, um das Skript aus einem Amazon Simple Storage Service (Amazon S3) -Bucket herunterzuladen.

2. Erstellen Sie ein AWS Systems Manager Automation Automation-Runbook, um das PowerShell Windows-Skript aufzurufen.
3. Ordnen Sie das Runbook mithilfe des Instance-Tags der ESCWA-Instance zu.
4. Erstellen Sie mithilfe der Startvorlage eine ESCWA-Skalierungsgruppe für automatische Skalierung.

Sie können das folgende CloudFormation AWS-Beispiel-Snippet verwenden, um das Automation-Runbook zu erstellen.

CloudFormation Beispielausschnitt für ein Systems Manager Automation-Runbook, das für die PAC-Erstellung verwendet wird

```
PACInitDocument:
   Type: AWS::SSM::Document
   Properties:
     DocumentType: Command
     Content:
       schemaVersion: '2.2'
       description: Operation Runbook to create Enterprise Server PAC
       mainSteps:
       - action: aws:runPowerShellScript
         name: CreatePAC
         inputs:
           onFailure: Abort
           timeoutSeconds: "1200"
           runCommand:
           - |
             C:\Scripts\PAC-Init.ps1
PacInitAutomation:
   Type: AWS::SSM::Document
   Properties:
     DocumentType: Automation
     Content:
       description: Prepare Micro Focus PAC Cluster via ESCWA Server
       schemaVersion: '0.3'
       assumeRole: !GetAtt SsmAssumeRole.Arn
       mainSteps:
         - name: RunPACInitDocument
           action: aws:runCommand
```

```
            timeoutSeconds: 300
            onFailure: Abort
            inputs:
              DocumentName: !Ref PACInitDocument
              Targets:
                - Key: tag:Enterprise Server - ESCWA
                  Values:
                    - "true"
  PacInitDocumentAssociation:
    Type: AWS::SSM::Association
    Properties:
      DocumentVersion: "$LATEST"
      Name: !Ref PACInitDocument
      Targets:
        - Key: tag:Enterprise Server - ESCWA
          Values:
            - "true"
```

Weitere Informationen finden Sie unter Micro Focus Enterprise Server — Konfiguration eines PAC.

Automatisierung für die horizontale Skalierung mit einer neuen Enterprise Server-Instanz

Wenn eine Enterprise Server-Instanz horizontal skaliert wird, muss ihre Enterprise Server-Region der PAC hinzugefügt werden. In den folgenden Schritten wird erklärt, wie ESCWA aufgerufen APIs und die Enterprise Server-Region zur PAC hinzugefügt wird.

1. Installieren Sie die PAC-Definition in den Enterprise Server-Regionen.

```
POST '/server/v1/config/mfds'
POST /native/v1/config/groups/pacs/${pac_uid}/install
```

2. Warmstart der Region im PAC.

```
POST /native/v1/regions/${host_ip}/${port}/${region_name}/start
```

3. Fügen Sie die Enterprise Server-Instanz dem Load Balancer hinzu, indem Sie die automatische Skalierungsgruppe dem Load Balancer zuordnen.

Die vorherigen Schritte können mithilfe eines Windows-Skripts implementiert werden. PowerShell Weitere Informationen finden Sie unter Micro Focus Enterprise Server — Konfiguration eines PAC.

Die folgenden Schritte können verwendet werden, um eine ereignisgesteuerte Automatisierung zu erstellen, bei der eine neu gestartete Enterprise Server-Instanz durch Wiederverwendung des PowerShell Windows-Skripts zu einer PAC hinzugefügt wird.

1. Erstellen Sie eine EC2 Amazon-Startvorlage für eine Enterprise Server-Instance, die beim Bootstrap eine Enterprise Serverregion bereitstellt. Sie können beispielsweise den Micro Focus Enterprise Server-Befehl mfds verwenden, um eine Regionskonfiguration zu importieren. Weitere Informationen und Optionen, die für diesen Befehl verfügbar sind, finden Sie in der Enterprise Server-Referenz.
2. Erstellen Sie eine automatische Skalierungsgruppe für Enterprise Server, die die im vorherigen Schritt erstellte Startvorlage verwendet.
3. Erstellen Sie ein Systems Manager Automation-Runbook, um das PowerShell Windows-Skript aufzurufen.
4. Ordnen Sie das Runbook mithilfe des Instance-Tags der ESCWA-Instanz zu.
5. Erstellen Sie eine EventBridge Amazon-Regel, um nach dem Ereignis EC2 Instance Launch Successful für die automatische Skalierungsgruppe Enterprise Server zu filtern, und erstellen Sie das Ziel für die Verwendung des Automation-Runbooks.

Sie können den folgenden CloudFormation Beispielausschnitt verwenden, um das Automation-Runbook und die Regel zu erstellen. EventBridge

CloudFormation Beispielausschnitt für Systems Manager, der für die Skalierung von Enterprise Server-Instanzen verwendet wird

```
ScaleOutDocument:
   Type: AWS::SSM::Document
   Properties:
     DocumentType: Command
     Content:
       schemaVersion: '2.2'
       description: Operation Runbook to Adding MFDS Server into an existing PAC
       parameters:
         MfdsPort:
           type: String
         InstanceIpAddress:
           type: String
           default: "Not-Available"
         InstanceId:
           type: String
```

```
            default: "Not-Available"
        mainSteps:
        - action: aws:runPowerShellScript
          name: Add_MFDS
          inputs:
            onFailure: Abort
            timeoutSeconds: "300"
            runCommand:
            - |
              $ip = "{{InstanceIpAddress}}"
              if ( ${ip} -eq "Not-Available" ) {
                $ip = aws ec2 describe-instances --instance-id {{InstanceId}} --output
text --query "Reservations[0].Instances[0].PrivateIpAddress"
              }
              C:\Scripts\Scale-Out.ps1 -host_ip ${ip} -port {{MfdsPort}}

  PacScaleOutAutomation:
    Type: AWS::SSM::Document
    Properties:
      DocumentType: Automation
      Content:
        parameters:
          MfdsPort:
            type: String
          InstanceIpAddress:
            type: String
            default: "Not-Available"
          InstanceId:
            type: String
            default: "Not-Available"
        description: Scale Out 1 New Server in Micro Focus PAC Cluster via ESCWA
Server
        schemaVersion: '0.3'
        assumeRole: !GetAtt SsmAssumeRole.Arn
        mainSteps:
          - name: RunScaleOutCommand
            action: aws:runCommand
            timeoutSeconds: 300
            onFailure: Abort
            inputs:
              DocumentName: !Ref ScaleOutDocument
              Parameters:
                InstanceIpAddress: "{{InstanceIpAddress}}"
                InstanceId: "{{InstanceId}}"
```

```
                MfdsPort: "{{MfdsPort}}"
              Targets:
                - Key: tag:Enterprise Server - ESCWA
                  Values:
                    - "true"
```

Automatisierung für die Skalierung in einer Enterprise Server-Instanz

Ähnlich wie beim Skalieren wird bei der Skalierung einer Enterprise Server-Instanz das Ereignis EC2 Instance-Terminate Lifecycle Action ausgelöst, und die folgenden Prozess- und API-Aufrufe sind erforderlich, um eine Micro Focus Enterprise Server-Instanz aus dem PAC zu entfernen.

1. Beenden Sie die Region in der beendenden Enterprise Server-Instanz.

```
POST "/native/v1/regions/${host_ip}/${port}/${region_name}/stop"
```

2. Entfernen Sie die Enterprise Server-Instanz aus dem PAC.

```
DELETE "/server/v1/config/mfds/${uid}"
```

3. Senden Sie ein Signal, um mit dem Beenden der Enterprise Server-Instanz fortzufahren.

Die vorherigen Schritte können in einem PowerShell Windows-Skript implementiert werden. Weitere Informationen zu diesem Prozess finden Sie im Dokument Micro Focus Enterprise Server — Verwaltung einer PAC.

In den folgenden Schritten wird erklärt, wie Sie eine ereignisgesteuerte Automatisierung erstellen, um eine Enterprise Server-Instanz von einem PAC aus zu beenden, indem Sie das Windows-Skript wiederverwenden. PowerShell

1. Erstellen Sie ein Systems Manager Automation-Runbook, um das PowerShell Windows-Skript aufzurufen.
2. Ordnen Sie das Runbook mithilfe des Instance-Tags der ESCWA-Instanz zu.
3. Erstellen Sie einen Lifecycle-Hook für automatische Skalierungsgruppen zur EC2 Instanzbeendigung.
4. Erstellen Sie eine EventBridge Amazon-Regel, um das Ereignis EC2 Instance-Terminate Lifecycle Action für die automatische Skalierungsgruppe Enterprise Server zu filtern, und erstellen Sie das Ziel für die Verwendung des Automation-Runbooks.

Sie können die folgende CloudFormation Beispielvorlage verwenden, um ein Systems Manager Automation-Runbook, einen Lifecycle-Hook und eine EventBridge Regel zu erstellen.

CloudFormation Beispielausschnitt für ein Systems Manager Automation-Runbook, das für die Skalierung in einer Enterprise Server-Instanz verwendet wird

```
 ScaleInDocument:
    Type: AWS::SSM::Document
    Properties:
      DocumentType: Command
      Content:
        schemaVersion: '2.2'
        description: Operation Runbook to Remove MFDS Server from PAC
        parameters:
          MfdsPort:
            type: String
          InstanceIpAddress:
            type: String
            default: "Not-Available"
          InstanceId:
            type: String
            default: "Not-Available"
        mainSteps:
        - action: aws:runPowerShellScript
          name: Remove_MFDS
          inputs:
            onFailure: Abort
            runCommand:
            - |
              $ip = "{{InstanceIpAddress}}"
              if ( ${ip} -eq "Not-Available" ) {
                $ip = aws ec2 describe-instances --instance-id {{InstanceId}} --output
text --query "Reservations[0].Instances[0].PrivateIpAddress"
              }
              C:\Scripts\Scale-In.ps1 -host_ip ${ip} -port {{MfdsPort}}

  PacScaleInAutomation:
    Type: AWS::SSM::Document
    Properties:
      DocumentType: Automation
      Content:
        parameters:
          MfdsPort:
```

```
        type: String
      InstanceIpAddress:
        type: String
        default: "Not-Available"
      InstanceId:
        type: String
        default: "Not-Available"
description: Scale In 1 New Server in Micro Focus PAC Cluster via ESCWA Server
schemaVersion: '0.3'
assumeRole: !GetAtt SsmAssumeRole.Arn
mainSteps:
  - name: RunScaleInCommand
    action: aws:runCommand
    timeoutSeconds: "600"
    onFailure: Abort
    inputs:
      DocumentName: !Ref ScaleInDocument
      Parameters:
        InstanceIpAddress: "{{InstanceIpAddress}}"
        MfdsPort: "{{MfdsPort}}"
        InstanceId: "{{InstanceId}}"
      Targets:
        - Key: tag:Enterprise Server - ESCWA
          Values:
            - "true"
  - name: TerminateTheInstance
    action: aws:executeAwsApi
    inputs:
      Service: autoscaling
      Api: CompleteLifecycleAction
      AutoScalingGroupName: !Ref AutoScalingGroup
      InstanceId: "{{ InstanceId }}"
      LifecycleActionResult: CONTINUE
      LifecycleHookName: !Ref ScaleInLifeCycleHook
```

Automatisierung für einen EC2 automatischen Skalierungsauslöser von Amazon

Die Einrichtung einer Skalierungsrichtlinie für Enterprise Server-Instances erfordert ein Verständnis des Anwendungsverhaltens. In den meisten Fällen können Sie Skalierungsrichtlinien für die Zielverfolgung einrichten. Sie können beispielsweise die durchschnittliche CPU-Auslastung als CloudWatch Amazon-Metrik verwenden, um die automatische Skalierungsrichtlinie festzulegen. Weitere Informationen finden Sie unter Target-Tracking-Skalierungsrichtlinien für Amazon EC2 Auto Scaling. Für Anwendungen mit regelmäßigen Datenverkehrsmustern sollten Sie die Verwendung

einer Richtlinie zur vorausschauenden Skalierung in Betracht ziehen. Weitere Informationen finden Sie unter Prädiktive Skalierung für Amazon EC2 Auto Scaling.

Erstellen Sie einen fortschrittlichen Mainframe-Dateiviewer in der AWS-Cloud

Erstellt von Boopathy GOPALSAMY (AWS) und Jeremiah O'Connor (AWS)

Übersicht

Dieses Muster enthält Codebeispiele und Schritte, mit denen Sie mithilfe von serverlosen AWS-Services ein erweitertes Tool zum Durchsuchen und Überprüfen Ihrer Mainframe-Dateien im festen Format erstellen können. Das Muster bietet ein Beispiel dafür, wie eine Mainframe-Eingabedatei zum Durchsuchen und Suchen in ein Amazon OpenSearch Service-Dokument konvertiert wird. Das Datei-Viewer-Tool kann Ihnen dabei helfen, Folgendes zu erreichen:

- Behalten Sie die gleiche Mainframe-Dateistruktur und das gleiche Layout für Konsistenz in Ihrer AWS-Zielmigrationsumgebung bei (Sie können beispielsweise dasselbe Layout für Dateien in einer Batch-Anwendung beibehalten, die Dateien an externe Parteien überträgt)
- Beschleunigen Sie die Entwicklung und das Testen während Ihrer Mainframe-Migration
- Support von Wartungsaktivitäten nach der Migration

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine virtuelle private Cloud (VPC) mit einem Subnetz, das über Ihre Legacy-Plattform erreichbar ist
-

> **Note**
>
> Eine Eingabedatei und das dazugehörige COBOL-Copybook (Common Business-Oriented Language) (: Beispiele für Eingabedateien und COBOL-Copybooks finden Sie im Repository. gfs-mainframe-solutions GitHub Weitere Informationen zu COBOL-Copybooks finden Sie im Enterprise COBOL for z/OS 6.3 Programming Guide auf der IBM-Website.)

Einschränkungen

- Das Parsen von Copybooks ist auf nicht mehr als zwei verschachtelte Ebenen beschränkt (OCCURS)

Architektur

Quelltechnologie-Stack

- Eingabedateien im FB-Format (Fixed Blocked)
- COBOL-Copybook-Layout

Zieltechnologie-Stack

- Amazon Athena
- OpenSearch Amazon-Dienst
- Amazon Simple Storage Service (Amazon-S3)
- AWS Lambda
- AWS Step Functions

Zielarchitektur

Das folgende Diagramm zeigt den Prozess des Parsens und Konvertierens einer Mainframe-Eingabedatei in ein OpenSearch Servicedokument zum Durchsuchen und Suchen.

Das Diagramm zeigt den folgenden Workflow:

1. Ein Admin-Benutzer oder eine Admin-Anwendung überträgt Eingabedateien in einen S3-Bucket und COBOL-Copybooks in einen anderen S3-Bucket.
2.
> **Note**
>
> Der S3-Bucket mit den Eingabedateien ruft eine Lambda-Funktion auf, die einen serverlosen Step Functions Functions-Workflow startet. : Die Verwendung eines S3-Ereignisauslösers und einer Lambda-Funktion zur Steuerung des Step Functions Functions-Workflows in diesem Muster ist optional. Die GitHub Codebeispiele in diesem Muster beinhalten nicht die Verwendung dieser Dienste, aber Sie können diese Dienste je nach Ihren Anforderungen verwenden.

3. Der Step Functions Functions-Workflow koordiniert alle Batch-Prozesse aus den folgenden Lambda-Funktionen:

- Die `s3copybookparser.py` Funktion analysiert das Copybook-Layout und extrahiert Feldattribute, Datentypen und Offsets (erforderlich für die Verarbeitung der Eingabedaten).
- Die `s3toathena.py` Funktion erstellt ein Athena-Tabellenlayout. Athena analysiert die Eingabedaten, die von der `s3toathena.py` Funktion verarbeitet werden, und konvertiert die Daten in eine CSV-Datei.
- Die `s3toelasticsearch.py` Funktion nimmt die Ergebnisdatei aus dem S3-Bucket auf und überträgt die Datei an Service. OpenSearch

4. Benutzer greifen mit OpenSearch Service auf OpenSearch Dashboards zu, um die Daten in verschiedenen Tabellen- und Spaltenformaten abzurufen und dann Abfragen für die indizierten Daten auszuführen.

Tools

AWS-Services

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon Simple Storage Service (Amazon S3) analysieren können.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen. In diesem Muster verwenden Sie Lambda, um Kernlogik zu implementieren, z. B. das Parsen von Dateien, das Konvertieren von Daten und das Laden von Daten in OpenSearch Service für den interaktiven Dateizugriff.
- Amazon OpenSearch Service ist ein verwalteter Service, der Sie bei der Bereitstellung, dem Betrieb und der Skalierung von OpenSearch Service-Clustern in der AWS-Cloud unterstützt. In diesem Muster verwenden Sie OpenSearch Service, um die konvertierten Dateien zu indizieren und Benutzern interaktive Suchfunktionen bereitzustellen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie kontrollieren, wer authentifiziert und autorisiert ist, diese zu verwenden.

- AWS Step Functions ist ein serverloser Orchestrierungsservice, mit dem Sie Lambda-Funktionen und andere AWS-Services kombinieren können, um geschäftskritische Anwendungen zu erstellen. In diesem Muster verwenden Sie Step Functions, um Lambda-Funktionen zu orchestrieren.

Andere Tools

- GitHubist ein Code-Hosting-Dienst, der Tools für die Zusammenarbeit und Versionskontrolle bereitstellt.
- Python ist eine Programmiersprache auf hohem Niveau.

Code

Der Code für dieses Muster ist im GitHub gfs-mainframe-patternsRepository verfügbar.

Epen

Bereiten Sie die Zielumgebung vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den S3-Bucket.	Erstellen Sie einen S3-Bucket zum Speichern der Copybooks, Eingabeda teien und Ausgabedateien. Wir empfehlen die folgende Ordnerstruktur für Ihren S3-Bucket: • `copybook/` • `input/` • `output/` • `query/` • `results/`	Allgemeines AWS
Erstellen Sie die Funktion s3copybookparser.	1. Erstellen Sie eine Lambda-Funktion mit dem Namen `s3copybookparser` und	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	laden Sie den Quellcode (`s3copybookparser.py undcopybook.py`) aus dem GitHubRepository hoch. 2. Hängen Sie die IAM-Richtlinie `S3ReadOnly` an die Lambda-Funktion an.	
Erstellen Sie die Funktion s3toathena.	1. Erstellen Sie eine Lambda-Funktion namens `s3toathena` und laden Sie den Quellcode (`s3toathena.py`) aus dem GitHubRepository hoch. Konfigurieren Sie das Lambda-Timeout auf > 60 Sekunden. 2. Um Zugriff auf die erforderlichen Ressourcen zu gewähren, fügen Sie die IAM-Richtlinien `AmazonAthenaFullAccess` und die Lambda-Funktion `S3FullAccess` hinzu.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Funktion s3toelasticsearch.	1. **Important** Fügen Sie Ihrer Lambda-Umgebung eine Python-Abhängigkeit hinzu. : Um die `s3toelasticsearch` Funktion zu verwenden, müssen Sie die Python-Abhängigkeit hinzufügen, da die Lambda-Funktion Python-Elasticsearch-Clientabhängigkeiten (`Elasticsearch==7.9.0` und `requests_aws4auth`) verwendet. 2. Erstellen Sie eine Lambda-Funktion namens `s3toelasticsearch` und laden Sie den Quellcode (`s3toelasticsearch.py`) aus dem GitHubRepository hoch. 3. Importieren Sie die Python-Abhängigkeit als Lambda-Ebene. 4. Hängen Sie die IAM-Richtlinien `S3ReadOnly` und	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`AmazonOpenSearchServiceReadOnlyAccess` an die Lambda-Funktion an.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den OpenSearch Service-Cluster.	Erstellen Sie den Cluster 1. Erstellen Sie einen OpenSearch Servicecluster. Gehen Sie beim Erstellen des Clusters wie folgt vor: • **Note** Erstellen Sie einen Masterbenutzer und ein Kennwort für den Cluster, die Sie für die Anmeldung bei OpenSearch Dashboards verwenden können. : Dieser Schritt ist nicht erforderlich, wenn Sie die Authentifizierung über Amazon Cognito verwenden. • Wählen Sie eine differenzierte Zugriffskontrolle. Auf diese Weise haben Sie zusätzliche Möglichkeiten, den Zugriff auf Ihre Daten in OpenSearch Service zu kontrollieren.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Kopieren Sie die Domain-URL und übergeben Sie sie als Umgebungsvariable 'HOST' an die Lambda-Funktion `s3toelasticsearch` . Gewähren Sie Zugriff auf die IAM-Rolle Gehen Sie wie folgt vor, um einen detaillierten Zugriff auf die IAM-Rolle (`arn:aws:iam::**:role/service-role/s3toelasticsearch-role-**`) der Lambda-Funktion bereitzustellen: 1. Melden Sie sich als Masterbenutzer bei OpenSearch Dashboards an. 2. Wählen Sie die Registerkarte Sicherheit und dann Rollen, all_access, Benutzer zuordnen, Backend-Rollen aus. 3. Fügen Sie den Amazon-Ressourcennamen (ARN) der IAM-Rolle der Lambda-Funktion hinzu und wählen Sie dann Speichern. Weitere Informationen finden Sie unter Zuordnen von	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Rollen zu Benutzern in der OpenSearch Servicedo kumentation.	
Erstellen Sie Step Functions für die Orchestrierung.	1. Erstellen Sie eine Step Functions Functions-Zustandsmaschine mit dem Standardablauf. Die Definition ist im GitHub Repository enthalten. 2. Ersetzen Sie im JSON-Skri pt die Lambda-Funktion ARNs durch die Funktion ARNs from the Lambda in Ihrer Umgebung.	Allgemeines AWS

Bereitstellen und ausführen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Eingabedateien und Copybooks in den S3-Bucket hoch.	Laden Sie Beispieldateien aus dem GitHub Repositor y-Beispielordner herunter und laden Sie die Dateien in den S3-Bucket hoch, den Sie zuvor erstellt haben. 1. Laden Sie `Mockedcop y.cpy` und `acctix.cp y` in den `<S3_Bucket>/ copybook` Ordner hoch. 2. Laden Sie die Eingabeda teien `Modedupdate.txt` und die `acctindex.cpy`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Beispieldateien in den `<S3_Bucket>/input` Ordner hoch.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Rufen Sie die Step Functions auf.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Step Functions Functions-Konsole.
	2. Wählen Sie im Navigationsbereich State Machines aus.
	3. Wählen Sie Ihren Zustandsmaschine und dann Ausführung starten aus.
	4. Geben Sie im Eingabefeld den folgenden Copybook-/Dateipfad als JSON-Variable für den S3-Bucket ein und wählen Sie dann Ausführung starten aus.
	
	`{ "s3_copybook_bucket_name": "<BUCKET NAME>", "s3_copybook_bucket_key": "<COPYBOOK PATH>", "s3_source_bucket_name": "<BUCKET NAME", "s3_source_bucket_key": "INPUT FILE PATH" }`
	
	Zum Beispiel:
	
	`{`
		Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"s3_copybook_bucket_name": "fileaidtest",
	"s3_copybook_bucket_key": "copybook/acctix.cpy",
	"s3_source_bucket_name": "fileaidtest",
	"s3_source_bucket_key": "input/acctindex"
	}</pre>	

Validieren Sie die Workflow-Ausführung in Step Functions.	Überprüfen Sie in der Step Functions Functions-Konsole die Workflow-Ausführung im Graph Inspector. Die Status des Ausführungslaufs sind farblich gekennzeichnet, um den Ausführungsstatus darzustellen. Blau steht beispielsweise für In Bearbeitung, Grün für Erfolgreich und Rot für Fehlgeschlagen. Ausführlichere Informationen zu den Ausführungsereignissen finden Sie auch in der Tabelle im Abschnitt Verlauf der Ausführungsereignisse. Ein Beispiel für eine grafische Workflow-Ausführung finden Sie im Diagramm Step Functions im Abschnitt Zusätzliche Informationen dieses Musters.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Lieferprotokolle in Amazon CloudWatch.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudWatch -Konsole. 2. Erweitern Sie im Navigationsbereich die Option Protokolle und wählen Sie dann Protokollgruppen aus. 3. Suchen Sie im Suchfeld nach der Protokollgruppe der `s3toelasticsearch` Funktion. Ein Beispiel für erfolgreiche Zustellungsprotokolle finden Sie unter CloudWatch Übermittlungsprotokolle im Abschnitt Zusätzliche Informationen dieses Musters.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die formatierte Datei in OpenSearch Dashboards und führen Sie Dateioperationen durch.	1. Melden Sie sich bei der AWS-Managementkonsole an. Wählen Sie unter Analytics Amazon OpenSearch Service aus. 2. Wählen Sie im Navigationsbereich Domains aus. 3. Geben Sie im Suchfeld die URL für Ihre Domain in OpenSearch Dashboards ein. 4. Wählen Sie Ihr Dashboard aus und melden Sie sich dann als Masterbenutzer an. 5. Durchsuchen Sie die indizierten Daten im Tabellenformat. 6. Vergleichen Sie die Eingabedatei mit der formatierten Ausgabedatei (indiziertes Dokument) in Dashboards. OpenSearch In der Dashboard-Ansicht werden die hinzugefügten Spaltenüberschriften für Ihre formatierten Dateien angezeigt. Vergewissern Sie sich, dass die Quelldaten aus Ihren unformatierten Eingabedateien mit den Zieldaten in der Dashboard-Ansicht übereinstimmen.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Führen Sie Aktionen wie Suchen (z. B. mithilfe von Feldnamen, Werten oder Ausdrücken), Filter und DQL-Operationen (Dashboard Query Language) für die indizierte Datei aus.	

Zugehörige Ressourcen

Referenzen

- Beispiel für ein COBOL-Copybook (IBM-Dokumentation)
- BMC Compuware File-AID (BMC-Dokumentation)

Tutorials

- Tutorial: Verwenden eines Amazon S3 S3-Triggers zum Aufrufen einer Lambda-Funktion (AWS Lambda Lambda-Dokumentation)
- Wie erstelle ich einen serverlosen Workflow mit AWS Step Functions und AWS Lambda (AWS-Dokumentation)
- Verwenden von OpenSearch Dashboards mit Amazon OpenSearch Service (AWS-Dokumentation)

Zusätzliche Informationen

Diagramm der Step Functions

Das folgende Beispiel zeigt ein Step Functions Functions-Diagramm. Das Diagramm zeigt den Ausführungsstatus der in diesem Muster verwendeten Lambda-Funktionen.

CloudWatch Lieferprotokolle

Das folgende Beispiel zeigt erfolgreiche Zustellungsprotokolle für die Ausführung der `s3toelasticsearch` Ausführung.

2022-08-10T 15:53:33. 033-05:00	Anzahl der Verarbeitungsdokumente: 100	
	2022-08-10T 15:53:33. 171-05:00	[INFO] 20.08.2022 20:53:33. 171 Z a1b2c3d4-5678-90ab -cdef- Beitrag:443/_Bulk [Status:200 Anfrage:0,100s] EXAMPLE11111 https://search-essearch-3h4uqclifeqaj2vg4mphe7ffle.us-east-2.es.amazonaws.com
	10.08.2022 15:53:33. 172-05:00	Massen-Schreibvorgänge waren erfolgreich: 100 Dokumente

Containerisieren Sie Mainframe-Workloads, die von Blu Age modernisiert wurden

Erstellt von Richard Milner-Watts (AWS)

Übersicht

Dieses Muster bietet ein Beispiel für eine Container-Umgebung zum Ausführen von Mainframe-Workloads, die mithilfe des Blu Age-Tools modernisiert wurden. Blu Age konvertiert ältere Mainframe-Workloads in modernen Java-Code. Dieses Muster bietet einen Wrapper für die Java-Anwendung, sodass Sie sie mithilfe von Container-Orchestrierungsdiensten wie Amazon Elastic Container Service (Amazon ECS) oder Amazon Elastic Kubernetes Service (Amazon EKS) ausführen können.

Weitere Informationen zur Modernisierung Ihrer Workloads mithilfe von Blu Age- und AWS-Services finden Sie in den folgenden Publikationen zu AWS Prescriptive Guidance:

- Ausführung modernisierter Blu-Age-Mainframe-Workloads auf einer serverlosen AWS-Infrastruktur
- Stellen Sie mithilfe von Terraform eine Umgebung für containerisierte Blu Age-Anwendungen bereit

Wenn Sie Unterstützung bei der Nutzung von Blu Age zur Modernisierung Ihrer Mainframe-Workloads benötigen, wenden Sie sich an das Blu Age-Team, indem Sie auf der Blu Age-Website die Option Kontaktieren Sie unsere Experten auswählen. Wenn Sie Unterstützung bei der Migration Ihrer modernisierten Workloads zu AWS, ihrer Integration mit AWS-Services und ihrer Umstellung auf die Produktion benötigen, wenden Sie sich an Ihren AWS-Kundenbetreuer oder füllen Sie das AWS Professional Services-Formular aus.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine modernisierte Java-Anwendung, die von Blu Age erstellt wurde. Zu Testzwecken bietet dieses Muster eine Java-Beispielanwendung, die Sie als Machbarkeitsnachweis verwenden können.
- Eine Docker-Umgebung, mit der Sie den Container erstellen können.

Einschränkungen

Je nachdem, welche Container-Orchestrierungsplattform Sie verwenden, sind die Ressourcen, die dem Container zur Verfügung gestellt werden können (wie CPU, RAM und Speicher), möglicherweise

begrenzt. Wenn Sie beispielsweise Amazon ECS mit AWS Fargate verwenden, finden Sie in der Amazon ECS-Dokumentation Einschränkungen und Überlegungen.

Architektur

Quelltechnologie-Stack

- Blaues Zeitalter
- Java

Zieltechnologie-Stack

- Docker

Zielarchitektur

Das folgende Diagramm zeigt die Architektur der Blu Age-Anwendung in einem Docker-Container.

1. Der Einstiegspunkt für den Container ist das Wrapper-Skript. Dieses Bash-Skript ist dafür verantwortlich, die Laufzeitumgebung für die Blu Age-Anwendung vorzubereiten und die Ausgaben zu verarbeiten.
2. Umgebungsvariablen innerhalb des Containers werden verwendet, um Variablen im Wrapper-Skript zu konfigurieren, wie z. B. die Bucket-Namen und Datenbankanmeldeinformationen von Amazon Simple Storage Service (Amazon S3). Umgebungsvariablen werden entweder von AWS Secrets Manager oder Parameter Store, einer Funktion von AWS Systems Manager, bereitgestellt. Wenn Sie Amazon ECS als Container-Orchestrierungsservice verwenden, können Sie die Umgebungsvariablen auch in der Amazon ECS-Aufgabendefinition hartcodieren.
3. Das Wrapper-Skript ist dafür verantwortlich, alle Eingabedateien aus dem S3-Bucket in den Container zu ziehen, bevor Sie die Blu Age-Anwendung ausführen. Die AWS-Befehlszeilenschnittstelle (AWS CLI) ist im Container installiert. Dies bietet einen Mechanismus für den Zugriff auf Objekte, die in Amazon S3 gespeichert sind, über den Gateway-Endpunkt der Virtual Private Cloud (VPC).
4. Die Java-Archivdatei (JAR) für die Blu Age-Anwendung muss möglicherweise mit anderen Datenquellen wie Amazon Aurora kommunizieren.
5. Nach Abschluss liefert das Wrapper-Skript die resultierenden Ausgabedateien zur weiteren Verarbeitung (z. B. durch Amazon CloudWatch Logging Services) in einen S3-Bucket. Das Muster

unterstützt auch die Übermittlung komprimierter Protokolldateien an Amazon S3, wenn Sie eine Alternative zur CloudWatch Standardprotokollierung verwenden.

Tools

AWS-Services

- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Beenden und Verwalten von Containern in einem Cluster vereinfacht.

Tools

- Docker ist eine Softwareplattform zum Erstellen, Testen und Bereitstellen von Anwendungen. Docker packt Software in standardisierte Einheiten, sogenannte Container, die alles enthalten, was die Software zum Ausführen benötigt, einschließlich Bibliotheken, Systemtools, Code und Laufzeit. Sie können Docker verwenden, um Anwendungen in jeder Umgebung bereitzustellen und zu skalieren.
- Bash ist eine Befehlssprachenschnittstelle (Shell) für das GNU-Betriebssystem.
- Java ist die Programmiersprache und Entwicklungsumgebung, die in diesem Muster verwendet werden.
- Blu Age ist ein AWS-Mainframe-Modernisierungstool, das ältere Mainframe-Workloads, einschließlich Anwendungscode, Abhängigkeiten und Infrastruktur, in moderne Workloads für die Cloud umwandelt.

Code-Repository

Der Code für dieses Muster ist im GitHub Blu Age-Beispielcontainer-Repository verfügbar.

Bewährte Methoden

- Externalisieren Sie die Variablen, um das Verhalten Ihrer Anwendung mithilfe von Umgebungsvariablen zu ändern. Diese Variablen ermöglichen es der Container-Orchestrierungslösung, die Laufzeitumgebung zu ändern, ohne den Container neu erstellen zu

müssen. Dieses Muster enthält Beispiele für Umgebungsvariablen, die für Blu Age-Anwendungen nützlich sein können.

- Überprüfen Sie alle Anwendungsabhängigkeiten, bevor Sie Ihre Blu Age-Anwendung ausführen. Stellen Sie beispielsweise sicher, dass die Datenbank verfügbar und die Anmeldeinformationen gültig sind. Schreiben Sie Tests in das Wrapper-Skript, um Abhängigkeiten zu überprüfen, und schlagen Sie frühzeitig fehl, wenn sie nicht erfüllt werden.
- Verwenden Sie eine ausführliche Protokollierung innerhalb des Wrapper-Skripts. Die direkte Interaktion mit einem laufenden Container kann je nach Orchestrierungsplattform und Dauer der Aufgabe eine Herausforderung sein. Stellen Sie sicher, dass nützliche Informationen geschrieben werden, `STDOUT` um Probleme diagnostizieren zu können. Die Ausgabe kann beispielsweise den Inhalt des Arbeitsverzeichnisses der Anwendung sowohl vor als auch nach der Ausführung der Anwendung enthalten.

Epen

Besorgen Sie sich eine JAR-Datei für die Blu-Age-Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 1 — Arbeiten Sie mit Blu Age zusammen, um die JAR-Datei Ihrer Anwendung zu erhalten.	Der Container in diesem Muster erfordert eine Blu Age-Anwendung. Alternativ können Sie die Java-Beispielanwendung, die mit diesem Muster geliefert wird, für einen Prototyp verwenden. Arbeiten Sie mit dem Blu Age-Team zusammen, um eine JAR-Datei für Ihre Anwendung zu erhalten, die in den Container integriert werden kann. Wenn die JAR-Datei nicht verfügbar ist, lesen Sie die nächste Aufgabe,	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	um stattdessen die Beispiela nwendung zu verwenden.	
Option 2 — Erstellen oder verwenden Sie die mitgelief erte JAR-Datei der Beispiela nwendung.	Dieses Muster stellt eine vorgefertigte Beispiel-JAR-Datei bereit. Diese Datei gibt die Umgebungsvariablen der Anwendung an aus, `STDOUT` bevor sie 30 Sekunden lang in den Ruhemodus wechselt und dann beendet wird. Diese Datei hat einen Namen `bluAgeSample.jar` und befindet sich im Docker-Or dner des GitHub Repositorys. Wenn Sie den Code ändern und Ihre eigene Version der JAR-Datei erstellen möchten, verwenden Sie den Quellcode unter. /java_ sample/src/ sample _java_app.java im Repository. GitHub Sie können das Build-Skript unter verwenden. /java_sample/build .sh, um den Java-Quellcode zu kompilieren und eine neue JAR-Datei zu erstellen.	App-Developer

Erstellen Sie den Blue Age-Container

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das GitHub Repository.	Klonen Sie das Beispielcode-Repository mit dem folgenden Befehl: `git clone https://github.com/aws-samples/aws-blu-age-sample-container`	AWS DevOps
Verwenden Sie Docker, um den Container zu erstellen.	Verwenden Sie Docker, um den Container zu erstellen, bevor Sie ihn in eine Docker-Registry wie Amazon ECR übertragen: 1. Navigieren Sie von Ihrem ausgewählten Terminal aus zu dem `docker` Ordner in Ihrem lokalen Repository. GitHub 2. Verwenden Sie diesen Befehl, um den Container zu erstellen: `docker build -t <tag> .` wo `<tag>` ist der Container-Name, den Sie verwenden möchten.	AWS DevOps
Testen Sie den Blu Age-Container.	(Optional) Testen Sie den Container gegebenenfalls	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	lokal mit dem folgenden Befehl: `docker run -it <tag> / bin/bash`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Authentifizieren Sie sich bei Ihrem Docker-Repository.	Wenn Sie Amazon ECR verwenden möchten, folgen Sie den Anweisungen in der Amazon ECR-Dokumentation, um die AWS-CLI zu installieren und zu konfigurieren und die Docker-CLI bei Ihrer Standardregistrierung zu authentifizieren. Wir empfehlen Ihnen, den Befehl zur Authentifizierung zu verwenden. get-login-password **Note** Die Amazon ECR-Konsole bietet eine vorausgefüllte Version dieses Befehls, wenn Sie die Schaltfläche „Push-Befehle anzeigen“ verwenden. Weitere Informationen finden Sie in der Amazon ECR-Dokumentation. `aws ecr get-login -password --region <region> | docker login --username AWS --password-stdin <account>.dkr.ecr.`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`<region>.amazonaws.com` Wenn Sie Amazon ECR nicht verwenden möchten, folgen Sie den Anweisungen für Ihr Container-Registrierungssystem.	
Erstellen Sie ein Container-Repository.	Erstellen Sie ein Repository in Amazon ECR. Anweisungen finden Sie im Muster Bereitstellen einer Umgebung für containerisierte Blu Age-Anwendungen mithilfe von Terraform. Wenn Sie ein anderes Container-Registrierungssystem verwenden, folgen Sie den Anweisungen für dieses System.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Markieren Sie Ihren Container und übertragen Sie ihn in das Ziel-Repository.	Wenn Sie Amazon ECR verwenden:
	
	1. Kennzeichnen Sie das lokale Docker-Image mit der Amazon ECR-Registrierung und dem Repository, damit Sie es in Ihr Remote-Repository übertragen können:
	
	`docker tag <tag>:latest <account>.dkr.ecr.<region>.amazonaws.com/<repository>:<versionNumber>`
	
	2. Übertragen Sie das Image in das Remote-Repository:
	
	`docker push <account>.dkr.ecr.<region>.amazonaws.com/<repository>:<versionNumber>`
	
	Weitere Informationen finden Sie unter Pushing a Docker-Image im Amazon ECR-Benutzerhandbuch.
		AWS DevOps

Zugehörige Ressourcen

AWS-Ressourcen

- AWS Blu Age Age-Probencontainer-Repository

- Ausführung modernisierter Blu-Age-Mainframe-Workloads auf einer serverlosen AWS-Infrastruktur
- Stellen Sie mithilfe von Terraform eine Umgebung für containerisierte Blu Age-Anwendungen bereit
- Verwenden von Amazon ECR mit der AWS-CLI (Amazon ECR-Benutzerhandbuch)
- Authentifizierung in privaten Registern (Amazon ECR-Benutzerhandbuch)
- Amazon ECS-Dokumentation
- Amazon EKS-Dokumentation

Weitere Ressourcen

- Blu Age-Webseite
- Docker-Webseite

EBCDIC-Daten mithilfe von Python in ASCII auf AWS konvertieren und entpacken

Erstellt von Luis Gustavo Dantas (AWS)

Übersicht

Da Mainframes in der Regel wichtige Geschäftsdaten hosten, ist die Modernisierung von Daten eine der wichtigsten Aufgaben bei der Migration von Daten in die Amazon Web Services (AWS) -Cloud oder eine andere American Standard Code for Information Interchange (ASCII) -Umgebung. Auf Mainframes werden Daten in der Regel im EBCDIC-Format (Extended Binary-Coded Decimal Interchange Code) codiert. Beim Exportieren von Datenbank-, Virtual Storage Access Method-(VSAM) oder Flatfiles werden im Allgemeinen gepackte, binäre EBCDIC-Dateien erzeugt, deren Migration komplexer ist. Die am häufigsten verwendete Lösung für die Datenbankmigration ist Change Data Capture (CDC), bei der in den meisten Fällen die Datenkodierung automatisch konvertiert wird. CDC-Mechanismen sind jedoch möglicherweise nicht für diese Datenbank-, VSAM-oder Flatfiles verfügbar. Für diese Dateien ist ein alternativer Ansatz zur Modernisierung der Daten erforderlich.

Dieses Muster beschreibt, wie EBCDIC-Daten modernisiert werden, indem sie in das ASCII-Format konvertiert werden. Nach der Konvertierung können Sie die Daten in verteilte Datenbanken laden oder Anwendungen in der Cloud die Daten direkt verarbeiten lassen. Das Muster verwendet das Konvertierungsskript und die Beispieldateien im mainframe-data-utilities GitHub Repository.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine EBCDIC-Eingabedatei und das dazugehörige COBOL-Copybook (Common Business-Oriented Language). Eine EBCDIC-Beispieldatei und ein COBOL-Copybook sind im Repository enthalten. mainframe-data-utilities GitHub Weitere Informationen zu COBOL-Copybooks finden Sie im Enterprise COBOL for z/OS 6.4 Programming Guide auf der IBM-Website.

Einschränkungen

- In COBOL-Programmen definierte Datei-Layouts werden nicht unterstützt. Sie müssen separat zur Verfügung gestellt werden.

Produktversionen

- Python-Version 3.8 oder höher

Architektur

Quelltechnologie-Stack

- EBCDIC-Daten auf einem Mainframe
- COBOL-Copybook

Zieltechnologie-Stack

- Amazon Elastic Compute Cloud (Amazon EC2) -Instanz in einer virtuellen privaten Cloud (VPC)
- Amazon Elastic Block Store (Amazon EBS)
- Python und die erforderlichen Pakete, JavaScript Object Notation (JSON), sys und datetime
- ASCII-Flatdatei, die bereit ist, von einer modernen Anwendung gelesen oder in eine relationale Datenbanktabelle geladen zu werden

Zielarchitektur

Das Architekturdiagramm zeigt den Prozess der Konvertierung einer EBCDIC-Datei in eine ASCII-Datei auf einer Instanz: EC2

1. Mithilfe des Skripts parse_copybook_to_json.py konvertieren Sie das COBOL-Copybook in eine JSON-Datei.
2. Mithilfe der JSON-Datei und des Skripts extract_ebcdic_to_ascii.py konvertieren Sie die EBCDIC-Daten in eine ASCII-Datei.

Automatisierung und Skalierung

Sobald die für die ersten manuellen Dateikonvertierungen benötigten Ressourcen vorhanden sind, können Sie die Dateikonvertierung automatisieren. Dieses Muster enthält keine Anweisungen zur Automatisierung. Es gibt mehrere Möglichkeiten, die Konvertierung zu automatisieren. Im Folgenden finden Sie einen Überblick über einen möglichen Ansatz:

1. Kapseln Sie die AWS-Befehlszeilenschnittstelle (AWS CLI) und die Python-Skriptbefehle in ein Shell-Skript.
2. Erstellen Sie eine AWS-Lambda-Funktion, die den Shell-Skriptjob asynchron an eine Instance weiterleitet. EC2 Weitere Informationen finden Sie unter SSH-Jobs mit AWS Lambda planen.
3. Erstellen Sie einen Amazon Simple Storage Service (Amazon S3) -Trigger, der die Lambda-Funktion jedes Mal aufruft, wenn eine Legacy-Datei hochgeladen wird. Weitere Informationen finden Sie unter Verwenden eines Amazon S3 S3-Triggers zum Aufrufen einer Lambda-Funktion.

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server starten, wie Sie benötigen, und diese schnell nach oben oder unten skalieren.
- Amazon Elastic Block Store (Amazon EBS) bietet Speichervolumes auf Blockebene zur Verwendung mit Amazon Elastic Compute Cloud (Amazon EC2) -Instances.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.

Andere Tools

- GitHubist ein Code-Hosting-Dienst, der Tools für die Zusammenarbeit und Versionskontrolle bereitstellt.
- Python ist eine Programmiersprache auf hohem Niveau.

Code-Repository

Der Code für dieses Muster ist im mainframe-data-utilities GitHub Repository verfügbar.

Epen

Bereite die Instanz vor EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie eine EC2 Instanz.	Die EC2 Instance muss über ausgehenden Internetzugang verfügen. Dadurch kann die Instanz auf den Python-Qu ellcode zugreifen, der auf verfügbar ist GitHub. Um die Instanz zu erstellen: 1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2. 2. Starten Sie eine EC2 Linux-Instance. Verwenden Sie eine öffentliche IP-Adresse und erlauben Sie eingehend en Zugriff über Port 22. Stellen Sie sicher, dass die Speichergröße der Instanz mindestens doppelt so groß ist wie die EBCDIC-Datendatei. Anweisung en finden Sie in der EC2 Amazon-Dokumentation.	Allgemeines AWS
Installieren Sie Git.	1. Stellen Sie mithilfe eines Secure Shell (SSH) -Clients eine Verbindung zu der EC2 Instance her, die Sie gerade gestartet haben. Weitere Informationen	Allgemein AWS, Linux

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	finden Sie unter Connect zu Ihrer Linux-Instance herstellen.
	2. Führen Sie in der EC2 Amazon-Konsole den folgenden Befehl aus. Dadurch wird Git auf der EC2 Instanz installiert.
	`sudo yum install git`
	3. Führen Sie den folgenden Befehl aus und vergewissern Sie sich, dass Git erfolgreich installiert wurde.
	`git --version`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie Python.	1. Führen Sie in der EC2 Amazon-Konsole den folgenden Befehl aus. Dadurch wird Python auf der EC2 Instanz installiert.
	`sudo yum install python3`
	2. Führen Sie in der EC2 Amazon-Konsole den folgenden Befehl aus. Dadurch wird Pip3 auf der EC2 Instance installiert.
	`sudo yum install python3-pip`
	3. Führen Sie in der EC2 Amazon-Konsole den folgenden Befehl aus. Dadurch wird das AWS-SDK SDK for Python (Boto3) auf der EC2 Instance installiert.
	`sudo pip3 install boto3`
	4. Führen Sie in der EC2 Amazon-Konsole den folgenden Befehl aus, in dem `<us-east-1>` sich der Code für Ihre AWS-Region befindet. Eine vollständige Liste
		Allgemein AWS, Linux

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Regionscodes finden Sie in der EC2 Amazon-Dokumentation unter Verfügbare Regionen. `export AWS_DEFAULT_REGION=<us-east-1>`	
Klonen Sie das GitHub Repository.	1. Führen Sie in der EC2 Amazon-Konsole den folgenden Befehl aus. Dadurch wird das mainframe-data-utilitiesRepository aus dem home Ordner geklont GitHub und der standardmäßige Speicherort für Kopien geöffnet. `git clone https://github.com/aws-samples/mainframe-data-utilities.git` 2. Vergewissern Sie sichhome, dass der `mainframe-data-utilities` Ordner in dem Ordner vorhanden ist.	Allgemeines AWS, GitHub

Erstellen Sie die ASCII-Datei aus den EBCDIC-Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie das COBOL-Copybook in die JSON-Layoutdatei.	Führen Sie innerhalb des **`mainframe-data-utilities`** Ordners das Skript parse_copybook_to_json.py aus. Dieses Automatisierungsmodul liest das Datei-Layout aus einem COBOL-Copybook und erstellt eine JSON-Datei. Die JSON-Datei enthält die Informationen, die zum Interpretieren und Extrahieren der Daten aus der Quelldatei erforderlich sind. Dadurch werden die JSON-Metadaten aus dem COBOL-Copybook erstellt. Der folgende Befehl konvertiert das COBOL-Copybook in eine JSON-Datei. `python3 parse_copybook_to_json.py \ -copybook LegacyReference/COBPACK2.cpy \ -output sample-data/cobpack2-list.json \ -dict sample-data/cobpack2-dict.json \ -ebcdic sample-data/COBPACK.OUTFILE.txt \ -ascii sample-data/COBPACK.ASCII.txt \ -print 10000`	Allgemein AWS, Linux

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Das Skript druckt die empfangenen Argumente.
	
	`----------`
	`----------`
	`----------`
	`----------`
	`Copybook file.....`
	`.....| LegacyRef`
	`erence/COBPACK2.cpy`
	`Parsed copybook (JSON`
	` List).| sample-data/`
	`cobpack2-list.json`
	`JSON Dict (document`
	`ation)...| sample-da`
	`ta/cobpack2-dict.json`
	`ASCII file.....`
	`.....| sample-`
	`data/COBPACK.ASCII.t`
	`xt`
	`EBCDIC file.....`
	`.....| sample-`
	`data/COBPACK.OUTFILE`
	`.txt`
	`Print each.....`
	`.....| 10000`
	`----------`
	`----------`
	`----------`
	`----------`
	
	Weitere Informationen zu den Argumenten finden Sie in der README-Datei im GitHub Repository.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Untersuchen Sie die JSON-Layoutdatei.	1. Navigieren Sie zu dem im Skript parse_copybook_to_json.py definierten Ausgabepfad. 2. Überprüfen Sie die Erstellungszeit der Datei sample-data/cobpack2-list.json, um sicherzustellen, dass Sie die entsprechende JSON-Layoutdatei ausgewählt haben. 3. Untersuchen Sie die JSON-Datei und stellen Sie sicher, dass der Inhalt dem Folgenden ähnelt. `"input": "extract-ebcdic-to-ascii/COBPACK.OUTFILE.txt", "output": "extract-ebcdic-to-ascii/COBPACK.ASCII.txt", "max": 0, "skip": 0, "print": 10000, "lrecl": 150, "rem-low-values": true, "separator": "|", "transf": [ { "type": "ch", "bytes": 19, "name": "OUTFILE-TEXT" }`	Allgemein AWS, JSON

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Die wichtigsten Attribute der JSON-Layoutdatei sind: • `input`— Enthält den Pfad der zu konvertierenden EBCDIC-Datei • `output`— Definiert den Pfad, in dem die ASCII-Datei generiert wird • `lrecl`— Gibt die Größe der logischen Datensatzlänge in Byte an • `transf`— Listet alle Felder und ihre Größe in Byte auf Weitere Informationen zur JSON-Layoutdatei finden Sie in der README-Datei im GitHub Repository.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie die ASCII-Datei.	Führen Sie das Skript extract_ebcdic_to_ascii.py aus, das im GitHub geklonten Repository enthalten ist. Dieses Skript liest die EBCDIC-Datei und schreibt eine konvertierte und lesbare ASCII-Datei.
	`python3 extract_ebcdic_to_ascii.py -local-json sample-data/cobpack2-list.json`
	Während das Skript die EBCDIC-Daten verarbeitet, druckt es für jeden Stapel von 10.000 Datensätzen eine Nachricht. Sehen Sie sich das folgende Beispiel an.
	`---------- 2023-05-15 21:21:46.322253 | Local Json file | -local-json | sample-data/cobpack2-list.json 2023-05-15 21:21:47.034556 | Records processed | 10000 2023-05-15 21:21:47.736434 | Records processed | 20000`
		Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2023-05-15 21:21:48. 441696 | Records processed | 30000 2023-05-15 21:21:49. 173781 | Records processed | 40000 2023-05-15 21:21:49. 874779 | Records processed | 50000 2023-05-15 21:21:50. 705873 | Records processed | 60000 2023-05-15 21:21:51. 609335 | Records processed | 70000 2023-05-15 21:21:52. 292989 | Records processed | 80000 2023-05-15 21:21:52. 938366 | Records processed | 89280 2023-05-15 21:21:52. 938448 Seconds 6.616232 Informationen zum Ändern der Druckfrequenz finden Sie in der README-Datei im Repository. GitHub	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Untersuchen Sie die ASCII-Datei.	1. Überprüfen Sie die Erstellungszeit der Datei extract-ebcdic-to-ascii/CobPack.ASCII.txt, um sicherzustellen, dass sie kürzlich erstellt wurde. 2. Geben Sie in der EC2 Amazon-Konsole den folgenden Befehl ein. Dadurch wird der erste Datensatz der ASCII-Datei geöffnet. `head sample-data/COBPACK.ASCII.txt -n 1| xxd` 3. Untersuchen Sie den Inhalt des ersten Datensatzes. Da EBCDIC-Dateien normalerweise binär sind, enthalten sie keine CRLF-Sonderzeichen (Carriage Return and Line Feed). Das Skript extract_ebcdic_to_ascii.py fügt ein Pipezeichen als Spaltentrennzeichen hinzu, das in den Skriptparametern definiert ist. Wenn Sie die bereitgestellte EBCDIC-Beispieldatei verwendet haben, ist der folgende Datensatz der erste Datensatz in der ASCII-Datei.	Allgemein AWS, Linux

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	00000000: 2d30 3030 3030 3030 3030 3130 3030 3030 -000000000100000 00000010: 3030 307c 3030 3030 3030 3030 3031 3030 000|00000 0000100 00000020: 3030 3030 3030 7c2d 3030 3030 3030 3030 000000|-0 0000000 00000030: 3031 3030 3030 3030 3030 7c30 7c30 7c31 0100000000| 0|0|1 00000040: 3030 3030 3030 3030 7c2d 3130 3030 3030 00000000| -100000 00000050: 3030 307c 3130 3030 3030 3030 307c 2d31 000|10000 0000|-1 00000060: 3030 3030 3030 3030 7c30 3030 3030 7c30 00000000| 00000|0 00000070: 3030 3030 7c31 3030 3030 3030 3030 7c2d 0000|1000 00000|- 00000080: 3130 3030 3030 3030 307c 3030 3030 3030 100000000| 000000 00000090: 3030 3030 3130 3030 3030 3030 307c 2d30 000010000 0000|-0 000000a0: 3030 3030 3030 3030 3031 3030	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3030 3030 000000000 1000000 000000b0: 3030 7c41 7c41 7c0a 00|A|A|.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Evaluieren Sie die EBCDIC-Datei.	Geben Sie in der EC2 Amazon-Konsole den folgenden Befehl ein. Dadurch wird der erste Datensatz der EBCDIC-Datei geöffnet. `head sample-data/COBPACK.OUTFILE.txt -c 150 | xxd` Wenn Sie die EBCDIC-Beispieldatei verwendet haben, ist das Ergebnis wie folgt. `00000000: 60f0 f0f0 f0f0 f0f0 f0f0 f0f0 f1f0 f0f0 f0f0 `........ .... 00000010: f0f0 f0f0 f0f0 f0f0 f0f0 f0f0 f1f0 f0f0 .... 00000020: f0f0 f0f0 f0f0 f0f0 f0f0 f0f0 f0f0 f1f0 .... 00000030: f0f0 f0f0 f0f0 d000 0000 0005 f5e1 00fa .... 00000040: 0a1f 0000 0000 0005 f5e1 00ff ffff fffa .... 00000050: 0a1f 0000 000f 0000 0c10 0000 000f 1000 ....`	Allgemein AWS, Linux, EBCDIC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	00000060: 0000 0d00 0000 0000 1000 0000 0f00 0000 .... 00000070: 0000 1000 0000 0dc1 c100 0000 0000 0000 .... 00000080: 0000 0000 0000 0000 0000 0000 0000 0000 .... 00000090: 0000 0000 0000 ...... Um die Gleichwertigkeit zwischen den Quell- und Zieldateien zu bewerten, sind umfassende Kenntnisse über EBCDIC erforderlich. Das erste Zeichen der EBCDIC-Beispieldatei ist beispielsweise ein Bindestrich (). - In der hexadezimalen Schreibweise der EBCDIC-Datei wird dieses Zeichen durch dargestellt60, und in der hexadezimalen Schreibweise der ASCII-Datei wird dieses Zeichen durch dargestellt. 2D Eine EBCDIC-to-ASCII Umrechnungstabelle finden Sie auf der IBM-Website unter EBCDIC zu ASCII.	

Zugehörige Ressourcen

Referenzen

- Der EBCDIC-Zeichensatz (IBM-Dokumentation)
- EBCDIC zu ASCII (IBM-Dokumentation)
- COBOL (IBM-Dokumentation)
- Grundlegende JCL-Konzepte (IBM-Dokumentation)
- Connect zu Ihrer Linux-Instance her (EC2 Amazon-Dokumentation)

Tutorials

- Planung von SSH-Jobs mit AWS Lambda (AWS-Blogbeitrag)
- Verwenden eines Amazon S3 S3-Triggers zum Aufrufen einer Lambda-Funktion (AWS Lambda Lambda-Dokumentation)

Konvertieren Sie Mainframe-Dateien mithilfe von AWS Lambda vom EBCDIC-Format in das durch Zeichen getrennte ASCII-Format in Amazon S3

Erstellt von Luis Gustavo Dantas (AWS)

Übersicht

Dieses Muster zeigt Ihnen, wie Sie eine AWS Lambda Lambda-Funktion starten, die Mainframe-EBCDIC-Dateien (Extended Binary Coded Decimal Interchange Code) automatisch in durch Zeichen getrennte ASCII-Dateien (American Standard Code for Information Interchange) konvertiert. Die Lambda-Funktion wird ausgeführt, nachdem die ASCII-Dateien in einen Amazon Simple Storage Service (Amazon S3) -Bucket hochgeladen wurden. Nach der Dateikonvertierung können Sie die ASCII-Dateien auf x86-basierten Workloads lesen oder die Dateien in moderne Datenbanken laden.

Der in diesem Muster vorgestellte Ansatz zur Dateikonvertierung kann Ihnen helfen, die Herausforderungen bei der Arbeit mit EBCDIC-Dateien in modernen Umgebungen zu bewältigen. In EBCDIC kodierte Dateien enthalten häufig Daten, die in einem binären oder komprimierten Dezimalformat dargestellt werden, und Felder haben eine feste Länge. Diese Eigenschaften stellen Hindernisse dar, da moderne x86-basierte Workloads oder verteilte Umgebungen im Allgemeinen mit ASCII-kodierten Daten arbeiten und EBCDIC-Dateien nicht verarbeiten können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein S3-Bucket
- Ein Benutzer von AWS Identity and Access Management (IAM) mit Administratorberechtigungen
- AWS CloudShell
- Python 3.8.0 oder höher
- Eine in EBCDIC kodierte Flatfile und die dazugehörige Datenstruktur in einem COBOL-Copybook (Common Business Oriented Language)

> **Note**
>
> Dieses Muster verwendet eine EBCDIC-Beispieldatei (Client.EBCDIC.txt) und das entsprechende COBOL-Copybook (COBKS05.cpy). Beide GitHub mainframe-data-utilitiesDateien sind im Repository verfügbar.

Einschränkungen

- COBOL-Copybooks enthalten normalerweise mehrere Layoutdefinitionen. Das mainframe-data-utilitiesProjekt kann diese Art von Copybook analysieren, kann aber nicht ableiten, welches Layout bei der Datenkonvertierung berücksichtigt werden soll. Das liegt daran, dass Copybooks diese Logik nicht verwenden (die stattdessen bei COBOL-Programmen verbleibt). Folglich müssen Sie die Regeln für die Auswahl von Layouts manuell konfigurieren, nachdem Sie das Copybook analysiert haben.
- Dieses Muster unterliegt Lambda-Quoten.

Architektur

Quelltechnologie-Stack

- IBM z/OS, IBM i und andere EBCDIC-Systeme
- Sequentielle Dateien mit in EBCDIC codierten Daten (z. B. IBM Db2-Entladungen)
- COBOL-Copybook

Zieltechnologie-Stack

- Amazon S3
- Amazon S3 S3-Ereignisbenachrichtigung
- IAM
- Lambda-Funktion
- Python 3.8 oder höher
- Mainframe-Datendienstprogramme
- JSON-Metadaten
- ASCII-Dateien, die durch Zeichen getrennt sind

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur für die Konvertierung von Mainframe-EBCDIC-Dateien in ASCII-Dateien.

Das Diagramm zeigt den folgenden Workflow:

1. Der Benutzer führt das Copybook-Parser-Skript aus, um das COBOL-Copybook in eine JSON-Datei zu konvertieren.
2. Der Benutzer lädt die JSON-Metadaten in einen S3-Bucket hoch. Dadurch werden die Metadaten von der Lambda-Funktion zur Datenkonvertierung lesbar.
3. Der Benutzer oder ein automatisierter Prozess lädt die EBCDIC-Datei in den S3-Bucket hoch.
4. Das S3-Benachrichtigungsereignis löst die Lambda-Funktion zur Datenkonvertierung aus.
5. AWS überprüft die Lese- und Schreibberechtigungen des S3-Buckets für die Lambda-Funktion.
6. Lambda liest die Datei aus dem S3-Bucket und konvertiert die Datei lokal von EBCDIC nach ASCII.
7. Lambda protokolliert den Prozessstatus in Amazon CloudWatch.
8. Lambda schreibt die ASCII-Datei zurück nach Amazon S3.

> **Note**
>
> Das Copybook-Parser-Skript wird nur einmal ausgeführt, nachdem es die Metadaten in JSON konvertiert und diese Daten dann in einen S3-Bucket hochgeladen hat. Nach der ersten Konvertierung verwendet jede EBCDIC-Datei, die dieselbe JSON-Datei verwendet, die in den S3-Bucket hochgeladen wurde, dieselben Metadaten.

Tools

AWS-Tools

- Amazon CloudWatch hilft Ihnen dabei, die Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie auf AWS ausführen, in Echtzeit zu überwachen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

- AWS CloudShell ist eine browserbasierte Shell, mit der Sie AWS-Services mithilfe der AWS-Befehlszeilenschnittstelle (AWS CLI) und einer Reihe vorinstallierter Entwicklungstools verwalten können.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.

Andere Tools

- GitHubist ein Code-Hosting-Dienst, der Tools für die Zusammenarbeit und Versionskontrolle bereitstellt.
- Python ist eine Programmiersprache auf hohem Niveau.

Code

Der Code für dieses Muster ist im GitHub mainframe-data-utilitiesRepository verfügbar.

Bewährte Methoden

Beachten Sie die folgenden bewährten Methoden:

- Legen Sie die erforderlichen Berechtigungen auf der Ebene des Amazon-Ressourcennamens (ARN) fest.
- Gewähren Sie immer Berechtigungen mit den geringsten Rechten für IAM-Richtlinien. Weitere Informationen finden Sie in der IAM-Dokumentation unter Bewährte Sicherheitsmethoden in IAM.

Epen

Erstellen Sie Umgebungsvariablen und einen Arbeitsordner

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Umgebungs variablen.	Kopieren Sie die folgenden Umgebungsvariablen in einen	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Texteditor und ersetzen Sie dann die <placeholder>Werte im folgenden Beispiel durch Ihre Ressourcenwerte:
	
	`bucket=<your_bucket_name>`
	`account=<your_account_number>`
	`region=<your_region_code>`
	
	Note
	Sie werden später Verweise auf Ihren S3-Bucket, Ihr AWS-Konto und Ihre AWS-Region erstellen.
	
	Um Umgebungsvariablen zu definieren, öffnen Sie die CloudShell Konsole und kopieren Sie dann Ihre aktualisierten Umgebungsvariablen und fügen Sie sie in die Befehlszeile ein.
	
	Note
	Sie müssen diesen Schritt bei jedem Neustart der	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CloudShell Sitzung wiederholen.	
Erstellen Sie einen Arbeitsordner.	Um die spätere Bereinigung von Ressourcen zu vereinfachen, erstellen Sie einen Arbeitsordner in, CloudShell indem Sie den folgenden Befehl ausführen: `mkdir workdir; cd workdir` **Note** Sie müssen jedes Mal, wenn Sie die Verbindung zu Ihrer CloudShell Sitzung verlieren, das Verzeichnis in das Arbeitsverzeichnis (`workdir`) ändern.	Allgemeines AWS

Definieren Sie eine IAM-Rolle und -Richtlinie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Vertrauensrichtlinie für die Lambda-Funktion.	Der EBCDIC-Konverter läuft in einer Lambda-Funktion. Die Funktion muss eine IAM-Rolle haben. Bevor Sie die IAM-Rolle erstellen	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	, müssen Sie ein Dokument mit einer Vertrauensrichtlinie definieren, das es Ressourcen ermöglicht, diese Richtlinie zu übernehmen.
	
	Erstellen Sie im CloudShel l Arbeitsordner ein Richtlini endokument, indem Sie den folgenden Befehl ausführen:
	
	`E2ATrustPol=$(cat <<EOF`
	`{`
	`"Version":`
	`"2012-10-17",`
	`"Statement": [`
	`{`
	`"Effect":`
	`"Allow",`
	`"Principa`
	`l": {`
	
	`"Service": "lambda.a`
	`mazonaws.com"`
	`},`
	`"Action":`
	`"sts:AssumeRole"`
	`}`
	`]`
	`}`
	`EOF`
	`)`
	`printf "$E2ATrustPol" >`
	`E2ATrustPol.json`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Rolle für die Lambda-Konvertierung.	Um eine IAM-Rolle zu erstellen, führen Sie den folgenden AWS-CLI-Befehl im CloudShell Arbeitsordner aus: `aws iam create-role --role-name E2AConvLambdaRole --assume-role-policy-document file://E2ATrustPol.json`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie das IAM-Richtliniendokument für die Lambda-Funktion.	Die Lambda-Funktion muss Lese- und Schreibzugriff auf den S3-Bucket und Schreibbe rechtigungen für Amazon Logs haben. CloudWatch
	
	Um eine IAM-Richtlinie zu erstellen, führen Sie den folgenden Befehl im Arbeitsor dner aus: CloudShell
	
	`E2APolicy=$(cat <<EOF`
	`{`
	`"Version": "2012-10-17",`
	`"Statement": [`
	`{`
	`"Sid": "Logs",`
	`"Effect": "Allow",`
	`"Action": [`
	`"logs:PutLogEvents",`
	`"logs:CreateLogStream",`
	`"logs:CreateLogGroup"`
	`],`
	`"Resource": [`
	`"arn:aws:logs:*:*:log-group:*",`
	`"arn:aws:logs:*:*:log-group:*:log-stream:*"`
	`]
		Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

```
        },
        {
            "Sid": "S3",
            "Effect":
 "Allow",
            "Action": [

 "s3:GetObject",

 "s3:PutObject",

 "s3:GetObjectVersion"
            ],
            "Resource":
 [

 "arn:aws:s3:::%s/*",

 "arn:aws:s3:::%s"
            ]
        }
    ]
}
EOF
)
printf "$E2APolicy"
 "$bucket" "$bucket"
 > E2AConvLambdaPolic
y.json
```

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Hängen Sie das IAM-Richt liniendokument an die IAM-Rolle an.	Um die IAM-Richtlinie an die IAM-Rolle anzuhängen, führen Sie den folgenden Befehl in Ihrem Arbeitsordner aus: CloudShell `aws iam put-role-policy --role-name E2AConvLambdaRole --policy-name E2AConvLambdaPolicy --policy-document file://E2AConvLambdaPolicy.json`	Allgemeines AWS

Erstellen Sie die Lambda-Funktion für die EBCDIC-Konvertierung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Quellcode für die EBCDIC-Konvertierung herunter.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um den mainframe-data-utilities Quellcode herunterzuladen: GitHub `git clone https://github.com/aws-samples/mainframe-data-utilities.git mdu`	Allgemeines AWS
Erstellen Sie das ZIP-Paket.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um das ZIP-Paket zu erstellen, das die Lambda-Funktion für die EBCDIC-Konvertierung erstellt:	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cd mdu; zip ../mdu.zip *.py; cd ..`	
So erstellen Sie die Lambda-Funktion:	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um die Lambda-Funktion für die EBCDIC-Konvertierung zu erstellen: `aws lambda create-function \ --function-name E2A \ --runtime python3.9 \ --zip-file fileb://mdu.zip \ --handler extract_ebcdic_to_ascii.lambda_handler \ --role arn:aws:iam::$account:role/E2AConvLambdaRole \ --timeout 10 \ --environment "Variables={layout=$bucket/layout/}"` **Note** Das Layout der Umgebungsvariablen teilt der Lambda-Funktion mit, wo sich die JSON-Metadaten befinden.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die ressourcenbasierte Richtlinie für die Lambda-Funktion.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, damit Ihre Amazon S3 S3-Ereignisbenachrichtigung die Lambda-Funktion für die EBCDIC-Konvertierung auslöst: `aws lambda add-permission \ --function-name E2A \ --action lambda:InvokeFunction \ --principal s3.amazonaws.com \ --source-arn arn:aws:s3:::$bucket \ --source-account $account \ --statement-id 1`	Allgemeines AWS

Erstellen Sie die Amazon S3 S3-Ereignisbenachrichtigung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Konfigurationsdokument für die Amazon S3 S3-Ereignisbenachrichtigung.	Die Amazon S3 S3-Ereignisbenachrichtigung initiiert die Lambda-Funktion für die EBCDIC-Konvertierung, wenn Dateien im Eingabeordner platziert werden. Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um das JSON-Dokument für die Amazon S3	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	S3-Ereignisbenachrichtigung zu erstellen: `{ "LambdaFunctionConfigurations": [{ "Id": "E2A", "LambdaFunctionArn": "arn:aws:lambda:%s:%s:function:E2A", "Events": ["s3:ObjectCreated:Put"], "Filter": { "Key": { "FilterRules": [{ "Name": "prefix", "Value": "input/" }] } } }] } EOF) printf "$S3E2AEvent" "$region" "$account" > S3E2AEvent.json`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Amazon S3 S3-Ereignisbenachrichtigung.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um die Amazon S3 S3-Ereignisbenachr ichtigung zu erstellen: `aws s3api put-bucke t-notification-con figuration --bucket  $bucket --notific ation-configuratio n file://S3E2AEvent. json`	Allgemeines AWS

Erstellen Sie die JSON-Metadaten und laden Sie sie hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie das COBOL-Copybook.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um ein COBOL-Beispiel-Copybook in eine JSON-Datei zu parsen (die definiert, wie die Datendatei richtig gelesen und aufgeteilt wird): `python3 mdu/parse _copybook_to_json.py  \ -copybook mdu/Legac yReference/COBKS05 .cpy \ -output CLIENT.js on \`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`-output-s3key CLIENT.ASCII.txt \`
	`-output-s3bkt $bucket \`
	`-output-type s3 \`
	`-print 25`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Fügen Sie die Transformationsregel hinzu.	Bei der Beispieldatendatei und dem entsprechenden COBOL-Copybook handelt es sich um eine Datei mit mehreren Layouts. Das bedeutet, dass bei der Konvertierung Daten nach bestimmten Regeln aufgeteilt werden müssen. In diesem Fall definieren die Bytes an den Positionen 3 und 4 in jeder Zeile das Layout.
	
	Bearbeiten Sie die `CLIENT.json` Datei im CloudShell Arbeitsordner und ändern Sie `"transf-rule": [],` den Inhalt wie folgt:
	
	`"transf-rule": [`
	`{`
	`"offset": 4,`
	`"size": 2,`
	`"hex": "0002",`
	`"transf": "transf1"`
	`},`
	`{`
	`"offset": 4,`
	`"size": 2,`
	`"hex": "0000",`
	`"transf": "transf2"`
	`}`
	`],`
		Allgemein AWS, IBM Mainframe, Cobol

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die JSON-Meta daten in den S3-Bucket hoch.	Führen Sie im CloudShell Arbeitsordner den folgenden AWS-CLI-Befehl aus, um die JSON-Metadaten in Ihren S3-Bucket hochzuladen: `aws s3 cp CLIENT.json s3://$bucket/layout/CLIENT.json`	Allgemeines AWS

Konvertieren Sie die EBCDIC-Datei

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie die EBCDIC-Datei an den S3-Bucket.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um die EBCDIC-Datei an den S3-Bucket zu senden: `aws s3 cp mdu/sample-data/CLIENT.EBCDIC.txt s3://$bucket/input/` **Note** Wir empfehlen, unterschiedliche Ordner für Eingabe- (EBCDIC) und Ausgabedateien (ASCII) festzulegen, um zu vermeiden, dass die Lambda-	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Konvertierungsfunktion erneut aufgerufen wird, wenn die ASCII-Datei in den S3-Bucket hochgeladen wird.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Ausgabe.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um zu überprüfen, ob die ASCII-Datei in Ihrem S3-Bucket generiert wurde:
	`awss3 ls s3://$bucket/`
	Note
	Die Datenkonvertierung kann mehrere Sekunden dauern. Wir empfehlen Ihnen, einige Male nach der ASCII-Datei zu suchen.
	Wenn die ASCII-Datei verfügbar ist, führen Sie den folgenden Befehl aus, um die Datei aus dem S3-Bucket in den aktuellen Ordner herunterzuladen:
	`aws s3 cp s3://$bucket/ CLIENT.ASCII.txt .`
	Überprüfen Sie den Inhalt der ASCII-Datei:
	`head CLIENT.ASCII.txt`
		Allgemeines AWS

Säubere die Umwelt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

(Optional) Bereiten Sie die Variablen und den Ordner vor.	Wenn Sie die Verbindung mit verlieren CloudShell, stellen Sie die Verbindung erneut her und führen Sie dann den folgenden Befehl aus, um das Verzeichnis in den Arbeitsordner zu ändern:
	`cd workdir`
	Stellen Sie sicher, dass die Umgebungsvariablen definiert sind:
	`bucket=<your_bucket_name>`
	`account=<your_account_number>`
	`region=<your_region_code>`
		Allgemeines AWS

Entfernen Sie die Benachrichtigungskonfiguration für den Bucket.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um die Konfiguration der Amazon S3 S3-Ereignisbenachrichtigung zu entfernen:
	`aws s3api put-bucket-notification-configuration \`
	`--bucket=$bucket \`
	`--notification-configuration="{}"`
		Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die Lambda-Funktion.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um die Lambda-Funktion für den EBCDIC-Konverter zu löschen: `awslambdadelete-function--function-nameE2A`	Allgemeines AWS

Löschen Sie die IAM-Rolle und -Richtlinie.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um die EBCDIC-Konverterrolle und -Richtlinie zu entfernen:
	`aws iam delete-role-policy --role-name E2AConvLambdaRole --policy-name E2AConvLambdaPolicy`
	
	`aws iam delete-role --role-name E2AConvLambdaRole`
		Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Löschen Sie die im S3-Bucket generierten Dateien.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um die im S3-Bucket generierten Dateien zu löschen:
	`aws s3 rm s3://$bucket/layout --recursive`
	`aws s3 rm s3://$bucket/input --recursive`
	`aws s3 rm s3://$bucket/CLIENT.ASCII.txt`
		Allgemeines AWS

Löschen Sie den Arbeitsordner.	Führen Sie im CloudShell Arbeitsordner den folgenden Befehl aus, um ihn `workdir` und seinen Inhalt zu entfernen: `cd ..; rm -Rf workdir`	Allgemeines AWS

Zugehörige Ressourcen

- README () für Mainframe-Datendienstprogramme GitHub
- Der EBCDIC-Zeichensatz (IBM-Dokumentation)
- EBCDIC zu ASCII (IBM-Dokumentation)
- COBOL (IBM-Dokumentation)
- Verwenden eines Amazon S3 S3-Triggers zum Aufrufen einer Lambda-Funktion (AWS Lambda Lambda-Dokumentation)

Konvertieren Sie Mainframe-Datendateien mit komplexen Datensatzlayouts mit Micro Focus

Erstellt von Peter West

Übersicht

Dieses Muster zeigt Ihnen, wie Sie Mainframe-Datendateien mit Nicht-Textdaten und komplexen Datensatzlayouts mithilfe einer Micro Focus-Strukturdatei von der EBCDIC-Zeichenkodierung (Extended Binary Coded Decimal Interchange Code) in die ASCII-Zeichenkodierung (American Standard Code for Information Interchange) konvertieren. Um die Dateikonvertierung abzuschließen, müssen Sie wie folgt vorgehen:

1. Bereiten Sie eine einzelne Quelldatei vor, die alle Datenelemente und Datensatzlayouts in Ihrer Mainframe-Umgebung beschreibt.
2. Erstellen Sie mit dem Micro Focus Data File Editor als Teil der Micro Focus Classic Data File Tools oder Data File Tools eine Strukturdatei, die das Datensatzlayout der Daten enthält. Die Strukturdatei identifiziert die Nicht-Textdaten, sodass Sie Ihre Mainframe-Dateien korrekt von EBCDIC nach ASCII konvertieren können.
3. Testen Sie die Strukturdatei mithilfe der Classic Data File Tools oder Data File Tools.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Micro Focus Enterprise Developer für Windows, erhältlich über AWS Mainframe Modernization

Produktversionen

- Micro Focus Enterprise Server 7.0 und höher

Tools

- Micro Focus Enterprise Developer bietet die Ausführungsumgebung für Anwendungen, die mit einer beliebigen IDE-Variante (Integrated Development Environment) von Enterprise Developer erstellt wurden.

- Die Micro Focus Classic Data File Tools helfen Ihnen beim Konvertieren, Navigieren, Bearbeiten und Erstellen von Datendateien. Zu den klassischen Datendatei-Tools gehören der Datendateikonverter, der Datensatzlayout-Editor und der Datendatei-Editor.
- Mit den Micro Focus Data File Tools können Sie Datendateien erstellen, bearbeiten und verschieben. Zu den Datendateitools gehören der Datendatei-Editor, die Dateikonvertierungsprogramme und das Befehlszeilenprogramm für die Datendateistruktur.

Epen

Bereiten Sie die Quelldatei vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Quellkomponenten.	Identifizieren Sie alle möglichen Datensatzlayouts für die Datei, einschließlich aller Neudefinitionen, die Daten enthalten, die keine Textdaten enthalten. Wenn Sie Layouts haben, die Neudefinitionen enthalten , müssen Sie diese Layouts auf eindeutige Layouts reduzieren, die jede mögliche Permutation der Datenstru ktur beschreiben. In der Regel können die Datensatz layouts einer Datendatei durch die folgenden Archetypen beschrieben werden: • Datensatzlayout mit nur Textdaten • Datensatzlayout mit Nicht-Textdaten	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Datensatzlayout mit Nicht-Textdaten, die einer REDEFINES-Klausel untergeordnet sind Weitere Informationen zum Erstellen vereinfachter Datensatzlayouts für Dateien, die komplexe Datensatz layouts enthalten, finden Sie unter Rehosting von EBCDIC-Anwendungen in ASCII-Umgebungen für Mainframe-Migrationen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Identifizieren Sie die Bedingungen für das Datensatzlayout.	Identifizieren Sie bei Dateien mit mehreren Datensatz layouts oder bei Dateien, die komplexe Layouts mit einer REDEFINES-Klausel enthalten, die Daten und Bedingungen innerhalb eines Datensatzes, anhand derer Sie definieren können, welches Layout bei der Konvertierung verwendet werden soll. Wir empfehlen Ihnen, diese Aufgabe mit einem Fachexperten (SME) zu besprechen, der sich mit den Programmen auskennt, die diese Dateien verarbeiten.
	
	Eine Datei kann beispiels weise zwei Datensatztypen enthalten, die keine Textdaten enthalten. Sie können die Quelle überprüfen und möglicherweise Code finden, der dem folgenden ähnelt:
	
	`MOVE "M" TO PART-TYPE`
	`MOVE "MAIN ASSEMBLY" TO`
	`PART-NAME`
	`MOVE "S" TO PART-TYPE`
	`MOVE "SUB ASSEMBLY 1"`
	`TO PART-NAME`
	
	Der Code hilft Ihnen dabei, Folgendes zu identifizieren:
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Das Feld „PART-TYPE“ wird verwendet, um den Datensatztyp zu bestimmen • Der Wert „M“ wird für den „M-PART-RECORD“ verwendet • Der Wert „S“ wird für den „S-PART-RECORD“ verwendet Sie können die Werte dokumentieren, die von diesem Feld verwendet werden, um die Datensatz layouts den richtigen Datensätzen in der Datei zuzuordnen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Quelldatei.	Wenn die Datei in mehreren Quelldateien beschrieben wird oder wenn das Datensatzlayout Nicht-Textdaten enthält, die einer REDEFINES-Klausel untergeordnet sind, erstellen Sie eine neue Quelldatei, die die Datensatzlayouts enthält. Das neue Programm muss die Datei nicht mit SELECT- und FD-Anweisungen beschreiben. Das Programm kann die Datensatzbeschreibungen einfach als 10 Stufen innerhalb von Working-Storage enthalten. **Note** Sie können für jede Datendatei eine Quelldatei oder eine Master-Quelldatei erstellen, die alle Datendateien beschreibt.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kompilieren Sie die Quelldatei.	Kompilieren Sie die Quelldatei, um das Datenwörterbuch zu erstellen. Es wird empfohlen, die Quelldatei mit dem EBCDIC-Zeichensatz zu kompilieren. Wenn die IBMCOMP-Direktive oder die ODOSLIDE-Direktive verwendet werden, müssen Sie diese Direktiven auch in der Quelldatei verwenden. **Note** IBMCOMP beeinflusst die Bytespeicherung von COMP-Feldern und ODOSLIDE beeinflusst die Auffüllung von OCCURS VARIIEREN DEN Strukturen. Wenn diese Direktiven falsch gesetzt sind, liest das Konvertierungstool den Datensatz nicht korrekt. Dies führt zu fehlerhaften Daten in der konvertierten Datei.	App-Developer

(Option A) Erstellen Sie die Strukturdatei mit den klassischen Datendatei-Tools

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie das Tool und laden Sie das Wörterbuch.	1. Wählen Sie das Windows-Startmenüsymbol, suchen Sie nach Micro Focus Enterprise Developer, wählen Sie es aus und wählen Sie dann Classic Data File Tools. 2. Wählen Sie „Datei“ und anschließend „Datensatz layout“. 3. Wählen Sie im Dialogfel d Wählen Sie eine Datei aus, aus der die Layouts erstellt werden sollen, unter Dateiname die IDY (`.idy`) -Datei aus, die beim Kompilieren der Quelldate i zuvor erstellt wurde. Wählen Sie dann Open (Öffnen) aus. 4. Um zu überprüfen, ob Classic Data File Tools EBCDIC verwendet, wählen Sie im Dialogfeld Data File Tools die Option YES aus, wenn die IDY-Datei auf EBCDIC und Datatools auf ANSI eingestellt ist.	App-Developer
Erstellen Sie das Standard-Datensatzlayout.	Verwenden Sie das Standard-Datensatzlayout für alle Datensätze, die keinen	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bedingten Layouts entsprechen. 1. Erweitern Sie im Layoutfenster die Datenstruktur und suchen Sie dann nach der Ebene 01, die für das Standardlayout verwendet wird. 2. Klicken Sie mit der rechten Maustaste auf das Element 01 und wählen Sie dann Neues Layout. 3. Wählen Sie im Dialogfeld „Assistent für neue Datensatzlayouts“ die Option „Standardlayout“ und dann „Weiter“. 4. Wählen Sie Finish (Abschließen). Das Standardlayout wird im Bereich Layouts angezeigt und ist an dem roten Ordnersymbol zu erkennen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein bedingtes Datensatzlayout.	Verwenden Sie das bedingte Datensatzlayout, wenn eine Datei mehr als ein Datensatz layout enthält. 1. Erweitern Sie im Bereich Layouts die Datenstruktur und suchen Sie dann nach der Ebene 01, die für das bedingte Layout verwendet wird. 2. Klicken Sie mit der rechten Maustaste auf das Element 01 und wählen Sie dann Neues Layout. 3. Wählen Sie im Dialogfel d „Assistent für neues Datensatzlayout“ die Option „Bedingtes Layout“ und dann „Weiter“. 4. Wählen Sie Finish (Abschlie ßen). Das bedingte Layout wird im Bereich Layouts angezeigt und ist an dem gelben Ordnersymbol zu erkennen. 5. Erweitern Sie das bedingte Layout, klicken Sie mit der rechten Maustaste auf das Feld, in das Sie eine Bedingung einfügen müssen, und wählen Sie dann Eigenschaften aus.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Geben Sie im Dialogfeld Feldeigenschaften die Bedingung ein. Vergewissern Sie sich, dass der Zeichensatz auf EBCDIC eingestellt ist, und wählen Sie dann OK. Neben dem Feld, für das eine Bedingung festgelegt ist, wird ein Häkchen angezeigt. 7. Wiederholen Sie die Schritte 5—6 für alle anderen Felder, die Bedingungen für dieses Layout erfordern. 8. Wiederholen Sie die Schritte 1—6 für alle anderen bedingten Layouts, die hinzugefügt werden müssen. 9. Wählen Sie „Datei“, wählen Sie „Speichern unter“ und speichern Sie dann die Strukturdatei auf der Festplatte.	

(Option B) Erstellen Sie die Strukturdatei mit den Datendatei-Tools

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie das Tool und laden Sie das Wörterbuch.	1. Wählen Sie das Windows-Startmenüsymbol, suchen Sie nach Micro Focus	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Enterprise Developer, wählen Sie es aus und wählen Sie dann Data File Tools aus. 2. Wählen Sie „Datei“, „Neu“, „Datei strukturieren“. 3. Wählen Sie im Dialogfeld Öffnen unter Dateiname die IDY (`.idy`) -Datei aus, die beim Kompilieren der Quelldatei zuvor erstellt wurde. Wählen Sie dann Open (Öffnen) aus. 4. Um zu überprüfen, ob Data File Tools EBCDIC verwendet, stellen Sie sicher, dass das Dropdownmenü im Abschnitt Debug-Datei auf EBCDIC eingestellt ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Standard-Datensatzlayout.	Verwenden Sie das Standard-Datensatzlayout für alle Datensätze, die keinen bedingten Layouts entsprechen. 1. Erweitern Sie im Bereich Verfügbare Layouts im linken Bereich die Datenstruktur und suchen Sie dann die Ebene 01, die für das Standardlayout verwendet wird. 2. Klicken Sie mit der rechten Maustaste auf das Element 01 und wählen Sie dann Standardlayout erstellen. Das Standardlayout wird im Bereich Layouts angezeigt und ist an dem blauen „D“ -Symbol zu erkennen.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein bedingtes Datensatzlayout.	Verwenden Sie das bedingte Datensatzlayout, wenn eine Datei mehr als ein Datensatz layout enthält. 1. Erweitern Sie im Bereich Ausgewählte Layouts im rechten Bereich die Datenstruktur und suchen Sie dann nach der Ebene 01, die für das bedingte Layout verwendet wird. 2. Klicken Sie mit der rechten Maustaste auf das Element 01 und wählen Sie dann Bedingtes Layout erstellen . Das bedingte Layout wird im Bereich Layouts auf der rechten Seite angezeigt und ist an dem grünen „C“ - Symbol zu erkennen. 3. Erweitern Sie das bedingte Layout, klicken Sie mit der rechten Maustaste auf das Feld, in das Sie eine Bedingung einfügen müssen, und wählen Sie dann Eigenschaften aus. 4. Geben Sie im Dialogfel d Feldeigenschaften die Bedingung ein. Vergewiss ern Sie sich, dass der Zeichensatz auf EBCDIC eingestellt ist, und wählen	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie dann OK. Neben dem Feld, für das eine Bedingung festgelegt ist, wird ein rotes „WENN“ - Symbol angezeigt. 5. Wiederholen Sie die Schritte 3—4 für alle anderen Felder, die Bedingungen für dieses Layout erfordern. 6. Wiederholen Sie die Schritte 1—4 für alle anderen bedingten Layouts, die hinzugefügt werden müssen. 7. Wählen Sie „Datei“, wählen Sie „Speichern unter“ und speichern Sie dann die Strukturdatei auf der Festplatte.	

(Option A) Testen Sie die Strukturdatei mit den klassischen Datendatei-Tools

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie eine EBCDIC-Datendatei.	Vergewissern Sie sich, dass Sie Ihre Strukturdatei verwenden können, um eine EBCDIC-Testdatendatei korrekt anzuzeigen. 1. Wählen Sie das Windows-Startmenüsymbol, suchen und wählen Sie Micro	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Focus Enterprise Developer und wählen Sie dann Classic Data Tools. 2. Wählen Sie „Datei“ und anschließend „Öffnen“. 3. Wählen Sie im Dialogfeld Öffnen unter Dateiname den EBCDIC-Datensatz aus, und klicken Sie dann auf Öffnen. 4. Wählen Sie „Datei“, „Datendatei-Editor“ und „Datensatzlayouts laden“. 5. Wählen Sie im Dialogfeld Öffnen unter Dateiname die Strukturdatei aus, und klicken Sie dann auf Öffnen. 6. Um zu überprüfen, ob der Zeichensatzmodus auf EBCDIC eingestellt ist, stellen Sie sicher, dass das Dropdownmenü auf EBCDIC eingestellt ist. Sie können die Rohdaten des Datensatzes im linken Bereich und die formatier ten Daten im rechten Bereich sehen. 7. Wählen Sie verschied ene Datensätze aus, um sicherzustellen, dass alle Formate mit dem richtigen Layout gerendert werden.	

(Option B) Testen Sie die Strukturdatei mit den Datendatei-Tools

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie eine EBCDIC-Datendatei.	Vergewissern Sie sich, dass Sie Ihre Strukturdatei verwenden können, um eine EBCDIC-Testdatendatei korrekt anzuzeigen. 1. Wählen Sie das Windows-Startmenüsymbol, suchen und wählen Sie Micro Focus Enterprise Developer aus und wählen Sie dann Data File Tools aus. 2. Wählen Sie „Datei“, „Öffnen“, „Datendatei“. 3. Wählen Sie im Dialogfeld Datendatei öffnen auf der Registerkarte Lokal für Dateiname die Option Durchsuchen, um den Speicherort der EBCDIC-Testdatei zu finden. 4. Wählen Sie für Strukturdatei (optional) die Option Durchsuchen, um den Speicherort der Strukturdatei zu ermitteln. 5. Geben Sie im Abschnitt Dateidetails die Details der Datei ein und vergewissern Sie sich, dass die Kodierung auf EBCDIC eingestellt ist.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Wählen Sie je nach Ihren Anforderungen entweder den Modus „Gemeinsam öffnen“ oder „Exklusiv öffnen“. 7. Vergewissern Sie sich, dass das Drop-down-Menü im Bereich Erscheinungsbild der Werkzeugleiste auf EBCDIC eingestellt ist. Sie sehen die Rohdaten des Datensatzes im linken Bereich und die formatier ten Daten im rechten Bereich. 8. Wählen Sie verschied ene Datensätze aus, um sicherzustellen, dass alle Formate mit dem richtigen Layout gerendert werden.	

Testen Sie die Konvertierung der Datendatei

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Konvertierung einer EBCDIC-Datei.	1. Wählen Sie das Windows-Startmenüsymbol, suchen und wählen Sie Micro Focus Enterprise Developer und wählen Sie dann Classic Data Tools aus. 2. Wählen Sie „Tools“ und anschließend „Konvertie ren“.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie im Dialogfeld „Datendatei konvertieren“ im Bereich „Eingabedatei“ für „Dateiname“ die Option „Durchsuchen“, um die EBCDIC-Eingabedatei zu suchen und auszuwählen. Vergewissern Sie sich, dass der Zeichensatz auf EBCDIC eingestellt ist. 4. Aktivieren Sie im Bereich Zeichensatzkonvertierung die Kontrollkästchen Zeichensatz konvertieren und Datensätze enthalten Datenelemente, die keine Textdaten enthalten. Wählen Sie „Layout für die Konvertierung auswählen“ und anschließend „Durchsuchen“, um die Strukturdatei zu suchen und auszuwählen. 5. Geben Sie im Abschnitt Neue Datei für Dateiname den Pfad und den Dateinamen der ASCII-Ausgabedatei ein, die Sie erstellen möchten. Standardmäßig verwendet das Konvertierungstool dasselbe Format wie die Eingabedatei. Lassen Sie zum Testen die Optionen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	auf ihre Standardwerte eingestellt. 6. Wählen Sie „Konvertieren“. 7. Folgen Sie den Schritten im Abschnitt (Option A) Testen Sie die Strukturdatei mit den klassischen Datendate itools oder (Option B) Testen Sie die Strukturdatei mit den Datendateitools, laden Sie jedoch die ASCII-Ausgabedatei anstelle der EBCDIC-Datei. 8. Laden Sie sowohl die EBCDIC- als auch die ASCII-Dateien in den Datendatei-Editor und vergleichen Sie dann die Dateien nebeneinander, um die Genauigkeit der Konvertierung zu überprüfe n.	

Zugehörige Ressourcen

- Micro Focus (Micro Focus-Dokumentation)
- Mainframe- und Legacy-Code (AWS-Blogbeiträge)
- AWS Prescriptive Guidance (AWS-Dokumentation)
- AWS-Dokumentation (AWS-Dokumentation)
- Allgemeine AWS-Referenz (AWS-Dokumentation)
- AWS-Glossar (AWS-Dokumentation)

Stellen Sie mithilfe von Terraform eine Umgebung für containerisierte Blu Age-Anwendungen bereit

Erstellt von Richard Milner-Watts (AWS)

Übersicht

Durch die Migration älterer Mainframe-Workloads in moderne Cloud-Architekturen können die Kosten für die Wartung eines Mainframes eingespart werden — Kosten, die mit zunehmendem Alter der Umgebung nur noch steigen. Die Migration von Jobs von einem Mainframe kann jedoch besondere Herausforderungen mit sich bringen. Interne Ressourcen sind möglicherweise nicht mit der Joblogik vertraut, und die hohe Leistung von Mainframes bei diesen speziellen Aufgaben kann im Vergleich zu herkömmlichen, generellen Aufgaben schwierig zu replizieren sein. CPUs Das Umschreiben dieser Jobs kann ein großes Unterfangen sein und erheblichen Aufwand erfordern.

Blu Age konvertiert ältere Mainframe-Workloads in modernen Java-Code, den Sie dann als Container ausführen können.

Dieses Muster bietet ein Beispiel für eine serverlose Architektur zum Ausführen einer containerisierten Anwendung, die mit dem Blu Age-Tool modernisiert wurde. Die enthaltenen HashiCorp Terraform-Dateien bilden eine sichere Architektur für die Orchestrierung von Blu Age-Containern, die sowohl Batch-Aufgaben als auch Echtzeitdienste unterstützt.

Weitere Informationen zur Modernisierung Ihrer Workloads mithilfe von Blu Age- und AWS-Services finden Sie in den folgenden Publikationen zu AWS Prescriptive Guidance:

- Ausführung von Mainframe-Workloads, die mit Blu Age modernisiert wurden, auf einer serverlosen AWS-Infrastruktur
- Containerisieren Sie Mainframe-Workloads, die von Blu Age modernisiert wurden

Wenn Sie Unterstützung bei der Nutzung von Blu Age zur Modernisierung Ihrer Mainframe-Workloads benötigen, wenden Sie sich an das Blu Age-Team, indem Sie auf der Blu Age-Website auf Kontaktieren Sie unsere Experten klicken. Wenn Sie Unterstützung bei der Migration Ihrer modernisierten Workloads zu AWS, ihrer Integration mit AWS-Services und ihrer Umstellung auf die Produktion benötigen, wenden Sie sich an Ihren AWS-Kundenbetreuer oder füllen Sie das AWS Professional Services-Formular aus.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Die containerisierte Blu-Age-Beispielanwendung, die von den Containerize-Mainframe-Workloads bereitgestellt wird, die nach dem Blu Age-Muster modernisiert wurden. Die Beispielanwendung bietet die Logik für die Verarbeitung von Eingabe und Ausgabe für die modernisierte Anwendung und kann in diese Architektur integriert werden.
- Terraform ist erforderlich, um diese Ressourcen bereitzustellen.

Einschränkungen

- Amazon Elastic Container Service (Amazon ECS) begrenzt die Aufgabenressourcen, die dem Container zur Verfügung gestellt werden können. Zu diesen Ressourcen gehören CPU, RAM und Speicher. Wenn Sie beispielsweise Amazon ECS mit AWS Fargate verwenden, gelten die Limits für Aufgabenressourcen.

Produktversionen

Diese Lösung wurde mit den folgenden Versionen getestet:

- Terraform 1.3.6
- Terraform AWS-Anbieter 4.46.0

Architektur

Quelltechnologie-Stack

- Blaues Zeitalter
- Terraform

Zieltechnologie-Stack

- Amazon Aurora PostgreSQL-Compatible Edition
- AWS Backup
- Amazon Elastic Container Registry (Amazon ECR)

- Amazon ECS
- AWS Identity and Access Management Service (IAM)
- AWS-Schlüsselverwaltungsserver (AWS KMS)
- AWS Secrets Manager
- Amazon-Simple-Notification-Service (Amazon-SNS)
- Amazon Simple Storage Service (Amazon-S3)
- AWS Step Functions
- AWS Systems Manager

Zielarchitektur

Das folgende Diagramm zeigt die Lösungsarchitektur.

1. Die Lösung stellt die folgenden IAM-Rollen bereit:
   - Batch-Task-Rolle
   - Rolle zur Ausführung von Batch-Tasks
   - Rolle bei der Dienstaufgabe
   - Rolle bei der Ausführung von Servicetasks
   - Rolle „Step Functions“
   - AWS-Backup-Rolle
   - Rolle „RDS Enhanced Monitoring“.

   Die Rollen entsprechen den Prinzipien des am wenigsten privilegierten Zugriffs.
2. Amazon ECR wird verwendet, um das Container-Image zu speichern, das nach diesem Muster orchestriert wird.
3. Der AWS Systems Manager Parameter Store stellt der Amazon ECS-Aufgabendefinition zur Laufzeit Konfigurationsdaten zu jeder Umgebung bereit.
4. AWS Secrets Manager stellt der Amazon ECS-Aufgabendefinition zur Laufzeit sensible Konfigurationsdaten über die Umgebung zur Verfügung. Die Daten wurden von AWS KMS verschlüsselt.
5. Die Terraform-Module erstellen Amazon ECS-Aufgabendefinitionen für alle Echtzeit- und Batch-Aufgaben.

6. Amazon ECS führt eine Batch-Aufgabe mithilfe von AWS Fargate als Rechen-Engine aus. Dies ist eine kurzlebige Aufgabe, die nach Bedarf von AWS Step Functions initiiert wird.
7. Amazon Aurora PostgreSQL-Compatible bietet eine Datenbank zur Unterstützung der modernisierten Anwendung. Dies ersetzt Mainframe-Datenbanken wie IBM Db2 oder IBM IMS DB.
8. Amazon ECS bietet einen langlebigen Service zur Bereitstellung eines modernisierten Echtzeit-Workloads. Diese statusfreien Anwendungen werden permanent mit Containern ausgeführt, die über Availability Zones verteilt sind.
9. Ein Network Load Balancer wird verwendet, um Zugriff auf den Echtzeit-Workload zu gewähren. Der Network Load Balancer unterstützt frühere Protokolle wie IBM CICS. Alternativ können Sie einen Application Load Balancer mit HTTP-basierten Workloads verwenden.
10. Amazon S3 bietet Objektspeicher für Auftragseingaben und -ausgaben. Der Container sollte Pull- und Push-Operationen in Amazon S3 durchführen, um das Arbeitsverzeichnis für die Blu Age-Anwendung vorzubereiten.
11. Der AWS Step Functions Functions-Service wird verwendet, um die Ausführung der Amazon ECS-Aufgaben zur Verarbeitung von Batch-Workloads zu orchestrieren.
12. SNS-Themen für jeden Batch-Workload werden verwendet, um die modernisierte Anwendung in andere Systeme wie E-Mail zu integrieren oder um zusätzliche Aktionen zu initiieren, wie z. B. die Übermittlung von Ausgabeobjekten von Amazon S3 an FTP.

> **Note**
>
> Standardmäßig hat die Lösung keinen Zugang zum Internet. Dieses Muster geht davon aus, dass die Virtual Private Cloud (VPC) über einen Service wie AWS Transit Gateway mit anderen Netzwerken verbunden wird. Daher werden VPC-Endpunkte mit mehreren Schnittstellen bereitgestellt, um Zugriff auf die von der Lösung verwendeten AWS-Services zu gewähren. Um den direkten Internetzugang zu aktivieren, können Sie den Schalter im Terraform-Modul verwenden, um die VPC-Endpunkte durch ein Internet-Gateway und die zugehörigen Ressourcen zu ersetzen.

Automatisierung und Skalierung

Die Verwendung serverloser Ressourcen in diesem Muster trägt dazu bei, dass durch die Skalierung des Designs nur wenige Grenzen gesetzt werden. Auf diese Weise werden Probleme mit unnötigen Nebenkosten vermieden, z. B. die Konkurrenz um Rechenressourcen, die auf dem ursprünglichen

Mainframe auftreten könnten. Batch-Aufgaben können so geplant werden, dass sie bei Bedarf gleichzeitig ausgeführt werden.

Einzelne Container sind durch die von Fargate unterstützten Maximalgrößen begrenzt. Weitere Informationen finden Sie im Abschnitt CPU und Speicher für Aufgaben in der Amazon ECS-Dokumentation.

Um Echtzeit-Workloads horizontal zu skalieren, können Sie Container hinzufügen.

Tools

AWS-Services

- Amazon Aurora PostgreSQL-Compatible Edition ist eine vollständig verwaltete, ACID-konforme relationale Datenbank-Engine, die Sie bei der Einrichtung, dem Betrieb und der Skalierung von PostgreSQL-Bereitstellungen unterstützt.
- AWS Backup ist ein vollständig verwalteter Service, der Sie bei der Zentralisierung und Automatisierung des AWS-Services Datenschutzes in der Cloud und vor Ort unterstützt.
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Beenden und Verwalten von Containern in einem Cluster vereinfacht.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Key Management Service (AWS KMS) unterstützt Sie bei der Erstellung und Kontrolle kryptografischer Schlüssel, um Ihre Daten zu schützen.
- AWS Secrets Manager hilft Ihnen dabei, hartcodierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Geheimnis programmgesteuert abzurufen.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

- AWS Step Functions ist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Funktionen und andere Funktionen kombinieren können, um geschäftskritische AWS-Services Anwendungen zu erstellen.
- AWS Systems Manager Parameter Store bietet sicheren, hierarchischen Speicher für die Verwaltung von Konfigurationsdaten und Geheimnissen.

Andere Dienste

- HashiCorp Terraform ist ein Infrastructure-as-Code-Tool (IaC), mit dem Sie mithilfe von Code Cloud-Infrastruktur und -Ressourcen bereitstellen und verwalten können. Dieses Muster verwendet Terraform, um die Beispielarchitektur zu erstellen.

Code-Repository

Der Quellcode für dieses Muster ist im GitHub Blu Age Sample ECS Infrastructure (Terraform) - Repository verfügbar.

Bewährte Methoden

- Verwenden Sie für Testumgebungen Funktionen wie die `forceDate` Option, die modernisierte Anwendung so zu konfigurieren, dass sie konsistente Testergebnisse generiert, indem sie immer für einen bekannten Zeitraum ausgeführt wird.
- Passen Sie jede Aufgabe einzeln an, um die optimale Menge an Ressourcen zu verbrauchen. Sie können Amazon CloudWatch Container Insights verwenden, um Hinweise zu potenziellen Engpässen zu erhalten.

Epen

Bereiten Sie die Umgebung für den Einsatz vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie den Quellcode der Lösung.	Klonen Sie den Lösungscode aus dem GitHub Projekt.	DevOps Ingenieur
Booten Sie die Umgebung, indem Sie Ressource	1. Öffnen Sie ein Terminalf enster und vergewissern	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
n bereitstellen, um den Terraform-Status zu speichern .	Sie sich, dass Terraform installiert ist und dass die Anmeldeinformationen verfügbar sind. AWS 2. Navigieren Sie zum Verzeichnis `bootstrap-terraform` . 3. Bearbeiten Sie die Datei, `main.tf` wenn Sie die Namen des S3-Buckets (`<accountId>-terraform-backend`) und der Amazon DynamoDB-Tabelle (`terraform-lock`) ändern möchten. 4. Führen Sie den `terraform apply` Befehl aus, um die Ressourcen bereitzustellen. Notieren Sie sich die Namen des S3-Buckets und der DynamoDB-Tabellen.	

Stellen Sie die Lösungsinfrastruktur bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen und aktualisieren Sie die Terraform-Konfigur ation.	Öffnen Sie die Datei im Stammverzeichnis, `main.tf`, überprüfen Sie den Inhalt und erwägen Sie, die folgenden Aktualisierungen vorzunehm en:	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Aktualisieren Sie die, AWS-Region indem Sie nach der Zeichenfolge `eu-west-1` suchen und diese durch die gewünschte Region ersetzen, die Sie verwenden möchten. 2. Aktualisieren Sie den Bucket-Namen im `Terraform Backend` Block, falls der Standard im vorherigen Epic geändert wurde. 3. Aktualisieren Sie den `dynamodb_table` Wert, falls der Standard im vorherigen Epic geändert wurde. 4. Aktualisieren Sie den Wert der `stack_prefix` Variablen auf die gewünschte Zeichenfolge. Diese Zeichenfolge wird den Namen aller Ressourcen vorangestellt, die nach diesem Muster erstellt wurden. 5. Aktualisieren Sie den Wert von `vpc_cidr` Dies sollte mindestens ein `/24` Adressbereich sein. 6. Lesen Sie den `Locals` Abschnitt durch. Dies wird verwendet, um die Blu Age-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Aufgaben zu definieren, die bereitgestellt werden. Die Lösung iteriert über das Listenobjekt `bluage_batch_modules` und erstellt die zugehörigen Ressourcen (Step Functions Functions-Zustandsmaschine, Aufgabendefinition und SNS-Thema) für jedes Element der Liste. In einigen Fällen möchten Sie möglicherweise Variablen für verschiedene Umgebungen anpassen. Um beispielsweise die Laufzeit in Testumgebungen zu erzwingen, können Sie den Wert der `force_execution_time` Variablen ändern. 7. Um den Internetzugang zu aktivieren, ändern Sie den Wert für `direct_internet_access_required` von `false` bis `true`. Dadurch wird ein Internet-Gateway zusammen mit den NAT-Gateways und Routing-Tabellen bereitgestellt, die den öffentlichen Internetzugang für die Infrastruktur aktivieren. Standardmäßig stellt die	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Lösung Schnittstellen-VPC-Endpunkte in einer VPC ohne direkten Internetzugang bereit. 8. Um Zugriff auf alle Client-Server-Workloads zu gewähren, die über Elastic Load Balancing bedient werden, aktualisieren Sie die Werte von `additional_nlb_igress_cidrs` mit den CIDR-Netzwerken, die zugelassen werden sollen.	
Stellen Sie die Terraform-Datei bereit.	Führen Sie von Ihrem Terminal aus den `terraform apply` Befehl aus, um alle Ressourcen bereitzustellen. Überprüfen Sie die von Terraform generierten Änderungen und geben Sie Ja ein, um den Build zu starten. Beachten Sie, dass die Bereitstellung dieser Infrastruktur über 15 Minuten dauern kann.	DevOps Ingenieur

(Optional) Stellen Sie eine gültige containerisierte Blu-Age-Anwendung bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Senden Sie das Blu Age-Container-Image an Amazon ECR.	Schieben Sie den Container in das Amazon ECR-Repos itory, das Sie im vorherigen Epic erstellt haben. Anweisung en finden Sie in der Amazon ECR-Dokumentation. Notieren Sie sich den URI des Container-Images.	DevOps Ingenieur
Aktualisieren Sie die Terraform so, dass sie auf das Blu Age-Container-Image verweist.	Aktualisieren Sie die Datei so, dass `main.tf` sie auf das Container-Image verweist, das Sie hochgeladen haben.	DevOps Ingenieur
Stellen Sie die Terraform-Datei erneut bereit.	Führen Sie von Ihrem Terminal aus den Befehl aus, `terraform apply` um alle Ressourcen bereitzus tellen. Überprüfen Sie die von Terraform vorgeschlagenen Updates und geben Sie dann Ja ein, um mit der Bereitste llung fortzufahren.	DevOps Ingenieur

Zugehörige Ressourcen

- Blu Age
- Ausführung von Mainframe-Workloads, die mit Blu Age modernisiert wurden, auf einer serverlosen AWS-Infrastruktur
- Containerisieren Sie Mainframe-Workloads, die von Blu Age modernisiert wurden

Generieren Sie Einblicke in Db2 z/OS-Daten mithilfe von Amazon AWS Mainframe Modernization Q in QuickSight

Erstellt von Shubham Roy (AWS), Roshna Razack (AWS) und Santosh Kumar Singh (AWS)

Übersicht

Wenn Ihr Unternehmen geschäftskritische Daten in einer IBM Db2-Mainframe-Umgebung hostet, ist es entscheidend, Erkenntnisse aus diesen Daten zu gewinnen, um Wachstum und Innovation voranzutreiben. Durch die Erschließung von Mainframe-Daten können Sie schnellere, sichere und skalierbare Business Intelligence aufbauen, um datengestützte Entscheidungen, Wachstum und Innovation in der Amazon Web Services ()AWS Cloud zu beschleunigen.

Dieses Muster bietet eine Lösung für die Generierung von Geschäftseinblicken und die Erstellung gemeinsam nutzbarer Geschichten aus Mainframe-Daten in IBM Db2 for z/OS-Tabellen. Mainframe-Datenänderungen werden mithilfe von AWS Mainframe Modernization Data Replication with Precisely zum Thema Amazon Managed Streaming for Apache Kafka (Amazon MSK) gestreamt. Mithilfe von Amazon Redshift Streaming Ingestion werden Amazon MSK-Themendaten in Amazon Redshift Serverless Data Warehouse-Tabellen für Analysen in Amazon gespeichert. QuickSight

Sobald die Daten verfügbar sind QuickSight, können Sie mit Amazon Q in natürlicher Sprache Eingabeaufforderungen verwenden, QuickSight um Zusammenfassungen der Daten zu erstellen, Fragen zu stellen und Datenstorys zu generieren. Sie müssen keine SQL-Abfragen schreiben oder ein Business Intelligence (BI) -Tool erlernen.

Geschäftlicher Kontext

Dieses Muster stellt eine Lösung für Anwendungsfälle von Mainframe-Datenanalysen und Datenerkenntnissen dar. Mithilfe des Musters erstellen Sie ein visuelles Dashboard für die Daten Ihres Unternehmens. Um die Lösung zu demonstrieren, verwendet dieses Muster ein Gesundheitsunternehmen, das seinen Mitgliedern in den USA medizinische, zahnärztliche und augenärztliche Pläne anbietet. In diesem Beispiel werden demografische Daten und Tarifinformationen der Mitglieder in den IBM Db2 for z/OS-Datentabellen gespeichert. Das visuelle Dashboard zeigt Folgendes:

- Verteilung der Mitglieder nach Regionen
- Verteilung der Mitglieder nach Geschlecht
- Verteilung der Mitglieder nach Alter

- Verteilung der Mitglieder nach Tariftyp
- Mitglieder, die die Schutzimpfung noch nicht abgeschlossen haben

Beispiele für die Verteilung der Mitglieder nach Regionen und Mitgliedern, die die präventive Impfung nicht abgeschlossen haben, finden Sie im Abschnitt Zusätzliche Informationen.

Nachdem Sie das Dashboard erstellt haben, generieren Sie eine Datenstory, die die Erkenntnisse aus der vorherigen Analyse erklärt. Die Datenstory enthält Empfehlungen zur Erhöhung der Zahl der Mitglieder, die präventive Impfungen abgeschlossen haben.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto. Diese Lösung wurde auf Amazon Linux 2 auf Amazon Elastic Compute Cloud (Amazon EC2) entwickelt und getestet.
- Eine virtuelle private Cloud (VPC) mit einem Subnetz, auf das Ihr Mainframe-System zugreifen kann.
- Eine Mainframe-Datenbank mit Geschäftsdaten. Die Beispieldaten, die zum Erstellen und Testen dieser Lösung verwendet wurden, finden Sie im Abschnitt Anlagen.
- Change Data Capture (CDC) ist in den Db2 z/OS-Tabellen aktiviert. Informationen zur Aktivierung von CDC auf Db2 z/OS finden Sie in der IBM-Dokumentation.
- Precisiely Connect CDC for z/OS ist auf dem z/OS-System installiert, das die Quelldatenbanken hostet. Das Precisely Connect CDC for z/OS-Image wird als ZIP-Datei im AWS Mainframe Modernization - Data Replication for IBM z/OS Amazon Machine Image (AMI) bereitgestellt. Informationen zur Installation von Precisely Connect CDC for z/OS auf dem Mainframe finden Sie in der Precisely Installationsdokumentation.

Einschränkungen

- Ihre Mainframe-Db2-Daten sollten einen Datentyp haben, der von Precisely Connect CDC unterstützt wird. Eine Liste der unterstützten Datentypen finden Sie in der CDC-Dokumentation von Precisely Connect.
- Ihre Daten bei Amazon MSK sollten einen Datentyp haben, der von Amazon Redshift unterstützt wird. Eine Liste der unterstützten Datentypen finden Sie in der Amazon Redshift Redshift-Dokumentation.

- Amazon Redshift hat unterschiedliche Verhaltensweisen und Größenbeschränkungen für verschiedene Datentypen. Weitere Informationen finden Sie in der Amazon Redshift Redshift-Dokumentation.
- Wie viele Daten nahezu in Echtzeit eingehen, QuickSight hängt vom Aktualisierungsintervall ab, das für die Amazon Redshift Redshift-Datenbank festgelegt wurde.
- Einige AWS-Services sind nicht in allen AWS-Regionen verfügbar. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Amazon Q in QuickSight ist derzeit nicht in jeder Region verfügbar, die dies unterstützt QuickSight. Informationen zu bestimmten Endpunkten finden Sie auf der Seite Service-Endpunkte und Kontingente. Wählen Sie dort den Link für den Service.

Produktversionen

- AWS Mainframe Modernization Datenreplikation mit Precisiely Version 4.1.44
- Python-Version 3.6 oder höher
- Apache Kafka Version 3.5.1

Architektur

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur zur Generierung von Geschäftseinblicken aus Mainframe-Daten mithilfe von Data Replication AWS Mainframe Modernization with Precisely und Amazon Q in QuickSight.

Das Diagramm zeigt den folgenden Workflow:

1. Der Precisely Log Reader Agent liest Daten aus Db2-Protokollen und schreibt die Daten in einen transienten Speicher auf einem OMVS-Dateisystem auf dem Mainframe.
2. Der Publisher Agent liest die unformatierten Db2-Protokolle aus dem transienten Speicher.
3. Der lokale Controller-Daemon authentifiziert, autorisiert, überwacht und verwaltet Vorgänge.
4. Der Apply Agent wird mithilfe des vorkonfigurierten AMI auf Amazon EC2 bereitgestellt. Er stellt über den Controller-Daemon mithilfe von TCP/IP eine Verbindung zum Publisher Agent her. Der Apply Agent überträgt Daten mithilfe mehrerer Worker an Amazon MSK, um einen hohen Durchsatz zu erzielen.

5. Die Mitarbeiter schreiben die Daten im JSON-Format in das Amazon MSK-Thema. Als Zwischenziel für die replizierten Nachrichten bietet Amazon MSK die hochverfügbaren und automatisierten Failover-Funktionen.
6. Amazon Redshift Streaming Ingestion ermöglicht die schnelle Datenaufnahme mit geringer Latenz und hoher Geschwindigkeit von Amazon MSK in eine Amazon Redshift Serverless-Datenbank. Eine gespeicherte Prozedur in Amazon Redshift führt den Mainframe-Abgleich der Änderungsdaten (insert/update/deletes) in Amazon Redshift Redshift-Tabellen durch. Diese Amazon Redshift Redshift-Tabellen dienen als Datenanalysequelle für QuickSight.
7. Benutzer greifen auf die Daten zu, QuickSight um Analysen und Einblicke zu erhalten. Sie können Amazon Q in verwenden, um mit den Daten QuickSight zu interagieren, indem Sie Eingabeaufforderungen in natürlicher Sprache verwenden.

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server starten, wie Sie benötigen, und diese schnell vergrößern oder verkleinern.
- AWS Key Management Service (AWS KMS) hilft Ihnen dabei, kryptografische Schlüssel zu erstellen und zu kontrollieren, um Ihre Daten zu schützen.
- Amazon Managed Streaming for Apache Kafka (Amazon MSK) ist ein vollständig verwalteter Service, der Sie beim Erstellen und Ausführen von Anwendungen unterstützt, die Apache Kafka zur Verarbeitung von Streaming-Daten verwenden.
- Amazon QuickSight ist ein Business Intelligence (BI) -Service auf Cloud-Ebene, mit dem Sie Ihre Daten in einem einzigen Dashboard visualisieren, analysieren und melden können. Dieses Muster verwendet die generativen BI-Funktionen von Amazon Q in QuickSight.
- Amazon Redshift Serverless ist eine serverlose Option von Amazon Redshift, mit der Analysen in Sekundenschnelle effizienter ausgeführt und skaliert werden können, ohne dass eine Data Warehouse-Infrastruktur eingerichtet und verwaltet werden muss.
- Mit AWS Secrets Manager können Sie fest codierte Anmeldeinformationen im Code (einschließlich Passwörter) durch einen API-Aufruf an Secrets Manager ersetzen und das Geheimnis programmgesteuert abrufen.

Andere Tools

- Precisely Connect CDC sammelt und integriert Daten aus Altsystemen in Cloud- und Datenplattformen.

Code-Repository

Der Code für dieses Muster ist im GitHub Mainframe_ DataInsights _change_data_reconciliation-Repository verfügbar. Der Code ist eine gespeicherte Prozedur in Amazon Redshift. Diese gespeicherte Prozedur gleicht Mainframe-Datenänderungen (Einfügungen, Aktualisierungen und Löschungen) aus Amazon MSK mit den Amazon Redshift Redshift-Tabellen ab. Diese Amazon Redshift Redshift-Tabellen dienen als Datenanalysequelle für QuickSight.

Bewährte Methoden

- Folgen Sie bei der Einrichtung Ihres Amazon MSK-Clusters den Best Practices.
- Folgen Sie den Best Practices für das Analysieren von Amazon Redshift Redshift-Daten, um die Leistung zu verbessern.
- Wenn Sie die AWS Identity and Access Management (IAM-) Rollen für das Precisely Setup erstellen, folgen Sie dem Prinzip der geringsten Rechte und gewähren Sie die Mindestberechtigungen, die zur Ausführung einer Aufgabe erforderlich sind. Weitere Informationen finden Sie in der IAM-Dokumentation unter Gewährung der geringsten Rechte und bewährte Methoden zur Sicherheit.

Epen

Richten Sie die AWS Mainframe Modernization Datenreplikation mit Precisely auf Amazon ein EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie eine Sicherhei tsgruppe ein.	Um eine Verbindung mit dem Controller-Daemon und dem Amazon MSK-Cluster herzustellen, erstellen Sie eine Sicherheitsgruppe für die EC2 Instance. Fügen Sie die folgenden Regeln für eingehenden und ausgehend en Datenverkehr hinzu:	DevOps Ingenieur, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	• Regel 1 für eingehenden Datenverkehr:
	  • Wählen Sie für Typ die Option Benutzerdefinierte s TCP aus.
	  • Wählen Sie für Protocol TCP aus.
	  • Wählen Sie als Portberei ch 2626 (Standardport für den Precisely Controlle r-Daemon) oder die Portnummer des Controlle r-Daemons, der auf dem Mainframe läuft.
	  • Wählen Sie als Quelle den CIDR-Block aus.
	• Regel 2 für eingehende Nachrichten:
	  • Wählen Sie für Type (Typ) die Option Custom TCP (Benutzerdefiniertes TCP) aus.
	  • Wählen Sie als Protokoll die Option SSH aus.
	  • Wählen Sie für Portberei ch die Option 22.
	  • Wählen Sie als Quelle die IP-Adresse oder die Präfixliste aus.
	• Regel 3 für eingehende Nachrichten:
	  • Wählen Sie für Type (Typ) die Option Custom TCP	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(Benutzerdefiniertes TCP) aus. • Wählen Sie für Protocol TCP aus. • Wählen Sie als Portbereich die Option 9092-9098 aus. • Wählen Sie als Quelle den CIDR-Block aus. • Regel 1 für ausgehende Nachrichten: • Wählen Sie für Type (Typ) die Option Custom TCP (Benutzerdefiniertes TCP) aus. • Wählen Sie für Protocol TCP aus. • Wählen Sie als Portbereich die Option 9092-9098 aus. • Wählen Sie als Quelle den CIDR-Block aus. • Regel 2 für ausgehende Nachrichten: • Wählen Sie für Type (Typ) die Option Custom TCP (Benutzerdefiniertes TCP) aus. • Wählen Sie für Protocol TCP aus. • Wählen Sie als Portbereich 2626 (Standardport für	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den Precisely Controller-Daemon) oder die Portnummer des Controller-Daemons, der auf dem Mainframe läuft. • Wählen Sie als Quelle den CIDR-Block aus. Notieren Sie sich den Namen der Sicherheitsgruppe. Sie müssen den Namen angeben, wenn Sie die EC2 Instance starten und den Amazon MSK-Cluster konfigurieren.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Richtlinie und eine IAM-Rolle.	1. Folgen Sie den Anweisungen in der AWS-Dokumentation, um eine IAM-Richtlinie und eine IAM-Rolle zu erstellen. Die IAM-Richtlinie gewährt Zugriff auf das Erstellen von Themen auf dem Amazon MSK-Cluster und das Senden von Daten an diese Themen. 2. Nachdem Sie die IAM-Rolle erstellt haben, ordnen Sie ihr die Richtlinie zu. Notieren Sie sich den Namen der IAM-Rolle. Diese Rolle wird als IAM-Instanzprofil verwendet, wenn Sie die EC2 Instance starten.	DevOps Ingenieur, AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie eine EC2 Instanz bereit.	Gehen Sie wie folgt vor, um eine EC2 Instance für die Ausführung von Precisely CDC und die Verbindung zu Amazon MSK bereitzustellen: 1. Melden Sie sich bei AWS Marketplace an und abonnieren Sie AWS Mainframe Modernization – Data Replication for IBM z/OS. 2. Wählen Sie das AMI aus den verwalteten Abonnements aus und klicken Sie auf Neue Instanz starten. 3. Geben Sie weitere Konfigurationsdetails an, z. B. den Instanznamen, den Instanztyp, das key pair, die VPC und die Subnetze. Weitere Informationen finden Sie in der EC2 Amazon-Dokumentation. 4. Wählen Sie in der Dropdownliste die Sicherheitsgruppe aus, die Sie zuvor erstellt haben. 5. Unter Erweiterte Details, IAM-Instanzprofil müssen Sie die Rolle auswählen, die Sie zuvor erstellt haben.	AWS-Administrator, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Wählen Sie Launch Instance (Instance starten) aus.	

Amazon MSK einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den Amazon MSK-Cluster.	Gehen Sie wie folgt vor, um einen Amazon MSK-Cluster zu erstellen: 1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon MSK-Konsole unter https://console.aws.amazon.com/msk/. 2. Wählen Sie Cluster erstellen. 3. Wählen Sie für die Methode zur Clustererstellung die Option Benutzerdefiniert und für den Clustertyp die Option Bereitgestellt. 4. Geben Sie einen Namen für den Cluster ein. 5. Aktualisieren Sie die Clustereinstellungen nach Bedarf und behalten Sie die Standardeinstellungen für die anderen Einstellungen bei.	AWS DevOps, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Beachten Sie die < Kafka-Version>. Sie benötigen es bei der Einrichtung des Kafka-Clients. 7. Wählen Sie Weiter aus. 8. Wählen Sie dieselbe VPC und dieselben Subnetze aus, die Sie für die Precisely EC2 Instance verwendet haben, und wählen Sie die Sicherheitsgruppe aus, die Sie zuvor erstellt haben. 9. Aktivieren Sie im Abschnitt Sicherheitseinstellungen sowohl die rollenbasierte SASL/SCRAM - als auch die IAM-Authentifizierung. Precisely Connect CDC verwendet SASL/SCRAM (Simple Authentication and Security Layer/Salted Challenge Response Mechanism), und für die Verbindung zu Amazon Redshift ist IAM erforderlich. 10. Wählen Sie Weiter aus. 11. Wählen Sie zur Überprüfung die Methode zur Übermittlung von Überwachungs- und Broker-Protokollen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	12. Wählen Sie Weiter und anschließend Cluster erstellen aus. Die Erstellung eines bereitgestellten Clusters dauert in der Regel bis zu 15 Minuten. Nachdem der Cluster erstellt wurde, ändert sich sein Status von Creating zu Active.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die SASL/SCRAM-Authentifizierung ein.	Gehen Sie wie folgt vor, um die SASL/SCRAM-Authentifizierung für einen Amazon MSK-Cluster einzurichten: 1. Folgen Sie den Anweisungen in der AWS Dokumentation, um ein Geheimnis in Secrets Manager einzurichten. 2. Öffnen Sie die Amazon MSK-Konsole und wählen Sie den Amazon MSK-Cluster aus, den Sie zuvor erstellt haben. 3. Wählen Sie die Registerkarte Eigenschaften aus. 4. Wählen Sie Associate Secrets, Choose the Secrets, wählen Sie den Secrets-Schlüssel aus, den Sie erstellt haben, und wählen Sie dann Associate Secrets aus. Sie erhalten eine Erfolgsmeldung, die der folgenden ähnelt: `Successfully associated 1 secret for cluster <chosen cluster name>` 5. Wählen Sie den Clusternamen.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Wählen Sie in der Cluster-Zusammenfassung die Option Client-Informationen anzeigen aus. 7. Notieren Sie sich die Verbindungszeichenfolge für den privaten Endpunkt für den Authentifizierungstyp SASL/SCRAM.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie das Amazon MSK-Thema.	Gehen Sie wie folgt vor, um das Amazon MSK-Thema zu erstellen:
	1. Stellen Sie Connect zu der EC2 Instanz her, die Sie zuvor erstellt haben, und installieren Sie die neuesten Updates, indem Sie den folgenden Befehl ausführen:
	`sudo yum update -y`
	2. Installieren Sie die Java- und Kafka-Bibliothek, indem Sie den folgenden Befehl ausführen:
	`sudo yum install -y java-11 librdkafka librdkafka-devel`
	3. Um einen Ordner mit dem Namen `kafka` in zu erstellen`/home/ec2-user`, navigieren Sie zu diesem Ordner und führen Sie den folgenden Befehl aus:
	`mkdir kafka;cd kafka`
	4. Laden Sie die `kafka` Client-Bibliothek in den `kafka` Ordner herunter und `<YOUR MSK VERSION>` ersetzen Sie sie durch
		Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	die Kafka-Version, die Sie bei der Erstellung des Amazon MSK-Clusters notiert haben:
	
	`wget https://archive.apache.org/dist/kafka//kafka_2.13-<YOUR MSK VERSION>.tgz`
	
	5. Um die heruntergeladene Datei zu entpacken, führen Sie den folgenden Befehl aus und ersetzen Sie: `YOUR MSK VERSION>`
	
	`tar -xzf kafka_2.13-<YOUR MSK VERSION>.tgz`
	
	6. Um zu dem `kafka libs` Verzeichnis zu navigieren und die Java-Archive-Datei (JAR) für die Java-IAM-Authentifizierung herunterzuladen, führen Sie die folgenden Befehle aus und ersetzen `<YOUR MSK VERSION>` Sie:
	
	`cd kafka_2.13-<YOUR MSK VERSION>/libs`
	`wget https://github.com/aws/aws-msk-iam-auth/releases/download/v1.1.`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	1/aws-msk-iam-auth -1.1.1-all.jarkafka
	7. Führen Sie die folgenden Befehle aus, um zum `bin` Kafka-Verzeichnis zu navigieren und die `client.properties` Datei zu erstellen:
	`cd /home/ec2-user/kafka/kafka_2.13-<YOUR MSK VERSION>/bin`
	`cat >client.properties`
	8. Aktualisieren Sie die `client.properties` Datei mit dem folgenden Inhalt:
	`security.protocol=SASL_SSL`
	`sasl.mechanism=AWS_MSK_IAM`
	`sasl.jaas.config=software.amazon.msk.auth.iam.IAMLoginModule required;`
	`sasl.client.callback.handler.class=software.amazon.msk.auth.iam.IAMClientCallbackHandler`
	9. Um ein Kafka-Thema zu erstellen, navigieren Sie zum Kafka-Bin und führen Sie den folgenden Befehl	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	aus, `<kafka broker>` wobei Sie ihn durch den privaten Endpunkt des IAM-Bootstrap-Servers ersetzen, den Sie bei der Erstellung des Amazon MSK-Clusters notiert haben: `./kafka-topics.sh --bootstrap-server <kafka broker> --command-config client.properties --create --replication-factor 3 –partitions 6 --topic <topic name>` 10. Wenn die Meldung `Created topic <topic name>` angezeigt wird, notieren Sie sich den Namen des Themas.	

Konfigurieren Sie die Precisely Apply Engine bei Amazon EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Precisely Scripts ein, um Datenänderungen zu replizieren.	Gehen Sie wie folgt vor, um die Precisely Connect CDC-Skripts so einzurichten, dass sie geänderte Daten vom Mainframe in das Amazon MSK-Thema replizieren:	App-Entwickler, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	1. Um einen genauen Ordnernamen zu erstellen und zu diesem Ordner zu wechseln, führen Sie den folgenden Befehl aus:
	`mkdir /home/ec2-user/precisely;cd /home/ec2-user/precisely`
	2. Führen Sie den folgenden Befehl aus`ddls`, um zwei Ordner innerhalb von Precisione called `scripts` and zu erstellen und dann zu dem `scripts` Ordner zu wechseln:
	`mkdir scripts;mkdir ddls;cd scripts`
	3. Führen Sie den folgenden Befehl aus, um eine Datei mit dem Namen `sqdata_kafka_producer.conf` im `scripts` Ordner zu erstellen:
	`cat >sqdata_kafka_producer.conf`
	4. Aktualisiere die `sqdata_kafka_producer.conf` Datei mit dem folgenden Inhalt:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`builtin.features=SASL_SCRAM security.protocol=SASL_SSL sasl.mechanism=SCRAM-SHA-512 sasl.username=<User Name> sasl.password=<Password> metadata.broker.list=<SASL/SCRAM Bootstrap servers>` **Note** Aktualisieren Sie `<SASL/SCRAM Bootstrap servers>` mit der Amazon MSK SASL/SCRAM-Brokerliste, die Sie zuvor konfiguriert haben. Aktualisieren Sie `<User Name>` und `<Password>` verwenden Sie den Benutzernamen und das Passwort, die Sie zuvor in Secrets Manager eingerichtet haben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	5. Erstellen Sie eine `script.sqd` Datei in dem `scripts` Ordner.
	
	`cat >script.sqd`
	
	Die Apply Engine verarbeitet `script.sqd` Quelldaten und repliziert die Quelldaten auf das Ziel. Ein Beispiel für ein Apply Engine-Skript finden Sie im Abschnitt Zusätzliche Informationen.
	6. Führen Sie die folgenden Befehle aus, um zu dem `ddls` Ordner zu wechseln und eine .ddl-Datei für jede Db2-Tabelle zu erstellen:
	
	`cd /home/ec2-user/precisely/ddls`
	`cat >mem_details.ddl`
	`cat >mem_plans.ddl`
	
	Beispielweise.ddl-Dateien finden Sie im Abschnitt Zusätzliche Informationen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Generieren Sie den Netzwerk-ACL-Schlüssel.	Gehen Sie wie folgt vor, um den Netzwerk-ACL-Schlüssel (Network Access Control List) zu generieren:
	1. Führen Sie den folgenden Befehl aus, um den `sqdata` Installationspfad zu exportieren:
	`export PATH=$PATH:/usr/sbin:/opt/precisely/di/sqdata/bin`
	2. Führen Sie die folgenden Befehle aus, um in das `/home/ec2-user` Verzeichnis zu wechseln und den Netzwerk-ACL-Schlüssel zu generieren:
	`cd /home/ec2-user`
	`sqdutil keygen --force`
	Nachdem die öffentlichen und privaten Schlüssel generiert wurden, wird die folgende Meldung angezeigt:
	`SQDUT04I Generating a private key in file /home/ec2-user/.nacl/id_nacl`
		Cloud-Architekt, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`SQDC017I sqdutil(p id=27344) terminated successfully` 3. Notieren Sie sich den generierten öffentlichen Schlüssel, der im `.nacl` Ordner gespeichert ist.	

Bereiten Sie die Mainframe-Quellumgebung vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Standardeinstellungen im ISPF-Bildschirm.	Folgen Sie den Anweisungen in der Precisely Dokumentation, um die Standardeinstellungen in der Interactive System Productivity Facility (ISPF) zu konfigurieren.	Mainframe-Systemadministrator
Konfigurieren Sie den Controller-Daemon.	Gehen Sie wie folgt vor, um den Controller-Daemon zu konfigurieren: 1. Wählen Sie auf dem SQData z/OS-Hauptmenübildschirm Option 2 aus. 2. Geben Sie auf dem Bildschirm „Daemon zur Liste hinzufügen“ in das Feld Daemon-Name einen Namen für den Daemon ein, und drücken Sie dann die Eingabetaste.	Mainframe-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den Herausgeber.	Gehen Sie wie folgt vor, um den Herausgeber zu konfigurieren: 1. Wählen Sie auf dem SQData z/OS-Hauptmenübildschirm Option 3 aus. Dadurch gelangen Sie zum Bildschirm mit der Zusammenfassung von Capture/Publisher. 2. Wählen Sie die Option zum Hinzufügen einer CAB-Datei. Dadurch gelangen Sie zum Bildschirm CAB-Datei zur Liste hinzufügen. 3. Geben Sie im Feld Name einen Namen für die CAB-Datei ein. Geben Sie für Db2 den Typ als `D` ein. 4. Drücken Sie die Eingabetaste. Dadurch gelangen Sie zum Bildschirm Neue DB2-Capture-CAB-Datei erstellen. 5. Geben Sie im Feld ZFS Dir den Speichermountpunkt an. 6. Drücken Sie die Eingabetaste, um zu speichern und fortzufahren.	Mainframe-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Daemon-Konfigurationsdatei.	Gehen Sie wie folgt vor, um die Herausgeberdetails in der Controller-Daemon-Konfigurationsdatei zu aktualisieren: 1. Wählen Sie auf dem SQData z/OS-Haupmenübildschirm Option 2 aus. 2. Treten Sie S in die Nähe des Daemons ein, den Sie erstellt haben, um die Daemon-Details zu sehen. 3. Geben Sie die Eingabetaste ein1, und drücken Sie dann die Eingabetaste, um die Agentendatei zu bearbeiten. 4. Fügen Sie Ihre CAB-Datei details hinzu. Das folgende Beispiel zeigt die Details für eine CAB-Datei mit dem NamenDB2ZTOMSK . Verwenden Sie Ihre Mainframe-Benutzer-ID anstelle von. <userid> `ÝDB2ZTOMSK¨ type=capture cab=/u/<userid>/sqdata/DB2ZTOMSK.cab` 5. Drücken Sie F3. 6. Geben Sie 2 die Eingabetaste ein, um die ACL-Datei zu bearbeiten. Fügen	Mainframe-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Sie Ihre `userid` zur `acl` Konfigurationsdatei hinzu, wie im folgenden Beispiel gezeigt:
	`Ýacls¨`
	`prod=admin,<userid>`
	7. Drücken Sie F3, um zu speichern und zu beenden.	

Erstellen Sie den Job, um den Controller-Daemon zu starten.	Gehen Sie wie folgt vor, um den Job zu erstellen: 1. Geben Sie im Feld Optionen den Wert ein`G`. 2. Geben Sie die JOB-Karte , die Job- und Proc-Bibl iotheken sowie die `Db2 load` Bibliotheksdetails ein. 3. Geben Sie die Netzwerk-ACL-Datei ein und geben Sie Option 2 ein, um die Job Control Language (JCL) -Datei in der angegebenen Job-Bibli othek zu generieren.	Mainframe-Systemadministrat or

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie die JCL-Datei für den Capture Publisher.	Gehen Sie wie folgt vor, um die Capture Publisher-JCL-Datei zu generieren: 1. Wählen Sie auf dem SQData z/OS-Haup tmenübildschirm Option 3 aus. Dadurch gelangen Sie zum Bildschirm mit der Zusammenfassung von Capture/Publisher. 2. Geben Sie `S` neben der CAB-Datei ein, um sie auszuwählen. Dadurch gelangen Sie zum Detailbil dschirm von Db2 Capture/P ublisher. 3. Geben Sie unter Optionen die Optionen zum `G` Generieren des Jobs ein. `capture/publisher` 4. Geben Sie die JOB-Karte , die Job- und Prozedurb ibliotheken sowie die Details zur DB2-Ladeb ibliothek ein. 5. Um den Job zu erstellen, wählen Sie Option 4. Der Job wird in der Job-Bibli othek erstellt, die in der Job-Bibliothek angegeben ist.	Mainframe-Systemadministrat or

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen und aktualisieren Sie CDC.	1. Überprüfen Sie das `DATACAPTURE` Flag für die Db2-Tabelle, indem Sie die folgende Abfrage ausführen und `<table name>` zu Ihrem Db2-Tabellennamen wechseln:
	`SELECT DATACAPTU RE FROM SYSIBM.SY STABLES WHERE NAME='<table name>';`
	Vergewissern Sie sich, dass das Ergebnis als angezeigt `DATACAPTURE` wird. `Y`
	2. Wenn `DATACAPTURE` nicht`Y`, führen Sie die folgende Abfrage aus, um CDC für die Db2-Tabelle zu aktivieren, und wechseln Sie `<table name>` zu Ihrem Db2-Tabellennamen:
	`ALTER TABLE <table name> DATA CAPTURE CHANGES;`
		Mainframe-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Reichen Sie die JCL-Dateien ein.	Reichen Sie die folgenden JCL-Dateien ein, die Sie in den vorherigen Schritten konfiguriert haben: • JCL-Datei, um den Controller-Daemon zu starten • JCL-Datei zum Starten der Erfassung und Veröffentlichung Nachdem Sie die JCL-Dateien eingereicht haben, können Sie die Apply Engine in Precisely auf der EC2 Instanz starten.	Mainframe-Systemadministrator

Führen Sie CDC aus und validieren Sie es

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Apply Engine und validieren Sie das CDC.	Gehen Sie wie folgt vor, um die Apply Engine auf der EC2 Instanz zu starten und das CDC zu validieren: 1. Folgen Sie den Anweisungen in der AWS Dokumentation, um eine Verbindung mit der EC2 Instanz herzustellen. 2. Wechseln Sie in das Verzeichnis, das die `script.sqd` Datei enthält:	Cloud-Architekt, App-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`cd /home/ec2-user/precisely/scripts`
	3. Führen Sie den folgenden Startbefehl aus, um die Apply Engine `sqdeng` zu starten:
	`sqdeng -s script.sqd --identity=/home/ec2-user/.nacl/id_nacl`
	Die Apply Engine beginnt, auf Updates von der Mainframe-Quelle zu warten.
	4. Um CDC zu testen, fügen Sie einige Datensätze ein oder aktualisieren Sie sie in der Db2-Tabelle.
	5. Stellen Sie sicher, dass das Apply Engine-Protokoll die Anzahl der Datensätze anzeigt, die erfasst und in das Ziel geschrieben wurden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die Datensätze zum Thema Amazon MSK.	Gehen Sie wie folgt vor, um die Nachricht aus dem Kafka-Thema zu lesen:
	
	1. Um in das `bin` Verzeichnis zu wechseln, in dem sich der Installationspfad des Kafka-Clients auf der EC2 Instanz befindet, führen Sie den folgenden Befehl aus und `<Kafka version>` ersetzen Sie ihn durch Ihre Version:
	
	`cd /home/ec2-user/kafka/kafka_2.13-<Kafka version>/bin`
	
	2. Um das als Nachrichten im Kafka-Thema geschriebene Db2-CDC zu überprüfen, führen Sie den folgenden Befehl aus `<kafka broker>` und `<Topic Name>` ersetzen Sie dabei das Thema, das Sie zuvor erstellt haben:
	
	`./kafka-console-consumer.sh --bootstrap-server <kafka broker>:9098 --topic <Topic Name> --from-beginning --consumer.config client.properties`
		App-Entwickler, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Stellen Sie sicher, dass die Nachrichten der Anzahl der in der Db2-Tabelle aktualisierten Datensätze entsprechen.	

Speichern Sie Mainframe-Änderungsdaten in einem Amazon Redshift Serverless Data Warehouse

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Amazon Redshift Serverless ein.	Folgen Sie den Anweisungen in der Dokumentation, um ein Amazon Redshift Serverless Data Warehouse zu erstellen .AWS Überprüfen Sie im Amazon Redshift Serverless-Dashboard, ob der Namespace und die Arbeitsgruppe erstellt wurden und verfügbar sind. Bei diesem Beispielmuster kann der Vorgang 2—5 Minuten dauern.	Dateningenieur
Richten Sie die IAM-Rolle und die Vertrauensrichtlinie ein, die für die Streaming-Aufnahme erforderlich sind.	Gehen Sie wie folgt vor, um die serverlose Amazon Redshift Redshift-Streaming-Aufnahme von Amazon MSK einzurichten: 1. Erstellen Sie eine IAM-Richtlinie für Amazon Redshift für den Zugriff auf Amazon MSK.	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Führen Sie als Ersatz `[region]` AWS-Region für Amazon MSK, `[account-id]` durch Ihre AWS-Konto ID und `[msk-cluster-name]` durch den Namen des Amazon MSK-Clusters den folgenden Code aus: `{"Version": "2012-10-17","Statement": [{"Sid": "MSKIAMpolicy","Effect": "Allow","Action": ["kafka-cluster:ReadData","kafka-cluster:DescribeTopic","kafka-cluster:Connect"],"Resource": ["arn:aws:kafka:[region]:[account-id]:cluster/[msk-cluster-name]/*","arn:aws:kafka:[region]:[account-id]:topic/[msk-cluster-name]/*"]},{"Effect": "Allow","Action": ["kafka-cluster:AlterGroup","kafka-cluster:DescribeGro`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`up"],"Resource": ["arn:aws:kafka:[region]:[account-id]:group/[msk-cluster-name]/*"]}]}` Sie finden den Clusternamen und den Amazon-Ressourcennamen (ARN) auf der Amazon MSK-Konsole. Wählen Sie in der Konsole Cluster-Zusammenfassung und anschließend ARN aus. 2. Folgen Sie den Anweisungen in der AWS Dokumentation, um eine IAM-Rolle zu erstellen und die Richtlinie anzuhängen. 3. Gehen Sie wie folgt vor, um die IAM-Rolle dem Amazon Redshift Serverless-Namespace zuzuweisen: a. Melden Sie sich bei der Konsole an und öffnen Sie die Amazon Redshift Redshift-Konsole unter https://console.aws.amazon.com/redshiftv2/. b. Wählen Sie das Serverless dashboard (Serverless-Dashboard) aus. c. Wählen Sie Namespace.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	d. Wählen Sie den Tab Sicherheit und Verschlüsselung. e. Wählen Sie Permission und hängen Sie die IAM-Rolle an, die Sie erstellt haben. 4. Erstellen Sie in Ihrer Amazon Redshift Serverless-Sicherheitsgruppe eine Regel für eingehenden Datenverkehr mit den folgenden Details: • Wählen Sie für Type (Typ) die Option Custom TCP (Benutzerdefiniertes TCP) aus. • Wählen Sie für Protocol TCP aus. • Wählen Sie als Portbereich 9098, 9198 aus. • Wählen Sie als Quelle die Amazon MSK-Sicherheitsgruppe aus. 5. Erstellen Sie in Ihrer Amazon MSK-Sicherheitsgruppe eine Regel für eingehenden Datenverkehr mit den folgenden Details: • Wählen Sie für Type (Typ) die Option Custom TCP (Benutzerdefiniertes TCP) aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wählen Sie für Protocol TCP aus. • Wählen Sie als Portbereich 9098, 9198 aus. • Wählen Sie als Quelle die Amazon Redshift Redshift-Sicherheitsgruppe aus. Dieses Muster verwendet den Port für die IAM-Authentifizierung sowohl für die Amazon Redshift- als auch für die Amazon MSK-Konfiguration. Weitere Informationen finden Sie in der AWS Dokumentation (Schritt 2). 6. Aktivieren Sie das erweiterte VPC-Routing für die Amazon Redshift Serverless-Arbeitsgruppe. Weitere Informationen finden Sie in der AWS -Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Connect Amazon Redshift Serverless mit Amazon MSK.	Um eine Verbindung zum Amazon MSK-Thema herzustellen, erstellen Sie ein externes Schema in Amazon Redshift Serverless. Führen Sie im Amazon Redshift Query Editor v2 den folgenden SQL-Befehl aus, `'iam_role _arn'` ersetzen Sie ihn durch die Rolle, die Sie zuvor erstellt haben, und ersetzen Sie `'MSK_cluster_arn` 'durch den ARN für Ihren Cluster. `CREATE EXTERNAL SCHEMA member_schema FROM MSK IAM_ROLE 'iam_role _arn' AUTHENTICATION iam URI 'MSK_cluster_arn';`	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine materialisierte Ansicht.	Um die Daten aus dem Amazon MSK-Thema in Amazon Redshift Serverless zu nutzen, erstellen Sie eine materialisierte Ansicht. Führen Sie im Amazon Redshift Query Editor v2 die folgenden SQL-Befehle aus und `<MSK_Topic_name>` ersetzen Sie sie durch den Namen Ihres Amazon MSK-Themas. `CREATE MATERIALIZED VIEW member_view AUTO REFRESH YES AS SELECT kafka_partition, kafka_offset, refresh_time, json_parse(kafka_value) AS Data FROM member_schema.<MSK_Topic_name> WHERE CAN_JSON_PARSE(kafka_value);`	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie Zieltabellen in Amazon Redshift.	Amazon Redshift Redshift-Tabellen bieten die Eingabe für QuickSight. Dieses Muster verwendet die Tabellen `member_dtls` und`member_plans` , die den Db2-Quelltabellen auf dem Mainframe entsprechen.
	
	Um die beiden Tabellen in Amazon Redshift zu erstellen, führen Sie die folgenden SQL-Befehle im Amazon Redshift Query Editor v2 aus:
	
	`-- Table 1: members_dtls`
	`CREATE TABLE members_dtls (`
	`memberid INT ENCODE AZ64,`
	`member_name VARCHAR(100) ENCODE ZSTD,`
	`member_type VARCHAR(50) ENCODE ZSTD,`
	`age INT ENCODE AZ64,`
	`gender CHAR(1) ENCODE BYTEDICT,`
	`email VARCHAR(100) ENCODE ZSTD,`
	`region VARCHAR(50) ENCODE ZSTD`
	`) DISTSTYLE AUTO;`
	
	`-- Table 2: member_plans`
	`CREATE TABLE member_plans (`
		Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>memberid INT ENCODE AZ64,
	medical_plan CHAR(1) ENCODE BYTEDICT,
	dental_plan CHAR(1) ENCODE BYTEDICT,
	vision_plan CHAR(1) ENCODE BYTEDICT,
	preventive_immuniz ation VARCHAR(50) ENCODE ZSTD
	) DISTSTYLE AUTO;</pre>	

Erstellen Sie eine gespeicherte Prozedur in Amazon Redshift.	Dieses Muster verwendet eine gespeicherte Prozedur, um Änderungsdaten (`INSERT`,`UPDATE`,`DELETE`) vom Quell-Mainframe mit der Amazon Redshift Redshift-Data-Warehouse-Zieltabelle für Analysen zu synchronisieren. QuickSight Um die gespeicherte Prozedur in Amazon Redshift zu erstellen, verwenden Sie den Abfrage-Editor v2, um den Code der gespeicherten Prozedur auszuführen, der sich im GitHub Repository befindet.	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Lesen Sie aus der materialisierten Streaming-Ansicht und laden Sie sie in die Zieltabellen.	Die gespeicherte Prozedur liest Datenänderungen aus der materialisierten Streaming-Ansicht und lädt die Datenänderungen in die Zieltabellen. Verwenden Sie den folgenden Befehl, um die gespeicherte Prozedur auszuführen: `call SP_Members_Load();` Sie können Amazon verwenden EventBridge, um die Jobs in Ihrem Amazon Redshift Data Warehouse so zu planen, dass diese gespeicherte Prozedur auf der Grundlage Ihrer Datenlatenzanforderungen aufgerufen wird. EventBridge führt Jobs in festen Intervallen aus. Um zu überprüfen, ob der vorherige Aufruf der Prozedur abgeschlossen wurde, müssen Sie möglicherweise einen Mechanismus wie eine AWS Step Functions Zustandsmaschine verwenden. Weitere Informationen finden Sie in den folgenden Ressourcen:	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Eine EventBridge Amazon-Regel erstellen, die nach einem Zeitplan ausgeführt wird • Beschleunigen Sie die Orchestrierung eines ELT-Prozesses mithilfe AWS Step Functions einer Amazon Redshift Data API. Eine weitere Option besteht darin, den Amazon Redshift Query Editor v2 zu verwenden , um die Aktualisierung zu planen. Weitere Informationen finden Sie unter Planen einer Abfrage mit dem Abfrage-Editor v2.	

Connect QuickSight zu Daten in Amazon Redshift her

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Einrichten QuickSight.	Folgen Sie zur Einrichtung QuickSight den Anweisungen in der AWS Dokumentation.	Ingenieur für Migration
Richten Sie eine sichere Verbindung zwischen Amazon Redshift QuickSight und Amazon Redshift ein.	Gehen Sie wie folgt vor, um eine sichere Verbindung zwischen QuickSight und Amazon Redshift einzurichten 1. Um Verbindungen von zu Amazon Redshift QuickSigh	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	t zu autorisieren, öffnen Sie die Amazon Redshift Redshift-Konsole und fügen Sie der Amazon Redshift Redshift-Sicherheitsgruppe eine Regel für eingehend en Datenverkehr hinzu. Die Regel sollte Datenverk ehr zu Port 5439 (dem standardmäßigen Redshift-Port) aus dem CIDR-Bere ich zulassen, in dem Sie ihn eingerichtet haben. QuickSight Eine Liste der IP-Adressen AWS-Regio nen und ihrer IP-Adressen finden Sie unter Unterstüt zt für. AWS-Regionen QuickSight 2. Wählen Sie in der Amazon Redshift Redshift-Konsole Arbeitsgruppe, Datenzugr iff, Netzwerk und Sicherheit und aktivieren Sie Öffentlich zugänglich.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Datensatz für QuickSight.	Gehen Sie wie folgt vor, um einen Datensatz für QuickSight aus Amazon Redshift zu erstellen: 1. Wählen Sie auf der QuickSight Konsole im Navigationsbereich Datasets aus. 2. Klicken Sie auf der Seite Datensätze auf Neuer Datensatz. 3. Wählen Sie Redshift Manual Connect. 4. Geben Sie im Fenster Neue Redshift-Datenquelle die Verbindungsinformationen ein: • Geben Sie unter Datenquellenname einen Namen für die Amazon Redshift Redshift-Datenquelle ein. • Geben Sie für Datenbankserver den Endpunkt des Amazon Redshift Redshift-Clusters ein. Sie können den Endpunktwert aus dem Feld Endpoint im Abschnitt Allgemeine Informationen für die Cluster-Arbeitsgruppe im Amazon Redshift Serverless-	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Dashboard abrufen. Die Serveradresse ist der erste Teil des Endpunkts vor dem Doppelpunkt, wie im folgenden Beispiel gezeigt: `mfdata-insights.NNNNNNNN.us-east-1.redshift-serverless.amazonaws.com:5439/dev` • Geben Sie als Port `5439` (den Standardport für Amazon Redshift) ein. • Geben Sie den Namen der Datenbank ein (nach dem Schrägstrich im Endpunkt). In diesem Fall lautet `dev` der Datenbankname. • Geben Sie unter Benutzername und Passwort den Benutzernamen und das Passwort für die Amazon Redshift Redshift-Datenbank ein. 5. Wählen Sie Verbindung validieren. Wenn der Vorgang erfolgreich ist, sollte ein grünes Häkchen angezeigt werden, das auf eine Überprüfung hinweist. Schlägt die Überprüfung	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	fehl, finden Sie weitere Informationen im Abschnitt Fehlerbehebung. 6. Klicken Sie auf Create data source.	
Treten Sie dem Datensatz bei.	Um Analysen zu erstellen QuickSight, verknüpfen Sie die beiden Tabellen, indem Sie den Anweisungen in der AWS Dokumentation folgen. Wählen Sie im Bereich Join-Konfiguration für Verbindungstyp die Option Left aus. Verwenden Sie unter Join-Klauseln die Option `memberid from member_plans = memberid from members_details .`	Ingenieur für Migration

Gewinnen Sie geschäftliche Einblicke aus den Mainframe-Daten mithilfe von Amazon Q in QuickSight

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Amazon Q in ein QuickSight.	Folgen Sie den Anweisungen in der AWS Dokumentation, um die Funktion Amazon Q in QuickSight Generative BI einzurichten.	Ingenieur für Migration
Analysieren Sie Mainframe-Daten und erstellen Sie ein visuelles Dashboard.	Gehen Sie wie folgt vor QuickSight, um Ihre Daten zu analysieren und zu visualisieren:	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Folgen Sie den Anweisungen in der AWS Dokumentation, um die Mainframe-Datenanalyse zu erstellen. Wählen Sie für den Datensatz den Datensatz aus, den Sie erstellt haben. 2. Wählen Sie auf der Analyseseite Visual erstellen aus. 3. Wählen Sie im Fenster „Thema für Analyse erstellen“ die Option Bestehendes Thema aktualisieren aus. 4. Wählen Sie in der Dropdownliste Thema auswählen das Thema aus, das Sie zuvor erstellt haben. 5. Wählen Sie Themenverknüpfung aus. 6. Nachdem Sie das Thema verknüpft haben, wählen Sie Visual erstellen, um das Amazon Q-Fenster Build a Visual zu öffnen. 7. Schreiben Sie in der Eingabeaufforderungsleiste Ihre Analysefragen. Die für dieses Muster verwendeten Beispielfragen sind die folgenden:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Verteilung der Mitglieder nach Regionen anzeigen • Verteilung der Mitglieder nach Alter anzeigen • Verteilung der Mitgliede r nach Geschlecht anzeigen • Verteilung der Mitglieder nach Tariftyp anzeigen • Zeigt Mitglieder an, die die Schutzimpfung noch nicht abgeschlossen haben Nachdem Sie Ihre Fragen eingegeben haben, wählen Sie Build. Amazon Q in QuickSight erstellt die Grafiken. 8. Um die Grafiken zu Ihrem visuellen Dashboard hinzuzufügen, wählen Sie ZUR ANALYSE HINZUFÜGEN. Wenn Sie fertig sind, können Sie Ihr Dashboard veröffent lichen, um es mit anderen in Ihrer Organisation zu teilen. Beispiele finden Sie unter Visuelles Mainframe-Dashboar d im Abschnitt Zusätzliche Informationen.	

Erstellen Sie eine Datenstory mit Amazon Q in QuickSight aus Mainframe-Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Datenstory.	Erstellen Sie eine Datenstor y, um die Erkenntnisse aus der vorherigen Analyse zu erläutern, und geben Sie eine Empfehlung zur Erhöhung der präventiven Impfungen für Mitglieder ab: 1. Folgen Sie den Anweisung en in der AWS Dokumenta tion, um die Data Story zu erstellen. 2. Verwenden Sie für den Data Story-Prompt Folgendes: `Build a data story about Region with most numbers of members. Also show the member distribution by medical plan, vision plan, dental plan. Recommend how to motivate members to complete immunizat ion. Include 4 points of supportin g data for this pattern.`	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie können auch Ihre eigene Aufforderung erstellen, um Datenstor ys für andere Geschäfts einblicke zu generieren. 3. Wählen Sie Visuals hinzufügen aus und fügen Sie die Grafiken hinzu, die für die Data Story relevant sind. Verwenden Sie für dieses Muster die Grafiken, die Sie zuvor erstellt haben. 4. Wählen Sie Build aus. 5. Ein Beispiel für die Ausgabe von Data Storys finden Sie unter Data Story-Ausgabe im Abschnitt Zusätzliche Informationen.	
Sehen Sie sich die generierte Datenstory an.	Um die generierte Datenstor y anzuzeigen, wählen Sie diese Story auf der Seite Data Stories aus.	Ingenieur für Migration
Bearbeiten Sie eine generierte Datenstory.	Folgen Sie den Anweisung en in der AWS Dokumenta tion, um die Formatierung, das Layout oder die visuelle Darstellung in einer Data Story zu ändern.	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Teilen Sie eine Datenstory.	Folgen Sie den Anweisungen in der AWS Dokumentation, um eine Data Story mit anderen zu teilen.	Ingenieur für Migration

Fehlerbehebung

Problem	Lösung
Für QuickSight die Erstellung von Amazon Redshift Redshift-Datensätzen `Validate Connection` ist ein Fehler aufgetreten.	1. Vergewissern Sie sich, dass die mit der Amazon Redshift Serverless Instance verbundene Sicherheitsgruppe eingehende Datenverkehr aus dem IP-Adressbereich zulässt, der der Region zugeordnet ist, in der Sie sie eingerichtet haben. QuickSight 2. Vergewissern Sie sich, dass die VPC, auf der Amazon Redshift Serverless bereitgestellt wird, öffentlich verfügbar ist. 3. Vergewissern Sie sich, dass Sie den richtigen Benutzernamen und das richtige Passwort für Amazon Redshift verwenden. Sie können den Benutzernamen und das Passwort auf der Amazon Redshift Redshift-Konsole zurücksetzen.
Beim Versuch, die Apply Engine auf der EC2 Instance zu starten, wird der folgende Fehler zurückgegeben: `-bash: sqdeng: command not found`	Exportieren Sie den `sqdata` Installationspfad, indem Sie den folgenden Befehl ausführen: `export PATH=$PATH:/usr/sbin:/opt/precisely/di/sqdata/bin`
Beim Versuch, die Apply Engine zu starten, wird einer der folgenden Verbindungsfehler zurückgegeben:	Überprüfen Sie den Mainframe-Spool, um sicherzustellen, dass die Controller-Daemon-Jobs ausgeführt werden.

Problem	Lösung
• SQDD018E Cannot connect to transfer socket(rc==0x18468). Agent:<Agent Name > Socket:/u /./sqdata/.DB2ZTOMSK.cab.data • SQDUR06E Error opening url cdc:// <VPC end point name>:2626/ DB2ZTOMSK/DB2ZTOMSK : errno:112 8 (Unknown error 1128)	

Zugehörige Ressourcen

- Generieren Sie Einblicke mithilfe AWS Mainframe Modernization von Amazon Q in QuickSight (Muster)
- Generieren Sie Dateneinblicke mithilfe AWS Mainframe Modernization von Amazon Q in QuickSight (Demo)
- AWS Mainframe Modernization - Datenreplikation für IBM z/OS
- Amazon Redshift Streaming-Aufnahme in eine materialisierte Ansicht

Zusätzliche Informationen

Beispieldateien im Format .ddl

members_details.ddl

```
CREATE TABLE MEMBER_DTLS (
memberid INTEGER NOT NULL,
member_name VARCHAR(50),
member_type VARCHAR(20),
age INTEGER,
gender CHAR(1),
email VARCHAR(100),
region VARCHAR(20)
);
```

member_plans.ddl

```
CREATE TABLE MEMBER_PLANS (
memberid INTEGER NOT NULL,
medical_plan CHAR(1),
dental_plan CHAR(1),
vision_plan CHAR(1),
preventive_immunization VARCHAR(20)
);
```

Beispiel für eine .sqd-Datei

<kafka topic name>Ersetzen Sie es durch den Namen Ihres Amazon MSK-Themas.

script.sqd

```
-- Name: DB2ZTOMSK: DB2z To MSK JOBNAME DB2ZTOMSK;REPORT EVERY 1;OPTIONS
 CDCOP('I','U','D');-- Source Descriptions
JOBNAME DB2ZTOMSK;
REPORT EVERY 1;
OPTIONS CDCOP('I','U','D');

-- Source Descriptions
BEGIN GROUP DB2_SOURCE;
DESCRIPTION DB2SQL /var/precisely/di/sqdata/apply/DB2ZTOMSK/ddl/mem_details.ddl AS
 MEMBER_DTLS;
DESCRIPTION DB2SQL /var/precisely/di/sqdata/apply/DB2ZTOMSK/ddl/mem_plans.ddl AS
 MEMBER_PLANS;
END GROUP;
-- Source Datastore
DATASTORE cdc://<zos_host_name>/DB2ZTOMSK/DB2ZTOMSK
OF UTSCDC
AS CDCIN
DESCRIBED BY GROUP DB2_SOURCE ;
-- Target Datastore(s)
DATASTORE 'kafka:///<kafka topic name>/key'
OF JSON
AS TARGET
DESCRIBED BY GROUP DB2_SOURCE;
PROCESS INTO TARGET
SELECT
{
REPLICATE(TARGET)
}
FROM CDCIN;
```

Visuelles Mainframe-Dashboard

Das folgende Datenbild wurde von Amazon Q QuickSight für die Analysefrage erstellt `show member distribution by region`.

Das folgende Datenbild wurde von Amazon Q QuickSight für die Frage erstelltshow `member distribution by Region who have not completed preventive immunization, in pie chart`.

Ausgabe von Data Story

Die folgenden Screenshots zeigen Abschnitte der Data Story, die von Amazon Q QuickSight für die Aufforderung erstellt wurde`Build a data story about Region with most numbers of members. Also show the member distribution by age, member distribution by gender. Recommend how to motivate members to complete immunization. Include 4 points of supporting data for this pattern`.

In der Einleitung wird in der Datenstory empfohlen, die Region mit den meisten Mitgliedern auszuwählen, um die größtmögliche Wirkung der Impfmaßnahmen zu erzielen.

Die Datenstory bietet eine Analyse der Mitgliederzahlen für die vier Regionen. Die Regionen Nordosten, Südwesten und Südosten haben die meisten Mitglieder.

Die Datenstory enthält eine Analyse der Mitglieder nach Alter.

Die Datengeschichte konzentriert sich auf Impfmaßnahmen im Mittleren Westen.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Generieren Sie Dateneinblicke mithilfe von AWS Mainframe Modernization und Amazon Q in QuickSight

Erstellt von Shubham Roy (AWS), Roshna Razack (AWS) und Santosh Kumar Singh (AWS)

Übersicht

Wenn Ihr Unternehmen geschäftskritische Daten in einer Mainframe-Umgebung hostet, ist es entscheidend, Erkenntnisse aus diesen Daten zu gewinnen, um Wachstum und Innovation voranzutreiben. Durch die Erschließung von Mainframe-Daten können Sie schnellere, sichere und skalierbare Business Intelligence aufbauen, um datengestützte Entscheidungen, Wachstum und Innovation in der Amazon Web Services ()AWS Cloud zu beschleunigen.

Dieses Muster bietet eine Lösung für die Generierung von Geschäftseinblicken und die Erstellung gemeinsam nutzbarer Geschichten aus Mainframe-Daten mithilfe von AWS Mainframe Modernization File Transfer mit BMC und Amazon Q in. QuickSight Mainframe-Datensätze werden mithilfe von AWS Mainframe Modernization File Transfer mit BMC an Amazon Simple Storage Service (Amazon S3) übertragen. Eine AWS Lambda Funktion formatiert die Mainframe-Datendatei und bereitet sie für das Laden in Amazon QuickSight vor.

Sobald die Daten verfügbar sind QuickSight, können Sie mit Amazon Q in natürlicher Sprache Aufforderungen verwenden, QuickSight um Zusammenfassungen der Daten zu erstellen, Fragen zu stellen und Datenstorys zu generieren. Sie müssen keine SQL-Abfragen schreiben oder ein Business Intelligence (BI) -Tool erlernen.

Geschäftlicher Kontext

Dieses Muster stellt eine Lösung für Anwendungsfälle von Mainframe-Datenanalysen und Datenerkenntnissen dar. Mithilfe des Musters erstellen Sie ein visuelles Dashboard für die Daten Ihres Unternehmens. Um die Lösung zu demonstrieren, verwendet dieses Muster ein Gesundheitsunternehmen, das seinen Mitgliedern in den USA medizinische, zahnärztliche und augenärztliche Pläne anbietet. In diesem Beispiel werden demografische Daten und Versicherungsinformationen der Mitglieder in den Mainframe-Datensätzen gespeichert. Das visuelle Dashboard zeigt Folgendes:

- Verteilung der Mitglieder nach Regionen
- Verteilung der Mitglieder nach Geschlecht
- Verteilung der Mitglieder nach Alter
- Verteilung der Mitglieder nach Tariftyp

- Mitglieder, die die Schutzimpfung noch nicht abgeschlossen haben

Nachdem Sie das Dashboard erstellt haben, generieren Sie eine Datenstory, die die Erkenntnisse aus der vorherigen Analyse erklärt. Die Datenstory enthält Empfehlungen zur Erhöhung der Zahl der Mitglieder, die präventive Impfungen abgeschlossen haben.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Mainframe-Datensätze mit Geschäftsdaten
- Zugriff auf die Installation eines File Transfer Agents auf dem Mainframe

Einschränkungen

- Ihre Mainframe-Datendatei sollte in einem der Dateiformate vorliegen, die von unterstützt werden. QuickSight Eine Liste der unterstützten Dateiformate finden Sie in der QuickSight Amazon-Dokumentation.

  Dieses Muster verwendet eine Lambda-Funktion, um die Mainframe-Datei in ein Format zu konvertieren, das von unterstützt wird. QuickSight

Architektur

Das folgende Diagramm zeigt eine Architektur zur Generierung von Geschäftseinblicken aus Mainframe-Daten mithilfe von AWS Mainframe Modernization File Transfer mit BMC und Amazon Q in. QuickSight

Das Diagramm zeigt den folgenden Workflow:

1. Ein Mainframe-Datensatz mit Geschäftsdaten wird mithilfe von AWS Mainframe Modernization File Transfer with BMC an Amazon S3 übertragen.
2. Die Lambda-Funktion konvertiert die Datei, die sich im S3-Bucket des Ziels für die Dateiübertragung befindet, in das CSV-Format (Comma-Separated Values).
3. Die Lambda-Funktion sendet die konvertierte Datei an den S3-Bucket des Quelldatensatzes.

4. Die Daten in der Datei werden von aufgenommen. QuickSight
5. Benutzer greifen auf die Daten in QuickSight zu. Sie können Amazon Q in verwenden, um mit den Daten QuickSight zu interagieren, indem Sie Eingabeaufforderungen in natürlicher Sprache verwenden.

Tools

AWS-Services

- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Mainframe Modernization File Transfer with BMC konvertiert Mainframe-Datensätze und überträgt sie an Amazon S3 für Anwendungsfälle zur Mainframe-Modernisierung, -Migration und Erweiterung.
- Amazon QuickSight ist ein BI-Service auf Cloud-Ebene, mit dem Sie Ihre Daten in einem einzigen Dashboard visualisieren, analysieren und melden können. Dieses Muster verwendet die generativen BI-Funktionen von Amazon Q in QuickSight.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Bewährte Methoden

- Wenn Sie die AWS Identity and Access Management (IAM-) Rollen für AWS Mainframe Modernization File Transfer mit BMC und der Lambda-Funktion erstellen, folgen Sie dem Prinzip der geringsten Rechte.
- Stellen Sie sicher, dass Ihr Quelldatensatz Datentypen für unterstützt. QuickSight Wenn Ihr Quelldatensatz Datentypen enthält, die nicht unterstützt werden, konvertieren Sie diese in unterstützte Datentypen. Informationen zu nicht unterstützten Mainframe-Datentypen und deren Konvertierung in von Amazon Q unterstützte Datentypen finden Sie im QuickSight Abschnitt Verwandte Ressourcen.

Epen

Richten Sie die AWS Mainframe Modernization Dateiübertragung mit BMC ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den File Transfer Agent.	Folgen Sie den Anweisungen in der AWS Dokumentation, um AWS Mainframe Modernization File Transfer Agent auf Ihrem Mainframe zu installieren.	Mainframe-Systemadministrator
Erstellen Sie einen S3-Bucket für die Mainframe-Dateiübertragung.	Erstellen Sie einen S3-Bucket, um die Ausgabedatei von AWS Mainframe Modernization File Transfer with BMC zu speichern. Im Architekturdiagramm ist dies der Ziel-Bucket für die Dateiübertragung.	Ingenieur für Migration
Erstellen Sie den Endpunkt für die Datenübertragung.	1. Erstellen Sie einen S3-Bucket, um die Mainframe-Eingabedatei für die AWS Mainframe Modernization Dateiübertragung mit BMC bereitzustellen. 2. Folgen Sie den Anweisungen in der Dokumentation, um den Mainframe-Datenübertragungsendpunkt zu erstellen.AWS	Spezialist AWS AWS-Mainframe-Modernisierung

Konvertieren Sie die Mainframe-Dateinamenerweiterung für die Integration QuickSight

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Erstellen Sie einen S3-Bucket für die Lambda-Funktion, um die konvertierte Mainframe-Datei von der Quelle in den endgültigen Ziel-Bucket zu kopieren.	Ingenieur für Migration
Erstellen Sie eine Lambda-Funktion.	Gehen Sie wie folgt vor, um eine Lambda-Funktion zu erstellen, die die Dateierweiterung ändert und die Mainframe-Datei in den Ziel-Bucket kopiert: 1. Melden Sie sich bei der AWS Management Console an und navigieren Sie zur AWS Lambda Konsole. 2. Wählen Sie „Funktion erstellen“ und anschließend „Von Grund auf neu erstellen“. 3. Geben Sie unter Funktionsname einen Namen für Ihre Funktion ein. 4. Wählen Sie in der Runtime-Dropdown-Liste Python.3.X aus. 5. Erweitern Sie Standardausführungsrolle ändern und wählen Sie dann Neue Rolle mit grundlegenden	Migrationsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Lambda-Berechtigungen erstellen aus. 6. Wählen Sie Funktion erstellen. 7. Wählen Sie die Registerkarte Code und fügen Sie dann den `S3CopyLambda.py` Python-Code ein, der im Abschnitt Zusätzliche Informationen bereitgestellt wird. Der Python-Code wurde mithilfe von Amazon Q Developer in der integrierten Entwicklungsumgebung (IDE) von Microsoft Visual Studio generiert. 8. Bearbeiten Sie den `destination_bucket_name` auf den Namen des S3-Buckets, den Sie zuvor erstellt haben, und `change destination_file_key` auf den Namen der Mainframe-Datei. 9. Stellen Sie die Lambda-Funktion bereit.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Amazon S3 S3-Trigger, um die Lambda-Funktion aufzurufen.	Gehen Sie wie folgt vor, um einen Trigger zu konfiguri eren, der die Lambda-Funktion aufruft: 1. Öffnen Sie in der Lambda-Konsole die Seite Funktione n. 2. Wählen Sie die Lambda-Fu nktion. 3. Wählen Sie in der Funktions übersicht die Option Trigger hinzufügen aus. 4. Wählen Sie in der Dropdownliste Trigger-K onfiguration die Option S3 aus. 5. Geben Sie im Feld Bucket den Namen Ihres Quell-Buc kets ein. 6. Wählen Sie in der Dropdownliste Ereignistyp die Option Alle Ereignisse zur Objekterstellung aus. 7. Aktivieren Sie das Kontrollk ästchen Ich bestätige, dass die Verwendung desselben S3-Buckets für Eingabe und Ausgabe nicht empfohlen wird, und wählen Sie dann Hinzufügen aus.	Leiter der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter Tutorial: Verwenden eines Amazon S3-Auslösers zum Aufrufen einer Lambda-Funktion.	
Stellen Sie IAM-Berechtigungen für die Lambda-Funktion bereit.	Für den Zugriff der Lambda-Funktion auf die S3-Buckets des Dateiübertragungsziels und des Quelldatensatzes sind IAM-Berechtigungen erforderlich. Aktualisieren Sie die Richtlinie, die mit der Lambda-Funktionsausführungsrolle verknüpft ist, indem Sie den Ziel-S3-Bucket für die Dateiübertragung `s3:GetObject` und `s3:DeleteObject` den `s3:PutObject` Zugriff auf den S3-Bucket des Quelldatensatzes zulassen und gewähren. Weitere Informationen finden Sie im Abschnitt Erstellen einer Berechtigungsrichtlinie in Tutorial: Verwenden eines Amazon S3 S3-Triggers zum Aufrufen einer Lambda-Funktion.	Leiter der Migration

Definieren Sie eine Mainframe-Datenübertragungsaufgabe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Übertragungsaufgabe, um die Mainframe-Datei in den S3-Bucket zu kopieren.	Folgen Sie den Anweisungen in der Dokumentation, um eine Mainframe-Dateiübertragungsaufgabe zu erstellen.AWS Mainframe Modernization **Note** Geben Sie die Quellcodepage-Kodierung auf IBM1 047 und die Ziel-Codepage-Kodierung auf UTF-8 an.	Ingenieur für Migration
Überprüfen Sie die Übertragungsaufgabe.	Folgen Sie den Anweisungen in der AWS Mainframe Modernization Dokumentation, um zu überprüfen, ob die Datenübertragung erfolgreich war. Vergewissern Sie sich, dass sich die Mainframe-Datei im Ziel-S3-Bucket für die Dateiübertragung befindet.	Leiter der Migration
Überprüfen Sie die Lambda-Kopierfunktion.	Stellen Sie sicher, dass die Lambda-Funktion initiiert wurde und dass die Datei mit der Erweiterung.csv in den S3-Bucket des Quelldatensatzes kopiert wurde.	Leiter der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Die von der Lambda-Fu nktion erstellte .csv-Datei ist die Eingabedatendatei für. QuickSight Beispieldaten finden Sie in der `Sample-da ta-member-healthca re-APG` Datei im Abschnitt Anlagen.	

Connect QuickSight zu den Mainframe-Daten her

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Einrichten QuickSight.	Folgen Sie zur Einrichtung QuickSight den Anweisungen in der AWS Dokumentation.	Leitung der Migration
Erstellen Sie einen Datensatz für QuickSight.	Folgen Sie den Anweisung en in der AWS Dokumenta tion QuickSight, um einen Datensatz für zu erstellen. Die Eingabedatendatei ist die konvertierte Mainframe-Datei, die bei der Definition der Mainframe-Datenübertragungs aufgabe erstellt wurde.	Leiter der Migration

Gewinnen Sie geschäftliche Einblicke aus den Mainframe-Daten mithilfe von Amazon Q in QuickSight

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Amazon Q in ein QuickSight.	Für diese Funktion ist die Enterprise Edition erforderl ich. Gehen Sie wie folgt vor	Leiter der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	QuickSight, um Amazon Q in einzurichten: 1. Um das Amazon Q-Add-on zu erhalten, folgen Sie den Anweisungen Schritt 1: Holen Sie sich das Q-Add-on in der AWS Dokumentation. 2. Um die generativen BI-Funktionen in Amazon Q zu nutzen, aktualisieren Sie die Konten Ihrer Benutzer. Folgen Sie den Anweisungen in der AWS Dokumentation. 3. Erstellen Sie ein Amazon Q-Thema, indem Sie den Datensatz verwenden, den Sie zuvor erstellt haben. Folgen Sie den Anweisungen in der AWS Dokumentation. 4. Folgen Sie den Anweisungen in der Dokumentation, um die Metadaten des Themas so zu konfigurieren, dass sie für natürliche Sprachen geeignet sind.AWS	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie Mainframe-Daten und erstellen Sie ein visuelles Dashboard.	Gehen Sie wie folgt vor QuickSight, um Ihre Daten zu analysieren und zu visualisieren: 1. Folgen Sie den Anweisungen in der AWS Dokumentation, um die Mainframe-Datenanalyse zu erstellen. Wählen Sie für den Datensatz den Datensatz aus, der im vorherigen Schritt erstellt wurde. 2. Wählen Sie auf der Analyseseite Visual erstellen aus. 3. Wählen Sie im Fenster „Thema für Analyse erstellen“ die Option Bestehendes Thema aktualisieren aus. 4. Wählen Sie in der Dropdownliste Thema auswählen das Thema aus, das Sie zuvor erstellt haben. 5. Wählen Sie Themenverknüpfung aus. 6. Nachdem Sie das Thema verknüpft haben, wählen Sie Visual erstellen, um das Amazon Q-Fenster Build a Visual zu öffnen.	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Schreiben Sie in der Eingabeaufforderungsleiste Ihre Analysefragen. Die für dieses Muster verwendeten Beispielfragen sind die folgenden: • Verteilung der Mitglieder nach Regionen anzeigen • Verteilung der Mitglieder nach Alter anzeigen • Verteilung der Mitglieder nach Geschlecht anzeigen • Verteilung der Mitglieder nach Tariftyp anzeigen • Zeigt das Mitglied an, das die präventive Impfung nicht abgeschlossen hat Nachdem Sie Ihre Fragen eingegeben haben, wählen Sie Build. Amazon Q in QuickSight erstellt die Grafiken. 8. Um die Grafiken zu Ihrem visuellen Dashboard hinzuzufügen, wählen Sie ZUR ANALYSE HINZUFÜGEN. Wenn Sie fertig sind, können Sie Ihr Dashboard veröffentlichen, um es mit anderen in Ihrer Organisation zu teilen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Beispiele finden Sie unter Visuelles Mainframe-Dashboard im Abschnitt Zusätzliche Informationen.	

Erstellen Sie eine Datenstory mit Amazon Q in QuickSight aus den Mainframe-Daten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Datenstory.	Erstellen Sie eine Datenstory, um die Erkenntnisse aus der vorherigen Analyse zu erläutern, und geben Sie eine Empfehlung zur Erhöhung der präventiven Impfungen für Mitglieder ab: 1. Folgen Sie den Anweisungen in der AWS Dokumentation, um die Data Story zu erstellen. 2. Verwenden Sie für den Data Story-Prompt Folgendes: `Build a data story about Region with most numbers of members. Also show the member distribution by medical plan, vision plan, dental plan. Recommend how to motivate members to`	Ingenieur für Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`complete immunizat ion. Include 4 points of supportin g data for this pattern.` Sie können auch Ihre eigene Eingabeaufforderun g erstellen, um Datenstor ys für andere Geschäfts einblicke zu generieren. 3. Wählen Sie Visuals hinzufügen aus und fügen Sie die Grafiken hinzu, die für die Data Story relevant sind. Verwenden Sie für dieses Muster die Grafiken, die Sie zuvor erstellt haben. 4. Wählen Sie Build aus. 5. Ein Beispiel für die Ausgabe von Data Storys finden Sie unter Data Story-Ausgabe im Abschnitt Zusätzliche Informationen.	
Sehen Sie sich die generierte Datenstory an.	Folgen Sie den Anweisungen in der AWS Dokumentation, um die generierte Datenstory anzusehen.	Leitung der Migration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bearbeiten Sie eine generierte Datenstory.	Folgen Sie den Anweisungen in der AWS Dokumentation, um die Formatierung, das Layout oder die visuelle Darstellung in einer Data Story zu ändern.	Leiter der Migration
Teilen Sie eine Datenstory.	Folgen Sie den Anweisungen in der AWS Dokumentation, um eine Data Story mit anderen zu teilen.	Ingenieur für Migration

Fehlerbehebung

Problem	Lösung
Die Mainframe-Dateien oder Datensätze, die in die Suchkriterien für Datensätze für die Aufgabe Übertragung erstellen in AWS Mainframe Modernization File Transfer with BMC eingegeben wurden, konnten nicht gefunden werden.	1. Überprüfen Sie zunächst die Verbindung, indem Sie in der Konsole „Übertragung mit BMC“ die Option AWS Mainframe Modernization Datenübertragungsendpunkte auswählen. Wenn die letzte Heartbeat-Zeit länger als zwei Minuten ist, wurde die Verbindung für die Dateiübertragung nicht hergestellt. Wenn die letzte Heartbeat-Zeit für den auf dem Mainframe ausgeführten Agenten weniger als 2 Minuten beträgt, ist die Verbindung zum Agenten erfolgreich. Fahren Sie mit Schritt 2 fort. 2. Überprüfen Sie das AWS Secrets Manager Setup. Ein geheimer Schlüssel muss in Secrets Manager mit einem Schlüssel von `userId` (Großbuchstabe I) mit dem Wert der Benutzer-ID des Mainframes und einem Schlüssel `password` mit dem Wert

Problem	Lösung
	des Mainframe-Kennworts konfiguriert werden. Bei den `userId` und `password` geheimen Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden und sie müssen unverändert eingegeben werden.

Zugehörige Ressourcen

Um Mainframe-Datentypen wie PACKED-DECIMAL (COMP-3) oder BINARY (COMP oder COMP-4) in einen Datentyp zu konvertieren, der von unterstützt wird, verwenden Sie die folgenden Muster: QuickSight

- EBCDIC-Daten mithilfe von Python in ASCII umwandeln und entpacken AWS
- Konvertieren Sie Mainframe-Dateien vom EBCDIC-Format in das durch Zeichen getrennte ASCII-Format in Amazon S3 mit AWS Lambda

Zusätzliche Informationen

S3 .py CopyLambda

Der folgende Python-Code wurde mithilfe einer Aufforderung mit Amazon Q Developer in einer IDE generiert:

```
#Create a lambda function triggered by S3. display the S3 bucket name and key
import boto3
s3 = boto3.client('s3')
def lambda_handler(event, context):
print(event)
bucket = event['Records'][0]['s3']['bucket']['name']
key = event['Records'][0]['s3']['object']['key']
print(bucket, key)
#If key starts with object_created, skip copy, print "copy skipped". Return lambda with
 key value.
if key.startswith('object_created'):
print("copy skipped")
return {
'statusCode': 200,
```

```
'body': key
}
# Copy the file from the source bucket to the destination bucket.
 Destination_bucket_name = 'm2-filetransfer-final-opt-bkt'. Destination_file_key =
 'healthdata.csv'
copy_source = {'Bucket': bucket, 'Key': key}
s3.copy_object(Bucket='m2-filetransfer-final-opt-bkt', Key='healthdata.csv',
 CopySource=copy_source)
print("file copied")
#Delete the file from the source bucket.
s3.delete_object(Bucket=bucket, Key=key)
return {
'statusCode': 200,
'body': 'Copy Successful'
}
```

Visuelles Mainframe-Dashboard

Das folgende Datenbild wurde von Amazon Q QuickSight für die Analysefrage erstellt `show member distribution by region`.

Das folgende Datenbild wurde von Amazon Q QuickSight für die Frage erstellt`show member distribution by Region who have not completed preventive immunization, in pie chart`.

Ausgabe von Data Story

Die folgenden Screenshots zeigen Abschnitte der Datenstory, die von Amazon Q QuickSight für die Aufforderung erstellt wurden. `Build a data story about Region with most numbers of members. Also show the member distribution by medical plan, vision plan, dental plan. Recommend how to motivate members to complete immunization. Include 4 points of supporting data.`

In der Einleitung wird in der Datenstory empfohlen, die Region mit den meisten Mitgliedern auszuwählen, um die größtmögliche Wirkung der Impfmaßnahmen zu erzielen.

Die Datenstory enthält eine Analyse der Mitgliederzahlen für die drei wichtigsten Regionen und nennt den Südwesten als die Region, in der der Schwerpunkt auf Impfmaßnahmen liegt.

> **Note**
>
> Die Regionen Südwesten und Nordosten haben jeweils acht Mitglieder. Im Südwesten gibt es jedoch mehr Mitglieder, die nicht vollständig geimpft sind, sodass er mehr Potenzial hat, von Initiativen zur Erhöhung der Impfraten zu profitieren.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Integrieren Sie den Stonebranch Universal Controller in die AWS-Mainframe-Modernisierung

Erstellt von Vaidy Sankaran (AWS), Robert Lemieux (Stonebranch), Hüseyin Gomleksizoglu (Stonebranch) und Pablo Alonso Prieto (AWS)

Übersicht

Dieses Muster erklärt, wie die Workload-Orchestrierung des Stonebranch Universal Automation Center (UAC) in den Mainframe-Modernisierungsservice von Amazon Web Services (AWS) integriert wird. Der AWS Mainframe Modernization Service migriert und modernisiert Mainframe-Anwendungen in die AWS-Cloud. Es bietet zwei Muster: AWS Mainframe Modernization Replatform mit Micro Focus Enterprise-Technologie und AWS Mainframe Modernization Automated Refactor mit AWS Blu Age.

Stonebranch UAC ist eine Plattform für IT-Automatisierung und Orchestrierung in Echtzeit. UAC wurde entwickelt, um Jobs, Aktivitäten und Workflows in hybriden IT-Systemen zu automatisieren und zu orchestrieren, von On-Premise bis hin zu AWS. Unternehmenskunden, die Mainframe-Systeme verwenden, stellen auf Cloud-zentrierte, modernisierte Infrastrukturen und Anwendungen um. Die Tools und professionellen Services von Stonebranch erleichtern die Migration vorhandener Scheduler und Automatisierungsfunktionen in die AWS-Cloud.

Wenn Sie Ihre Mainframe-Programme mithilfe des AWS Mainframe Modernization Service in die AWS-Cloud migrieren oder modernisieren, können Sie diese Integration nutzen, um die Batch-Planung zu automatisieren, die Agilität zu erhöhen, die Wartung zu verbessern und die Kosten zu senken.

Dieses Muster enthält Anweisungen für die Integration von Stonebranch Scheduler in Mainframe-Anwendungen, die zur Laufzeit des AWS Mainframe Modernization Service Micro Focus Enterprise migriert wurden. Dieses Muster richtet sich an Lösungsarchitekten, Entwickler, Berater, Migrationsspezialisten und andere Personen, die in den Bereichen Migrationen, Modernisierungen, Betrieb oder tätig sind. DevOps

Angestrebtes Ergebnis

Dieses Muster konzentriert sich auf die Erzielung der folgenden Zielergebnisse:

- Die Möglichkeit, Mainframe-Batch-Jobs, die im AWS Mainframe Modernization Service (Microfocus Runtime) ausgeführt werden, von Stonebranch Universal Controller aus zu planen, zu automatisieren und auszuführen.

- Überwachen Sie die Batch-Prozesse der Anwendung vom Stonebranch Universal Controller aus.
- Start/Restart/Rerun/StopBatch-Prozesse automatisch oder manuell vom Stonebranch Universal Controller aus.
- Rufen Sie die Ergebnisse der Batch-Prozesse für die AWS Mainframe-Modernisierung ab.
- Erfassen Sie die CloudWatchAWS-Protokolle der Batch-Jobs in Stonebranch Universal Controller.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Micro Focus Bank-Demo-Anwendung mit Job Control Language (JCL) -Dateien und einem Batch-Prozess, der in einer AWS Mainframe Modernization Service-Umgebung (Micro Focus Runtime) bereitgestellt wird
- Grundkenntnisse zum Erstellen und Bereitstellen einer Mainframe-Anwendung, die auf Micro Focus Enterprise Server läuft
- Grundkenntnisse über Stonebranch Universal Controller
- Stonebranch-Testlizenz (wenden Sie sich an Stonebranch)
- Windows- oder Linux-Instances von Amazon Elastic Compute Cloud (Amazon EC2) (z. B. xlarge) mit mindestens vier Kernen, 8 GB Arbeitsspeicher und 2 GB Festplattenspeicher
- Apache Tomcat Version 8.5.x oder 9.0.x
- Oracle Java Runtime Environment (JRE) oder OpenJDK Version 8 oder 11
- Amazon Aurora MySQL-kompatible Edition
- Amazon Simple Storage Service (Amazon S3) -Bucket für das Export-Repository
- Amazon Elastic File System (Amazon EFS) für Agenten Stonebranch Universal Message Service (OMS) -Verbindungen für Hochverfügbarkeit (HA)
- Installationsdateien für Stonebranch Universal Controller 7.2 Universal Agent 7.2
- Vorlage für die Aufgabenplanung von AWS Mainframe Modernization (neueste veröffentlichte Version der ZIP-Datei)

Einschränkungen

- Das Produkt und die Lösung wurden nur mit OpenJDK 8 und 11 getestet und ihre Kompatibilität validiert.

- Die Aufgabenplanungsvorlage aws-mainframe-modernization-stonebranch-integration funktioniert nur mit dem AWS Mainframe Modernization Service.
- Diese Vorlage zur Aufgabenplanung funktioniert nur auf einer Unix-, Linux- oder Windows-Edition von Stonebranch-Agenten.
- Einige AWS-Services sind nicht in allen AWS-Regionen verfügbar. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie unter AWS-Services nach Regionen. Informationen zu bestimmten Endpunkten finden Sie auf der Seite Service-Endpunkte und Kontingente. Wählen Sie dort den Link für den Service.

Architektur

Architektur des Zielzustands

Das folgende Diagramm zeigt die AWS-Beispielumgebung, die für dieses Pilotprojekt erforderlich ist.

1. Das Stonebranch Universal Automation Center (UAC) umfasst zwei Hauptkomponenten: Universal Controller und Universal Agents. Stonebranch OMS wird als Nachrichtenbus zwischen dem Controller und einzelnen Agenten verwendet.
2. Die Stonebranch UAC-Datenbank wird von Universal Controller verwendet. Die Datenbank kann mit MySQL, Microsoft SQL Server, Oracle oder Aurora MySQL kompatibel sein.
3. AWS Mainframe Modernization Service — Micro Focus-Laufzeitumgebung mit der bereitgestellten BankDemo Anwendung. Die BankDemo Anwendungsdateien werden in einem S3-Bucket gespeichert. Dieser Bucket enthält auch die Mainframe-JCL-Dateien.
4. Stonebranch UAC kann die folgenden Funktionen für den Batchlauf ausführen:
    a. Starten Sie einen Batch-Job mit dem JCL-Dateinamen, der im S3-Bucket vorhanden ist, der mit dem AWS-Mainframe-Modernisierungsservice verknüpft ist.
    b. Rufen Sie den Status des ausgeführten Batch-Jobs ab.
    c. Warten Sie, bis die Batch-Job-Ausführung abgeschlossen ist.
    d. Ruft die Protokolle der Batch-Job-Ausführung ab.
    e. Führen Sie die fehlgeschlagenen Batch-Jobs erneut aus.
    f. Brechen Sie den Batch-Job ab, während der Job ausgeführt wird.
5. Stonebranch UAC kann die folgenden Funktionen für die Anwendung ausführen:
    a. Anwendung starten

b. Status der Bewerbung abrufen

c. Warten Sie, bis die Anwendung gestartet oder gestoppt ist

d. Anwendung beenden

e. Protokolle des Anwendungsbetriebs abrufen

Konvertierung von Stonebranch-Jobs

Das folgende Diagramm zeigt den Prozess der Umstellung von Arbeitsplätzen bei Stonebranch während der Modernisierung. Es wird beschrieben, wie die Jobpläne und Aufgabendefinitionen in ein kompatibles Format konvertiert werden, mit dem Batch-Aufgaben von AWS Mainframe Modernization ausgeführt werden können.

1. Für den Konvertierungsprozess werden die Jobdefinitionen aus dem vorhandenen Mainframe-System exportiert.
2. JCL-Dateien können in den S3-Bucket für die Mainframe-Modernisierungsanwendung hochgeladen werden, sodass diese JCL-Dateien vom AWS Mainframe Modernization Service bereitgestellt werden können.
3. Das Konvertierungstool konvertiert die exportierten Auftragsdefinitionen in UAC-Aufgaben.
4. Nachdem alle Aufgabendefinitionen und Jobpläne erstellt wurden, werden diese Objekte in den Universal Controller importiert. Die konvertierten Aufgaben führen dann die Prozesse im AWS Mainframe Modernization Service aus, anstatt sie auf dem Mainframe auszuführen.

Stonebranch UAC-Architektur

Das folgende Architekturdiagramm stellt ein active-active-passive Modell eines Universal Controllers mit hoher Verfügbarkeit (HA) dar. Stonebranch UAC wird in mehreren Availability Zones eingesetzt, um hohe Verfügbarkeit zu gewährleisten und Disaster Recovery (DR) zu unterstützen.

Universeller Controller

Zwei Linux-Server werden als Universal Controller bereitgestellt. Beide stellen eine Verbindung zum selben Datenbankendpunkt her. Jeder Server beherbergt eine Universal Controller-Anwendung und OMS. Zum Zeitpunkt der Bereitstellung wird die neueste Version von Universal Controller verwendet.

Die Universal Controller werden in der Tomcat-Webapp als Dokument ROOT bereitgestellt und auf Port 80 bereitgestellt. Diese Bereitstellung erleichtert die Konfiguration des Frontend-Load Balancers.

HTTP über TLS oder HTTPS wird mithilfe des Stonebranch-Platzhalterzertifikats aktiviert (z. B.). `https://customer.stonebranch.cloud` Dadurch wird die Kommunikation zwischen dem Browser und der Anwendung gesichert.

OMS

Ein Universal Agent und OMS (Opswise Message Service) befinden sich auf jedem Universal Controller-Server. Alle vom Kunden bereitgestellten Universal Agents sind so eingerichtet, dass sie eine Verbindung zu beiden OMS-Diensten herstellen. OMS fungiert als gemeinsamer Messaging-Dienst zwischen den Universal Agents und dem Universal Controller.

Amazon EFS mountet auf jedem Server ein Spool-Verzeichnis. OMS verwendet dieses gemeinsam genutzte Spool-Verzeichnis, um die Verbindungs- und Aufgabeninformationen von Controllern und Agenten zu speichern. OMS arbeitet in einem Hochverfügbarkeitsmodus. Wenn das aktive OMS ausfällt, hat das passive OMS Zugriff auf alle Daten und nimmt den aktiven Betrieb automatisch wieder auf. Universal Agents erkennen diese Änderung und stellen automatisch eine Verbindung zum neuen aktiven OMS her.

Datenbank

Amazon Relational Database Service (Amazon RDS) beherbergt die UAC-Datenbank, deren Engine mit Amazon Aurora MySQL kompatibel ist. Amazon RDS hilft bei der Verwaltung und Bereitstellung von geplanten Backups in regelmäßigen Abständen. Beide Universal Controller-Instances stellen eine Verbindung mit demselben Datenbank-Endpunkt her.

Load Balancer

Für jede Instanz wird ein Application Load Balancer eingerichtet. Der Load Balancer leitet den Datenverkehr zu einem bestimmten Zeitpunkt an den aktiven Controller weiter. Ihre Instance-Domainnamen verweisen auf die jeweiligen Load Balancer-Endpunkte.

URLs

Jede Ihrer Instances hat eine URL, wie im folgenden Beispiel gezeigt.

Umgebung	Instance

Produktion	`customer.stonebranch.cloud`
Entwicklung (Nichtproduktion)	`customerdev.stonebranch.cloud`
Testen (außerhalb der Produktion)	`customertest.stonebranch.cloud`

> **Note**
>
> Instanznamen, die nicht zur Produktion verwendet werden, können Ihren Anforderungen entsprechend festgelegt werden.

Hohe Verfügbarkeit

Hochverfügbarkeit (HA) ist die Fähigkeit eines Systems, über einen bestimmten Zeitraum kontinuierlich ohne Ausfall zu arbeiten. Zu diesen Ausfällen gehören unter anderem Speicher, Reaktionsverzögerungen bei der Serverkommunikation aufgrund von CPU- oder Speicherproblemen und Netzwerkkonnektivität.

Um die HA-Anforderungen zu erfüllen:

- Alle EC2 Instances, Datenbanken und anderen Konfigurationen werden in zwei separaten Availability Zones innerhalb derselben AWS-Region gespiegelt.
- Der Controller wird über ein Amazon Machine Image (AMI) auf zwei Linux-Servern in den beiden Availability Zones bereitgestellt. Wenn Sie beispielsweise in der Region Europa eu-west-1 bereitgestellt werden, haben Sie einen Universal Controller in der Availability Zone eu-west-1a und der Availability Zone eu-west-1c.
- Jobs dürfen nicht direkt auf den Anwendungsservern ausgeführt werden und es dürfen keine Daten auf diesen Servern gespeichert werden.
- Der Application Load Balancer führt Integritätsprüfungen auf jedem Universal Controller durch, um den aktiven Controller zu identifizieren und den Datenverkehr an ihn weiterzuleiten. Falls bei einem Server Probleme auftreten, versetzt der Load Balancer den passiven Universal Controller automatisch in einen aktiven Status. Der Load Balancer identifiziert dann die neue aktive Universal Controller-Instanz anhand der Integritätsprüfungen und leitet den Datenverkehr weiter. Der Failover erfolgt innerhalb von vier Minuten ohne Jobverlust, und die Frontend-URL bleibt unverändert.
- Der Aurora MySQL-kompatible Datenbankdienst speichert Universal Controller-Daten. Für Produktionsumgebungen wird ein Datenbankcluster mit zwei Datenbank-Instances in zwei

verschiedenen Availability Zones innerhalb einer einzigen AWS-Region erstellt. Beide Universal Controller verwenden eine Java Database Connectivity (JDBC) -Schnittstelle, die auf einen einzelnen Datenbankcluster-Endpunkt verweist. Falls bei einer Datenbankinstanz Probleme auftreten, verweist der Datenbankcluster-Endpunkt dynamisch auf die fehlerfreie Instanz. Es ist kein manueller Eingriff erforderlich.

Backup und Löschen

Stonebranch Universal Controller ist so eingestellt, dass alte Daten nach dem in der Tabelle angegebenen Zeitplan gesichert und gelöscht werden.

Typ	Plan
Aktivität	7 Tage
Prüfung	90 Tage
Verlauf	60 Tage

Backup-Daten, die älter als die angegebenen Daten sind, werden in das XML-Format exportiert und im Dateisystem gespeichert. Nach Abschluss des Sicherungsvorgangs werden ältere Daten aus der Datenbank gelöscht und für Produktionsinstanzen bis zu einem Jahr in einem S3-Bucket archiviert.

Sie können diesen Zeitplan in Ihrer Universal Controller-Oberfläche anpassen. Eine Verlängerung dieser Zeitrahmen kann jedoch zu längeren Ausfallzeiten während der Wartung führen.

Tools

AWS-Services

- AWS Mainframe Modernization ist eine Cloud-native AWS-Plattform, mit der Sie Ihre Mainframe-Anwendungen auf von AWS verwaltete Laufzeitumgebungen modernisieren können. Er bietet Tools und Ressourcen, die Sie bei der Planung und Implementierung von Migration und Modernisierung unterstützen.
- Amazon Elastic Block Store (Amazon EBS) bietet Speichervolumen auf Blockebene zur Verwendung mit Amazon-Instances. EC2
- Amazon Elastic File System (Amazon EFS) unterstützt Sie bei der Erstellung und Konfiguration gemeinsam genutzter Dateisysteme in der AWS-Cloud.

- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der AWS-Cloud. Dieses Muster verwendet Amazon Aurora MySQL-Compatible Edition.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Traffic auf EC2 Amazon-Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen. Dieses Muster verwendet einen Application Load Balancer.

Stonebranch

- Das Universal Automation Center (UAC) ist ein System von Produkten zur Workload-Automatisierung für Unternehmen. Dieses Muster verwendet die folgenden UAC-Komponenten:
  - Universal Controller, eine Java-Webanwendung, die in einem Tomcat-Webcontainer ausgeführt wird, ist die Lösung für Enterprise Job Scheduler und Workload Automation Broker von Universal Automation Center. Der Controller bietet eine Benutzeroberfläche zum Erstellen, Überwachen und Konfigurieren von Controller-Informationen, verwaltet die Planungslogik, verarbeitet alle Nachrichten an und von Universal Agents und synchronisiert einen Großteil des Hochverfügbarkeitsbetriebs von Universal Automation Center.
  - Universal Agent ist ein herstellerunabhängiger Planungsagent, der mit dem vorhandenen Job Scheduler auf allen wichtigen Computerplattformen zusammenarbeitet, sowohl auf älteren als auch auf verteilten Computerplattformen. Alle Scheduler, die auf z/Series, I/Series, Unix, Linux oder Windows laufen, werden unterstützt.
- Universal Agent ist ein herstellerunabhängiger Scheduling-Agent, der mit bestehenden Job-Schedulern auf allen wichtigen Computerplattformen, sowohl älteren als auch verteilten, zusammenarbeitet. Alle Scheduler, die auf z/Series, I/Series, Unix, Linux oder Windows laufen, werden unterstützt.
- Stonebranch aws-mainframe-modernization-stonebranch -integration AWS Mainframe Modernization Universal Extension ist die Integrationsvorlage zum Ausführen, Überwachen und erneuten Ausführen von Batch-Jobs auf der AWS Mainframe Modernization Platform.

Code

Der Code für dieses Muster ist im Repository -integration verfügbar. aws-mainframe-modernization-stonebranch GitHub

Epen

Installieren Sie Universal Controller und Universal Agent auf Amazon EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Installat ionsdateien herunter.	Laden Sie die Installation von den Stonebranch-Servern herunter. Wenden Sie sich an Stonebranch, um die Installat ionsdateien zu erhalten.	Cloud-Architekt
Starten Sie die EC2 Instanz.	Sie benötigen etwa 3 GB zusätzlichen Speicherplatz für die Universal Controller- und Universal Agent-Installationen. Stellen Sie also mindestens 30 GB Festplattenspeicher für die Instanz bereit. Fügen Sie der Sicherhei tsgruppe Port 8080 hinzu, damit darauf zugegriffen werden kann.	Cloud-Architekt
Überprüfen Sie die Vorausset zungen.	Gehen Sie vor der Installation wie folgt vor: 1. Installieren Sie Java wie unter Java Runtime Environment herunterladen beschrieben. ```$ sudo yum -y update```	Cloud-Administrator, Linux-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`$ sudo yum install java-11-amazon-corretto`
	
	Stellen Sie sicher, dass Sie eine der unterstützten JAVA-Versionen verwenden . Der vorherige Befehl sollte Java-11 installieren. Überprüfen Sie die Java-Version und stellen Sie sicher, dass Sie Version 11 verwenden, bevor Sie fortfahren.
	2. Führen Sie, wie unter Apache Tomcat installieren beschrieben, die folgenden Befehle aus.
	
	`$ sudo yum install tomcat tomcat-admin-webapps`
	`$ sudo systemctl enable tomcat`
	`$ sudo systemctl start tomcat`
	3. Erstellen Sie eine Amazon Aurora Aurora-Datenbank, wie unter Erstellen und Herstellen einer Verbindung zu einem Aurora MySQL-DB-Cluster beschrieben. Verwenden Sie die Amazon Aurora MySQL-kompatible Edition.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wählen Sie einen Master-Benutzernamen und ein Master-Passwort. Behalten Sie die Standardwerte für die restlichen Einstellungen bei.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie Universal Controller.	1. Laden Sie die `universal-controller-7.2.0.0.tar` Installationsdatei auf die EC2 Instanz hoch.
	2. Entarchivieren Sie die Installationsdateien in einem `temp` Ordner.
	`$ tar -xvf universal-controller-7.2.0.0.tar`
	3. Erteilen Sie dem Installationsskript die Ausführungsberechtigung.
	`$ chmod a+x install-controller.sh`
	4. Installieren Sie den Controller. In diesem Beispiel wird der folgende Befehl verwendet, um Universal Controller unter `/usr/share/tomcat` zu installieren. Verwenden Sie die Amazon Aurora Aurora-Datenbank, die Sie in den vorherigen Schritten erstellt haben.
	`$ sudo ./install-controller.sh --tomcat-dir /usr/share/tomcat/ --controller-file universal-controller-7.2.0.`
		Cloud-Architekt, Linux-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	0-build.145.war --dbuser admin --dbpass “****” --dbname uc --rdbms mysql --dburl jdbc:mysql://database-2-instance-1.cih63miincgy.us-east-1.rds.amazonaws.com:3306/ Die letzte Zeile der Skriptausgabe sollte „Installation abgeschlossen“ lauten. 5. Navigieren Sie in der EC2 Instanz zur folgenden URL. http://<public_ip>:8080/uc 6. Geben Sie auf dem Anmeldebildschirm im Bereich Nutzername ops.admin ein und lassen Sie das Feld Passwort leer. 7. Legen Sie ein neues Passwort für den `ops.admin` Benutzer fest.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie Universal Agent.	1. Laden Sie die `sb-7.2.0.1-linux-3.10-x86_64.tar.Z` Installationsdatei auf die EC2 Instanz hoch.
	2. Melden Sie sich bei der EC2 Instanz an.
	3. Entarchivieren Sie das Universal Agent-Installationspaket.
	`$ zcat sb-7.2.0.1-linux-3.10-x86_64.tar.Z | tar xvf -`
	4. Führen Sie den folgenden Befehl aus.
	`$ sudo ./unvinst --oms_servers 7878@localhost --oms_autostart yes --python yes`
	5. Erstellen Sie eine PAM-Datei.
	`$ cp /etc/pam.d/login /etc/pam.d/ucmd`
	6. Aktivieren Sie Autostart für Universal Agent.
	`$ /sbin/restorecon -v /etc/rc.d/init.d/ubrokerd`
		Cloud-Administrator, Linux-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie OMS zu Universal Controller hinzu.	1. Melden Sie sich mit dem `ops.admin` Benutzer bei Universal Controller an. 2. Wählen Sie in der oberen linken Ecke des Bildschirms das Menü Dienste und anschließend im System das Menü OMS-Server 3. Geben Sie im Feld OMS-Serveradresse den Text ein `localhost` , und speichern Sie dann. 4. Der Status des OMS-Servers wird als Verbunden und der Sitzungsstatus als Betriebsbereit angezeigt.	Universeller Controller-Administrator

Importieren Sie AWS Mainframe Modernization Universal Extension und erstellen Sie eine Aufgabe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Integrationsvorlage importieren.	Für diesen Schritt benötigen Sie die AWS Mainframe Modernization Universal Extension. Stellen Sie sicher, dass die neueste veröffentlichte Version der ZIP-Datei heruntergeladen wurde. 1. Melden Sie sich mit dem `ops.admin` Benutzer am Universal Controller an.	Universeller Controller-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Navigieren Sie zu Dienste, Integrationsvorlage importieren. 3. Wählen Sie die ZIP-Datei (`aws_mainframe_modernization_stonebranch_extension.zip`) der Integrationsvorlage aus und klicken Sie auf Importieren. Nachdem die Integrationsvorlage importiert wurde, werden unter Verfügbare Services AWS Mainframe Modernization Tasks angezeigt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie auflösbare Anmeldeinformationen.	1. Navigieren Sie zu Services, AWS Mainframe Modernization Tasks. 2. Füllen Sie im rechten Bereich die erforderlichen Felder aus: • Name: Neue Aufgabe zur Mainframe-Modernisierung • Agent: Wählen Sie den einzigen Agenten aus (AGNT0001). Unter Details zur AWS-Mainframe-Modernisierung: • Aktion: Umgebungen auflisten • AWS-Anmeldeinformationen: Wenn Sie der EC2 Instance eine AWS Identity and Access Management (IAM) -Rolle hinzugefügt haben, können Sie dieses Feld leer lassen. Wenn Sie `AWSAccessKeyID` und verwenden möchten`AWSSecretKey`, wählen Sie das Symbol () neben dem Feld. Geben Sie in dem sich öffnenden Fenster mit den	Universeller Controller-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anmeldeinformationen die folgenden Informationen ein und speichern Sie dann. • Name: Anmeldeinformationen für die AWS-Mainframe-Modernisierung • Runtime-Benutzer: Schreiben Sie die AWS-Zugriffsschlüssel-ID in dieses Feld. • Runtime-Passwort: Schreiben Sie den geheimen AWS-Schlüssel in dieses Feld. • Endpunkt: Stellen Sie sicher, dass der Endpunkt die richtige AWS-Region hat. Der Standardwert ist `https://m2.us-east-1.amazonaws.com` . • Region: Geben Sie die Region des AWS Mainframe Modernization Service ein. Der Standardwert ist `us-east-1` . 3. Behalten Sie die Standardwerte in den übrigen Feldern bei und speichern Sie die Aufgabe.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Aufgabe.	1. Wählen Sie oben im rechten Bereich die Option „Aufgabe starten“. 2. Wählen Sie im Bestätigungsfenster die Option Starten aus. Danach zeigt die Universal Controller Console eine Meldung an, die der folgenden Meldung ähnelt. 24.08.2022 10:11:49 Uhr Die Universalaufgabe „New Mainframe Modernization Task“ mit der Task-Instanz sys_id 166129149 3634146313 E38 OZJY wurde erfolgreich gestartet. NC8 DB8 3. Navigieren Sie zur Registerkarte „Instances“. Wenn Sie den Tab „Instances“ nicht sehen, klicken Sie auf den Rechtspfeil, um nach rechts zu scrollen. 4. Öffnen Sie das Kontextmenü (Rechtsklick) für die Task-Instanz in der Liste, wählen Sie „Ausgabe abrufen“ und wählen Sie dann unter „Ausgabe	Universeller Controller-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	abrufen“ die Option „Senden“ 5. Im Fenster „Ausgabe abrufen“ sehen Sie die Liste der Umgebungen in STDOUT.	

Testen Sie das Starten eines Batch-Jobs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Aufgabe für den Batch-Job.	1. Navigieren Sie zu Services, AWS Mainframe Modernization Tasks. 2. Füllen Sie im rechten Bereich die erforderlichen Felder aus: • Name: Neue Aufgabe zur Mainframe-Modernisierung • Agent: Wählen Sie den einzigen Agenten aus (AGNT0001). Unter Details zur AWS-Mainframe-Modernisierung: • Aktion: Batch starten (oder Batch starten und warten, bis der Batch-Job ausgeführt wird und bis die Aufgabe in AWS abgeschlossen ist)	Universeller Controller-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• AWS-Anmeldeinformationen: Wenn Sie der EC2 Instance eine IAM-Rolle hinzugefügt haben, können Sie dieses Feld leer lassen. Wenn Sie `AWSAccessKeyID` und verwenden möchten`AWSSecretKey`, wählen Sie das Symbol () neben dem Feld. • Endpunkt: Stellen Sie sicher, dass der Endpunkt die richtige AWS-Region hat. Der Standardwert ist https://m2.us-east-1.amazonaws.com. • Region: Geben Sie die Region des AWS Mainframe Modernization Service ein. Der Standardwert ist `us-east-1`. • Anwendung: Wählen Sie das Symbol neben dem Feld () und wählen Sie unter „Refresh Application Choices“ die Option „Senden“ aus. Dadurch wird eine Verbindung zum AWS Mainframe Moderniza	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	tion Service hergestel lt und die Liste der Anwendungen zurückgeg eben. Jetzt können Sie die Anwendung aus der Drop-down-Liste auswählen. Wählen Sie die Anwendung aus, mit der Sie den Batch-Job ausführen möchten. • JCL-Dateiname: `RUNHELLO.jcl` • Auf Erfolg oder Fehler warten: Wenn diese Option ausgewählt ist, wartet die Aufgabe, bis der Batch-Job den Status „Erfolg“ oder „Fehlschlag“ hat. • Abfrageintervall: Dies ist der Zeitraum zwischen den einzelnen Abfragen. • Ausführungsprotokolle abrufen: Wenn diese Option ausgewählt ist, werden Protokolle automatisch abgerufen , wenn der Batch-Job abgeschlossen ist. • Protokollformat: Dies ist das Format der Protokoll e, die ausgedruckt werden sollen. Es kann	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	im Text- oder JSON-Form at sein. 3. Behalten Sie die Standardw erte in den übrigen Feldern bei und speichern Sie die Aufgabe.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Aufgabe.	1. Wählen Sie oben im rechten Bereich die Option „Aufgabe starten“. 2. Wählen Sie im Bestätigungsfenster die Option Starten aus. Danach zeigt die Universal Controller Console eine Meldung an, die der folgenden Meldung ähnelt. 24.08.2022 11:11:59 Uhr Die Universalaufgabe „Mainframe Modernization Start Batch“ wurde erfolgreich mit der Taskinstanz sys_id gestartet. <sys id> 3. Navigieren Sie zur Registerkarte Instances. Wenn Sie den Tab Instances nicht sehen, klicken Sie auf den Rechtspfeil, um nach rechts zu blättern. 4. Öffnen Sie das Kontextmenü (Rechtsklick) für die Task-Instanz in der Liste, wählen Sie „Ausgabe abrufen“ und wählen Sie dann unter „Ausgabe abrufen“ die Option „Senden“	Universeller Controller-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Im Fenster „Ausgabe abrufen“ sehen Sie die Liste der Umgebungen in STDOUT.	

Erstellen Sie einen Workflow für mehrere Aufgaben

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopieren Sie die Aufgaben.	1. Öffnen Sie das Kontextmenü (Rechtsklick) für die Aufgabe, von der Sie Kopien erstellen möchten, und wählen Sie Kopieren. 2. Geben Sie im Fenster Copy AWS Mainframe Modernization Task den folgenden neuen Namen für die neue Aufgabe ein: Mainframe Modernization Start Batch -. RUNAWS2 3. Kopieren Sie die Aufgabe erneut und verwenden Sie dabei den folgenden Namen: Mainframe Modernization Start Batch - RUNAWS3. 4. Kopieren Sie erneut mit der Aufgabe und verwenden Sie dabei den folgenden Namen: Mainframe Modernization Start Batch - RUNAWS4.	Universeller Controller-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Kopieren Sie die Aufgabe ein letztes Mal und verwenden Sie dabei den folgenden Namen: Mainframe Modernization Start Batch - FOOBAR.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aufgaben aktualisieren.	1. Öffnen Sie die Aufgabe Mainframe Modernization Start Batch — RUNAWS2 Task (Doppelklicken), ändern Sie das Feld JCL-Dateiname in und `RUNAWS2.jcl` speichern Sie. 2. Öffnen Sie die Aufgabe Mainframe Modernization Start Batch — RUNAWS3 Task (Doppelklicken), ändern Sie das Feld JCL-Dateiname in und `RUNAWS3.jcl` speichern Sie. 3. Öffnen Sie die Aufgabe Mainframe Modernization Start Batch — RUNAWS4 Task (Doppelklicken), ändern Sie das Feld JCL-Dateiname in und `RUNAWS4.jcl` speichern Sie. 4. Öffnen (doppelklicken) Sie die Aufgabe Mainframe Modernization Start Batch — FOOBAR, ändern Sie das Feld JCL-Datei name in und speichern Sie*`MISSING.jcl`* . Diese Aufgabe schlägt fehl, weil	Universeller Controller-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Wert für den JCL-Datei namen falsch ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Workflow.	1. Navigieren Sie zu Dienste, Workflows. 2. Geben Sie im rechten Bereich Mainframe Modernization Workflow in das Feld Name ein und speichern Sie. 3. Wählen Sie im rechten Bereich die Option Workflow bearbeiten aus. 4. Klicken Sie auf der Registerkarte Workflow-Editor auf die Schaltfläche „Aufgabe hinzufügen“ (+). 5. Wählen Sie im Fenster „Aufgaben suchen“ die Option „Suchen“, um alle Aufgaben im Universal Controller anzuzeigen. 6. Klicken Sie auf das Symbol neben Mainframe Modernization Start Batch Task und ziehen Sie das Symbol an eine leere Stelle im Workflow-Editor. 7. Wiederholen Sie dieselbe Aktion für die anderen Mainframe-Modernis ierungsaufgaben und platzieren Sie sie wie im Abschnitt Zusätzliche Informationen gezeigt.	Universeller Controller-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Wählen Sie die Schaltfläche Connect () und verbinden Sie die Aufgaben miteinander. Um eine Aufgabe mit einer anderen zu verbinden, klicken Sie in die Mitte einer Aufgabe und ziehen Sie sie auf die Zielaufgabe. 9. Connect die Aufgaben wie im Abschnitt Zusätzliche Informationen gezeigt, und speichern Sie den Workflow. 10. Klicken Sie mit der rechten Maustaste auf eine leere Stelle im Workflow-Editor, wählen Sie Workflow starten und dann OK.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Status des Workflows.	1. Wählen Sie im linken Menü die Aktivität 2. Wählen Sie in der Mitte des Fensters Start. Sie sehen die Liste der Task-Instanzen in der Liste. 3. Öffnen Sie den Mainframe Modernization Workflow in der Liste (doppelklicken Sie darauf) oder öffnen Sie das Kontextmenü (mit der rechten Maustaste) und wählen Sie Workflow-Aufgabenbefehle, Workflow anzeigen aus. Sie sehen die Aufgaben so, wie sie im Abschnitt Zusätzliche Informati onen dargestellt sind. Es wurde erwartet, dass die zweite Aufgabe fehlschla gen würde, weil Sie eine fehlende JCL-Datei verwendet haben.	Universeller Controller-Administrator

Beheben Sie fehlgeschlagene Batch-Jobs und führen Sie sie erneut aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Korrigieren Sie die fehlgesch lagene Aufgabe und führen Sie sie erneut aus.	1. Öffnen Sie die fehlgesch lagene Aufgabe (doppelkl icken Sie darauf), um den	Universeller Controller-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Fehler für die Aufgabe zu sehen. 2. Sie haben zwei Möglichkeiten, die fehlgeschlagene Aufgabe zu reparieren. • Korrigieren Sie den JCL-Dateinamen und setzen Sie ihn auf`F00BAR.jcl` . • Fügen Sie dem JCL-Dateinamen (Temp) den richtigen JCL-Dateinamen hinzu. Dieses Feld überschreibt das Feld JCL-Dateiname. Wählen Sie für dieses Pilotprojekt die zweite Option und speichern Sie die Task-Instanz. 3. Öffnen Sie im Workflow-Monitor das Kontextmenü (Rechtsklick) für die fehlgeschlagene Aufgabe und wählen Sie Befehle, Erneut ausführen. 4. Danach werden alle Aufgaben erfolgreich abgeschlossen.	

Aufgaben „Anwendung starten“ und „Anwendung beenden“ erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Aktion „Anwendung starten“.	1. Navigieren Sie zu Services, AWS Mainframe Modernization Tasks. 2. Füllen Sie im rechten Bereich die erforderlichen Felder aus. • Name: Anwendung zur Mainframe-Modernisierung starten • Agent: Wählen Sie den einzigen Agenten aus (AGNT0001) Unter Details zur AWS-Mainframe-Modernisierung: • Aktion: Anwendung starten • AWS-Anmeldeinformationen: Wenn Sie der EC2 Instance eine IAM-Rolle hinzugefügt haben, können Sie dieses Feld leer lassen. Wenn Sie `AWSAccessKeyID` und verwenden möchten`AWSSecretKey`, wählen Sie die Anmeldeinformationen aus, die Sie zuvor erstellt haben. • Endpunkt: Stellen Sie sicher, dass	Universeller Controller-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Endpunkt die richtige Region hat. Der Standardwert ist `https://m2.us-east-1.amazonaws.com` . • Region: Geben Sie die Region des AWS Mainframe Moderniza tion Service ein. Der Standardwert ist `us-east-1` . • Anwendung: Wählen Sie das Symbol neben dem Feld () und wählen Sie unter „Refresh Application Choices“ die Option „Senden“ aus. Dadurch wird eine Verbindung zum AWS Mainframe Moderniza tion Service hergestel lt und die Liste der Anwendungen zurückgeg eben. Jetzt können Sie die Anwendung aus der Drop-down-Liste auswählen. Wählen Sie die Anwendung aus, mit der Sie den Batch-Job ausführen möchten. • Auf Erfolg oder Fehler warten: Wenn diese Option ausgewählt ist, wartet die Aufgabe, bis	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Status des Batch-Jobs erfolgreich oder fehlgeschlagen ist. • Abfrageintervall: Dies ist der Zeitraum zwischen den einzelnen Abfragen. • Ausführungsprotokolle abrufen: Wenn diese Option ausgewählt ist, werden Protokolle automatisch abgerufen , wenn der Batch-Job abgeschlossen ist. • Protokollformat: Dies ist das Format der Protokoll e, die ausgedruckt werden sollen. Es kann im Text- oder JSON-Form at sein. 3. Behalten Sie die Standardw erte in den übrigen Feldern bei und speichern Sie die Aufgabe. 4. Kopieren Sie nun diese Aufgabe und erstellen Sie eine Aufgabe für „Anwendung beenden“. Ändern Sie den Namen in Mainframe Moderniz ation Stop Application und ändern Sie die Aktion in Stop Application.	

Eine Aufgabe zum Abbrechen der Batch-Ausführung erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Aktion „Batch stornieren“.	1. Navigieren Sie zu Services, AWS Mainframe Modernization Tasks. 2. Füllen Sie im rechten Bereich die erforderlichen Felder aus. • Name: Mainframe-Modernisierung Batch-Ausführung abbrechen • Agent: Wählen Sie den einzigen Agenten (AGNT0001) Unter Details zur AWS-Mainframe-Modernisierung: • Aktion: Batch-Ausführung abbrechen • AWS-Anmeldeinformationen: Wenn Sie der EC2 Instance eine IAM-Rolle hinzugefügt haben, können Sie dieses Feld leer lassen. Wenn Sie `AWSAccessKeyID` und verwenden möchten`AWSSecretKey`, wählen Sie die Anmeldeinformationen aus, die Sie zuvor erstellt haben. • Endpunkt: Stellen Sie sicher, dass	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Endpunkt die richtige Region hat. Der Standardwert ist `https://m2.us-east-1.amazonaws.com` . • Region: Geben Sie die Region des AWS Mainframe Moderniza tion Service ein. Der Standardwert ist `us-east-1` . • Anwendung: Wählen Sie das Symbol neben dem Feld () und wählen Sie unter „Refresh Application Choices“ die Option „Senden“ aus. Dadurch wird eine Verbindung zum AWS Mainframe Moderniza tion Service hergestel lt und die Liste der Anwendungen zurückgeg eben. Jetzt können Sie die Anwendung aus der Drop-down-Liste auswählen. Wählen Sie die Anwendung aus, mit der Sie den Batch-Job ausführen möchten. • Auf Erfolg oder Fehler warten: Wenn diese Option ausgewählt ist, wartet die Aufgabe, bis	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Status des Batch-Jobs erfolgreich oder fehlgeschlagen ist. • Abfrageintervall: Dies ist der Zeitraum zwischen den einzelnen Abfragen. • Ausführungsprotokolle abrufen: Wenn diese Option ausgewählt ist, werden Protokolle automatisch abgerufen , wenn der Batch-Job abgeschlossen ist. • Protokollformat: Dies ist das Format der Protokoll e, die ausgedruckt werden sollen. Es kann im Text- oder JSON-Form at sein. 3. Behalten Sie die Standardw erte in den übrigen Feldern bei und speichern Sie die Aufgabe.	

Zugehörige Ressourcen

- Universeller Controller
- Universeller Agent
- LDAP-Einstellungen
- SAML-Single-Sign-On
- Xpress-Konvertierungstool

Zusätzliche Informationen

Symbole im Workflow-Editor

Alle Aufgaben sind miteinander verbunden

Status des Workflows

Migrieren und replizieren Sie VSAM-Dateien mit Connect von Precisely zu Amazon RDS oder Amazon MSK

Erstellt von Prachi Khanna (AWS) und Boopathy GOPALSAMY (AWS)

Übersicht

Dieses Muster zeigt Ihnen, wie Sie mithilfe von Connect from Precisely VSAM-Dateien (Virtual Storage Access Method) von einem Mainframe in eine Zielumgebung in der AWS-Cloud migrieren und replizieren. Zu den Zielumgebungen, die in diesem Muster behandelt werden, gehören Amazon Relational Database Service (Amazon RDS) und Amazon Managed Streaming for Apache Kafka (Amazon MSK). Connect verwendet Change Data Capture (CDC), um Aktualisierungen Ihrer VSAM-Quelldateien kontinuierlich zu überwachen und diese Updates dann in eine oder mehrere Ihrer AWS-Zielumgebungen zu übertragen. Sie können dieses Muster verwenden, um Ihre Ziele im Bereich Anwendungsmodernisierung oder Datenanalyse zu erreichen. Beispielsweise können Sie Connect verwenden, um Ihre VSAM-Anwendungsdateien mit geringer Latenz in die AWS-Cloud zu migrieren, oder Ihre VSAM-Daten zu einem AWS-Data Warehouse oder Data Lake für Analysen migrieren, die Synchronisationslatenzen tolerieren können, die höher sind als für die Anwendungsmodernisierung erforderlich.

Voraussetzungen und Einschränkungen

Voraussetzungen

- IBM z/OS V2R1 oder höher
- CICS Transaction Server für z/OS (CICS TS) V5.1 oder höher (CICS/VSAM-Datenerfassung)
- IBM MQ 8.0 oder höher
- Einhaltung der z/OS-Sicherheitsanforderungen (z. B. APF-Autorisierung für SQData Ladebibliotheken)
- Die VSAM-Wiederherstellungsprotokolle sind aktiviert
- (Optional) CICS VSAM Recovery Version (CICS VR) zur automatischen Erfassung von CDC-Protokollen
- Ein aktives AWS-Konto
- Eine Amazon Virtual Private Cloud (VPC) mit einem Subnetz, das über Ihre Legacy-Plattform erreichbar ist
- Eine VSAM Connect-Lizenz von Precisely

Einschränkungen

- Connect unterstützt keine automatische Erstellung von Zieltabellen auf der Grundlage von Quell-VSAM-Schemas oder Copybooks. Sie müssen die Zieltabellenstruktur zum ersten Mal definieren.
- Für Nicht-Streaming-Ziele wie Amazon RDS müssen Sie die Zuordnung von Konvertierungsquelle zu Ziel im Apply Engine-Konfigurationsskript angeben.
- Protokollierungs-, Überwachungs- und Warnfunktionen werden über externe Komponenten (wie Amazon CloudWatch) implementiert APIs und erfordern, dass sie voll funktionsfähig sind.

Produktversionen

- SQData 40134 für z/OS
- SQData 4.0.43 für das Amazon Linux Amazon Machine Image (AMI) auf Amazon Elastic Compute Cloud (Amazon) EC2

Architektur

Quelltechnologie-Stack

- Sprache zur Jobkontrolle (JCL)
- z/OS Unix-Shell und Interactive System Productivity Facility (ISPF)
- VSAM-Dienstprogramme (IDCAMS)

Zieltechnologie-Stack

- Amazon EC2
- Amazon MSK
- Amazon RDS
- Amazon VPC

Zielarchitektur

Migrieren von VSAM-Dateien zu Amazon RDS

Das folgende Diagramm zeigt, wie VSAM-Dateien in Echtzeit oder nahezu in Echtzeit in eine relationale Datenbank wie Amazon RDS migriert werden, indem der CDC-Agent/Publisher in der

Quellumgebung (lokaler Mainframe) und die Apply Engine in der Zielumgebung (AWS Cloud) verwendet werden.

Das Diagramm zeigt den folgenden Batch-Workflow:

1. Connect erfasst Änderungen an einer Datei, indem es VSAM-Dateien mit Backupdateien vergleicht, um Änderungen zu identifizieren, und sendet die Änderungen dann an den Logstream.
2. Der Herausgeber verwendet Daten aus dem System-Logstream.
3. Der Herausgeber übermittelt die erfassten Datenänderungen über TCP/IP an eine Ziel-Engine. Der Controller-Daemon authentifiziert die Kommunikation zwischen der Quell- und der Zielumgebung.
4. Die Apply Engine in der Zielumgebung empfängt die Änderungen vom Publisher-Agent und wendet sie auf eine relationale oder nicht-relationale Datenbank an.

Das Diagramm zeigt den folgenden Online-Workflow:

1. Connect erfasst Änderungen in der Online-Datei mithilfe einer Protokollreplikation und streamt dann die erfassten Änderungen in einen Logstream.
2. Der Herausgeber verwendet Daten aus dem System-Logstream.
3. Der Herausgeber übermittelt die erfassten Datenänderungen über TCP/IP an die Ziel-Engine. Der Controller-Daemon authentifiziert die Kommunikation zwischen der Quell- und der Zielumgebung.
4. Die Apply Engine in der Zielumgebung empfängt die Änderungen vom Publisher-Agent und wendet sie dann auf eine relationale oder nicht-relationale Datenbank an.

Migrieren von VSAM-Dateien zu Amazon MSK

Das folgende Diagramm zeigt, wie Sie VSAM-Datenstrukturen im Hochleistungsmodus von einem Mainframe zu Amazon MSK streamen und automatisch JSON- oder AVRO-Schemakonvertierungen generieren, die in Amazon MSK integriert werden.

Das Diagramm zeigt den folgenden Batch-Workflow:

1. Connect erfasst Änderungen an einer Datei mithilfe von CICS VR oder durch den Vergleich von VSAM-Dateien mit Backupdateien, um Änderungen zu identifizieren. Erfasste Änderungen werden an den Logstream gesendet.

2. Der Herausgeber verwendet Daten aus dem System-Logstream.
3. Der Herausgeber übermittelt die erfassten Datenänderungen über TCP/IP an die Ziel-Engine. Der Controller-Daemon authentifiziert die Kommunikation zwischen der Quell- und der Zielumgebung.
4. Die Replicator Engine, die im Parallelverarbeitungsmodus arbeitet, teilt die Daten in eine Arbeitseinheit auf.
5. Worker-Threads erfassen die Daten aus dem Cache.
6. Daten werden aus den Worker-Threads in Amazon MSK-Themen veröffentlicht.
7. Benutzer wenden mithilfe von Konnektoren Änderungen von Amazon MSK auf Ziele wie Amazon DynamoDB, Amazon Simple Storage Service (Amazon S3) oder Amazon OpenSearch Service an.

Das Diagramm zeigt den folgenden Online-Workflow:

1. Änderungen in der Online-Datei werden mithilfe eines Protokollreplikats erfasst. Erfasste Änderungen werden in den Logstream gestreamt.
2. Der Herausgeber verwendet Daten aus dem System-Logstream.
3. Der Herausgeber übermittelt die erfassten Datenänderungen über TCP/IP an die Ziel-Engine. Der Controller-Daemon authentifiziert die Kommunikation zwischen der Quell- und der Zielumgebung.
4. Die Replicator Engine, die im Parallelverarbeitungsmodus arbeitet, teilt die Daten in eine Arbeitseinheit auf.
5. Worker-Threads erfassen die Daten aus dem Cache.
6. Daten werden aus den Worker-Threads in Amazon MSK-Themen veröffentlicht.
7. Benutzer wenden Änderungen von Amazon MSK mithilfe von Konnektoren auf Ziele wie DynamoDB, Amazon S3 oder OpenSearch Service an.

Tools

- Amazon Managed Streaming for Apache Kafka (Amazon MSK) ist ein vollständig verwalteter Service, der Sie beim Erstellen und Ausführen von Anwendungen unterstützt, die Apache Kafka zur Verarbeitung von Streaming-Daten verwenden.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der AWS-Cloud.

Epen

Bereiten Sie die Quellumgebung (Mainframe) vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Connect CDC 4.1.	1. Wenden Sie sich an das Precisely Support Team, um eine Lizenz und Installationspakete zu erhalten. 2. Verwenden Sie JCLs das Beispiel, um Connect CDC 4.1 zu installieren. Anweisungen finden Sie unter Connect CDC (SQData) mithilfe von JCL installieren in der Precisely Dokumentation. 3. Führen Sie den `SETPROG APF` Befehl aus, um die Connect-Ladebibliotheken SQData.V4NNN.LoadLib zu autorisieren.	IBM Mainframe-Entwickler/ Administrator
Richten Sie das ZFS-Verzeichnis ein.	Um ein ZFS-Verzeichnis einzurichten, folgen Sie den Anweisungen unter ZFS-Variablenverzeichnisse in der Dokumentation Precisely. **Note** Controller Daemon und Capture/Publisher agent configurations are stored in the z/OS UNIX Systems	IBM Mainframe-Entwickler/ Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Services-Dateisystem (als ZFS bezeichne t). Die Agenten Controller Daemon, Capture, Storage und Publisher benötigen eine vordefinierte ZFS-Verzeichnisstruktur zum Speichern einer kleinen Anzahl von Dateien.	
Konfigurieren Sie die TCP/IP-Ports.	Folgen Sie zur Konfigura tion von TCP/IP-Ports den Anweisungen unter TCP/IP-Ports in der Dokumentation Precisely. **Note** Der Controller-Daemon benötigt TCP/IP-Ports auf den Quellsystemen. Die Ports werden von den Engines auf den Zielsystemen referenzi ert (auf denen die erfassten Änderungs daten verarbeitet werden).	IBM Mainframe-Entwickler/ Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen z/OS-Logstream.	Um einen z/OS-Logstream zu erstellen, folgen Sie den Anweisungen unter Create z/OS system LogStreams in der Dokumentation Precisely. **Note** Connect verwendet den Logstream, um während der Migration Daten zwischen Ihrer Quell- und Zielumgebung zu erfassen und zu streamen. Ein Beispiel für eine JCL, mit der ein z/OS-System erstellt wird LogStream, finden Sie in der Dokumentation Precisely unter Create z/OS system LogStreams.	IBM Mainframe-Entwickler
Identifizieren und autorisieren Sie IDs ZFS-Benutzer und gestartete Aufgaben.	Verwenden Sie RACF, um Zugriff auf das OMVS ZfS-Dateisystem zu gewähren. Ein Beispiel für eine JCL finden Sie in der Dokumentation Precisely unter Identifizieren und Autorisieren des ZFS-Benutzers und der gestarteten Aufgabe. IDs	IBM Mainframe-Entwickler/Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie öffentliche/private z/OS-Schlüssel und die autorisierte Schlüsseldatei.	Führen Sie die JCL aus, um das key pair zu generieren. Ein Beispiel finden Sie unter Schlüsselpaar-Beispiel im Abschnitt Zusätzliche Informationen dieses Musters. Eine Anleitung dazu finden Sie in der Dokumentation Precisely unter Generieren von öffentlichen und privaten z/OS-Schlüsseln und autorisierter Schlüsseldatei.	IBM Mainframe-Entwickler/Administrator

Aktivieren Sie das CICS VSAM Log Replicate und hängen Sie es an den Logstream an.	Führen Sie das folgende JCL-Skript aus:
	
	`//STEP1 EXEC PGM=IDCAMS`
	`//SYSPRINT DD SYSOUT=*`
	`//SYSIN DD *`
	`ALTER SQDATA.CICS.FILEA -`
	`LOGSTREAMID(SQDATA.VSAMCDC.LOG1) -`
	`LOGREPLICATE`
		IBM Mainframe-Entwickler/Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktivieren Sie das VSAM-Date iwiederherstellungsprotokoll über ein FCT.	Ändern Sie die File Control Table (FCT), um die folgenden Parameteränderungen widerzuspiegeln:
	`Configure FCT Parms`
	`CEDA ALT FILE(name) GROUP(groupname)`
	`DSNAME(data set name)`
	`RECOVERY(NONE|BACKOUTONLY|ALL)`
	`FWDRECOVLOG(NO|1-99)`
	`BACKUPTYPE(STATIC|DYNAMIC)`
	`RECOVERY PARAMETERS`
	`RECOVery : None | Backoutonly | All`
	`Fwdrecovlog : No | 1-99`
	`BAckuptype : Static | Dynamic`
		IBM Mainframe-Entwickler/ Administrator

Richten Sie CDCz Log für den Publisher-Agent ein.	1. Erstellen Sie die CDCz Log Publisher-CAB-Datei. 2. Verschlüsseln Sie die veröffentlichten Daten. 3. Bereiten Sie die CDCz Log Publisher Runtime JCL vor.	IBM Mainframe-Entwickler/ Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie den Controller-Daemon.	1. Öffnen Sie das ISPF-Panel und führen Sie den folgenden Befehl aus, um das Menü Precisely zu öffnen: `EXEC 'SQDATA.V4nnnnn.ISPFLIB(SQDC$STA)' 'SQDATA.V4nnnnn'` 2. Um den Controller-Daemon einzurichten, wählen Sie Option 2 aus dem Menü.	IBM Mainframe-Entwickler/ Administrator
Aktivieren Sie den Herausgeber.	1. Öffnen Sie das ISPF-Bedienfeld und führen Sie den folgenden Befehl aus, um das Menü Precisely zu öffnen: `EXEC 'SQDATA.V4nnnnn.ISPFLIB(SQDC$STA)' 'SQDATA.V4nnnnn'` 2. Um den Publisher einzurichten, wählen Sie Option 3 aus dem Menü und I für Einfügen.	IBM Mainframe-Entwickler/ Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie den Logstream.	1. Öffnen Sie das ISPF-Panel und führen Sie den folgenden Befehl aus, um das Menü Precisely zu öffnen: `EXEC 'SQDATA.V4nnnnn.ISPFLIB(SQDC$STA)' 'SQDATA.V4nnnnn'` 2. Um den Logstream einzurichten, wählen Sie Option 4 aus dem Menü und I für Einfügen. Geben Sie dann den Namen des Logstreams ein, der in den vorherigen Schritten erstellt wurde.	IBM Mainframe-Entwickler/ Administrator

Bereiten Sie die Zielumgebung vor (AWS)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Genau auf einer EC2 Instanz installieren.	Um Connect von Precisely auf dem Amazon Linux AMI für Amazon zu installieren EC2, folgen Sie den Anweisungen unter Connect CDC (SQData) unter UNIX installieren in der Dokumentation Precisely.	Allgemeines AWS
Öffnen Sie die TCP/IP-Ports.	Um die Sicherheitsgruppe so zu ändern, dass sie die Controller-Daemon-Ports für eingehenden und ausgehenden Zugriff enthält, folgen Sie	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den Anweisungen unter TCP/IP in der Dokumentation von Precisely.	
Erstellen Sie Dateiverzeichnisse.	Um Dateiverzeichnisse zu erstellen, folgen Sie den Anweisungen unter Prepare target apply environment in der Dokumentation Precisely.	Allgemeines AWS

Erstellen Sie die Apply Engine-Konfigurationsdatei.	Erstellen Sie die Apply Engine-Konfigurationsdatei im Arbeitsverzeichnis der Apply Engine. Die folgende Beispielkonfigurationsdatei zeigt Apache Kafka als Ziel:
	`builtin.features=SASL_SCRAM`
	`security.protocol=SASL_SSL`
	`sasl.mechanism=SCRAM-SHA-512`
	`sasl.username=`
	`sasl.password=`
	`metadata.broker.list=`
	Note
	Weitere Informationen finden Sie unter Sicherheit in der Apache Kafka-Dokumentation.
		Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Skripts für die Apply Engine-Verarbeitung.	Erstellen Sie die Skripts für die Apply Engine, um Quelldaten zu verarbeiten und Quelldaten auf das Ziel zu replizieren. Weitere Informationen finden Sie in der Dokumentation Precisely unter Erstellen eines Apply-Engine-Skripts.	Allgemeines AWS
Führen Sie die Skripte aus.	Verwenden Sie die `SQDENG` Befehle `SQDPARSE` und, um das Skript auszuführen. Weitere Informationen finden Sie unter Parse a script for zOS in der Precisely Dokumentation.	Allgemeines AWS

Validieren Sie die Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Liste der VSAM-Dateien und Zieltabellen für die CDC-Verarbeitung.	1. Validieren Sie VSAM-Dateien, einschließlich Replikationsprotokollen, Wiederherstellungsprotokollen, FCT-Parametern und dem Logstream. 2. Überprüfen Sie die Zieldatenbanktabellen, einschließlich der Frage, ob die Tabellen gemäß der erforderlichen Schemadefinition, dem Tabellenz	Allgemein AWS, Mainframe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ugriff und anderen Kriterien erstellt wurden.	
Stellen Sie sicher, dass das Connect SQData CDC-Produkt verknüpft ist.	Führen Sie einen Testauftrag aus und stellen Sie sicher, dass der Rückgabecode für diesen Job 0 (erfolgreich) lautet. **Note** Die Statusmeldungen der Connect CDC SQData Apply Engine sollten aktive Verbindungsmeldungen anzeigen.	Allgemein AWS, Mainframe

Testfälle ausführen und validieren (Batch)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den Batch-Job auf dem Mainframe aus.	Führen Sie den Batch-Anwendungsauftrag mit einer modifizierten JCL aus. Fügen Sie Schritte in die modifizierte JCL ein, die Folgendes bewirken: 1. Erstellen Sie eine Sicherungskopie der Datendateien. 2. Vergleichen Sie die Sicherungsdatei mit den	Allgemein AWS, Mainframe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	geänderten Datendateien, generieren Sie die Delta-Datei und notieren Sie sich dann die Anzahl der Delta-Datensätze aus den Nachrichten. 3. Übertragen Sie die Delta-Datei in den z/OS-Logs tream. 4. Führen Sie die JCL aus. Ein Beispiel für eine JCL finden Sie unter Prepare file compare capture JCL in der Dokumentation Precisely.	
Überprüfen Sie den Logstream .	Überprüfen Sie den Logstream , um sicherzustellen, dass Sie die Änderungsdaten für den abgeschlossenen Mainframe-Batch-Job sehen können.	Allgemein AWS, Mainframe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Anzahl der Quell-Delta-Änderungen und der Zieltabelle.	Gehen Sie wie folgt vor, um zu überprüfen, ob die Datensätze gezählt wurden: 1. Erfassen Sie die Anzahl der Quell-Deltas aus den Batch-JCL-Meldungen. 2. Überwachen Sie mit der Apply Engine die Anzahl der in die VSAM-Datei eingefügten, aktualisierten oder gelöschten Datensätze auf Datensatzebene. 3. Fragen Sie die Zieltabel le nach der Anzahl der Datensätze ab. 4. Vergleichen und zählen Sie die verschied enen Datensatzzahlen zusammen.	Allgemein AWS, Mainframe

Testfälle ausführen und validieren (online)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Online-Tr ansaktion in einer CICS-Regi on aus.	1. Führen Sie die Online-Tr ansaktion aus, um den Testfall zu validieren. 2. Validieren Sie den Transakti onsausführungscode (RC=0 — Erfolgreich).	IBM Mainframe-Entwickler
Überprüfen Sie den Logstream .	Vergewissern Sie sich, dass der Logstream mit bestimmte	AWS-Mainframe-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	n Änderungen auf Datensatz ebene gefüllt ist.	
Überprüfen Sie die Anzahl in der Zieldatenbank.	Überwachen Sie die Apply Engine auf Zählungen auf Datensatzebene.	Genau, Linux
Überprüfen Sie die Anzahl der Datensätze und Datensätze in der Zieldatenbank.	Fragen Sie die Zieldaten bank ab, um die Anzahl der Datensätze und Datensätze zu überprüfen.	Allgemeines AWS

Zugehörige Ressourcen

- VSAM z/OS (Genaue Dokumentation)
- Engine anwenden (Präzise Dokumentation)
- Replicator-Engine (Präzise Dokumentation)
- Der Logstream (IBM-Dokumentation)

Zusätzliche Informationen

Beispiel für eine Konfigurationsdatei

Dies ist eine Beispielkonfigurationsdatei für einen Logstream, bei dem die Quellumgebung ein Mainframe und die Zielumgebung Amazon MSK ist:

```
 -- JOBNAME -- PASS THE SUBSCRIBER NAME
 -- REPORT  progress report will be produced after "n" (number) of Source records
processed.

 JOBNAME VSMTOKFK;
 --REPORT EVERY 100;
 -- Change Op has been ‘I’ for insert, ‘D’ for delete , and ‘R’ for Replace. For RDS
it is 'U' for update
 -- Character Encoding on z/OS is Code Page 1047, on Linux and UNIX it is Code Page
819 and on Windows, Code Page 1252
```

```
 OPTIONS
 CDCOP('I', 'U', 'D'),
 PSEUDO NULL = NO,
 USE AVRO COMPATIBLE NAMES,
 APPLICATION ENCODING SCHEME = 1208;

 --       SOURCE DESCRIPTIONS

 BEGIN GROUP VSAM_SRC;
 DESCRIPTION COBOL ../copybk/ACCOUNT AS account_file;
 END GROUP;

 --       TARGET DESCRIPTIONS

 BEGIN GROUP VSAM_TGT;
 DESCRIPTION COBOL ../copybk/ACCOUNT AS account_file;
 END GROUP;

 --       SOURCE DATASTORE (IP & Publisher name)

 DATASTORE cdc://10.81.148.4:2626/vsmcdct/VSMTOKFK
 OF VSAMCDC
 AS CDCIN
 DESCRIBED BY GROUP VSAM_SRC ACCEPT ALL;

 --       TARGET DATASTORE(s) - Kafka and topic name

 DATASTORE 'kafka:///MSKTutorialTopic/key'
 OF JSON
 AS CDCOUT
 DESCRIBED BY GROUP VSAM_TGT FOR INSERT;

 --       MAIN SECTION

 PROCESS INTO
 CDCOUT
 SELECT
 {
 SETURL(CDCOUT, 'kafka:///MSKTutorialTopic/key')
 REMAP(CDCIN, account_file, GET_RAW_RECORD(CDCIN, AFTER), GET_RAW_RECORD(CDCIN,
BEFORE))
 REPLICATE(CDCOUT, account_file)
 }
```

```
  FROM CDCIN;
```

Beispiel für ein Schlüsselpaar

Dies ist ein Beispiel dafür, wie die JCL ausgeführt wird, um das key pair zu generieren:

```
//SQDUTIL EXEC PGM=SQDUTIL //SQDPUBL DD DSN=&USER..NACL.PUBLIC, //
 DCB=(RECFM=FB,LRECL=80,BLKSIZE=21200), // DISP=(,CATLG,DELETE),UNIT=SYSDA, //
 SPACE=(TRK,(1,1)) //SQDPKEY DD DSN=&USER..NACL.PRIVATE, //
 DCB=(RECFM=FB,LRECL=80,BLKSIZE=21200), // DISP=(,CATLG,DELETE),UNIT=SYSDA, //
 SPACE=(TRK,(1,1)) //SQDPARMS DD  keygen //SYSPRINT DD SYSOUT= //SYSOUT DD SYSOUT=* //
SQDLOG DD SYSOUT=* //*SQDLOG8 DD DUMMY
```

Modernisieren Sie das Mainframe-Output-Management mithilfe AWS von Rocket Enterprise Server und LRS X PageCenter

Erstellt von Shubham Roy (AWS), Abraham Rondon (Micro Focus) und Guy Tucker (Levi, Ray and Shoup Inc)

Übersicht

Durch die Modernisierung Ihres Mainframe-Output-Managements können Sie Kosteneinsparungen erzielen, den technischen Aufwand für die Wartung älterer Systeme verringern und die Ausfallsicherheit und Agilität mithilfe DevOps der Cloud-nativen Technologien von Amazon Web Services (AWS) verbessern. Dieses Muster zeigt Ihnen, wie Sie Ihre geschäftskritischen Mainframe-Output-Management-Workloads in der AWS-Cloud modernisieren können. Das Muster verwendet Rocket Enterprise Server als Laufzeit für eine modernisierte Mainframe-Anwendung, wobei Levi, Ray & Shoup, Inc. (LRS) VPSX/MFI (Micro Focus Interface) als Druckserver und LRS X als Archivserver verwendet werden. PageCenter LRS PageCenter X bietet Output-Management-Lösungen für die Anzeige, Indizierung, Suche, Archivierung und Sicherung des Zugriffs auf Geschäftsergebnisse.

Das Muster basiert auf dem Ansatz der Replatform Mainframe-Modernisierung. Mainframe-Anwendungen werden von AWS Mainframe Modernization auf Amazon Elastic Compute Cloud (Amazon) migriert. EC2 Mainframe-Output-Management-Workloads werden zu Amazon migriert EC2, und eine Mainframe-Datenbank wie IBM Db2 for z/OS wird zu Amazon Relational Database Service (Amazon RDS) migriert. Der LRS Directory Integration Server (LRS/DIS) arbeitet mit AWS Directory Service for Microsoft Active Directory für die Workflow-Authentifizierung und Autorisierung des Output-Management-Workflows zusammen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein Mainframe-Workload für das Output-Management.
- Grundkenntnisse zum Wiederaufbau und zur Bereitstellung einer Mainframe-Anwendung, die auf Rocket Enterprise Server läuft. Weitere Informationen finden Sie im Rocket Enterprise Server-Datenblatt in der Rocket Software-Dokumentation.
- Grundkenntnisse der Cloud-Printing-Lösungen und -Konzepte von LRS. Weitere Informationen finden Sie unter Output Modernization in der LRS-Dokumentation.

- Rocket Enterprise Server-Software und -Lizenz. Für weitere Informationen wenden Sie sich an Rocket Software.
- VPSX/MFI, LRS PageCenterX, LRS/Queue, and LRS/DISLRS-Software und -Lizenzen. Weitere Informationen erhalten Sie bei LRS. Sie müssen die Hostnamen der EC2 Instanzen angeben, auf denen die LRS-Produkte installiert werden.

> **Note**
>
> Weitere Informationen zu Überlegungen zur Konfiguration von Mainframe-Output-M anagement-Workloads finden Sie unter Überlegungen im Abschnitt Zusätzliche Informati onen dieses Musters.

Produktversionen

- Rocket Enterprise Server 10.0
- LRS VPSX/MFI
- LRS X V1R3 oder später PageCenter

Architektur

Quelltechnologie-Stack

- Betriebssystem — IBM z/OS
- Programmiersprache — Common Business Oriented Language (COBOL), Job Control Language (JCL) und Customer Information Control System (CICS)
- Datenbank — IBM Db2 für z/OS, IBM Information Management System (IMS) -Datenbank und Virtual Storage Access Method (VSAM)
- Sicherheit — Resource Access Control Facility (RACF), CA Top Secret für z/OS und Access Control Facility 2 () ACF2
- Druck- und Archivierungslösungen — IBM Mainframe-z/OS-Ausgabe- und Druckprodukte (IBM Infoprint Server for z/OS, LRS und CA Deliver) und Archivierungslösungen (CA Deliver, ASG Mobius oder CA Bundle)

Quellarchitektur

Das folgende Diagramm zeigt eine typische aktuelle Architektur für einen Mainframe-Output-Management-Workload.

Das Diagramm zeigt den folgenden Workflow:

1. Benutzer führen Geschäftstransaktionen auf einem System of Engagement (SoE) durch, das auf einer in COBOL geschriebenen IBM CICS-Anwendung basiert.
2. Das SoE ruft den Mainframe-Service auf, der die Geschäftstransaktionsdaten in einer system-of-records (SoR) -Datenbank wie IBM Db2 for z/OS aufzeichnet.
3. Das SoR speichert die Geschäftsdaten aus dem SoE.
4. Der Batch-Job-Scheduler initiiert einen Batch-Job, um eine Druckausgabe zu generieren.
5. Der Batch-Job extrahiert Daten aus der Datenbank. Er formatiert die Daten entsprechend den Geschäftsanforderungen und generiert anschließend Geschäftsergebnisse wie Abrechnungen, Personalausweise oder Kreditauszüge. Schließlich leitet der Batch-Job die Ausgabe an das Output Management weiter, um die Ausgabe entsprechend den Geschäftsanforderungen zu formatieren, zu veröffentlichen und zu speichern.
6. Das Output-Management empfängt die Ausgabe des Batch-Jobs. Output Management indexiert, ordnet und veröffentlicht die Ausgabe an einem bestimmten Ziel im Output-Management-System, z. B. LRS PageCenter X-Lösungen (wie in diesem Muster gezeigt) oder CA View.
7. Benutzer können die Ausgabe anzeigen, suchen und abrufen.

Zieltechnologie-Stack

- Betriebssystem — Windows Server läuft auf Amazon EC2
- Rechnen — Amazon EC2
- Speicher — Amazon Elastic Block Store (Amazon EBS) und Amazon FSx für Windows File Server
- Programmiersprache — COBOL, JCL und CICS
- Datenbank — Amazon RDS
- Sicherheit — AWS Managed Microsoft AD
- Drucken und Archivieren — LRS-Druck- (VPSX) und Archivierungslösung (PageCenterX) auf AWS
- Mainframe-Laufzeitumgebung — Rocket Enterprise Server

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur für einen Mainframe-Output-Management-Workload, der in der AWS-Cloud bereitgestellt wird.

Das Diagramm zeigt den folgenden Workflow:

1. Der Batch-Job-Scheduler initiiert einen Batch-Job, um Ausgaben wie Abrechnungen, Personalausweise oder Kreditauszüge zu erstellen.
2. Der Mainframe-Batch-Job (auf Amazon umgestellt EC2) verwendet die Rocket Enterprise Server-Laufzeit, um Daten aus der Anwendungsdatenbank zu extrahieren, Geschäftslogik auf die Daten anzuwenden und die Daten zu formatieren. Anschließend werden die Daten mithilfe des Druckerexit-Moduls von Rocket Software (OpenText Micro Focus-Dokumentation) an ein Ausgabeziel gesendet.
3. Die Anwendungsdatenbank (ein SoR, der auf Amazon RDS läuft) speichert Daten für die Druckausgabe.
4. Der VPSX/MFI printing solution is deployed on Amazon EC2, and its operational data is stored in Amazon EBS. LRS VPSX/MFI uses the TCP/IP-based LRS/Queue LRS-Übertragungsagent zur Erfassung von Ausgabedaten über die JES Print Exit API von Rocket Software.

   LRS VPSX/MFI führt eine Datenvorverarbeitung durch, z. B. die Umwandlung von EBCDIC in ASCII. Es erledigt auch komplexere Aufgaben, einschließlich der Konvertierung von Mainframe-exklusiven Datenströmen wie IBM Advanced Function Presentation (AFP) und Xerox Line Conditioned Data Stream (LCDS) in gängigere Datenströme zum Anzeigen und Drucken wie Printer Command Language (PCL) und PDF.

   Während des Wartungsfensters von LRS PageCenter X tauscht LRS die Bereitschaft und den Abschluss der Aufträge VPSX/MFI persists the output queue and serves as backup for the output queue. LRS VPSX/MFI connects and sends output to LRS PageCenterX by using the LRS/Queue protocol. LRS/Queue aus, um sicherzustellen, dass die Datenübertragung stattfindet.

   Hinweise:

   Weitere Informationen zu Druckdaten, die von Rocket Software Print Exit an LRS/Queue and LRS VPSX/MFI unterstützte Mainframe-Batch-Mechanismen weitergegeben werden, finden Sie unter Druckdatenerfassung im Abschnitt Zusätzliche Informationen.

LRS VPSX/MFI kann Zustandsprüfungen auf Druckerflottenebene durchführen. Weitere Informationen finden Sie im Abschnitt „Zusätzliche Informationen“ dieses Musters unter „Printer-Fleet Health Checks“.

5. Die Output-Management-Lösung LRS PageCenter X wird auf Amazon bereitgestellt EC2, und ihre Betriebsdaten werden in Amazon FSx for Windows File Server gespeichert. LRS PageCenter X bietet ein zentrales Berichtsverwaltungssystem für alle in LRS PageCenter X importierten Dateien sowie für alle Benutzer, die auf die Dateien zugreifen können. Benutzer können bestimmte Dateiinhalte anzeigen oder in mehreren Dateien nach übereinstimmenden Kriterien suchen.

   Der LRS/NetX component is a multi-threaded web application server that provides a common runtime environment for the LRS PageCenterX application and other LRS applications. The LRS/Web Connect component is installed on your web server and provides a connector from the web server to the LRS/NetX Webanwendungsserver.
6. LRS PageCenter X bietet Speicher für Dateisystemobjekte. Die Betriebsdaten von LRS PageCenter X werden in Amazon FSx for Windows File Server gespeichert.
7. Die Authentifizierung und Autorisierung des Output-Managements erfolgt durch AWS Managed Microsoft AD mit LRS/DIS.

> **Note**
>
> Die Ziellösung erfordert in der Regel keine Änderungen an der Anwendung, um Mainframe-Formatierungssprachen wie IBM AFP oder Xerox LCDS zu berücksichtigen.

AWS-Infrastrukturarchitektur

Das folgende Diagramm zeigt eine hochverfügbare und sichere AWS-Infrastrukturarchitektur für einen Mainframe-Output-Management-Workload.

Das Diagramm zeigt den folgenden Workflow:

1. Der Batch-Scheduler initiiert den Batch-Prozess und wird auf Amazon EC2 in mehreren Availability Zones für hohe Verfügbarkeit (HA) bereitgestellt.

> **Note**
>
> Dieses Muster deckt die Implementierung des Batch-Schedulers nicht ab. Weitere Informationen zur Implementierung finden Sie in der Dokumentation des Softwareanbieters für Ihren Scheduler.

2. Der Mainframe-Batchjob (geschrieben in einer Programmiersprache wie JCL oder COBOL) verwendet die Kerngeschäftslogik, um Druckausgaben wie Abrechnungen, Ausweise und Kreditauszüge zu verarbeiten und zu generieren. Der Batch-Job wird auf Amazon EC2 in zwei Availability Zones für HA bereitgestellt. Es verwendet die Rocket Software Print Exit API, um die Druckausgabe zur Datenvorverarbeitung an LRS VPSX/MFI weiterzuleiten.
3. Der LRS-VPSX/MFI-Druckserver wird auf Amazon EC2 in zwei Availability Zones für HA (redundantes Active-Standby-Paar) bereitgestellt. Es verwendet Amazon EBS als Betriebsdatenspeicher. Der Network Load Balancer führt eine Integritätsprüfung der EC2 LRS-VPSX/MFI-Instanzen durch. Wenn sich eine aktive Instance in einem fehlerhaften Zustand befindet, leitet der Load Balancer den Datenverkehr an Hot-Standby-Instances in der anderen Availability Zone weiter. Die Druckanforderungen werden in jeder Instanz lokal in der LRS-Auftragswarteschlange gespeichert. EC2 Im Falle eines Fehlers muss eine ausgefallene Instanz neu gestartet werden, bevor die LRS-Dienste die Verarbeitung der Druckanforderung fortsetzen können.

> **Note**
>
> LRS VPSX/MFI kann auch Zustandsprüfungen auf Druckerflottenebene durchführen. Weitere Informationen finden Sie im Abschnitt „Zusätzliche Informationen“ dieses Musters unter „Druckerflottenzustandsprüfungen“.

4. Das LRS PageCenter X-Output-Management wird auf Amazon EC2 in zwei Availability Zones für HA (redundantes Active-Standby-Paar) bereitgestellt. Es verwendet Amazon FSx for Windows File Server als Betriebsdatenspeicher. Wenn sich eine aktive Instance in einem fehlerhaften Zustand befindet, führt der Load Balancer eine Integritätsprüfung der LRS PageCenter EC2 X-Instances durch und leitet den Datenverkehr an Standby-Instances in der anderen Availability Zone weiter.
5. Ein Network Load Balancer stellt einen DNS-Namen bereit, um den LRS VPSX/MFI Server mit LRS X zu integrieren. PageCenter

> **Note**
>
> LRS X unterstützt PageCenter einen Layer-4-Load Balancer.

6. LRS PageCenter X verwendet Amazon FSx for Windows File Server als Betriebsdatenspeicher, der in zwei Availability Zones für HA bereitgestellt wird. LRS PageCenter X versteht nur Dateien, die sich in der Dateifreigabe befinden, nicht in einer externen Datenbank.
7. AWS Managed Microsoft AD wird mit LRS/DIS verwendet, um Workflow-Authentifizierung und Autorisierung im Output-Management-Workflow durchzuführen. Weitere Informationen finden Sie unter Authentifizierung und Autorisierung von Druckausgaben im Abschnitt Zusätzliche Informationen.

Tools

AWS-Services

- AWS Directory Service für Microsoft Active Directory ermöglicht Ihren verzeichnissensitiven Workloads und AWS-Ressourcen die Nutzung von Microsoft Active Directory in der AWS-Cloud.
- Amazon Elastic Block Store (Amazon EBS) bietet Speichervolumes auf Blockebene zur Verwendung mit Amazon Elastic Compute Cloud (Amazon EC2) -Instances.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Elastic Load Balancing (ELB) verteilt eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Traffic auf EC2 Amazon-Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen. Dieses Muster verwendet einen Network Load Balancer.
- Amazon FSx bietet Dateisysteme, die branchenübliche Konnektivitätsprotokolle unterstützen und Hochverfügbarkeit und Replikation in allen AWS-Regionen bieten. Dieses Muster verwendet Amazon FSx for Windows File Server.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der AWS-Cloud.

Andere Tools

- Die LRS PageCenter X-Software bietet eine skalierbare Content-Management-Lösung für Dokumente und Berichte, mit der Benutzer mithilfe automatisierter Indexierung, Verschlüsselung und erweiterter Suchfunktionen maximalen Nutzen aus Informationen ziehen können.
- LRS VPSX/MFI (Micro Focus Interface), das gemeinsam von LRS und Rocket Software entwickelt wurde, erfasst die Ausgabe von einem JES-Spool von Rocket Software und überträgt sie zuverlässig an ein bestimmtes Druckziel.
- LRS/Queue is a transmission agent that's TCP/IP based. LRS VPSX/MFI uses LRS/Queueum Druckdaten über die JES Print Exit-Programmierschnittstelle von Rocket Software zu sammeln oder zu erfassen.
- Der LRS Directory Integration Server (LRS/DIS) wird für die Authentifizierung und Autorisierung während des Druckworkflows verwendet.
- Rocket Enterprise Server ist eine Umgebung zur Anwendungsbereitstellung für Mainframe-Anwendungen. Sie bietet die Laufzeitumgebung für Mainframe-Anwendungen, die mithilfe einer beliebigen Version von Rocket Enterprise Developer migriert oder erstellt wurden.

Epen

Richten Sie die Rocket-Laufzeit ein und stellen Sie eine Mainframe-Batch-Anwendung bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Runtime ein und stellen Sie eine Demo-Anwendung bereit.	Um Rocket Enterprise Server auf Amazon einzurichten EC2 und die BankDemo Demonstrationsanwendung von Rocket Software bereitzustellen, folgen Sie den Anweisungen im AWS Mainframe Modernization User Guide. Die BankDemo Anwendung ist eine Mainframe-Batch-Anwendung, die die Druckausgabe erstellt und dann initiiert.	Cloud-Architekt

Richten Sie einen LRS-Druckserver bei Amazon ein EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon EC2 Windows-Instance.	Um eine Amazon EC2 Windows-Instance zu starten, folgen Sie den Anweisung en unter Starten einer EC2 Amazon-Instance in der EC2 Amazon-Dokumentation. Verwenden Sie denselben Hostnamen, den Sie für Ihre LRS-Produktlizenz verwendet haben. Ihre Instance muss die folgenden Hardware- und Softwareanforderungen für LRS VPSX/MFI erfüllen: • Zentralprozessor — Doppelkern • RAM — 16 GB • Laufwerk — 500 GB • Minimale EC2 Instanz — `m5.xlarge` • Betriebssystem — Windows • Software — Interneti nformationsdienste (IIS) oder Apache **Note** Die oben genannten Hardware- und Softwareanforderun	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	gen sind für eine kleine Druckerflotte (etwa 500-1000) vorgesehen. Um die vollständigen Anforderungen zu erfahren, wenden Sie sich an Ihre LRS- und AWS-Ansprechpartner.	
	1. Wenn Sie Ihre Windows-Instance erstellen, stellen Sie sicher, dass der EC2 Hostname derselbe Hostname ist, der für die LRS-Produktlizenz verwendet wurde. 2. Connect zu Ihrer EC2 Instance her, indem Sie den Anweisungen unter Schritt 2: Connect zu Ihrer Instance herstellen in der EC2 Amazon-Dokumentation folgen. 3. Suchen und öffnen Sie im Windows-Startmenü den Server-Manager. 4. Wählen Sie im Server-Manager Dashboard, Schnellstart, Rollen und Funktionen hinzufügen und wählen Sie dann Serverrollen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Wählen Sie unter Serverrollen die Option WebServer (IIS) und dann Anwendungsentwicklung aus. 6. Aktivieren Sie unter Anwendungsentwicklung das Kontrollkästchen CGI. 7. Folgen Sie zur Installation von CGI den Anweisungen im Windows Server-Manager-Assistenten zum Hinzufügen von Rollen und Funktionen. 8. Öffnen Sie Port 5500 in der Windows-Firewall der EC2 Instanz für die LRS/Queue-Kommunikation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie LRS VPSX/MFI auf der Instanz. EC2	1. Connect zu Ihrer EC2 Instance her. 2. Öffnen Sie den Link zur Produkt-Download-Seite in der LRS-E-Mail-Nachricht, die Sie erhalten haben sollten. **Note** LRS-Produkte werden per elektronischer Dateiübertragung (EFT) vertrieben. 3. Laden Sie LRS VPSX/MFI herunter und entpacken Sie die Datei (Standardordner:). `c:\LRS` 4. Um LRS VPSX/MFI zu installieren, starten Sie den LRS Product Installer aus dem entpackten Ordner. 5. Wählen Sie im Menü Select Features die Option VPSX® Server und dann Next aus, um den Installationsvorgang zu starten. Sie erhalten eine Erfolgsmeldung, wenn die Installation abgeschlossen ist.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie LRS/Queue.	1. Connect zu Ihrer Rocket Enterprise EC2 Server-Instanz her. 2. Öffnen Sie in der LRS-E-Mail-Nachricht, die Sie erhalten haben sollten, den Link zur LRS-Produkt-Download-Seite, laden Sie LRS/Queue herunter und entpacken Sie dann die Datei. 3. Navigieren Sie zu dem Speicherort, an dem Sie die Dateien heruntergeladen haben, und starten Sie dann das LRS-Produktinstallationsprogramm, um LRS/Queue zu installieren. 4. Folgen Sie den Anweisungen im LRS-Produktinstallationsprogramm, um den Installationsvorgang abzuschließen.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie LRS/DIS.	Das LRS/DIS product often is included in LRS VPSX installation. However, if LRS/DIS wurde nicht zusammen mit LRS VPSX installiert. Gehen Sie wie folgt vor, um es zu installieren: 1. Connect zu Ihrer LRS EC2 VPSX/MFI-Instanz her. 2. Öffnen Sie in der LRS-E-Mail-Nachricht, die Sie erhalten haben sollten, den Link zur LRS-Produkt-Download-Seite, laden Sie LRS/DIS herunter und entpacken Sie dann die Datei. 3. Navigieren Sie zu dem Speicherort, an dem Sie die Dateien heruntergeladen haben, und starten Sie dann das LRS-Produktinstallationsprogramm. 4. Erweitern Sie im LRS Product Installer die Option LRS Misc Tools, wählen Sie LRS DIS und dann Weiter aus. 5. Folgen Sie den restlichen Anweisungen im LRS-Produktinstallationsprogramm, um den Installationsvorgang abzuschließen.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Zielgruppe.	Erstellen Sie eine Zielgruppe, indem Sie den Anweisungen unter Erstellen einer Zielgruppe für Ihren Network Load Balancer folgen. Wenn Sie die Zielgruppe erstellen, registrieren Sie die EC2 LRS-VPSX/MFI-Instanz als Ziel: 1. Wählen Sie auf der Seite Gruppendetails angeben für Wählen Sie einen Zieltyp die Option Instances aus. 2. Wählen Sie für Protokoll die Option TCP aus. 3. Wählen Sie für Port die Option 5500 aus. 4. Wählen Sie auf der Seite Ziele registrieren im Abschnitt Verfügbare Instanzen die LRS EC2 VPSX/MFI-Instance aus.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Network Load Balancer.	Folgen Sie den Anweisungen in der Elastic Load Balancing -Dokumentation, um den Network Load Balancer zu erstellen. Ihr Network Load Balancer leitet den Datenverkehr vom Rocket Enterprise Server zur EC2 LRS-VPSX/MFI-Instanz weiter. Wenn Sie den Network Load Balancer erstellen, wählen Sie auf der Seite Listener und Routing die folgenden Werte aus: 1. Wählen Sie für Protocol TCP aus. 2. Wählen Sie für Port die Option 5500 aus. 3. Wählen Sie unter Standardaktion die Option Weiterleiten an für die Zielgruppe, die Sie zuvor erstellt haben.	Cloud-Architekt

Integrieren Sie Rocket Enterprise Server mit LRS/Queue and LRS VPSX/MFI

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Rocket Enterprise Server für die LRS/Queue-Integration.	1. Connect zu Ihrer Rocket Enterprise EC2 Server-Instance her, indem Sie den Anweisungen in der EC2	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon-Dokumentation folgen. 2. Öffnen Sie im Windows-Startmenü die Rocket Enterprise Server-Administrationsoberfläche. 3. Wählen Sie in der Menüleiste NATIVE. 4. Wählen Sie im Navigationsbereich Directory Server und dann BANKDEMO für Ihre Enterprise Server-Region aus. 5. Scrollen Sie im linken Navigationsbereich von Allgemein nach unten zum Abschnitt Erweitert, um die Umgebungsvariablen (`LRSQ_ADDRESS` ,,`LRSQ_COMMAND`) so zu konfigurieren`LRSQ_PORT` , dass sie auf LRSQ verweisen. • Geben Sie für LRSQ_ADDRESS die IP-Adresse oder den DNS-Namen des Network Load Balancer ein, den Sie zuvor erstellt haben. • Geben Sie für LRSQ_PORT den VPSX LRSQ Listener Port (5500) ein.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Geben Sie für LRSQ_COMMAND den Pfad der ausführbaren LRSQ-Datei ein. **Note** LRS unterstützt derzeit eine maximale Zeichenbeschränkung von 50 für DNS-Namen. Wenn Ihr DNS-Name länger als 50 Zeichen ist, können Sie alternativ die IP-Adresse des Network Load Balancer verwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Rocket Enterprise Server für die LRS VPSX/MFI-Integration.	1. Kopieren Sie den `VPSX_MFI_R2` Ordner aus dem LRS VPSX/MFI-Installationsprogramm in den Rocket Enterprise Server-Speicherort unter. `C\BANKDEMO\print` 2. Connect zu Ihrer Rocket Enterprise EC2 Server-Instance her, indem Sie den Anweisungen in der EC2 Amazon-Dokumentation folgen. 3. Öffnen Sie im Windows-Startmenü die Rocket Enterprise Server-Administrationsoberfläche. 4. Wählen Sie in der Menüleiste NATIVE. 5. Wählen Sie im Navigationsbereich Directory Server und dann BANKDEMO aus. 6. Wählen Sie unter BANKDEMO die Option JES aus. 7. Fügen Sie unter JES-Programmpfad den `DLL(VPSX_MFI_R2)` Pfad von `C\BANKDEMO\print` hinzu.	Cloud-Architekt

Richten Sie die Druckwarteschlange und die Druckbenutzer ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ordnen Sie das Rocket Software Print Exit-Modul dem Serverausführungsprozess des Rocket Enterprise Server-Batchdruckers zu.	1. Connect zu Ihrer Rocket Enterprise EC2 Server-Instance her, indem Sie den Anweisungen in der EC2 Amazon-Dokumentation folgen. 2. Öffnen Sie im Windows-Startmenü die Rocket Focus Enterprise Server Administration UI. 3. Wählen Sie in der Menüleiste NATIVE. 4. Wählen Sie im Navigationsbereich Directory Server und dann BANKDEMO aus. 5. Wählen Sie unter BANKDEMO die Option JES aus, und scrollen Sie nach unten zu Printers. 6. Ordnen Sie unter Drucker das Modul Rocket Software Print Exit (LRSPRTE6 für Batch) dem Rocket Enterprise Server-Batchdrucker Server Execution Process (SEP) zu. Dadurch wird die Weiterleitung der Druckausgabe an LRS VPSX/MFI ermöglicht.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen zur Konfiguration finden Sie unter Using the Exit in der Micro Focus-Dokumentation. OpenText	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Druckausgabewarteschlange in LRS VPSX/MFI und integrieren Sie sie in LRS X. PageCenter	1. Connect zu Ihrer LRS EC2 VPSX/MFI-Instanz her. 2. Öffnen Sie im Windows-Startmenü das VPSX-Webinterface. 3. Wählen Sie im Navigationsbereich Drucker aus. 4. Wählen Sie Hinzufügen und dann Drucker hinzufügen. 5. Geben Sie auf der Seite Druckerkonfiguration als Druckername Lokal ein. 6. Geben Sie für VPSX ID ein. VPS1 7. Wählen Sie für CommTypeTCPIP/LRSQ aus. 8. Geben Sie für Host/IP-Adresse die IP-Adresse des Network Load Balancer ein, der den LRS X-Instances vorstellt. PageCenter EC2 9. Geben Sie für Remote-Port 5800 ein. 10. Geben Sie für Remote-Warteschlange den Namen des LRS PageCenter X-Dokumentenordners ein, in dem die Ausgabe gespeichert werden soll. 11. Wählen Sie Hinzufügen aus.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Druckbenutzer in LRS VPSX/MFI.	1. Connect zu Ihrer LRS EC2 VPSX/MFI-Instanz her. 2. Öffnen Sie im Windows-Startmenü das VPSX-Webinterface. 3. Wählen Sie im Navigationsbereich Sicherheit und dann Benutzer aus. 4. Wählen Sie in der Spalte Benutzername die Option admin und dann Kopieren aus. 5. Geben Sie im Fenster Benutzerprofilverwaltung für Benutzername einen Benutzernamen ein (z. B. PrintUser). 6. Geben Sie unter Beschreibung eine kurze Beschreibung ein (z. B. Benutzer für Testdruck). 7. Wählen Sie Aktualisieren. Dadurch wird ein Druckbenutzer erstellt (z. B. PrintUser). 8. Wählen Sie im Navigationsbereich unter Benutzer den neuen Benutzer aus, den Sie erstellt haben. 9. Wählen Sie im Menü Befehl die Option Sicherheit aus. 10. Wählen Sie auf der Seite Sicherheitsregeln alle	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zutreffenden Optionen für Druckersicherheit und Jobsicherheit aus, und klicken Sie dann auf Speichern. 11. Um Ihren neuen Druckbenutzer zur Administratorgruppe hinzuzufügen, wählen Sie im Navigationsbereich Sicherheit und dann Konfigurieren aus. 12. Fügen Sie im Fenster Sicherheitskonfiguration Ihren neuen Druckbenutzer zur Administratorspalte hinzu.	

Richten Sie einen LRS PageCenter X-Server bei Amazon ein EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon EC2 Windows-Instance.	Starten Sie eine Amazon EC2 Windows-Instance, indem Sie den Anweisungen in Schritt 1: Starten einer Instance in der EC2 Amazon-Dokumentation folgen. Verwenden Sie denselben Hostnamen, den Sie für Ihre LRS-Produktlizenz verwendet haben. Ihre Instance muss die folgenden Hardware- und	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Softwareanforderungen für PageCenter LRS X erfüllen: • CPU — Doppelkern • RAM — 16 GB • Laufwerk — 500 GB • Minimale EC2 Instanz — `m5.xlarge` • Betriebssystem — Windows • Software — IIS oder Apache **Note** Die oben genannten Hardware- und Softwareanforderungen sind für eine kleine Druckerflotte (etwa 500—1000) vorgesehen. Um die vollständigen Anforderungen zu erfahren, wenden Sie sich an Ihre LRS- und AWS-Ansprechpartner. 1. Wenn Sie Ihre Windows-Instance erstellen, stellen Sie sicher, dass der EC2 Hostname derselbe Hostname ist, der für	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die LRS-Produktlizenz verwendet wurde. 2. Connect zu Ihrer EC2 Instance her, indem Sie den Anweisungen in der EC2 Amazon-Dokumentation folgen. 3. Suchen und öffnen Sie im Windows-Startmenü den Server-Manager. 4. Wählen Sie im Server-Manager Dashboard, Schnellstart, Rollen und Funktionen hinzufügen und anschließend Serverrollen aus. 5. Wählen Sie unter Serverrollen die Option WebServer (IIS) und dann Anwendungsentwicklung aus. 6. Aktivieren Sie unter Anwendungsentwicklung das Kontrollkästchen CGI. 7. Folgen Sie zur Installation von CGI den Anweisungen im Windows Server-Manager-Assistenten zum Hinzufügen von Rollen und Funktionen. 8. Öffnen Sie den Port 5800 für TCP/IP traffic in the Windows firewall of the EC2 instance. LRS VPSX uses the TCPIP/LRSQ das	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eingehende Protokoll auf dem 5800-Port, um mit LRS X zu kommunizieren. PageCenter	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie LRS PageCenter X auf der EC2 Instanz.	1. Connect zu Ihrer EC2 Instance her. 2. Öffnen Sie den Link zur Produkt-Download-Seite in der LRS-E-Mail-Nachricht, die Sie erhalten haben sollten. **Note** LRS-Produkte werden per elektronischer Dateiübertragung (EFT) vertrieben. 3. Laden Sie LRS PageCenter X herunter und entpacken Sie die Datei (Standardordner:). `c:\LRS` 4. Um LRS PageCenter X zu installieren, starten Sie den LRS Product Installer aus dem entpackten Ordner. 5. Wählen Sie im Menü Select Features die Option PageCenterX und dann Next aus, um den Installationsvorgang zu starten. Sie erhalten eine Erfolgsmeldung, wenn die Installation abgeschlossen ist.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie LRS/DIS.	Das LRS/DIS product often is included in LRS VPSX installation. However, if LRS/DIS wurde nicht zusammen mit LRS VPSX installiert. Gehen Sie wie folgt vor, um es zu installieren: 1. Connect zu Ihrer LRS PageCenter EC2 X-Instanc e her. 2. Öffnen Sie in der LRS-E-Mail, die Sie erhalten haben sollten, den Link zur LRS-Produkt-Download-Seite, laden Sie LRS/DIS herunter und entpacken Sie dann die Datei. 3. Navigieren Sie zu dem Speicherort, an dem Sie die Dateien heruntergeladen haben, und starten Sie dann das LRS-Produktinstallationsprogramm. 4. Erweitern Sie im LRS Product Installer die Option LRS Misc Tools, wählen Sie LRS DIS und dann Weiter aus. 5. Folgen Sie den restlichen Anweisungen im LRS-Produktinstallationsprogramm, um den Installationsvorgang abzuschließen.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Zielgruppe.	Erstellen Sie eine Zielgruppe, indem Sie den Anweisungen unter Erstellen einer Zielgruppe für Ihren Network Load Balancer folgen. Wenn Sie die Zielgruppe erstellen, registrieren Sie die LRS PageCenter EC2 X-Instance als Ziel: 1. Wählen Sie auf der Seite Gruppendetails angeben für Wählen Sie einen Zieltyp die Option Instances aus. 2. Wählen Sie für Protokoll die Option TCP aus. 3. Wählen Sie für Port 5800 aus. 4. Wählen Sie auf der Seite Ziele registrieren im Abschnitt Verfügbare Instanzen die LRS PageCenter EC2 X-Instance aus.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Network Load Balancer.	Folgen Sie den Anweisungen in der Elastic Load Balancing -Dokumentation, um den Network Load Balancer zu erstellen. Ihr Network Load Balancer leitet den Datenverkehr von LRS VPSX/MFI zur LRS X-Instance weiter. PageCenter EC2 Wenn Sie den Network Load Balancer erstellen, wählen Sie auf der Seite Listener und Routing die folgenden Werte aus: 1. Wählen Sie für Protocol TCP aus. 2. Wählen Sie für Port 5800 aus. 3. Wählen Sie für Standardaktion die Option Weiterleiten an für die Zielgruppe, die Sie zuvor erstellt haben.	Cloud-Architekt

Richten Sie Output-Management-Funktionen in LRS X ein PageCenter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie die Importfunktion in LRS X. PageCenter	Sie können die LRS PageCenter X-Importfunktion verwenden, um die Ausgaben, die auf LRS PageCenter X landen, anhand von Kriterien	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wie Jobname oder Formular-ID zu erkennen. Anschließend können Sie die Ausgaben an bestimmte Ordner in LRS X weiterleiten. PageCenter Gehen Sie wie folgt vor, um die Importfunktion zu aktiviere n: 1. Connect zu Ihrer LRS PageCenter EC2 X-Instanc e her, indem Sie den Anweisungen in der EC2 Amazon-Dokumentation folgen. 2. Öffnen Sie im Windows-S tartmenü das PCX-Webin terface. 3. Wählen Sie im Folder Explorer Admin aus. 4. Wählen Sie auf der Konfigurationsseite Erweitert, Parameter importieren aus. 5. Aktivieren Sie im Abschnitt Parameter importieren das Kontrollkästchen Erweiterter Import. 6. Um die Änderungen zu übernehmen, wählen Sie Aktualisieren.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Richtlinie zur Aufbewahrung von Dokumenten.	LRS PageCenter X verwendet eine Richtlinie zur Aufbewahrung von Dokumenten, um zu entscheiden, wie lange ein Dokument in PageCenter LRS X aufbewahrt werden soll. Gehen Sie wie folgt vor, um die Richtlinie zur Aufbewahrung von Dokumenten zu konfigurieren: 1. Connect zu Ihrer LRS PageCenter EC2 X-Instanc e her. 2. Öffnen Sie im Windows-S tartmenü das PCX-Webin terface. 3. Wählen Sie im Folder Explorer Admin aus. 4. Wählen Sie auf der Admin-Seite Archivgruppenliste /Allgemeiner Administr ator und dann Aufbewahr ungsrichtlinie aus. 5. Wählen Sie im Abschnitt Aufbewahrungsrichtlinie die Option Hinzufügen aus, um eine Aufbewahrungsricht linie zu erstellen. 6. Geben Sie auf der Informati onsseite zur Aufbewahr ungsrichtlinie einen Namen, eine Beschreibung und	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	einen Aufbewahrungszeitraum für das Dokument ein. 7. Um Ihre Änderungen zu speichern und die Richtlinie zu erstellen, wählen Sie OK.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Regel, um das Ausgabedokument an einen bestimmten Ordner in LRS PageCenter X weiterzuleiten.	In LRS PageCenter X bestimmt Destination den Ordnerpfad, an den die Ausgabe gesendet wird, wenn dieses Ziel von der Berichtsdefinition aufgerufen wird. Erstellen Sie für dieses Beispiel einen Ordner, der auf dem Formular-ID-Ordner in der Berichtsdefinition basiert, und speichern Sie die Ausgabe in diesem Ordner. 1. Connect zu Ihrer LRS PageCenter EC2 X-Instanc e her. 2. Öffnen Sie im Windows-S tartmenü das PCX-Webin terface. 3. Wählen Sie im Folder Explorer Admin, Advance Import, Destination aus. 4. Wählen Sie im Abschnitt Ziel die Option Hinzufüge n aus, um das Formular Zielverwaltung zu öffnen. 5. Geben Sie im Formular Destination Maintenance die folgenden Werte ein: • Zielname — Formular • Beschreibung — Beschreibung des Ziels, z. B. formularbasierte Ordnerstruktur	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Zieltyp — Ordner • Ordnerparameter — Ordnerpfad für den Import (der Ordnerpfad, der in PageCenter X erstellt wird, wenn das Dokument ankommt; der Pfad **`/Test/&FORM/&IMPORTDATE/&IMPORTTIME`** erstellt beispielsweise einen **`Test`** Basisordner, einen Unterordner, der auf der angegebenen Formular-ID basiert, einen Unterordner, der auf dem Importdatum basiert **`STD`**, und dann einen Unterordner, der auf der Importzeit basiert) • Dokumentname — Dynamischer Name, der einem Dokument zugewiesen wird, wenn es im Ordner gespeichert wird. 6. Wählen Sie in der Dropdownliste eine Aufbewahrungsrichtlinie aus. Wählen Sie beispielsweise Jahr1, um das Dokument 1 Jahr lang aufzubewahren.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Um die Änderungen zu speichern, wählen Sie Ok.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Berichtsdefinition.	1. Connect zu Ihrer LRS PageCenter EC2 X-Instance her. 2. Öffnen Sie im Windows-Startmenü das PCX-Webinterface. 3. Wählen Sie im Folder Explorer Admin, Advance Import, Report Definition und dann Hinzufügen aus. 4. Geben Sie auf der Wartungsseite der Berichtsdefinition auf der Registerkarte Allgemein den Namen der Berichtsdefinition ein. 5. Auf der Registerkarte Allgemein können Sie unter Felder Auswahlkriterien wie Jobname, Formular, Klasse und Autor angeben. Sie könnten beispielsweise den Jobnamen MFIDEMO eingeben. Der Wert Auftragsname ist der Name des Batch-Auftrags, der die Druckausgabe generiert. 6. Wählen Sie auf der Registerkarte Ziel unter Verfügbares Ziel das zuvor erstellte Ziel (Formular) aus.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Wählen Sie Hinzufüge n, um das Formularziel als Zugewiesenes Ziel hinzuzufügen. **Note** Dieses Beispiel beinhaltet eine Berichtsdefinition , bei der eine von der MFIDEMO generierte und an LRS PageCenter X weitergeleitete Ausgabe in der in der Zieldefin ition definierten Ordnerstruktur gespeichert wird.	

Richten Sie Authentifizierung und Autorisierung für das Output-Management ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine von AWS verwaltete Microsoft AD-Domain mit Benutzern und Gruppen.	1. Um ein Verzeichnis auf AWS Managed Microsoft AD zu erstellen, folgen Sie den Anweisungen unter Erstellen Sie Ihr AWS Managed Microsoft AD-Verzeichnis. 2. Um eine EC2 Instance (Active Directory-Manager)	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bereitzustellen und Active Directory-Tools zur Verwaltung Ihres AWS Managed Microsoft AD zu installieren, folgen Sie den Anweisungen in Schritt 3: Bereitstellen einer EC2 Instance zur Verwaltung Ihres AWS Managed Microsoft AD. 3. Folgen Sie den Anweisungen in der EC2 Amazon-Dokumentation, um eine Verbindung zu Ihrer EC2 Instance herzustellen. **Note** Wenn Sie eine Verbindung mit der EC2 Instance herstellen, geben Sie im Windows-Sicherheitsfenster die Administratoranmeldedaten für das Verzeichnis ein, das Sie in Schritt 1 erstellt haben. 4. Wählen Sie im Windows-Startmenü unter Windows-Verwaltungstools die Option Active Directory-Benutzer und -Computer aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Folgen Sie den Anweisungen unter Benutzer erstellen, um einen Druckbenutzer in der Active Directory-Domäne zu erstellen.	
Verbinden Sie die EC2 Instances mit einer von AWS verwalteten Microsoft AD-Domain.	Verbinden Sie die LRS VPSX/MFI- und LRS PageCenter EC2 X-Instances automatisch (AWS Knowledge Center-Dokumentation) oder manuell (AWS Directory Service-Dokumentation) mit Ihrer AWS Managed Microsoft AD-Domain.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren und integrieren Sie LRS/DIS mit AWS Managed Microsoft AD für die LRS PageCenter X-Instance. EC2	1. Connect zu Ihrer LRS PageCenter EC2 X-Instance her. 2. Öffnen Sie im Windows-Startmenü das PCX-Webinterface. 3. Wählen Sie im Folder Explorer Admin aus. 4. Wählen Sie auf der Konfigurationsseite im Abschnitt Sicherheitsparameter für Sicherheitstyp die Option LRS/DIS aus. 5. Geben Sie Ihre Einstellungen für die restlichen Optionen im Abschnitt Sicherheitsparameter ein. 6. Öffnen Sie im Windows-Startmenü den Ordner PageCenterX, wählen Sie Server Start und dann Server Stop aus. 7. Melden Sie sich mit Ihrem Active Directory-Benutzernamen und -Passwort bei LRS PageCenter X an.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie eine Importgruppe, um die Ausgabe von LRS VPSX nach LRS X zu importieren. PageCenter	1. Connect zu Ihrer LRS PageCenter EC2 X-Instanc e her. 2. Öffnen Sie im Windows-S tartmenü das PCX-Webin terface. 3. Wählen Sie im Folder Explorer Admin, Security admin, Groups aus. 4. Wählen Sie im Abschnitt Gruppen die Option Hinzufügen aus, um das Formular für Gruppenei nstellungen zu öffnen. 5. Geben Sie im Formular Gruppeneinstellungen Werte für Gruppenname und Beschreibung ein. 6. Erweitern Sie Allgemeine Optionen und aktivieren Sie dann das Kontrollkästchen Importieren. 7. Um die Änderungen zu speichern, wählen Sie Ok.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie der Importgruppe eine Sicherheitsregel hinzu.	1. Öffnen Sie das Kontextmenü (Rechtsklick) für Gruppe importieren. 2. Wählen Sie „Erweitert“ und anschließend „Sicherheit“. 3. Wählen Sie im Bereich Sicherheit die Option Importieren und aktivieren Sie das Kontrollkästchen Unterordner. 4. Um die Änderungen zu speichern, wählen Sie Anwenden.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie in LRS PageCenter X einen Benutzer, um den Ausgabeimport von LRS VPSX/MFI durchzufü hren.	Wenn Sie in LRS PageCente r X einen Benutzer für den Ausgabeimport erstellen, sollte der Benutzername mit der VPSX-ID der Druckausg abewarteschlange in LRS VPSX/MFI identisch sein. In diesem Beispiel lautet die VPSX-ID. VPS1 1. Connect zu Ihrer LRS PageCenter EC2 X-Instanc e her. 2. Öffnen Sie im Windows-S tartmenü das PCX-Webin terface. 3. Wählen Sie im Folder Explorer Admin, Security admin, User aus. 4. Wählen Sie Hinzufügen, um das Formular zur Verwaltun g des Benutzerprofils zu öffnen. 5. Geben Sie im Feld Benutzerprofilverwaltung den Wert Benutzername ein VPS1.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie den LRS PageCenter X-Import-Benutzer der Gruppe Nur importieren hinzu.	Gehen Sie wie folgt vor, um die erforderlichen Berechtigungen für den Dokumentenimport von LRS VPSX nach LRS PageCenter X zu erteilen: 1. Connect zu Ihrer LRS PageCenter EC2 X-Instanc e her. 2. Öffnen Sie im Windows-S tartmenü das PCX-Webin terface. 3. Wählen Sie im Folder Explorer Admin, Security admin, Groups aus. 4. Öffnen Sie im Abschnitt Gruppen das Kontextmenü (mit der rechten Maustaste) für die Gruppe Nur importier en und wählen Sie dann Erweitert, Sicherheit aus. 5. Wählen Sie auf der Seite Folder Security Records (ImportOnly) die Registerk arte Benutzer aus. 6. Wählen Sie auf der Registerkarte Benutzer unter Name den Benutzer VPS1aus der Dropdownl iste aus und klicken Sie auf Anwenden.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
LRS/DIS with AWS Managed Microsoft AD for the LRS VPSX/MFI EC2 Instanz konfigurieren.	1. Connect zu Ihrer LRS EC2 VPSX/MFI-Instanz her. 2. Öffnen Sie im Windows-S tartmenü das VPSX-Webi nterface. 3. Wählen Sie im Navigatio nsbereich Sicherheit und dann Konfigurieren aus. 4. Wählen Sie auf der Seite Sicherheitskonfiguration im Abschnitt Sicherhei tsparameter für Sicherhei tstyp die Option LRS/DIS (Extern) aus. 5. Geben Sie Ihre Einstellu ngen für die restlichen Optionen im Abschnitt Sicherheitsparameter ein. 6. Öffnen Sie im Windows-Startmenü den Ordner LRS Output Management, wählen Sie Server Start und dann Server Stop aus. 7. Melden Sie sich mit Ihrem Active Directory-Benutzer namen und -Passwort bei LRS VPSX/MFI an.	Cloud-Architekt

Amazon FSx für Windows File Server als Betriebsdatenspeicher für LRS X PageCenter konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Dateisystem für LRS X. PageCenter	Um Amazon FSx for Windows File Server als Betriebsd atenspeicher für LRS PageCenter X in einer Multi-AZ-Umgebung zu verwenden , folgen Sie den Anweisungen in Schritt 1: Erstellen Sie Ihr Dateisystem.	Cloud-Architekt
Ordnen Sie die Dateifreigabe der LRS PageCenter EC2 X-Instanz zu.	Um die im vorherigen Schritt erstellte Dateifreigabe der LRS PageCenter EC2 X-Instanz zuzuordnen, folgen Sie den Anweisungen in Schritt 2: Ordnen Sie Ihre Dateifreigabe einer EC2 Instanz zu, auf der Windows Server ausgeführt wird.	Cloud-Architekt
Ordnen Sie das LRS PageCenter X Control Directory und das Master Folder Directory dem FSx Amazon-Netzwerk-Share-Laufwerk zu.	1. Connect zu Ihrer LRS PageCenter EC2 X-Instanc e her, indem Sie den Anweisungen in der EC2 Amazon-Dokumentation folgen. 2. Öffnen Sie im Windows-S tartmenü das PCX-Webin terface. 3. Wählen Sie im Folder Explorer Admin, Configura tion aus. 4. Wählen Sie auf der Konfigurationsseite	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Verzeichnisse und dann Control Directory aus. 5. Geben Sie im Feld Kontrollverzeichnisse den Wert ein `\\FSx file share DNS name\share\cntl` . 6. Geben Sie im Hauptordnerverzeichnis den Wert ein `\\FSx file share DNS name\share\mstr` .	

Testen Sie einen Output-Management-Workflow

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initiieren Sie eine Batch-Druckanfrage über die Rocket BankDemo Software-App.	1. Öffnen Sie den 3270-Terminal-Emulator in Ihrer Rocket Enterprise Server-Instanz. EC2 2. Connect zur BankDemo App her, indem Sie den Befehl ausführen `connect 127.0.0.1:9278` . 3. Geben Sie in der BankDemo Befehlszeilenschnittstelle B0001 als Benutzer-ID ein. Geben Sie als Passwort einen Schlüssel ein, der nicht leer ist. 4. Geben Sie für die Option Gedruckte Kontoauszüge	Testingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	anfordern in die leere Zeile X ein. 5. Geben Sie im Abschnitt Kontoauszug senden für E-Mail den Wert Y ein, und drücken Sie dann F10.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Druckausgabe in LRS X. PageCenter	1. Connect zu Ihrer LRS PageCenter EC2 X-Instance her, indem Sie den Anweisungen in der EC2 Amazon-Dokumentation folgen. 2. Öffnen Sie im Windows-Startmenü das PCX-Webinterface. 3. Öffnen Sie im Navigationsbereich den Ordner Test, öffnen Sie den Ordner STD und öffnen Sie dann den Ordner mit dem Job-Ausführungsdatum, z. B. `08-03-2023` (MM-DD-YYYY). **Note** Dabei handelt es sich um dieselbe Ordnerstruktur wie in der Story Erstellen Sie eine Regel, um das Ausgabedokument an einen bestimmten Ordner in LRS X weiterzuleiten. PageCenter 4. Öffnen Sie die `formtest-STD.txt` Datei.	Testingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie können jetzt die Druckausgabe eines Kontoauszugs mit Spalten für die Kontonummer sehen. , Beschreibung, Datum, Betrag und Saldo. Ein Beispiel finden Sie im `batch_print_output` Anhang zu diesem Muster.	

Zugehörige Ressourcen

- LRS
- Datenstrom zur Präsentation erweiterter Funktionen (IBM-Dokumentation)
- Linienkonditionierter Datenstrom (LCDS) (Compart-Dokumentation)
- Unterstützung von Enterprise-Mainframe-Workloads auf AWS mit Micro Focus (Blogbeitrag)
- Modernisieren Sie Ihre Mainframe-Online-Druck-Workloads auf AWS (AWS Prescriptive Guidance)
- Modernisieren Sie Ihre Mainframe-Batchdruck-Workloads auf AWS (AWS Prescriptive Guidance)

Zusätzliche Informationen

Überlegungen

Während Ihrer Modernisierung könnten Sie eine Vielzahl von Konfigurationen für Mainframe-Batch- und Online-Prozesse und die damit generierte Ausgabe in Betracht ziehen. Die Mainframe-Plattform wurde von allen Kunden und Anbietern, die sie verwenden, an spezielle Anforderungen angepasst, die sich direkt auf den Druck auswirken. Beispielsweise könnte Ihre aktuelle Plattform den IBM AFP-Datenstream oder Xerox LCDS in den aktuellen Workflow integrieren. Darüber hinaus können Mainframe-Wagen-Steuerzeichen und Kanalbefehle das Aussehen der gedruckten Seite beeinflussen und erfordern möglicherweise eine besondere Behandlung. Im Rahmen der Planung der Modernisierung empfehlen wir Ihnen, die Konfigurationen in Ihrer spezifischen Druckumgebung zu bewerten und zu verstehen.

Erfassung von Druckdaten

Rocket Software Print Exit leitet die erforderlichen Informationen weiter, damit LRS VPSX/MFI die Spool-Datei effektiv verarbeiten kann. Die Informationen bestehen aus Feldern, die in den entsprechenden Steuerblöcken übergeben werden, wie zum Beispiel den folgenden:

- JOBNAME
- BESITZER (BENUTZER-ID)
- ZIEL
- BILDEN
- DATEINAME
- SCHRIFTSTELLER

LRS VPSX/MFI unterstützt die folgenden Mainframe-Batch-Mechanismen zur Erfassung von Daten von Rocket Enterprise Server:

- BATCH-COBOL-Anweisungen. print/spool processing using standard z/OS JCL SYSOUT DD/ OUTPUT
- print/spool processing using standard z/OSBATCH-COBOL-JCL-CA-SPOOL-SUBSYS-DD-Anweisungen.
- IMS/COBOL print/spoolVerarbeitung mithilfe der CBLTDLI-Schnittstelle. Eine vollständige Liste der unterstützten Methoden und Programmierbeispiele finden Sie in der LRS-Dokumentation, die in Ihrer Produktlizenz enthalten ist.

Gesundheitschecks zwischen Drucker und Flotte

LRS VPSX/MFI (LRS LoadX) kann tiefgreifende Zustandsprüfungen durchführen, einschließlich Gerätemanagement und Betriebsoptimierung. Die Geräteverwaltung kann Fehler in einem Druckergerät erkennen und die Druckanforderung an einen fehlerfreien Drucker weiterleiten. Weitere Informationen zu umfassenden Integritätsprüfungen für Druckerflotten finden Sie in der LRS-Dokumentation, die in Ihrer Produktlizenz enthalten ist.

Authentifizierung und Autorisierung drucken

LRS/DIS enables LRS applications to authenticate user IDs and passwords by using Microsoft Active Directory or a Lightweight Directory Access Protocol (LDAP) server. In addition to

basic print authorization, LRS/DISkann in den folgenden Anwendungsfällen auch detaillierte Drucksicherheitskontrollen anwenden:

- Steuert, wer den Druckerauftrag durchsuchen kann.
- Verwaltet die Navigationsebene der Aufträge anderer Benutzer.
- Verwalten Sie betriebliche Aufgaben, z. B. Sicherheitsfunktionen auf Befehlsebene wie Sperren oder Freigeben, Löschen, Ändern, Kopieren und Umleiten. Die Sicherheit kann entweder anhand der Benutzer-ID oder der Gruppe eingerichtet werden, ähnlich wie bei einer Active Directory-Sicherheitsgruppe oder einer LDAP-Gruppe.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Modernisieren Sie die CardDemo Mainframe-Anwendung mithilfe von AWS Transform

Erstellt von Santosh Kumar Singh (AWS) und Cheryl du Preez (AWS)

Übersicht

AWS Transformwurde entwickelt, um die Modernisierung von Mainframe-Anwendungen zu beschleunigen. Es verwendet generative KI, um den Mainframe-Modernisierungsprozess zu rationalisieren. Es automatisiert komplexe Aufgaben wie: Analyse von Legacy-Code, Mainframe-Dokumentation, Extraktion von Geschäftsregeln, Zerlegung monolithischer Anwendungen in Geschäftsdomänen und Code-Refactoring. Es beschleunigt Modernisierungsprojekte durch die Automatisierung komplexer Aufgaben wie Anwendungsanalyse und Planung der Migrationssequenz. Bei der Zerlegung monolithischer Anwendungen erfolgt eine AWS Transform intelligente Sequenzierung der Mainframe-Anwendungstransformation, sodass Sie Geschäftsfunktionen parallel transformieren können. AWS Transform kann die Entscheidungsfindung beschleunigen und die betriebliche Flexibilität und Migrationseffizienz verbessern.

Dieses Muster enthält step-by-step Anleitungen, mit denen Sie die Möglichkeiten zur Mainframe-Modernisierung von AWS Transform by using CardDemotesten können. Dabei handelt es sich um ein Beispiel für eine Open-Source-Mainframe-Anwendung.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- AWS IAM Identity Center, aktiviert
- Berechtigungen, mit denen Administratoren Folgendes aktivieren können AWS Transform
- Berechtigungen, die es Administratoren ermöglichen, Verbindungsanfragen von Amazon Simple Storage Service (Amazon S3) für die AWS Transform Webanwendung anzunehmen

Einschränkungen

- AWS Transform ist nur in einigen Fällen verfügbar AWS-Regionen. Eine vollständige Liste der unterstützten Regionen finden Sie unter Unterstützte Regionen für AWS Transform.
- AWS Transform unterstützt Codeanalyse, Dokumentgenerierung, Extraktion, Dekomposition und Refactoring von Common Business-Oriented Language (COBOL) auf Java. Weitere

Informationen finden Sie unter Funktionen und Hauptfunktionen und Unterstützte Dateitypen für die Transformation von Mainframe-Anwendungen.

- Es gibt ein Servicekontingent für Mainframe-Transformationsfunktionen in. AWS Transform Weitere Informationen finden Sie unter Kontingente für AWS Transform.
- Um in einem gemeinsamen Arbeitsbereich zusammenarbeiten zu können, müssen alle Benutzer registrierte Benutzer derselben Instanz sein AWS IAM Identity Center , die mit Ihrer Instanz der AWS Transform Webanwendung verknüpft ist.
- Der Amazon S3 S3-Bucket AWS Transform muss sich in derselben AWS-Konto Region befinden.

Architektur

Das folgende Diagramm zeigt die Architektur, die Sie nach diesem Muster eingerichtet haben.

Das Diagramm zeigt den folgenden Workflow:

1. AWS Transform verwendet einen Connector für den Zugriff auf die CardDemo Mainframe-Anwendung, die in einem Amazon S3 S3-Bucket gespeichert ist.
2. AWS Transform verwendet AWS IAM Identity Center , um den Benutzerzugriff und die Authentifizierung zu verwalten. Das System implementiert mehrere Ebenen von Sicherheitskontrollen für Authentifizierung, Autorisierung, Verschlüsselung und Zugriffsverwaltung, um Code und Artefakte während der Verarbeitung zu schützen. Benutzer interagieren mit dem AWS Transform Agenten über eine Chat-Oberfläche. Sie können dem KI-Agenten Anweisungen für bestimmte Aufgaben auf Englisch geben. Weitere Informationen finden Sie in der AWS Transform Dokumentation unter Human in the Loop (HITL).
3. Der KI-Agent interpretiert die Anweisungen des Benutzers, erstellt einen Jobplan, unterteilt den Job in ausführbare Aufgaben und führt ihn selbstständig aus. Benutzer können die Transformation überprüfen und genehmigen. Zu den Transformationsaufgaben gehören die folgenden:
   - Codeanalyse — AWS Transform analysiert den Code in jeder Datei auf Details wie Dateiname, Dateityp, Codezeilen und deren Pfade. Der Agent analysiert den Quellcode, führt Klassifizierungen durch, erstellt Abhängigkeitszuordnungen und identifiziert alle fehlenden Artefakte. Er identifiziert auch doppelte Komponenten.
   - Dokumentgenerierung — AWS Transform generiert Dokumentation für die Mainframe-Anwendung. Durch die Analyse des Codes kann automatisch eine detaillierte Dokumentation der Anwendungsprogramme erstellt werden, einschließlich Beschreibungen der Geschäftslogik, Abläufe, Integrationen und Abhängigkeiten, die in Ihren Altsystemen vorhanden sind.

- Extraktion von Geschäftslogik — AWS Transform analysiert COBOL-Programme, um deren Kerngeschäftslogik zu dokumentieren und Ihnen zu helfen, die grundlegende Geschäftslogik zu verstehen.
- Codezerlegung — AWS Transform zerlegt den Code in Domänen, die Abhängigkeiten zwischen Programmen und Komponenten berücksichtigen. Die Gruppierung verwandter Dateien und Programme innerhalb derselben Domäne verbessert die Organisation und trägt dazu bei, die logische Struktur der Anwendung beizubehalten, wenn sie in kleinere Komponenten aufgeteilt wird.
- Planung von Migrationswellen — Basierend auf den Domänen, die Sie während der Zerlegungsphase erstellt haben, wird ein Migrationswellenplan mit der empfohlenen Modernisierungsreihenfolge AWS Transform generiert.
- Code-Refactoring — AWS Transform Refaktorierung des Codes in allen oder ausgewählten Domaindateien in Java-Code. Ziel dieses Schritts ist es, die kritische Geschäftslogik der Anwendung beizubehalten und sie gleichzeitig in eine modernisierte, Cloud-optimierte Java-Anwendung umzuwandeln.

4. AWS Transform speichert den umgestalteten Code, die generierten Dokumente, die zugehörigen Artefakte und die Laufzeitbibliotheken in Ihrem Amazon S3 S3-Bucket. Sie haben die folgenden Möglichkeiten:
   - Greifen Sie auf den Runtime-Ordner in Ihrem Amazon S3 S3-Bucket zu.
   - Folgen Sie beim Erstellen und Bereitstellen der Anwendung den Anweisungen zum Erstellen und Bereitstellen Ihrer modernisierten Anwendung nach dem Refactoring in der Dokumentation. AWS Transform
   - Fordern Sie über die Chat-Oberfläche ein Beispiel AWS CloudFormation oder eine Hashicorp Terraform-Vorlage an und laden Sie sie herunter. AWS Cloud Development Kit (AWS CDK) Diese Vorlagen können Ihnen dabei helfen, die AWS Ressourcen bereitzustellen, die zur Unterstützung der umgestalteten Anwendung erforderlich sind.
   - Verwenden Sie Reforge, um die Qualität von umgestaltetem Code mithilfe umfangreicher Sprachmodelle () zu verbessern. LLMs Die Refactoring-Engine bewahrt die funktionale Äquivalenz von COBOL und wandelt es gleichzeitig in Java-Code um. Reforge ist ein optionaler Schritt, der nach der Transformation verfügbar ist. In diesem Schritt wird der Code so umstrukturiert LLMs , dass er dem nativen Java sehr ähnlich ist, was die Lesbarkeit und Wartbarkeit verbessern kann. Reforge fügt außerdem menschenlesbare Kommentare hinzu, um Ihnen das Verständnis des Codes zu erleichtern, und implementiert moderne Codierungsmuster und bewährte Methoden.

Tools

AWS-Services

- AWS Transformverwendet agentische KI, um Ihnen zu helfen, die Modernisierung älterer Workloads wie .NET, Mainframe und Workloads zu beschleunigen. VMware
- AWS IAM Identity Centerhilft Ihnen dabei, den Single Sign-On-Zugriff (SSO) auf Ihre und Cloud-Anwendungen zentral zu verwalten. AWS-Konten
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code-Repository

Sie können die AWS CardDemoOpen-Source-Mainframe-Anwendung als Beispielanwendung verwenden, um mit der Mainframe-Modernisierung zu beginnen.

Bewährte Methoden

- Klein anfangen — Beginnen Sie mit kleinem, weniger komplexem Code (15.000—20.000 Codezeilen), um zu verstehen, wie Mainframe-Anwendungen AWS Transform analysiert und transformiert werden.
- Kombinieren Sie es mit menschlichem Fachwissen — Nutzen Sie es AWS Transform als Beschleuniger und setzen Sie gleichzeitig menschliches Fachwissen ein, um optimale Ergebnisse zu erzielen.
- Gründlich prüfen und testen — Überprüfen Sie den transformierten Code immer sorgfältig und führen Sie umfassende Tests durch, um die funktionale Gleichwertigkeit nach der Transformation zu überprüfen.
- Feedback geben — Um Feedback und Verbesserungsvorschläge zu geben, verwenden Sie die Schaltfläche Feedback senden im AWS Management Console oder erstellen Sie einen Fall mit. AWS -Support Weitere Informationen finden Sie unter Support-Anfrage erstellen. Ihr Beitrag ist wertvoll für Serviceverbesserungen und future Entwicklungen.

Epen

Bereiten Sie die Mainframe-Anwendung vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Bucket.	Erstellen Sie einen Amazon S3 S3-Bucket in derselben AWS-Konto Region, in der er aktiviert AWS Transform ist. Sie verwenden diesen Bucket zum Speichern des Mainframe -Anwendungscodes und AWS Transform diesen Bucket zum Speichern der generierten Dokumente, des umgestalt eten Codes und anderer mit der Transformation verknüpft er Dateien. Anweisungen finden Sie in der Amazon S3 S3-Dokumentation unter Bucket erstellen.	Allgemeines AWS
Bereiten Sie die Mainframe-Beispielanwendung vor.	1. Geben Sie den folgenden Befehl ein, um das CardDemoRepository auf Ihre lokale Workstation zu klonen: `git clone https://github.com/aws-samples/aws-mainframe-modernization-carddemo.git` 2. Erstellen Sie einen neuen Ordner mit dem Namen`carddemo`.	App-Entwickler, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Kopieren Sie den `app` Ordner, der den Mainframe-Quellcode enthält, aus dem geklonten Repository in den `carddemo` Ordner. 4. Komprimieren Sie den `cardemo` Ordner in eine ZIP-Datei. 5. Laden Sie die ZIP-Datei in den Amazon S3 S3-Bucket hoch, den Sie erstellt haben. Anweisungen finden Sie unter Objekte hochladen in der Amazon S3 S3-Dokumentation.	

Konfigurieren Sie IAM Identity Center und AWS Transform

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie Benutzer zum IAM Identity Center hinzu.	Fügen Sie Ihre potenziellen Benutzer zum IAM Identity Center hinzu. Folgen Sie den Anweisungen unter Hinzufügen von Benutzern in IAM Identity Center in der AWS Transform Dokumentation.	AWS-Administrator
Benutzer aktivieren AWS Transform und hinzufügen.	1. Aktivieren AWS Transform. Folgen Sie den Anweisungen unter Aktivieren AWS Transform. 2. Benutzer hinzufügen zu AWS Transform. Folgen	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie den Anweisungen unter Benutzer hinzufügen zu AWS Transform.	
Konfigurieren Sie den Benutzerzugriff auf die AWS Transform Webanwendung.	Jeder Benutzer muss die Einladung annehmen, um auf die AWS Transform Webanwendung zuzugreifen. Folgen Sie den Anweisungen in der AWS Transform Dokumentation unter Annahme der Einladung.	App-Entwickler, App-Besitzer
Loggen Sie sich in die AWS Transform Webanwendung ein.	Folgen Sie den Anweisungen unter Anmelden bei AWS Transform.	App-Entwickler, App-Besitzer
Richte einen Workspace ein.	Richten Sie einen Arbeitsbereich ein, in dem Benutzer in der AWS Transform Webanwendung zusammenarbeiten können. Folgen Sie den Anweisungen unter Einrichtung Ihres Workspace in der AWS Transform Dokumentation.	AWS-Administrator

Transformieren Sie die Mainframe-Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Transformationsjob.	Erstellen Sie einen Transformationsjob, um die CardDemo Mainframe-Anwendung zu modernisieren. Anweisungen	App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	finden Sie in der Dokumentation unter Einen Job erstellen und starten. AWS Transform Wenn Sie in der AWS Transform Chat-Oberfläche aufgefordert werden, die Ziele festzulegen, wählen Sie Mainframe-Modernisierung durchführen (IBM z/OS to AWS) und dann Code analysieren, Technische Dokumentation generieren, Geschäftslogik, Code zerlegen, Migrationssequenz planen und Code in Java umwandeln aus.	
Richten Sie den Connector ein.	Richten Sie einen Connector zum Amazon S3 S3-Bucket ein, der die CardDemo Mainframe-Anwendung enthält. Dieser Konnektor ermöglicht AWS Transform den Zugriff auf Ressourcen im Bucket und die Ausführung aufeinanderfolgender Transformationsfunktionen. Anweisungen finden Sie in der AWS Transform Dokumentation unter Einen Konnektor einrichten.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie eine Codeanalyse durch.	1. Geben Sie auf der Seite Asset-Standort angeben den Amazon S3 S3-Bucket-Pfad für die `carddemo` ZIP-Datei ein, die Sie hochgeladen haben. 2. Wählen Sie Genehmigen und senden an AWS Transform. Es beginnt mit der Analyse des Codes. 3. Überwachen Sie den Status auf der Registerkarte Worklog. 4. Wenn die Analyse abgeschlossen ist, wählen Sie im linken Navigationsbereich unter Code analysieren die Option Codeanalyseergebnisse anzeigen aus. 5. (Optional) Wählen Sie Herunterladen, um die vollständige Asset-Liste, den fehlenden Quellcode und die Abhängigkeitsdatei herunterzuladen. Weitere Informationen finden Sie in der AWS Transform Dokumentation unter Codeanalyse.	App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie technische Dokumentation.	1. Wählen Sie im linken Navigationsbereich unter Technische Dokumentation generieren die Option Dateien auswählen und Einstellungen konfigurieren aus. 2. Erweitern Sie COBOL oder JCL und wählen Sie dann eine oder mehrere Dateien aus. 3. Wählen Sie die Detailebene der Dokumentation aus: • Zusammenfassung — Bietet einen allgemeinen Überblick über jede Datei im Geltungsbereich. Enthält außerdem eine einzeilige Zusammenfassung der einzelnen Dateien. • Detaillierte Funktionsspezifikation — Enthält umfassende Informationen zu jeder Datei im Bereich der Mainframe-Anwendungstransformation. Einige Details umfassen Logik und Ablauf, identifizierte Geschäftsregeln, Datenfluss, Abhängigkeiten, Eingabe- und Ausgabeverarbeitun	App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	g sowie verschiedene Transaktionsdetails. 4. Wählen Sie Senden an AWS Transform. 5. Überwachen Sie den Fortschritt auf der Registerkarte Worklog. **Note** Die Dauer der Dokumentg enerierung variiert je nach Anzahl der Dateien und Codezeilen zwischen Minuten und Stunden. 6. Wenn Sie fertig sind, wählen Sie Dokumentationsergebnisse überprüfen aus. 7. Greifen Sie über die Webanwendung auf das generierte Dokument zu oder laden Sie es herunter. Die generierte Dokumentation wird auch im Amazon S3 S3-Bucket gespeichert. 8. Erkunden Sie die generierte Dokumentation, indem Sie in der Chat-Oberfläche spezifische Fragen stellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie können zum Beispiel sagen: „Erzählen Sie mir die Funktionen von CBACT01C“. Weitere Informationen finden Sie in der Dokumentation unter Generieren von technischer Dokumentation. AWS Transform	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Extrahieren Sie die Geschäftslogik.	1. Erweitern Sie im linken Navigationsbereich die Option Geschäftslogik extrahieren und wählen Sie dann Dateien für die Extraktion der Geschäftslogik auswählen aus. 2. Erweitern Sie COBOL oder JCL, und wählen Sie dann eine oder mehrere Dateien aus. 3. Wählen Sie Senden an. AWS Transform 4. Überwachen Sie den Fortschritt auf der Registerkarte Worklog. **Note** Die Extraktionszeit für die Geschäftslogik variiert je nach Anzahl der Dateien und Codezeilen zwischen Minuten und Stunden. 5. Wenn die Extraktion abgeschlossen ist, wählen Sie Ergebnisse der Geschäftslogik-Extraktion überprüfen aus. 6. Wählen Sie eine COBOL- oder JCL-Datei aus, und	App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	klicken Sie dann auf Anzeigen. 7. Ändern Sie den Umfang im Flussdiagramm und in den Funktionsregeln, um die verschiedenen Ebenen der Flussdiagramme, einschließlich des unterstützenden Codes, zu überprüfen. 8. (Optional) Überprüfen Sie die generierte Geschäftslogik, die im JSON-Format in Ihrem Amazon S3 S3-Bucket gespeichert ist. Weitere Informationen finden Sie in der AWS Transform Dokumentation unter Geschäftslogik extrahieren.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Zerlegen Sie den Code.	1. Erweitern Sie im linken Navigationsbereich den Bereich Code zerlegen, und wählen Sie dann In Domänen zerlegen aus. 2. Wählen Sie in der Liste Aktionen die Option Domäne erstellen aus. 3. Geben Sie einen Namen für die neue Domain ein, z. `Bill payment` B. 4. (Optional) Geben Sie eine Beschreibung ein. 5. Suchen Sie in der Suchleiste „Dateien suchen“ nach der Datei`CB00`, und wählen Sie sie dann aus. 6. Wählen Sie Als Startwert markieren aus. 7. Vergewissern Sie sich, dass sich die Startkennzeichnung von Nein auf Ja ändert. 8. Wählen Sie Erstellen aus. 9. Wählen Sie Speichern. 10. Wählen Sie Zerlegen. 11. Überprüfen Sie die Dekompositionsausgabe, indem Sie den Domainnamen auswählen. 12. Wenn die Zerlegung abgeschlossen ist, wählen	App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie Senden an. AWS Transform Weitere Informationen zu Zersetzung und Saatgut finden Sie in der Dokumentation unter Zersetzung. AWS Transform	
Planen Sie die Migrationswellen.	Planen Sie die Migrationswellen für die CardDemo Anwendung. Folgen Sie den Anweisungen unter Planung der Migrationswelle in der AWS Transform Dokumentation, um den Wellenplan zu überprüfen und zu bearbeiten.	App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Refaktorieren Sie den Code.	1. Refaktorieren Sie die CardDemo Mainframe-Anwendung in allen oder ausgewählten Domänendateien in Java-Code. Folgen Sie den Anweisungen unter Refactor-Code in der Dokumentation. AWS Transform 2. Nachdem der Refactoring-Prozess abgeschlossen ist, erstellen und implementieren Sie die modernisierte Java-Anwendung. Folgen Sie den Anweisungen in der Dokumentation unter Erstellen und Bereitstellen Ihrer modernisierten Anwendung nach dem Refactoring. AWS Transform	App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Verwenden Sie Reforge, um den Java-Code zu verbessern.	1. Erstellen Sie einen neuen Job und geben Sie dann ein Ziel von `Reforge the code` ein. 2. Geben Sie den Wert eines Projekts ein, das durch AWS Transform modernisiert wurde. Dieses Projekt sollte sich in Ihrem Amazon S3 S3-Bucket befinden. 3. Geben Sie die Java-Klassenliste ein, die angibt, welche Serviceklassen neu formatiert werden sollen. 4. Überprüfen Sie die generierte Ausgabe im Amazon S3 S3-Bucket. Weitere Informationen finden Sie in der AWS Transform Dokumentation unter Reforge.	App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rationalisieren Sie die Bereitstellung.	AWS Transform kann IaC-Vorlagen (Infrastructure as Code) für CloudFormation AWS CDK, oder Terraform bereitstellen. Diese Vorlagen helfen Ihnen bei der Bereitstellung von Kernkomponenten, einschließlich Rechen-, Datenbank-, Speicher- und Sicherheitsressourcen. 1. Fordern AWS Transform Sie die Vorlagen in der Chat-Oberfläche an, indem Sie eingeben`Share the mainframe refactor <service> templates` , wo `<service>` sich einer der unterstützten IaC-Dienste befindet. 2. Stellen Sie die Vorlage mithilfe Ihres bevorzugten Dienstes bereit. Sehen Sie sich zum Beispiel die folgenden Ressourcen an: • Einen Stack von der CloudFormation Konsole aus erstellen (CloudFormation Dokumentation) • AWS CDK Anwendungen bereitstellen (AWS CDK Dokumentation)	App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Infrastruktur aufbauen (Terraform-Dokumentation) Weitere Informationen finden Sie in der Dokumentation unter Bereitstellungsfunktionen. AWS Transform	

Fehlerbehebung

Problem	Lösung
Sie können den Quellcode oder das generierte Dokument in der AWS Transform Webanwendung nicht anzeigen.	Fügen Sie der CORS-Berechtigung eine Richtlinie hinzu, die der Amazon S3 S3-Bucket AWS Transform als Ursprung zulassen soll. Weitere Informationen finden Sie in der Dokumentation unter CORS-Berechtigungen für den AWS Transform S3-Bucket.

Zugehörige Ressourcen

AWS Dokumentation

- Transformation von Mainframe-Anwendungen (AWS Transform Dokumentation)

Andere Ressourcen AWS

- Beschleunigen Sie Ihre Mainframe-Modernisierung mithilfe von KI-Agenten mit AWS Transform (AWS Blogbeitrag)
- AWS Transform FAQs
- AWS IAM Identity Center FAQs

Videos und Tutorials

- Einführung in Amazon Q Developer: Transform (AWS Skill Builder)
- AWS re:Invent 2024 — Schnellere Modernisierung von Mainframe-Anwendungen mit Amazon Q Developer () YouTube
- AWS re:Invent 2024 — Automatisierung von Migration und Modernisierung zur Beschleunigung der Transformation () YouTube
- AWS re:Invent 2024 — Toyota treibt Innovationen voran und verbessert die betriebliche Effizienz mit KI der Generation () YouTube

> **Note**
>
> AWS Transform war zuvor als Amazon Q Developer Transform for Mainframe bekannt.

Modernisieren Sie Mainframe-Batchdruck-Workloads mithilfe AWS von Rocket Enterprise Server und LRS VPSX/MFI

Erstellt von Shubham Roy (AWS), Abraham Rondon (Micro Focus), Guy Tucker (Levi, Ray and Shoup Inc) und Kevin Yung (AWS)

Übersicht

Dieses Muster zeigt Ihnen, wie Sie Ihre geschäftskritischen Mainframe-Batchdruck-Workloads in der Amazon Web Services (AWS) Cloud modernisieren können, indem Sie Rocket Enterprise Server als Runtime für eine modernisierte Mainframe-Anwendung und LRS VPSX/MFI (Micro Focus Interface) als Druckserver verwenden. Das Muster basiert auf dem Ansatz der Replatform Mainframe-Modernisierung. Bei diesem Ansatz migrieren Sie Ihre Mainframe-Batch-Jobs zu Amazon Elastic Compute Cloud (Amazon EC2) und Ihre Mainframe-Datenbank, wie IBM DB2 for z/OS, zu Amazon Relational Database Service (Amazon RDS). Die Authentifizierung und Autorisierung für den modernisierten Druck-Workflow erfolgt durch AWS Directory Service for Microsoft Active Directory, auch bekannt als AWS Managed Microsoft AD. Der LRS Directory Information Server (LRS/DIS) ist in AWS Managed Microsoft AD integriert. Durch die Modernisierung Ihrer Batchdruck-Workloads können Sie die IT-Infrastrukturkosten senken, den technischen Aufwand für die Wartung älterer Systeme verringern, Datensilos beseitigen, die Agilität und Effizienz mit einem DevOps Modell erhöhen und die Vorteile von On-Demand-Ressourcen und Automatisierung in der AWS-Cloud nutzen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Mainframe-Druck- oder Output-Management-Workload
- Grundkenntnisse zum Wiederaufbau und zur Bereitstellung einer Mainframe-Anwendung, die auf Rocket Enterprise Server läuft (Weitere Informationen finden Sie im Rocket Enterprise Server-Datenblatt in der Rocket-Dokumentation.)
- Grundkenntnisse der Cloud-Printing-Lösungen und -Konzepte von LRS
- Rocket Enterprise Server-Software und -Lizenz (Weitere Informationen erhalten Sie vom Rocket-Vertrieb.)
- VPSX/MFI, LRS/Queue, and LRS/DISLRS-Software und -Lizenzen (Weitere Informationen erhalten Sie vom LRS-Vertrieb.)

> **Note**
>
> Weitere Informationen zu Überlegungen zur Konfiguration von Mainframe-Batchdruck-Workloads finden Sie unter Überlegungen im Abschnitt Zusätzliche Informationen dieses Musters.

Produktversionen

- Rocket Enterprise Server 6.0 (Produktupdate 7)
- LRS VPSX/MFI V1R3 oder höher

Architektur

Quelltechnologie-Stack

- Betriebssystem — IBM z/OS
- Programmiersprache — Common Business-Oriented Language (COBOL), Job Control Language (JCL) und Customer Information Control System (CICS)
- Datenbank — IBM DB2 für z/OS und Virtual Storage Access Method (VSAM)
- Sicherheit — Resource Access Control Facility (RACF), CA Top Secret für z/OS und Access Control Facility 2 () ACF2
- Druck- und Ausgabemanagement — IBM Mainframe-z/OS-Druckprodukte (IBM Tivoli Output Manager für z/OS, LRS und CA View)

Zieltechnologie-Stack

- Betriebssystem — Microsoft Windows Server läuft auf Amazon EC2
- Rechnen — Amazon EC2
- Programmiersprache — COBOL, JCL und CICS
- Datenbank — Amazon RDS
- Sicherheit — AWS Managed Microsoft AD
- Druck- und Ausgabemanagement — LRS-Drucklösung auf AWS
- Mainframe-Laufzeitumgebung — Rocket Enterprise Server

Quellarchitektur

Das folgende Diagramm zeigt eine typische aktuelle Architektur für einen Mainframe-Batchdruck-Workload:

Das Diagramm zeigt den folgenden Workflow:

1. Benutzer führen Geschäftstransaktionen auf einem System of Engagement (SoE) durch, das auf einer in COBOL geschriebenen IBM CICS-Anwendung basiert.
2. Das SoE ruft den Mainframe-Service auf, der die Geschäftstransaktionsdaten in einer system-of-records (SoR) -Datenbank wie IBM for z/OS aufzeichnet. DB2
3. Das SoR speichert die Geschäftsdaten aus dem SoE.
4. Der Batch-Job-Scheduler initiiert einen Batch-Job, um eine Druckausgabe zu generieren.
5. Der Batch-Job extrahiert Daten aus der Datenbank, formatiert die Daten entsprechend den Geschäftsanforderungen und generiert dann Geschäftsergebnisse wie Abrechnungen, Personalausweise oder Kreditauszüge. Schließlich leitet der Batch-Job die Ausgabe an das Printing Output Management weiter, wo sie auf der Grundlage der Geschäftsanforderungen verarbeitet und ausgegeben werden kann.
6. Das Printing Output Management empfängt die Druckausgabe des Batch-Auftrags und sendet diese Ausgabe dann an ein bestimmtes Ziel, z. B. eine E-Mail, eine Dateifreigabe, die sicheres FTP verwendet, einen physischen Drucker, der LRS-Drucklösungen verwendet (wie in diesem Muster gezeigt), oder IBM Tivoli.

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur für einen Mainframe-Batchdruck-Workload, der in der AWS-Cloud bereitgestellt wird:

Das Diagramm zeigt den folgenden Workflow:

1. Der Batch-Job-Scheduler initiiert einen Batch-Job, um Druckausgaben wie Abrechnungen, Personalausweise oder Kreditauszüge zu erstellen.
2. Der Mainframe-Batch-Job (auf Amazon umgestellt EC2) verwendet die Rocket Enterprise Server-Laufzeit, um Daten aus der Anwendungsdatenbank zu extrahieren, Geschäftslogik auf die Daten

anzuwenden, die Daten zu formatieren und die Daten dann mithilfe von Rocket Software Print Exit (Micro Focus-Dokumentation) an ein Druckziel zu senden.

3. Die Anwendungsdatenbank (ein SoR, der auf Amazon RDS läuft) speichert Daten für die Druckausgabe.
4. Der VPSX/MFI printing solution is deployed on Amazon EC2 and its operational data is stored in Amazon Elastic Block Store (Amazon EBS). LRS VPSX/MFI uses the TCP/IP-based LRS/Queue LRS-Übertragungsagent sammelt Druckdaten über die JES Print Exit API von Rocket Software und überträgt die Daten an ein bestimmtes Druckziel.

> **Note**
>
> Die Ziellösung erfordert in der Regel keine Änderungen an der Anwendung, um Mainframe-Formatierungssprachen wie IBM Advanced Function Presentation (AFP) oder Xerox Line Condition Data Stream (LCDS) zu berücksichtigen. Weitere Informationen zur Verwendung von Rocket Software für die Migration und Modernisierung von Mainframe-Anwendungen auf AWS finden Sie im Blogbeitrag Empowering Enterprise Mainframe Workloads on AWS with Micro Focus.

AWS-Infrastrukturarchitektur

Das folgende Diagramm zeigt eine hochverfügbare und sichere AWS-Infrastrukturarchitektur für einen Mainframe-Batchdruck-Workload:

Das Diagramm zeigt den folgenden Workflow:

1. Der Batch-Scheduler initiiert den Batch-Prozess und wird auf Amazon EC2 in mehreren Availability Zones für hohe Verfügbarkeit (HA) bereitgestellt.

   > **Note**
   >
   > Dieses Muster deckt die Implementierung des Batch-Schedulers nicht ab. Weitere Informationen zur Implementierung finden Sie in der Dokumentation des Softwareanbieters für Ihren Scheduler.

2. Der Mainframe-Batchjob (geschrieben in einer Programmiersprache wie JCL oder COBOL) verwendet die Kerngeschäftslogik, um Druckausgaben wie Abrechnungen, Ausweise und

Kreditauszüge zu verarbeiten und zu generieren. Der Auftrag wird auf Amazon EC2 in zwei Availability Zones für HA bereitgestellt und verwendet Rocket Software Print Exit, um die Druckausgabe für den Endbenutzer an LRS VPSX/MFI weiterzuleiten.

3. LRS-Befehle. VPSX/MFI uses a TCP/IP-based LRS/Queue transmission agent to collect or capture print data from the Rocket Software JES Print Exit programming interface. Print Exit passes the necessary information to enable LRS VPSX/MFI to effectively process the spool file and dynamically build LRS/Queue Die Befehle werden dann mit einer integrierten Standardfunktion von Rocket Software ausgeführt.

> **Note**
>
> Weitere Informationen zu Druckdaten, die von Rocket Software Print Exit an LRS/Queue and LRS VPSX/MFI unterstützte Mainframe-Batchmechanismen übergeben werden, finden Sie unter Druckdatenerfassung im Abschnitt Zusätzliche Informationen dieses Musters.

4.
> **Note**
>
> Ein Network Load Balancer stellt einen DNS-Namen zur Integration von Rocket Enterprise Server in LRS bereit VPSX/MFI. : LRS VPSX/MFI supports a Layer 4 load balancer. The Network Load Balancer also does a basic health check on LRS VPSX/MFI und leitet den Datenverkehr an die registrierten Ziele weiter, die fehlerfrei sind.

5.
> **Note**
>
> Der LRS VPSX/MFI-Druckserver wird auf Amazon EC2 in zwei Availability Zones für HA bereitgestellt und verwendet Amazon EBS als Betriebsdatenspeicher. LRS VPSX/MFI supports both the active-active and active-passive service modes. This architecture uses multiple AZs in an active-passive pair as an active and hot standby. The Network Load Balancer performs a health check on LRS VPSX/MFI EC2 instances and routes traffic to hot standby instances in the other AZ if an active instance is in an unhealthy state. The print requests are persisted in the LRS Job Queue locally in each of the EC2 instances. In the event of recovery, a failed instance has to be restarted for the LRS services to resume processing the print request. : LRS VPSX/MFI kann auch Zustandsprüfungen auf Ebene der Druckerflotte durchführen. Weitere Informationen finden Sie unter Integritätsprüfungen der Druckerflotte im Abschnitt Zusätzliche Informationen dieses Musters.

6. AWS Managed Microsoft AD lässt sich in LRS/DIS integrieren, um die Authentifizierung und Autorisierung von Druckworkflows durchzuführen. Weitere Informationen finden Sie unter Druckauthentifizierung und Autorisierung im Abschnitt Zusätzliche Informationen dieses Musters.
7. LRS VPSX/MFI verwendet Amazon EBS für Blockspeicher. Sie können Amazon EBS-Daten von aktiven EC2 Instances als point-in-time Snapshots auf Amazon S3 sichern und sie auf Hot-Standby-EBS-Volumes wiederherstellen. Um die Erstellung, Aufbewahrung und Löschung von Amazon EBS-Volume-Snapshots zu automatisieren, können Sie Amazon Data Lifecycle Manager verwenden, um die Häufigkeit automatisierter Snapshots festzulegen und sie auf der Grundlage Ihrer RTO/RPO-Anforderungen wiederherzustellen.

Tools

AWS-Services

- Amazon Elastic Block Store (Amazon EBS) bietet Speichervolumen auf Blockebene zur Verwendung mit EC2 Instances. EBS-Volumes verhalten sich wie unformatierte Blockgeräte. Sie können diese Volumes als Geräte auf Ihren Instances mounten.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können Amazon verwenden EC2 , um so viele oder so wenige virtuelle Server zu starten, wie Sie benötigen, und Sie können nach oben oder unten skalieren.
- Amazon Relational Database Service (Amazon RDS) ist ein Webservice, der die Einrichtung, den Betrieb und die Skalierung einer relationalen Datenbank in der AWS-Cloud erleichtert. Er bietet kosteneffiziente, anpassbare Kapazität für eine relationale Datenbank und verwaltet allgemeine Datenbankverwaltungsaufgaben.
- AWS Directory Service for Microsoft Active Directory, auch bekannt als AWS Managed Microsoft AD, ermöglicht Ihren verzeichnissensitiven Workloads und AWS-Ressourcen die Nutzung von Microsoft Active Directory in der AWS-Cloud.

Andere Tools

- LRS VPSX/MFI (Micro Focus Interface), das von LRS und Rocket Software gemeinsam entwickelt wurde, erfasst die Ausgabe von einem Rocket Enterprise Server JES-Spool und leitet sie zuverlässig an ein bestimmtes Druckziel weiter.
- Der LRS Directory Information Server (LRS/DIS) wird für die Authentifizierung und Autorisierung während des Druckworkflows verwendet.

- TCP/IP-based LRS/Queue transmission agent is used by LRS VPSX/MFIum Druckdaten über die JES Print Exit-Programmierschnittstelle von Rocket Software zu sammeln oder zu erfassen.
- Rocket Enterprise Server ist eine Umgebung zur Anwendungsbereitstellung für Mainframe-Anwendungen. Sie bietet die Ausführungsumgebung für Mainframe-Anwendungen, die mithilfe einer beliebigen Version von Rocket Software Enterprise Developer migriert oder erstellt wurden.

Epen

Rocket Enterprise Server auf Amazon einrichten EC2 und eine Mainframe-Batch-Anwendung bereitstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Rocket Enterprise Server ein und stellen Sie eine Demo-Anwendung bereit.	Richten Sie Rocket Enterpris e Server auf Amazon EC2 ein und stellen Sie dann die BankDemo Demonstra tionsanwendung von Rocket Software auf Amazon bereit EC2. Die BankDemo Anwendung ist eine Mainframe-Batch-An wendung, die die Druckausg abe erstellt und dann initiiert.	Cloud-Architekt

Richten Sie einen LRS-Druckserver bei Amazon ein EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Besorgen Sie sich eine LRS-Produktlizenz zum Drucken.	Um eine LRS-Produktlizenz für LRS zu erhaltenVPSX/MFI, LRS/Queue, and LRS/DIS, wenden Sie sich an das LRS Output Management-Team. Sie müssen die Hostnamen	Bauen Sie einen Vorsprung auf

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der EC2 Instanzen angeben, auf denen die LRS-Produkte installiert werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Amazon EC2 Windows-Instance, um LRS VPSX/MFI zu installieren.	Starten Sie eine Amazon EC2 Windows-Instance, indem Sie den Anweisungen unter Starten einer EC2 Amazon-Instance in der EC2 Amazon-Dokumentation folgen. Ihre Instance muss die folgenden Hardware- und Softwareanforderungen für LRS VPSX/MFI erfüllen: • CPU — Doppelkern • RAM — 16 GB • Laufwerk — 500 GB • Minimale EC2 Instanz — m5.xlarge • Betriebssystem — Windows/Linux • Software — Interneti nformationsdienst (IIS) oder Apache **Note** Die oben genannten Hardware- und Softwareanforderungen sind für eine kleine Druckerflotte (etwa 500—1000) vorgesehen. Um die vollständigen Anforderungen zu	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	erfahren, wenden Sie sich an Ihre LRS- und AWS-Ansprechpartner. Gehen Sie beim Erstellen Ihrer Windows-Instance wie folgt vor: 1. Vergewissern Sie sich, dass der EC2 Hostname derselbe Hostname ist, der für die LRS-Produktlizenz verwendet wurde. 2. Aktivieren Sie CGI in Amazon, EC2 indem Sie wie folgt vorgehen: a. Connect zu Ihrer EC2 Instance her, indem Sie den Anweisungen von folgen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie LRS VPSX/MFI auf der Instanz. EC2	1. Connect zu Ihrer EC2 Instance her, indem Sie den Anweisungen unter Schritt 2: Connect zu Ihrer Instance herstellen in der EC2 Amazon-Dokumentation folgen. 2. **Note** Öffnen Sie in der LRS-E-Mail, die Sie erhalten sollten, den Link zur Produkt-Download-Seite. : LRS-Produkte werden per elektronischer Dateiübertragung (EFT) vertrieben. 3. Laden Sie LRS VPSX/MFI herunter und entpacken Sie die Datei (Standardordner:). `c:\LRS` 4. Starten Sie den LRS Product Installer aus dem entpackten Ordner, um LRS VPSX/MFI zu installieren. 5. Wählen Sie im Menü „Funktionen auswählen“ die Option VPSX® Server (V1R3.022) und klicken Sie dann auf Weiter, um den Installationsvorgang zu	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	starten. Sie erhalten eine Erfolgsmeldung, wenn die Installation abgeschlossen ist.	
Installieren Sie LRS/Queue.	1. Connect zu Ihrer Rocket Enterprise EC2 Server-Instance her, indem Sie den Anweisungen in Schritt 2: Connect zu Ihrer Instance herstellen in der EC2 Amazon-Dokumentation folgen. 2. Öffnen Sie in der LRS-E-Mail, die Sie erhalten sollten, den Link zur LRS-Produkt-Download-Seite, laden Sie LRS/Queue herunter und entpacken Sie dann die Datei. 3. Gehen Sie zu dem Verzeichnis, in das Sie die Dateien heruntergeladen haben, und starten Sie dann das LRS-Produktinstallationsprogramm, um LRS/Queue zu installieren.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie LRS/DIS.	1. Connect zu Ihrer LRS EC2 VPSX/MFI-Instance her, indem Sie den Anweisungen in Schritt 2: Connect zu Ihrer Instance herstellen in der Amazon-Dokumentation folgen. EC2 2. Öffnen Sie in der LRS-E-Mail, die Sie erhalten sollten, den Link zur LRS-Produkt-Download-Seite, laden Sie LRS/DIS herunter und entpacken Sie dann die Datei. 3. Gehen Sie zu dem Verzeichnis, in das Sie die Dateien heruntergeladen haben, und starten Sie dann das LRS-Produktinstallationsprogramm. 4. Erweitern Sie im LRS Product Installer die Option LRS Misc Tools, wählen Sie LRS DIS und dann Weiter aus. 5. Folgen Sie den restlichen Anweisungen im LRS-Produktinstallationsprogramm, um den Installationsvorgang abzuschließen.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Zielgruppe und registrieren Sie LRS EC2 VPSX/MFI als Ziel.	Erstellen Sie eine Zielgruppe, indem Sie den Anweisungen unter Erstellen Sie eine Zielgruppe für Ihren Network Load Balancer in der Elastic Load Balancing Balancing-Dokumentation folgen. Gehen Sie beim Erstellen der Zielgruppe wie folgt vor: 1. Wählen Sie auf der Seite Gruppendetails angeben für Wählen Sie einen Zieltyp die Option Instances aus. 2. Wählen Sie für Protokoll die Option TCP aus. 3. Wählen Sie für Port 5500 aus. 4. Wählen Sie auf der Seite Ziele registrieren im Abschnitt Verfügbare Instanzen die LRS EC2 VPSX/MFI-Instances aus.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Network Load Balancer.	Folgen Sie den Anweisungen unter Network Load Balancer erstellen in der Elastic Load Balancing Balancing-Dokumentation. Ihr Network Load Balancer leitet den Verkehr vom Rocket Enterpris e Server an LRS VPSX/MFI weiter. EC2 Wenn Sie den Network Load Balancer erstellen, gehen Sie auf der Seite Listener und Routing wie folgt vor: 1. Wählen Sie für Protocol TCP aus. 2. Wählen Sie für Port die Option 5500 aus. 3. Wählen Sie unter Standardaktion die Option Weiterleiten an für die Zielgruppe, die Sie zuvor erstellt haben.	Cloud-Architekt

Integrieren Sie Rocket Enterprise Server in LRS VPSX/MFI and LRS/Queue

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Rocket Enterprise Server für die LRS/ Queue-Integration.	1. Connect zu Ihrer Rocket Enterprise EC2 Server-In stance her, indem Sie den Anweisungen in Schritt 2: Connect zu Ihrer Instance	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	herstellen in der EC2 Amazon-Dokumentation folgen. 2. Öffnen Sie im Windows-Startmenü die Rocket Enterprise Server-Ad ministrationsoberfläche. 3. Wählen Sie in der Menüleist e NATIVE. 4. Wählen Sie im Navigatio nsbereich Directory Server und dann BANKDEMO aus. 5. Scrollen Sie im linken Navigationsbereich von Allgemein nach unten zum Abschnitt Erweitert , um die Umgebungs variablen (LRSQ_ADD RESS, LRSQ_PORT, LRSQ_COMMAND) so zu konfigurieren, dass sie auf LRSQ verweisen. 6. Geben Sie für LRSQ_ADDR ESS die IP-Adresse oder den DNS-Namen des Network Load Balancer ein, den Sie zuvor erstellt haben. 7. Geben Sie für LRSQ_PORT den VPSX LRSQ Listener Port (5500) ein. 8. Geben Sie für LRSQ_COMMAND den	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Pfad der ausführbaren LRSQ-Datei ein. **Note** LRS unterstützt derzeit eine maximale Zeichenbeschränkung von 50 für DNS-Namen, dies kann sich jedoch in future ändern. Wenn Ihr DNS-Name größer als 50 ist, können Sie alternativ die IP-Adresse des Network Load Balancer verwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Rocket Enterprise Server für die LRS VPSX/MFI-Integration.	1. Kopieren Sie den `VPSX_MFI_R2` Ordner aus dem LRS VPSX/MFI-Installationsprogramm in den Rocket Enterprise Server-Speicherort unter. `C\BANKDEMO\print` 2. Connect zu Ihrer Rocket Enterprise EC2 Server-Instance her, indem Sie den Anweisungen in Schritt 2: Connect zu Ihrer Instance herstellen in der EC2 Amazon-Dokumentation folgen. 3. Öffnen Sie im Windows-Startmenü die Rocket Enterprise Server-Administrationsoberfläche. 4. Wählen Sie in der Menüleiste NATIVE. 5. Wählen Sie im Navigationsbereich Directory Server und dann BANKDEMO aus. 6. Wählen Sie unter BANKDEMO die Option JES aus. 7. Fügen Sie unter **`DLL(VPSX_MFI_R2)`** JES-Programmpfad den Pfad vom `C\BANKDEMO\print` Speicherort hinzu.	Cloud-Architekt

Richten Sie Drucker und Druckbenutzer in Rocket Enterprise Server und LRS VPSX/MFI ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ordnen Sie das Rocket Software Print Exit-Modul dem Serverausführungsprozess des Rocket Enterprise Server-Batchdruckers zu.	1. Connect zu Ihrer Rocket Enterprise EC2 Server-Instance her, indem Sie den Anweisungen in Schritt 2: Connect zu Ihrer Instance herstellen in der EC2 Amazon-Dokumentation folgen. 2. Öffnen Sie im Windows-Startmenü die Rocket Enterprise Server-Administrationsoberfläche. 3. Wählen Sie in der Menüleiste NATIVE. 4. Wählen Sie im Navigationsbereich Directory Server und dann BANKDEMO aus. 5. Wählen Sie unter BANKDEMO die Option JES aus, und scrollen Sie nach unten zu Printers. 6. Ordnen Sie unter Drucker das Modul Rocket Software Print Exit (LRSPRTE6 für Batch) dem Rocket Enterprise Server-Batchdrucker Server Execution Process (SEP) zu. Dies ermöglicht die Weiterleitung der Druckausgabe an LRS VPSX/MFI.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Melden Sie sich auf der Benutzeroberfläche der Enterprise Server Administration an. Weitere Informationen zur Konfiguration finden Sie unter Using the Exit in der Micro Focus-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie einen Drucker in LRS VPSX/MFI hinzu.	1. Connect zu Ihrer LRS EC2 VPSX/MFI-Instance her, indem Sie den Anweisung en in Schritt 2: Connect zu Ihrer Instance herstellen in der Amazon-Dokumentation folgen. EC2 2. Öffnen Sie das VPSX-Webi nterface über das Windows-Startmenü. 3. Wählen Sie im Navigatio nsbereich Drucker aus. 4. Wählen Sie Hinzufügen und dann Drucker hinzufügen. 5. Geben Sie auf der Seite Druckerkonfiguration als Druckername Lokal ein. 6. Geben Sie für VPSX ID ein. VPS1 7. Wählen Sie für CommTypeTCPIP/LRSQ aus. 8. Geben Sie für Host/IP-Adresse die IP-Adresse des physischen Druckers ein, den Sie hinzufügen möchten. 9. Geben Sie unter Gerät den Namen Ihres Geräts ein. 10. Wählen Sie entweder Windows-Treiber oder Linux/Mac-Treiber.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	11. Wählen Sie Hinzufügen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Druckbenutzer in LRS VPSX/MFI.	1. Connect zu Ihrer LRS EC2 VPSX/MFI-Instance her, indem Sie den Anweisungen in Schritt 2: Connect zu Ihrer Instance herstellen in der Amazon-Dokumentation folgen. EC2 2. Öffnen Sie das VPSX-Webinterface über das Windows-Startmenü. 3. Wählen Sie im Navigationsbereich Sicherheit und dann Benutzer aus. 4. Wählen Sie in der Spalte Benutzername die Option admin und dann Kopieren aus. 5. Geben Sie im Fenster Benutzerprofilverwaltung für Benutzername einen Benutzernamen ein (z. B. PrintUser). 6. Geben Sie unter Beschreibung eine kurze Beschreibung ein (z. B. Benutzer für Testdruck). 7. Wählen Sie Aktualisieren. Dadurch wird ein Druckbenutzer erstellt (z. B. PrintUser). 8. Wählen Sie im Navigationsbereich unter Benutzer	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den neuen Benutzer aus, den Sie erstellt haben. 9. Wählen Sie im Befehlsmenü die Option Sicherheit aus. 10. Wählen Sie auf der Seite Sicherheitsregeln alle zutreffenden Optionen für Druckersicherheit und Jobsicherheit aus und klicken Sie dann auf Speichern. 11. Um Ihren neuen Druckbenutzer zur Administratorgruppe hinzuzufügen, wechseln Sie zum Navigationsbereich, wählen Sie Sicherheit und dann Konfigurieren aus. 12. Fügen Sie im Fenster Sicherheitskonfiguration Ihren neuen Druckbenutzer zur Administratorspalte hinzu.	

Richten Sie die Druckauthentifizierung und -autorisierung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine von AWS verwaltete Microsoft AD-Domain mit Benutzern und Gruppen.	1. Erstellen Sie ein Active Directory auf AWS Managed Microsoft AD, indem Sie den Anweisungen unter Erstellen Sie Ihr	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	AWS Managed Microsoft AD-Verzeichnis in der AWS Directory Service Service-Dokumentation folgen. 2. Stellen Sie eine EC2 Instance (Active Directory -Manager) bereit und installieren Sie Active Directory-Tools zur Verwaltung Ihres AWS Managed Microsoft AD. Folgen Sie dazu den Anweisungen in Schritt 3: Bereitstellen einer EC2 Instanz zur Verwaltung Ihres AWS Managed Microsoft AD in der AWS Directory Service Service-Dokumentation. 3. **Note** Connect zu Ihrer EC2 Instance her, indem Sie den Anweisungen unter Schritt 2: Connect zu Ihrer Instance herstellen in der EC2 Amazon-Dokumentation folgen. : Wenn Sie eine Verbindung mit der EC2 Instance herstellen, geben	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie Ihre Administr atoranmeldedaten (für das Verzeichn is, das Sie in Schritt 1 erstellt haben) in das Windows-S icherheitsfenster ein. 4. Wählen Sie im Windows-S tartmenü unter Windows-V erwaltungstools die Option Active Directory-Benutzer und -Computer aus. 5. Erstellen Sie einen Druckbenutzer in der Active Directory-Domäne, indem Sie die Schritte unter Benutzer erstellen in der Dokumentation zum AWS-Verzeichnisdienst befolgen.	
Verbinden Sie LRS VPSX/MFI mit einer von AWS EC2 verwalteten Microsoft AD-Domain.	Verbinden Sie LRS VPSX/MFI EC2 automatisch (AWS Knowledge Center-Do kumentation) oder manuell (AWS Directory Service-Dokumentation) mit Ihrer AWS Managed Microsoft AD-Domain.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren und integrieren Sie LRS/DIS mit AWS Managed Microsoft AD.	1. Connect zu Ihrer LRS EC2 VPSX/MFI-Instance her, indem Sie den Anweisungen in Schritt 2: Connect zu Ihrer Instance herstellen in der Amazon-Dokumentation folgen. EC2 2. Öffnen Sie im Windows-Startmenü das VPSX-Webinterface. 3. Wählen Sie im Navigationsbereich Sicherheit und dann Konfigurieren aus. 4. Wählen Sie auf der Seite Sicherheitskonfiguration im Abschnitt Sicherheitsparameter für Sicherheitstyp die Option Intern aus. 5. Geben Sie Ihre Einstellungen für die restlichen Optionen im Abschnitt Sicherheitsparameter ein. 6. Öffnen Sie den Ordner LRS Output Management im Microsoft Windows-Startmenü, wählen Sie Serverstart und dann Serverstopp aus. 7. Melden Sie sich mit Ihrem Active Directory-Benutzernamen und -Passwort bei LRS VPSX/MFI an.	Cloud-Architekt

Testen Sie einen Druck-Workflow

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initiieren Sie eine Batch-Druckanfrage über die Rocket BankDemo Software-App.	1. Öffnen Sie den 3270-Terminal-Emulator in Ihrer Rocket Enterprise EC2 Server-Instanz. 2. Connect zur BankDemo App her, indem Sie den folgenden Befehl ausführen: `connect 127.0.0.1:9278` 3. Geben Sie in der BankDemo Befehlszeilenschnittstelle B0001 als Benutzer-ID ein. Geben Sie als Passwort einen Schlüssel ein, der nicht leer ist. 4. Geben Sie für die Option Gedruckte Kontoauszüge anfordern in die leere Zeile X ein. 5. Geben Sie im Abschnitt Kontoauszug senden für E-Mail den Wert Y ein, und drücken Sie dann F10.	Testingenieur
Überprüfen Sie die Druckausgabe in LRS VPSX/MFI.	1. Connect zu Ihrer LRS EC2 VPSX/MFI-Instance her, indem Sie den Anweisungen in Schritt 2: Connect zu Ihrer Instance herstellen in der Amazon-Dokumentation folgen. EC2	Testingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Öffnen Sie im Windows-Startmenü das VPSX-Webinterface. 3. Wählen Sie im Navigationsbereich Drucker und dann Ausgabewarteschlange aus. 4. Wählen Sie in der Spalte Spool-ID die Spool-ID für den Auftrag in der Druckerwarteschlange aus. 5. Wählen Sie auf der Registerkarte Aktionen in der Spalte COMMAND die Option Durchsuchen aus. Sie können jetzt die Druckausgabe eines Kontoauszugs mit Spalten für die Kontonummer sehen. , Beschreibung, Datum, Betrag und Saldo. Ein Beispiel finden Sie im Anhang batch_print_output für dieses Muster.	

Zugehörige Ressourcen

- Modernisierung der LRS-Leistung (LRS-Dokumentation)
- ANSI und Maschinenwagensteuerungen (IBM-Dokumentation)
- Kanalbefehle (IBM-Dokumentation)
- Unterstützung von Mainframe-Workloads für Unternehmen auf AWS mit Micro Focus (AWS-Partnernetzwerk-Blog)

- Erstellen Sie ein Micro Focus Enterprise Server PAC mit Amazon EC2 Auto Scaling und Systems Manager (Dokumentation zu AWS Prescriptive Guidance)
- AFP-Datenstream (Advanced Function Presentation) (IBM-Dokumentation)
- Line Conditioned Data Stream (LCDS) (Compart-Dokumentation)

Zusätzliche Informationen

Überlegungen

Während Ihrer Modernisierung können Sie eine Vielzahl von Konfigurationen sowohl für Mainframe-Batch-Prozesse als auch für die damit generierte Leistung in Betracht ziehen. Die Mainframe-Plattform wurde von allen Kunden und Anbietern, die sie verwenden, an spezielle Anforderungen angepasst, die sich direkt auf den Druck auswirken. Beispielsweise kann Ihre aktuelle Plattform IBM Advanced Function Presentation (AFP) oder den Xerox Line Condition Data Stream (LCDS) in den aktuellen Arbeitsablauf integrieren. Darüber hinaus können Mainframe-Wagen-Steuerzeichen und Kanalbefehle das Aussehen der gedruckten Seite beeinflussen und erfordern möglicherweise eine besondere Behandlung. Im Rahmen der Planung der Modernisierung empfehlen wir Ihnen, die Konfigurationen in Ihrer spezifischen Druckumgebung zu bewerten und zu verstehen.

Erfassung von Druckdaten

Rocket Software Print Exit leitet die erforderlichen Informationen weiter, damit LRS VPSX/MFI die Spool-Datei effektiv verarbeiten kann. Die Informationen bestehen aus Feldern, die in den entsprechenden Steuerblöcken übergeben werden, wie z. B.:

- NAME DES AUFTRAGS
- BESITZER (BENUTZER-ID)
- ZIEL
- BILDEN
- DATEINAME
- SCHRIFTSTELLER

LRS VPSX/MFI unterstützt die folgenden Mainframe-Batch-Mechanismen zur Erfassung von Daten von Rocket Enterprise Server.

- BATCH-COBOL-Anweisungen print/spool processing using standard z/OS JCL SYSOUT DD/OUTPUT

- print/spool processing using standard z/OSBATCH-COBOL-JCL-CA-SPOOL-SUBSYS-DD-Anweisungen
- IMS/COBOL print/spoolVerarbeitung mithilfe der CBLTDLI-Schnittstelle (Eine vollständige Liste der unterstützten Methoden und Programmierbeispiele finden Sie in der LRS-Dokumentation, die in Ihrer Produktlizenz enthalten ist.)

Zustandsprüfungen der Druckerflotte

LRS VPSX/MFI (LRS LoadX) kann tiefgreifende Zustandsprüfungen durchführen, einschließlich Geräteverwaltung und Betriebsoptimierung. Die Geräteverwaltung kann Fehler in einem Druckergerät erkennen und die Druckanforderung an einen fehlerfreien Drucker weiterleiten. Weitere Informationen zu umfassenden Integritätsprüfungen für Druckerflotten finden Sie in der LRS-Dokumentation, die in Ihrer Produktlizenz enthalten ist.

Authentifizierung und Autorisierung drucken

LRS/DIS enables LRS applications to authenticate user IDs and passwords by using Microsoft Active Directory or an LDAP server. In addition to basic print authorization, LRS/DISkann in den folgenden Anwendungsfällen auch detaillierte Drucksicherheitskontrollen anwenden:

- Steuert, wer den Druckerauftrag durchsuchen kann.
- Verwaltet die Navigationsebene der Aufträge anderer Benutzer.
- Operative Aufgaben verwalten. Zum Beispiel Sicherheitsfunktionen auf Befehlsebene wie „Sperren/Freigeben“, „Löschen“, „Ändern“, „Kopieren“ und „Umleiten“. Die Sicherheit kann entweder anhand der Benutzer-ID oder der Gruppe (ähnlich der AD-Gruppe oder der LDAP-Gruppe) eingerichtet werden.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Mainframe-Modernisierung: DevOps Weiter AWS mit Rocket Software Enterprise Suite

Erstellt von Kevin Yung (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Herausforderungen für Kunden

Organizations, die Kernanwendungen auf Mainframe-Hardware ausführen, stehen in der Regel vor einigen Herausforderungen, wenn die Hardware skaliert werden muss, um den Anforderungen digitaler Innovationen gerecht zu werden. Zu diesen Herausforderungen gehören die folgenden Einschränkungen.

- Mainframe-Entwicklungs- und Testumgebungen können aufgrund der geringen Flexibilität der Mainframe-Hardwarekomponenten und der hohen Änderungskosten nicht skaliert werden.
- In der Mainframe-Entwicklung mangelt es an Fachkräften, weil neue Entwickler sich mit den herkömmlichen Mainframe-Entwicklungstools nicht auskennen und auch nicht daran interessiert sind. Moderne Technologien wie Container, integration/continuous delivery (CI/CD (kontinuierliche) Pipelines und moderne Test-Frameworks sind in der Mainframe-Entwicklung nicht verfügbar.

Musterergebnisse

Um diesen Herausforderungen zu begegnen, haben Amazon Web Services (AWS) und Rocket Software Micro Focus, ein AWS Partner Network (APN) -Partner, zusammengearbeitet, um dieses Muster zu entwickeln. Die Lösung wurde entwickelt, um Sie dabei zu unterstützen, die folgenden Ergebnisse zu erzielen.

- Verbesserte Entwicklerproduktivität. Entwicklern können innerhalb von Minuten neue Mainframe-Entwicklungsinstanzen zur Verfügung gestellt werden.
- Verwendung von AWS Cloud zur Erstellung neuer Mainframe-Testumgebungen mit praktisch unbegrenzter Kapazität.
- Schnelle Bereitstellung einer neuen Mainframe-CI/CD-Infrastruktur. Die Bereitstellung auf AWS kann innerhalb einer Stunde mithilfe von und abgeschlossen werden. AWS CloudFormation AWS Systems Manager

- Nativer Einsatz von AWS DevOps Tools für die Mainframe-Entwicklung, einschließlich AWS CodeBuild, AWS CodeCommit, AWS CodePipeline AWS CodeDeploy, und Amazon Elastic Container Registry (Amazon ECR).
- Verwandeln Sie die traditionelle Wasserfallentwicklung in eine agile Entwicklung in Mainframe-Projekten.

Zusammenfassung der Technologien

In diesem Muster enthält der Zielstapel die folgenden Komponenten.

Logische Komponenten	Implementierungslösungen	Beschreibung
Quellcode-Repositorien	AccuRev Rocket-Softwareserver CodeCommit, Amazon ECR	Quellcodeverwaltung — Die Lösung verwendet zwei Arten von Quellcode: • Mainframe-Quellcode, zum Beispiel COBOL und JCL. • AWS Infrastrukturvorlagen und Automatisierungsskripte Beide Arten von Quellcode benötigen eine Versionskontrolle, werden aber unterschiedlich verwaltet SCMs. Quellcode, der auf Mainframe - oder Rocket Software Enterprise Servern bereitgestellt wird, wird auf Rocket Software Micro Focus AccuRev Server verwaltet. AWS Vorlagen und Automatisierungsskripte werden in CodeCommit verwaltet. Amazon ECR wird für die

		Docker-Image-Repositorys verwendet.
Instanzen für Unternehmensentwickler	Amazon Elastic Compute Cloud (Amazon EC2), Unternehmensentwickler von Rocket Software für Eclipse	Mainframe-Entwickler können mithilfe EC2 von Rocket Software Enterprise Developer for Eclipse Code in Amazon entwickeln. Dadurch müssen Sie sich nicht mehr auf Mainframe-Hardware verlassen, um Code zu schreiben und zu testen.
Lizenzverwaltung für die Rocket Software Enterprise Suite	License Manager für Rocket Software Enterprise Suite	Für die zentrale Lizenzverwaltung und Steuerung der Rocket Software Enterprise Suite verwendet die Lösung den Rocket Software Enterprise Suite License Manager, um die erforderliche Lizenz zu hosten.
CI/CD-Pipelines	CodePipeline, CodeBuild CodeDeploy, Rocket Software Enterprise Developer in einem Container, Rocket Software Enterprise Testserver in einem Container, Rocket Software Micro Focus Enterprise Server	Mainframe-Entwicklungsteams benötigen CI/CD-Pipelines, um Codekompilierung, Integrationstests und Regressionstests durchzuführen. In AWS CodePipeline und CodeBuild können nativ mit Rocket Software Enterprise Developer und Enterprise Test Server in einem Container arbeiten.

Voraussetzungen und Einschränkungen

Voraussetzungen

Name	Beschreibung
py3270	py3270 ist eine Python-Schnittstelle zu x3270, einem IBM 3270-Terminalemulator. Sie stellt eine API für einen x3270- oder s3270-Sub prozess bereit.
x3270	x3270 ist ein IBM 3270-Terminalemulator für das X Window System und Windows. Dies kann vom Entwickler für lokale Komponent entests verwendet werden.
Robot-Framework-Mainframe-3270-Bibliothek	Mainframe3270 ist eine Bibliothek für Robot Framework, die auf dem Projekt py3270 basiert.
Rocket Software Verastream	Rocket Software Verastream ist eine Integrati onsplattform, die das Testen von Mainframe-Assets auf die Art und Weise ermöglicht, wie mobile Apps, Webanwendungen und SOA-Webdienste getestet werden.
Installation und Lizenz für Rocket Software Unified Functional Testing (UFT)	Rocket Software Unified Functional Testing ist eine Software, die die Automatisierung von Funktions- und Regressionstests für Softwarea nwendungen und -umgebungen ermöglicht.
Installation und Lizenz für Rocket Software Enterprise Server	Enterprise Server bietet die Laufzeitumgebung für Mainframe-Anwendungen.
Installation und Lizenz für den Rocket Software Enterprise Test Server	Rocket Software Enterprise Test Server ist eine IBM Mainframe-Anwendungstestumgebung.
Rocket AccuRev Software-Installationsprogr amm und -Lizenz für Server und Rocket Software Micro AccuRev Focus-Installation sprogramm und -Lizenz für Windows- und Linux-Betriebssysteme	AccuRev bietet Quellcodeverwaltung (SCM). Das AccuRev System ist für die Verwendung durch ein Team von Personen konzipiert, die eine Reihe von Dateien entwickeln.

Installationsprogramm, Patch und Lizenz für Rocket Software Enterprise Developer für Eclipse	Enterprise Developer bietet Mainframe-Entwickl ern eine Plattform für die Entwicklung und Wartung der wichtigsten Mainframe-Online- und Batch-Anwendungen.

Einschränkungen

- Das Erstellen eines Windows Docker-Images wird in nicht unterstützt. CodeBuild Dieses gemeldete Problem benötigt Unterstützung von Windows Kernel/HCS- und Docker-Teams. Die Problemumgehung besteht darin, mithilfe von Systems Manager ein Docker-Image-Build-Runbook zu erstellen. Dieses Muster verwendet die Problemumgehung, um Container-Images für Rocket Software Enterprise Developer for Eclipse und Rocket Software Micro Focus Enterprise Test Server zu erstellen.
- Die Virtual Private Cloud (VPC) -Konnektivität von CodeBuild wird in Windows noch nicht unterstützt, daher verwendet das Pattern nicht den Rocket Software License Manager, um Lizenzen in OpenText Rocket Software Enterprise Developer- und Rocket Software Enterprise Test Server-Containern zu verwalten.

Produktversionen

- Rocket Software Enterprise Developer 5.5 oder höher
- Rocket Software Enterprise Test Server 5.5 oder höher
- Rocket Software Enterprise Server 5.5 oder höher
- Rocket Software AccuRev 7.x oder höher
- Windows Docker-Basisimage für Rocket Software Enterprise Developer und Enterprise Test Server: microsoft/dotnet-framework-4.7.2-runtime
- Linux-Docker-Basisimage für AccuRev den Client: amazonlinux:2

Architektur

Mainframe-Umgebung

Bei der konventionellen Mainframe-Entwicklung müssen die Entwickler Mainframe-Hardware verwenden, um Programme zu entwickeln und zu testen. Sie sind mit Kapazitätsbeschränkungen konfrontiert, z. B. mit eingeschränkten Millionen Anweisungen pro Sekunde (MIPS) für die

Entwicklungs-/Testumgebung, und sie müssen sich auf die Tools verlassen, die auf den Mainframe-Computern verfügbar sind.

In vielen Unternehmen folgt die Mainframe-Entwicklung der Methode der Wasserfallentwicklung, wobei sich die Teams bei der Veröffentlichung von Änderungen auf lange Zyklen verlassen. Diese Release-Zyklen sind in der Regel länger als die Entwicklung digitaler Produkte.

Das folgende Diagramm zeigt mehrere Mainframe-Projekte, bei deren Entwicklung Mainframe-Hardware gemeinsam genutzt wird. Bei Mainframe-Hardware ist es teuer, eine Entwicklungs- und Testumgebung für mehr Projekte zu skalieren.

AWS-Architektur

Dieses Muster erweitert die Mainframe-Entwicklung auf die. AWS Cloud Zunächst verwendet es AccuRev SCM, um den Mainframe-Quellcode zu hosten. AWS Anschließend stehen Enterprise Developer und Enterprise Test Server für die Erstellung und das Testen des Mainframe-Codes zur Verfügung. AWS

In den folgenden Abschnitten werden die drei Hauptkomponenten des Musters beschrieben.

1. SCM

In wird das Muster verwendet AWS, AccuRev um eine Reihe von SCM-Workspaces und Versionskontrolle für den Mainframe-Quellcode zu erstellen. Seine stream-basierte Architektur ermöglicht die parallel Mainframe-Entwicklung für mehrere Teams. AccuRev Verwendet das Promote-Konzept, um eine Änderung zusammenzuführen. Um diese Änderung zu anderen Arbeitsbereichen hinzuzufügen, AccuRev wird das Aktualisierungskonzept verwendet.

Auf Projektebene kann jedes Team einen oder mehrere Streams erstellen, AccuRev um Änderungen auf Projektebene nachzuverfolgen. Diese werden als Projekt-Streams bezeichnet. Diese Projekt-Streams werden von demselben übergeordneten Stream übernommen. Der übergeordnete Stream wird verwendet, um die Änderungen aus verschiedenen Projekt-Streams zusammenzuführen.

In jeden Projekt-Stream kann Code hochgestuft werden AccuRev, und es wird ein Trigger zum Heraufstufen nach der Veröffentlichung eingerichtet, um die AWS CI/CD-Pipeline zu initiieren. Der erfolgreiche Build für eine Änderung des Projekt-Streams kann für weitere Regressionstests in seinen übergeordneten Stream hochgestuft werden.

Normalerweise wird der übergeordnete Stream als Systemintegrationsstream bezeichnet. Bei einer Heraufstufung von einem Projekt-Stream zu einem Systemintegrationsstream initiiert ein Trigger nach der Heraufstufung eine weitere CI/CD-Pipeline zur Ausführung von Regressionstests.

Dieses Muster umfasst neben Mainframe-Code auch AWS CloudFormation Vorlagen, Systems Manager Automation-Dokumente und Skripts. Gemäß den infrastructure-as-code bewährten Methoden sind sie versionskontrolliert. CodeCommit

Wenn Sie Mainframe-Code für die Bereitstellung wieder mit einer Mainframe-Umgebung synchronisieren müssen, bietet Rocket Software die Enterprise Sync-Lösung, die Code vom SCM zurück zum AccuRev Mainframe-SCM synchronisiert.

2. Entwickler- und Testumgebungen

In einer großen Organisation ist die Skalierung von mehr als hundert oder sogar mehr als tausend Mainframe-Entwicklern eine Herausforderung. Um diese Einschränkung zu umgehen, verwendet das Muster Amazon EC2 Windows-Instances für die Entwicklung. Auf den Instances sind die Tools von Enterprise Developer for Eclipse installiert. Der Entwickler kann alle Mainframe-Codetests und das Debugging lokal auf der Instanz durchführen.

AWS Systems Manager State Manager- und Automation-Dokumente werden verwendet, um die Bereitstellung von Entwicklerinstanzen zu automatisieren. Die durchschnittliche Zeit für die Erstellung einer Entwicklerinstanz beträgt 15 Minuten. Die folgende Software und Konfigurationen sind vorbereitet:

- AccuRev Windows-Client zum Auschecken und Einspielen von Quellcode AccuRev
- Enterprise Developers for Eclipse Tool zum lokalen Schreiben, Testen und Debuggen von Mainframe-Code
- Open-Source-Testframeworks Python-Testframework Behavior-driven Development (BDD) Behavior, py3270 und der x3270-Emulator zum Erstellen von Skripten zum Testen von Anwendungen
- Ein Docker-Entwicklertool zum Erstellen des Enterprise Test Server-Docker-Images und zum Testen der Anwendung im Enterprise Test Server Docker-Container

Im Entwicklungszyklus verwenden Entwickler die EC2 Instanz, um Mainframe-Code lokal zu entwickeln und zu testen. Wenn die lokalen Änderungen erfolgreich getestet wurden, übertragen die Entwickler die Änderung auf dem AccuRev Server.

3. CI/CD-Rohrleitungen

In diesem Muster werden CI/CD-Pipelines für Integrationstests und Regressionstests vor der Bereitstellung in der Produktionsumgebung verwendet.

Wie im Abschnitt SCM erklärt, werden zwei Arten von Streams AccuRev verwendet: ein Projekt-Stream und ein Integrationsstream. Jeder Stream ist mit CI/CD-Pipelines verbunden. Um die Integration zwischen dem AccuRev Server und durchzuführen, verwendet das Pattern ein AccuRev Post-Promotion-Skript AWS CodePipeline, um ein Ereignis zur Initiierung von CI/CD zu erstellen.

Wenn ein Entwickler beispielsweise eine Änderung an einem Projekt-Stream heraufstuft, initiiert er ein Post-Promotion-Skript AccuRev, das auf dem Server ausgeführt wird. AccuRev Anschließend lädt das Skript die Metadaten der Änderung in einen Amazon Simple Storage Service (Amazon S3) - Bucket hoch, um ein Amazon S3-Ereignis zu erstellen. Dieses Ereignis initiiert die Ausführung einer CodePipeline konfigurierten Pipeline.

Derselbe Mechanismus zur Auslösung von Ereignissen wird für den Integrationsstream und die zugehörigen Pipelines verwendet.

Wird in der CI/CD-Pipeline CodeBuild zusammen mit dem AccuRev Linux-Client-Container CodePipeline verwendet, um den neuesten Code aus den Streams auszuchecken. AccuRev Dann beginnt die Pipeline, den Enterprise Developer Windows-Container CodeBuild zu verwenden, um den Quellcode zu kompilieren und den Enterprise Test Server Windows-Container zum Testen von CodeBuild Mainframe-Anwendungen zu verwenden.

Die CI/CD pipelines are built using CloudFormation templates, and the blueprint will be used for new projects. By using the templates, it takes less than an hour for a project to create a new CI/CD Pipeline in AWS.

Um Ihre Mainframe-Testkapazitäten zu skalieren AWS, besteht das Pattern aus der Rocket DevOps Software-Testsuite, Verastream und dem UFT-Server. Mithilfe der modernen DevOps Tools können Sie so viele Tests ausführen, wie Sie benötigen. AWS

Ein Beispiel für eine Mainframe-Entwicklungsumgebung mit aktivierter Rocket Software AWS ist in der folgenden Abbildung dargestellt.

Zieltechnologie-Stack

Dieser Abschnitt bietet einen genaueren Blick auf die Architektur der einzelnen Komponenten im Muster.

1. Quellcode-Repository — AccuRev SCM

AccuRev SCM ist für die Verwaltung von Mainframe-Quellcodeversionen eingerichtet. AccuRev Unterstützt für hohe Verfügbarkeit den Primär- und Replikatmodus. Betreiber können bei Wartungsarbeiten am Primärknoten einen Failover auf das Replikat durchführen.

Um die Reaktion der CI/CD-Pipeline zu beschleunigen, verwendet das Pattern Amazon CloudWatch Events, um Änderungen am Quellcode zu erkennen und den Start der Pipeline zu initiieren.

1. Die Pipeline ist für die Verwendung einer Amazon S3 S3-Quelle eingerichtet.
2. Eine CloudWatch Ereignisregel wird eingerichtet, um S3-Ereignisse aus einem S3-Quell-Bucket zu erfassen.
3. Die CloudWatch Ereignisregel legt ein Ziel für die Pipeline fest.
4. AccuRev SCM ist so konfiguriert, dass nach Abschluss der Heraufstufung ein Skript nach der Heraufstufung lokal ausgeführt wird.
5. AccuRev SCM generiert eine XML-Datei, die die Metadaten der Promotion enthält, und das Skript lädt die XML-Datei in den S3-Quell-Bucket hoch.
6. Nach dem Upload sendet der Quell-S3-Bucket Ereignisse, die der CloudWatch Ereignisregel entsprechen, und die CloudWatch Ereignisregel initiiert die Ausführung der Pipeline.

Wenn die Pipeline ausgeführt wird, startet sie ein CodeBuild Projekt, bei dem mithilfe eines AccuRev Linux-Client-Containers der neueste Mainframe-Code aus einem zugehörigen Stream ausgecheckt wird. AccuRev

Das folgende Diagramm zeigt ein AccuRev Server-Setup.

2. Vorlage für Unternehmensentwickler

Das Muster verwendet EC2 Amazon-Vorlagen, um die Erstellung der Entwicklerinstanz zu vereinfachen. Mithilfe von State Manager können Software- und Lizenzeinstellungen konsistent auf EC2 Instances angewendet werden.

Die EC2 Amazon-Vorlage integriert ihre VPC-Kontexteinstellungen und die Standard-Instance-Einstellungen und entspricht den Enterprise-Tagging-Anforderungen. Mithilfe einer Vorlage kann ein Team seine eigenen neuen Entwicklungsinstanzen erstellen.

Wenn eine Entwicklerinstanz durch Zuordnung zu Tags gestartet wird, verwendet Systems Manager State Manager, um die Automatisierung anzuwenden. Die Automatisierung umfasst die folgenden allgemeinen Schritte.

1. Installieren Sie die Enterprise Developer-Software und installieren Sie Patches.
2. Installieren Sie den AccuRev Client für Windows.
3. Installieren Sie das vorkonfigurierte Skript, damit Entwickler dem AccuRev Stream beitreten können. Initialisieren Sie Eclipse-Arbeitsbereiche.
4. Installieren Sie Entwicklungstools, einschließlich x3270, py3270 und Docker.
5. Konfigurieren Sie die Lizenzeinstellungen so, dass sie auf einen License Manager Manager-Load Balancer verweisen.

Das folgende Diagramm zeigt eine Enterprise Developer-Instance, die mit der EC2 Amazon-Vorlage erstellt wurde, wobei Software und Konfiguration von State Manager auf die Instance angewendet wurden. Enterprise-Developer-Instances stellen eine Verbindung AWS License Manager zu her, um ihre Lizenz zu aktivieren.

3. CI/CD-Rohrleitungen

Wie im Abschnitt AWS Architektur erklärt, gibt es in dem Muster CI/CD pipelines and system integration pipelines. Each mainframe project team creates a pipeline or multiple CI/CD pipelines for building the programs that they are developing in a project. These project CI/CD Pipelines auf Projektebene, die Quellcode aus einem zugehörigen Stream auschecken. AccuRev

In einem Projektteam bewerben Entwickler ihren Code im zugehörigen Stream. AccuRev Anschließend leitet die Beförderung die Projektpipeline ein, um den Code zu erstellen und Integrationstests durchzuführen.

Jede Projekt-CI/CD-Pipeline verwendet CodeBuild Projekte mit dem Enterprise Developer-Tool Amazon ECR Image und dem Enterprise Test Server-Tool Amazon ECR Image.

CodePipeline und CodeBuild werden zur Erstellung der CI/CD-Pipelines verwendet. Denn CodeBuild ohne Vorabgebühren oder Verpflichtungen zahlen Sie nur für das, was Sie tatsächlich nutzen. CodePipeline Im Vergleich zu Mainframe-Hardware reduziert die AWS Lösung die Vorlaufzeit für die Hardwarebereitstellung erheblich und senkt die Kosten Ihrer Testumgebung.

In der modernen Entwicklung werden mehrere Testmethoden verwendet. Zum Beispiel testgetriebene Entwicklung (TDD), BDD und Robot Framework. Mit diesem Muster können Entwickler diese modernen Tools für Mainframe-Tests verwenden. Mithilfe von x3270, py3270 und dem Python-Testtool Behave können Sie beispielsweise das Verhalten einer Online-Anwendung definieren. In diesen CI/CD-Pipelines können Sie auch das Build-Mainframe-Roboter-Framework 3270 verwenden.

Das folgende Diagramm zeigt die CI/CD-Pipeline für den Teamstream.

Das folgende Diagramm zeigt den CI/CD-Testbericht des Projekts, der CodePipeline im Mainframe3270 Robot Framework erstellt wurde.

Das folgende Diagramm zeigt den CI/CD-Testbericht des Projekts, der von in Py3270 und Behave BDD erstellt wurde. CodePipeline

Nachdem die Tests auf Projektebene erfolgreich bestanden wurden, wird der getestete Code manuell in den Integrationsstream in SCM hochgestuft. AccuRev Sie können diesen Schritt automatisieren, wenn sich die Teams darauf verlassen können, dass die Tests in ihrer Projektpipeline durchgeführt werden.

Wenn der Code beworben wird, checkt die CI/CD-Pipeline für die Systemintegration den zusammengeführten Code aus und führt Regressionstests durch. Der zusammengeführte Code wird aus allen parallel Projektstreams beworben.

Je nachdem, wie detailliert die Testumgebung sein muss, können Kunden mehr CI/CD-Pipelines für die Systemintegration in einer anderen Umgebung verwenden, z. B. UAT oder Pre-Production.

In dem Muster sind die in der Systemintegrationspipeline verwendeten Tools Enterprise Test Server, UFT Server und Verastream. All diese Tools können im Docker-Container bereitgestellt und mit verwendet werden. CodeBuild

Nach erfolgreichem Testen der Mainframe-Programme wird das Artefakt mit Versionskontrolle in einem S3-Bucket gespeichert.

Das folgende Diagramm zeigt eine CI/CD-Pipeline zur Systemintegration.

Nachdem das Artefakt erfolgreich in den CI/CD-Pipelines für die Systemintegration getestet wurde, kann es für den Produktionseinsatz freigegeben werden.

Wenn Sie Quellcode wieder auf dem Mainframe bereitstellen müssen, bietet Rocket Software die Enterprise Sync-Lösung an, mit der Sie den Quellcode von AccuRev hinten auf Mainframe Endeavour synchronisieren können.

Das folgende Diagramm zeigt eine CI/CD-Pipeline für die Produktion, bei der das Artefakt auf Unternehmensservern bereitgestellt wird. CodeDeploy Orchestriert in diesem Beispiel die Bereitstellung des getesteten Mainframe-Artefakts auf Enterprise Server.

Zusätzlich zur Architektur-Komplettlösung der CI/CD-Pipeline finden Sie im AWS DevOps Blogbeitrag Automatisieren von Tausenden von Mainframe-Tests AWS mit der Micro Focus Enterprise Suite weitere Informationen zum Testen von Mainframe-Anwendungen in und. CodeBuild CodePipeline (Micro Focus ist jetzt Rocket Software.) Im Blogbeitrag finden Sie bewährte Methoden und Einzelheiten zur Durchführung von Mainframe-Tests auf AWS.

Tools

AWS Tools für die Automatisierung

- AWS CloudFormation
- CloudWatch Amazon-Veranstaltungen
- AWS CodeBuild
- AWS CodeDeploy
- AWS CodePipeline
- Amazon ECR
- Amazon S3
- AWS Secrets Manager
- AWS Systems Manager

Softwaretools von Rocket

- Rocket Enterprise-Entwickler für Eclipse
- Rocket Enterprise-Testserver
- Rocket Enterprise Server (Produktionsbereitstellung)

- Rocket Software AccuRev
- License Manager für Rocket Software Enterprise Suite
- Rocket Software Verastream Hostintegrator
- Rocket Software UFT Eins

Andere Tools

- x3270
- py3270
- Robot-Framework-Mainframe-3270-Bibliothek

Epen

Erstellen Sie die AccuRev SCM-Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie einen primären AccuRev SCM-Server bereit, indem Sie CloudFormation		AWS CloudFormation
Erstellen Sie den AccuRev Administratorbenutzer.	Melden Sie sich bei AccuRev SCM Server an und führen Sie den CLI-Befehl aus, um einen Administratorbenutzer zu erstellen.	AccuRev SCM-Serveradministrator
AccuRev Streams erstellen.	Erstellen Sie AccuRev Streams, die nacheinander von den oberen Streams erben: Produktion, Systemintegration, Team-Streams.	AccuRev SCM-Administrator
Erstellen Sie die AccuRev Entwickler-Anmeldekonten.	Verwenden Sie AccuRev SCM-CLI-Befehle, um AccuRev Benutzera	AccuRev SCM-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	nmeldekonten für Mainframe-Entwickler zu erstellen.	

Erstellen Sie die Amazon EC2 Launch-Vorlage für Enterprise Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die EC2 Amazon-Startvorlage bereit, indem Sie CloudFormation	Wird verwendet CloudFormation , um eine EC2 Amazon-Startvorlage für Enterprise Developer-Instances bereitzustellen. Die Vorlage enthält ein Systems Manager Automation-Dokument für die Rocket Enterprise Developer-Instanz.	AWS CloudFormation
Erstellen Sie die Enterprise Developer-Instance aus der EC2 Amazon-Vorlage.		AWS-Konsolenanmeldung und Kenntnisse als Mainframe-Entwickler

Erstellen Sie das Docker-Image für das Enterprise Developer-Tool

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Docker-Image des Enterprise Developer-Tools.	Verwenden Sie den Docker-Befehl und das Enterprise Developer-Tool Dockerfile, um das Docker-Image zu erstellen .	Docker
Erstellen Sie das Docker-Repository in Amazon ECR.	Erstellen Sie auf der Amazon ECR-Konsole das Repository für das Enterprise Developer Docker-Image.	Amazon ECR

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Übertragen Sie das Docker-Image des Enterprise Developer-Tools auf Amazon ECR.	Führen Sie den Befehl Docker push aus, um das Docker-Image des Enterprise Developer-Tools zu pushen und es im Docker-Repository in Amazon ECR zu speichern.	Docker

Erstellen Sie das Docker-Image für den Enterprise Test Server

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Docker-Image für den Enterprise Test Server.	Verwenden Sie den Docker-Befehl und das Enterprise Test Server Dockerfile, um das Docker-Image zu erstellen.	Docker
Erstellen Sie das Docker-Repository in Amazon ECR.	Erstellen Sie auf der Amazon ECR-Konsole das Amazon ECR-Repository für das Enterprise Test Server Docker-Image.	Amazon ECR
Senden Sie das Enterprise Test Server Docker-Image an Amazon ECR.	Führen Sie den Befehl Docker push aus, um das Enterprise Test Server-Docker-Image in Amazon ECR zu pushen und zu speichern.	Docker

Erstellen Sie die CI/CD-Pipeline für den Teamstream

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das CodeCommit Repository.	Erstellen Sie auf der CodeCommit Konsole ein Git-basiertes Repository für Infrastruktur und CloudFormation Code.	AWS CodeCommit
Laden Sie die CloudFormation Vorlage und den Automatisierungscode in das CodeCommit Repository hoch.	Führen Sie den Befehl Git push aus, um CloudFormation Vorlagen- und Automatisierungscode in das Repository hochzuladen.	Git
Stellen Sie die CI/CD-Pipeline für den Teamstream bereit, indem Sie. CloudFormation	Verwenden Sie die vorbereitete CloudFormation Vorlage, um eine Teamstream-CI/CD-Pipeline bereitzustellen.	AWS CloudFormation

Erstellen Sie die CI/CD-Pipeline für die Systemintegration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das UFT-Docker-Image.	Verwenden Sie den Docker-Befehl und das UFT-Dockerfile, um das Docker-Image zu erstellen.	Docker
Erstellen Sie das Docker-Repository in Amazon ECR für das UFT-Image.	Erstellen Sie auf der Amazon ECR-Konsole das Docker-Repository für das UFT-Image.	Amazon ECR
Senden Sie das UFT-Docker-Image an Amazon ECR.	Führen Sie den Befehl Docker push aus, um das Enterprise Test Server-Docker-Image in	Docker

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon ECR zu pushen und zu speichern.	
Erstellen Sie das Verastream-Docker-Image.	Verwenden Sie den Docker-Befehl und das Verastream-Dockerfile, um das Docker-Image zu erstellen.	Docker
Erstellen Sie das Docker-Repository in Amazon ECR für das Verastream-Image.	Erstellen Sie auf der Amazon ECR-Konsole das Docker-Repository für das Verastream-Image.	Amazon ECR
Stellen Sie die CI/CD-Pipeline für die Systemintegration bereit, indem Sie CloudFormation	Verwenden Sie die vorbereitete CloudFormation Vorlage, um eine CI/CD-Pipeline für die Systemintegration bereitzustellen.	AWS CloudFormation

Erstellen Sie eine CI/CD-Pipeline für die Produktionsbereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Enterprise Server mithilfe des AWS Schnellstarts bereit.	Um Enterprise Server mithilfe von bereitzustellen CloudFormation, starten Sie den Enterprise Server auf AWS Quick Start.	AWS CloudFormation
Stellen Sie eine CI/CD-Pipeline für die Produktionsbereitstellung bereit.	Verwenden Sie auf der CloudFormation Konsole die CloudFormation Vorlage, um eine CI/CD-Pipeline für die Produktionsbereitstellung bereitzustellen.	AWS CloudFormation

Zugehörige Ressourcen

Referenzen

- AWS DevOps Blog — Automatisieren Sie Tausende von Mainframe-Tests AWS mit der Micro Focus Enterprise Suite (Micro Focus ist jetzt Rocket Software)
- py3270/py3270-Repository GitHub
- Altran-pt-gdc/Robot-Framework-Mainframe-3270-Bibliotheks-Repository GitHub
- Willkommen bei Behave!
- APN-Partnerblog — Tag: Micro Focus (Micro Focus ist jetzt Rocket Software.)
- Eine Instance über eine Startvorlage starten

AWS Marketplace

- Rocket Software UFT One

AWS Schnellstart

- Rocket Enterprise Server auf AWS

Modernisieren Sie Mainframe-Online-Druck-Workloads auf AWS mithilfe von Micro Focus Enterprise Server und LRS VPSX/MFI

Erstellt von Shubham Roy (AWS), Abraham Rondon (Micro Focus), Guy Tucker (Levi, Ray and Shoup Inc) und Kevin Yung (AWS)

Übersicht

Dieses Muster zeigt Ihnen, wie Sie Ihre geschäftskritischen Mainframe-Online-Druck-Workloads in der Amazon Web Services (AWS) -Cloud modernisieren können, indem Sie Micro Focus Enterprise Server als Laufzeit für eine modernisierte Mainframe-Anwendung und LRS VPSX/MFI (Micro Focus Interface) als Druckserver verwenden. Das Muster basiert auf dem Ansatz der Replatform Mainframe-Modernisierung. Bei diesem Ansatz migrieren Sie Ihre Mainframe-Online-Anwendung zu Amazon Elastic Compute Cloud (Amazon EC2) und Ihre Mainframe-Datenbank, wie IBM DB2 for z/OS, zu Amazon Relational Database Service (Amazon RDS). Die Authentifizierung und Autorisierung für den modernisierten Druck-Workflow erfolgt durch AWS Directory Service for Microsoft Active Directory, auch bekannt als AWS Managed Microsoft AD. Der LRS Directory Information Server (LRS/DIS) ist in AWS Managed Microsoft AD für die Authentifizierung und Autorisierung von Druckworkflows integriert. Durch die Modernisierung Ihrer Online-Druck-Workloads können Sie die IT-Infrastrukturkosten senken, den technischen Aufwand für die Wartung älterer Systeme verringern, Datensilos beseitigen, die Agilität und Effizienz mit einem DevOps Modell erhöhen und die Vorteile von On-Demand-Ressourcen und Automatisierung in der AWS-Cloud nutzen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein Mainframe-Workload für Online-Druck oder Output-Management
- Grundkenntnisse zur Neuerstellung und Bereitstellung einer Mainframe-Anwendung, die auf Micro Focus Enterprise Server ausgeführt wird (Weitere Informationen finden Sie im Enterprise Server-Datenblatt in der Micro Focus-Dokumentation.)
- Grundkenntnisse der LRS Cloud-Printing-Lösungen und -Konzepte (Weitere Informationen finden Sie unter Output Modernization in der LRS-Dokumentation.)
- Micro Focus Enterprise Server-Software und -Lizenz (Weitere Informationen erhalten Sie vom Micro Focus-Vertrieb.)

- VPSX/MFI, LRS/Queue, and LRS/DISLRS-Software und -Lizenzen (Weitere Informationen erhalten Sie vom LRS-Vertrieb.)

> **Note**
>
> Weitere Informationen zu Überlegungen zur Konfiguration von Mainframe-Online-Druck-Workloads finden Sie unter Überlegungen im Abschnitt Zusätzliche Informationen dieses Musters.

Produktversionen

- Micro Focus Enterprise Server 8.0 oder höher
- LRS VPSX/MFI V1R3 oder höher

Architektur

Quelltechnologie-Stack

- Betriebssystem — IBM z/OS
- Programmiersprache — Common Business-Oriented Language (COBOL) und Customer Information Control System (CICS)
- Datenbank — IBM DB2 für z/OS, IBM Information Management System (IMS) und Virtual Storage Access Method (VSAM)
- Sicherheit — Resource Access Control Facility (RACF), CA Top Secret für z/OS und Access Control Facility 2 () ACF2
- Druck- und Ausgabemanagement — IBM Mainframe-z/OS-Druckprodukte (IBM Infoprint Server für z/OS, LRS und CA View)

Zieltechnologie-Stack

- Betriebssystem — Microsoft Windows Server läuft auf Amazon EC2
- Rechnen — Amazon EC2
- Programmiersprache — COBOL und CICS
- Datenbank — Amazon RDS

- Sicherheit — AWS Managed Microsoft AD
- Druck- und Ausgabemanagement — LRS-Drucklösung auf AWS
- Mainframe-Laufzeitumgebung — Micro Focus Enterprise Server

Quellarchitektur

Das folgende Diagramm zeigt eine typische aktuelle Architektur für einen Mainframe-Online-Druck-Workload.

Das Diagramm zeigt den folgenden Workflow:

1. Benutzer führen Geschäftstransaktionen auf einem System of Engagement (SoE) durch, das auf einer in COBOL geschriebenen IBM CICS-Anwendung basiert.
2. Das SoE ruft den Mainframe-Service auf, der die Geschäftstransaktionsdaten in einer system-of-records (SoR) -Datenbank wie IBM for z/OS aufzeichnet. DB2
3. Das SoR speichert die Geschäftsdaten aus dem SoE.
4. Ein Benutzer initiiert eine Anforderung zur Generierung der Druckausgabe vom CICS-SoE, wodurch eine Drucktransaktionsanwendung zur Verarbeitung der Druckanforderung initiiert wird.
5. Die Anwendung für Drucktransaktionen (z. B. ein CICS- und COBOL-Programm) extrahiert Daten aus der Datenbank, formatiert die Daten gemäß den Geschäftsanforderungen und generiert Geschäftsergebnisse (Druckdaten) wie Abrechnungen, Personalausweise oder Kreditauszüge. Anschließend sendet die Anwendung mithilfe der Virtual Telecommunications Access Method (VTAM) eine Druckanforderung. Ein z/OS-Druckserver (wie IBM Infoprint Server) verwendet NetSpool oder eine ähnliche VTAM-Komponente, um die Druckanforderungen abzufangen, und erstellt dann Druckausgabedatensätze auf dem JES-Spool mithilfe von JES-Ausgabeparametern. Die JES-Ausgabeparameter geben Routing-Informationen an, die der Druckserver verwendet, um die Ausgabe an einen bestimmten Netzwerkdrucker zu übertragen. Der Begriff VTAM bezieht sich auf den z/OS Communications Server und das System Network Architecture (SNA) - Serviceelement von z/OS.
6. Die Komponente zur Übertragung der Druckausgabe überträgt die ausgegebenen Druckdatensätze vom JES-Spool an externe Drucker oder Druckserver wie LRS (wie in diesem Muster gezeigt), IBM Infoprint Server oder E-Mail-Ziele.

Zielarchitektur

Das folgende Diagramm zeigt eine Architektur für einen Mainframe-Online-Druck-Workload, der in der AWS-Cloud bereitgestellt wird:

Das Diagramm zeigt den folgenden Workflow:

1. Ein Benutzer initiiert über eine Online-Benutzeroberfläche (CICS) eine Druckanfrage, um Druckausgaben wie Rechnungsauszüge, Personalausweise oder Kreditauszüge zu erstellen.
2. Die Mainframe-Online-Anwendung (auf Amazon umgestellt EC2) verwendet die Micro Focus Enterprise Server-Laufzeit, um Daten aus der Anwendungsdatenbank zu extrahieren, Geschäftslogik auf die Daten anzuwenden, die Daten zu formatieren und die Daten dann mithilfe von Micro Focus CICS Print Exit (DFHUPRNT) an ein Druckziel zu senden.
3. Die Anwendungsdatenbank (ein SoR, der auf Amazon RDS läuft) speichert Daten für die Druckausgabe.
4. Der Name der VPSX/MFI printing solution is deployed on Amazon EC2, and its operational data is stored in Amazon Elastic Block Store (Amazon EBS). LRS VPSX/MFI uses a TCP/IP-based LRS/Queue transmission agent to collect print data through the Micro Focus CICS Print Exit API (DFHUPRNT) and deliver the data to a specified printer destination. The original TERMID (TERM) that's used in the modernized CICS application is used as the VPSX/MFI LRS-Warteschlange.

> **Note**
>
> Die Ziellösung erfordert in der Regel keine Anwendungsänderungen, um Mainframe-Formatierungssprachen wie IBM Advanced Function Presentation (AFP) oder Xerox Line Condition Data Stream (LCDS) zu berücksichtigen. Weitere Informationen zur Verwendung von Micro Focus für die Migration und Modernisierung von Mainframe-Anwendungen auf AWS finden Sie in der AWS-Dokumentation unter Empowering Enterprise Mainframe Workloads on AWS with Micro Focus.

AWS-Infrastrukturarchitektur

Das folgende Diagramm zeigt eine hochverfügbare und sichere AWS-Infrastrukturarchitektur für einen Mainframe-Online-Druck-Workload:

Das Diagramm zeigt den folgenden Workflow:

1. Die Mainframe-Online-Anwendung (geschrieben in einer Programmiersprache wie CICS oder COBOL) verwendet die Kerngeschäftslogik, um Druckausgaben wie Abrechnungen, Personalausweise und Kreditauszüge zu verarbeiten und zu generieren. Die Online-Anwendung wird auf Amazon EC2 in zwei Availability Zones (AZ) für Hochverfügbarkeit (HA) bereitgestellt und verwendet Micro Focus CICS Print Exit, um die Druckausgabe an LRS VPSX/MFI für das Drucken durch Endbenutzer weiterzuleiten.
2. LRS-Befehle. VPSX/MFI uses a TCP/IP-based LRS/Queue transmission agent to collect or capture print data from the Micro Focus online Print Exit programming interface. Online Print Exit passes the necessary information to enable LRS VPSX/MFI to effectively process the print file and dynamically build LRS/Queue

   > **Note**
   >
   > Weitere Informationen zu den verschiedenen Methoden der CICS-Anwendungsprogrammierung für den Druck und deren Unterstützung in Micro Focus Enterprise Server und LRS VPSX/MFI finden Sie unter Druckdatenerfassung im Abschnitt Zusätzliche Informationen dieses Musters.

3. > **Note**
   >
   > Ein Network Load Balancer stellt einen DNS-Namen zur Integration von Micro Focus Enterprise Server in LRS bereit VPSX/MFI. : LRS VPSX/MFI supports a Layer 4 load balancer. The Network Load Balancer also does a basic health check on LRS VPSX/MFI und leitet den Datenverkehr an die registrierten Ziele weiter, die fehlerfrei sind.

4. Der LRS VPSX/MFI-Druckserver wird auf Amazon EC2 in zwei Availability Zones für HA bereitgestellt und verwendet Amazon EBS als Betriebsdatenspeicher. VPSX/MFI supports both the active-active and active-passive service modes. This architecture uses multiple Availability Zones in an active-passive pair as an active and hot standby. The Network Load Balancer performs a health check on LRS VPSX/MFI EC2 LRS-Instances und leitet den Datenverkehr an Hot-Standby-Instances in einer anderen Availability Zone weiter, wenn sich eine aktive Instance in einem fehlerhaften Zustand befindet. Die Druckanforderungen werden in jeder Instanz lokal in der LRS-Auftragswarteschlange gespeichert. EC2 Im Falle einer Wiederherstellung muss eine ausgefallene Instanz neu gestartet werden, damit die LRS-Dienste die Verarbeitung der Druckanforderung fortsetzen können.

> **Note**
>
> LRS VPSX/MFI kann auch Zustandsprüfungen auf Ebene der Druckerflotte durchführen. Weitere Informationen finden Sie unter Integritätsprüfungen der Druckerflotte im Abschnitt Zusätzliche Informationen dieses Musters.

5. AWS Managed Microsoft AD lässt sich in LRS/DIS integrieren, um die Authentifizierung und Autorisierung von Druckworkflows durchzuführen. Weitere Informationen finden Sie unter Druckauthentifizierung und Autorisierung im Abschnitt Zusätzliche Informationen dieses Musters.
6. LRS VPSX/MFI verwendet Amazon EBS für Blockspeicher. Sie können Amazon EBS-Daten von aktiven EC2 Instances als point-in-time Snapshots auf Amazon S3 sichern und sie auf Hot-Standby-EBS-Volumes wiederherstellen. Um die Erstellung, Aufbewahrung und Löschung von Amazon EBS-Volume-Snapshots zu automatisieren, können Sie Amazon Data Lifecycle Manager verwenden, um die Häufigkeit automatisierter Snapshots festzulegen und sie auf der Grundlage Ihrer RTO/RPO-Anforderungen wiederherzustellen.

Tools

AWS-Services

- Amazon Elastic Block Store (Amazon EBS) bietet Speichervolumen auf Blockebene zur Verwendung mit Amazon-Instances. EC2 EBS-Volumes verhalten sich wie unformatierte Blockgeräte. Sie können diese Volumes als Geräte auf Ihren Instances mounten.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der AWS-Cloud.
- AWS Directory Service for Microsoft Active Directory (AD), auch bekannt als AWS Managed Microsoft Active Directory, ermöglicht es Ihren verzeichnissensitiven Workloads und AWS-Ressourcen, verwaltetes Active Directory in AWS zu verwenden.

Andere Tools

- LRS VPSX/MFI (Micro Focus Interface), das gemeinsam von LRS und Micro Focus entwickelt wurde, erfasst die Ausgabe von einem Micro Focus Enterprise Server JES-Spool und leitet sie zuverlässig an ein bestimmtes Druckziel weiter.
- Der LRS Directory Information Server (LRS/DIS) wird für die Authentifizierung und Autorisierung während des Druckworkflows verwendet.
- LRS/Queue is a TCP/IP-based LRS/Queue transmission agent, used by LRS VPSX/MFI, um Druckdaten über die Online-Programmierschnittstelle Print Exit von Micro Focus zu sammeln oder zu erfassen.
- Micro Focus Enterprise Server ist eine Umgebung zur Anwendungsbereitstellung für Mainframe-Anwendungen. Sie bietet die Ausführungsumgebung für Mainframe-Anwendungen, die mithilfe einer beliebigen Version von Micro Focus Enterprise Developer migriert oder erstellt wurden.

Epen

Richten Sie Micro Focus Enterprise Server auf Amazon ein EC2 und stellen Sie eine Mainframe-Online-Anwendung bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Micro Focus Enterprise Server ein und stellen Sie eine Demo-Online-Anwendung bereit.	Richten Sie Micro Focus Enterprise Server auf Amazon EC2 ein und stellen Sie dann die Micro Focus Account Demo-Anwendung (ACCT-Demo) auf Amazon bereit, EC2 indem Sie den Anweisungen unter Tutorial: CICS-Support in der Micro Focus-Dokumentation folgen. Die ACCT-Demo-Anwendung ist eine Mainframe-Online-Anwendung (CICS), die die Druckausgabe erstellt und dann initiiert.	Cloud-Architekt

Richten Sie einen LRS-Druckserver bei Amazon ein EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Besorgen Sie sich eine LRS-Produktlizenz zum Drucken.	Um eine LRS-Produktlizenz für LRS zu erhaltenVPSX/MFI, LRS/Queue, and LRS/DIS, wenden Sie sich an das LRS Output Management-Team. Sie müssen die Hostnamen der EC2 Instanzen angeben, auf denen die LRS-Produkte installiert werden.	Bauen Sie einen Vorsprung auf
Erstellen Sie eine Amazon EC2 Windows-Instance, um LRS VPSX/MFI zu installieren.	Starten Sie eine Amazon EC2 Windows-Instance, indem Sie den Anweisungen in Schritt 1: Starten einer Instance in der EC2 Amazon-Dokumentati on folgen. Ihre Instance muss die folgenden Hardware- und Softwareanforderungen für LRS VPSX/MFI erfüllen: • CPU — Doppelkern • RAM — 16 GB • Laufwerk — 500 GB • Minimale EC2 Instanz — m5.xlarge • Betriebssystem — Windows/Linux • Software — Interneti nformationsdienst (IIS) oder Apache	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Die oben genannten Hardware- und Softwareanforderungen sind für eine kleine Druckerflotte (etwa 500—1000) vorgesehen. Um die vollständigen Anforderungen zu erfahren, wenden Sie sich an Ihre LRS- und AWS-Ansprechpartner. Gehen Sie beim Erstellen Ihrer Windows-Instance wie folgt vor: 1. Vergewissern Sie sich, dass der EC2 Hostname derselbe Hostname ist, der für die LRS-Produktlizenz verwendet wurde. 2. Aktivieren Sie CGI in Amazon, EC2 indem Sie wie folgt vorgehen: a. Connect zu Ihrer EC2 Instance her, indem Sie den Anweisungen unter Schritt 2: Connect zu Ihrer Instance herstellen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in der EC2 Amazon-Dokumentation folgen. b. Suchen und öffnen Sie im Windows-Startmenü den Server-Manager. c. Wählen Sie im Server-Manager Dashboard, Schnellstart, Rollen und Funktionen hinzufügen aus. Wählen Sie dann Serverrollen aus. d. Wählen Sie unter Serverrollen die Option WebServer (IIS) und dann Anwendungsentwicklung aus. e. Aktivieren Sie unter Anwendungsentwicklung das Kontrollkästchen CGI. f. Folgen Sie den Anweisungen im Windows Server-Manager-Assistenten zum Hinzufügen von Rollen und Funktionen, um CGI zu installieren. g. Öffnen Sie Port 5500 in der Windows-Firewall der EC2 Instanz für die LRS/Queue-Kommunikation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie LRS VPSX/MFI auf der Instanz. EC2	1. Connect zu Ihrer EC2 Instance her, indem Sie den Anweisungen unter Schritt 2: Connect zu Ihrer Instance herstellen in der EC2 Amazon-Dokumentation folgen. 2. **Note** Öffnen Sie in der LRS-E-Mail, die Sie erhalten sollten, den Link zur Produkt-Download-Seite. : LRS-Produkte werden per elektronischer Dateiübertragung (EFT) vertrieben. 3. Laden Sie LRS VPSX/MFI herunter und entpacken Sie die Datei (Standardordner:). `c:\LRS` 4. Starten Sie den LRS Product Installer aus dem entpackten Ordner, um LRS VPSX/MFI zu installieren. 5. Wählen Sie im Menü „Funktionen auswählen“ die Option VPSX® Server (V1R3.022) und klicken Sie dann auf Weiter, um den Installationsvorgang zu	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	starten. Sie erhalten eine Erfolgsmeldung, wenn die Installation abgeschlossen ist.	
Installieren Sie LRS/Queue.	1. Connect zu Ihrer Micro Focus Enterprise EC2 Server-Instance her, indem Sie den Anweisungen in Schritt 2: Connect zu Ihrer Instance herstellen in der EC2 Amazon-Dokumentation folgen. 2. Öffnen Sie in der LRS-E-Mail, die Sie erhalten sollten, den Link zur LRS-Produkt-Download-Seite, laden Sie LRS/Queue herunter und entpacken Sie dann die Datei. 3. Gehen Sie zu dem Verzeichnis, in das Sie die Dateien heruntergeladen haben, und starten Sie dann das LRS-Produktinstallationsprogramm, um LRS/Queue zu installieren.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie LRS/DIS.	1. Connect zu Ihrer LRS EC2 VPSX/MFI-Instance her, indem Sie den Anweisungen in Schritt 2: Connect zu Ihrer Instance herstellen in der Amazon-Dokumentation folgen. EC2 2. Öffnen Sie in der LRS-E-Mail, die Sie erhalten sollten, den Link zur LRS-Produkt-Download-Seite, laden Sie LRS/DIS herunter und entpacken Sie dann die Datei. 3. Gehen Sie zu dem Verzeichnis, in das Sie die Dateien heruntergeladen haben, und starten Sie dann das LRS-Produktinstallationsprogramm. 4. Erweitern Sie im LRS Product Installer die Option LRS Misc Tools, wählen Sie LRS DIS und dann Weiter aus. 5. Folgen Sie den restlichen Anweisungen im LRS-Produktinstallationsprogramm, um den Installationsvorgang abzuschließen.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Zielgruppe und registrieren Sie LRS EC2 VPSX/MFI als Ziel.	Erstellen Sie eine Zielgruppe, indem Sie den Anweisungen unter Erstellen Sie eine Zielgruppe für Ihren Network Load Balancer in der Elastic Load Balancing Balancing-Dokumentation folgen. Gehen Sie beim Erstellen der Zielgruppe wie folgt vor: 1. Wählen Sie auf der Seite Gruppendetails angeben für Wählen Sie einen Zieltyp die Option Instances aus. 2. Wählen Sie für Protokoll die Option TCP aus. 3. Wählen Sie für Port 5500 aus. 4. Wählen Sie auf der Seite Ziele registrieren im Abschnitt Verfügbare Instanzen die LRS EC2 VPSX/MFI-Instances aus.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Network Load Balancer.	Folgen Sie den Anweisungen unter Network Load Balancer erstellen in der Elastic Load Balancing Balancing-Dokumentation. Ihr Network Load Balancer leitet den Datenverkehr vom Micro Focus Enterprise Server an LRS VPSX/MFI weiter. EC2 Wenn Sie den Network Load Balancer erstellen, gehen Sie auf der Seite Listener und Routing wie folgt vor: 1. Wählen Sie für Protocol TCP aus. 2. Wählen Sie für Port die Option 5500 aus. 3. Wählen Sie für Standarda ktion die Option Weiterleiten an für die Zielgruppe, die Sie zuvor erstellt haben.	Cloud-Architekt

Integrieren Sie Micro Focus Enterprise Server in LRS VPSX/MFI and LRS/Queue

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Micro Focus Enterprise Server für die LRS/ Queue-Integration.	1. Connect zu Ihrer Micro Focus Enterprise EC2 Server-Instance her, indem Sie den Anweisungen in Schritt 2: Connect zu Ihrer Instance herstellen in der	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	EC2 Amazon-Dokumentation folgen. 2. Öffnen Sie im Windows-Startmenü die Micro Focus Enterprise Server Administration UI. 3. Wählen Sie in der Menüleiste NATIVE. 4. Wählen Sie im Navigationsbereich Directory Server und dann BANKDEMO oder Ihre Enterprise-Serverregion aus. 5. Scrollen Sie im linken Navigationsbereich von Allgemein nach unten zum Abschnitt Erweitert, um die Umgebungsvariablen (LRSQ_ADDRESS, LRSQ_PORT, LRSQ_COMMAND) so zu konfigurieren, dass sie auf LRSQ verweisen. 6. Geben Sie für LRSQ_ADDRESS die IP-Adresse oder den DNS-Namen des Network Load Balancer ein, den Sie zuvor erstellt haben. 7. Geben Sie für LRSQ_PORT den VPSX LRSQ Listener Port (5500) ein.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Geben Sie für LRSQ_COMMAND den Pfad der ausführbaren LRSQ-Datei ein. 9. **Note** LRS unterstützt derzeit eine maximale Zeichenbeschränkung von 50 für DNS-Namen, dies kann sich jedoch in future ändern. Wenn Ihr DNS-Name größer als 50 ist, können Sie alternativ die IP-Adresse des Network Load Balancer verwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie CICS Print Exit (DFHUPRNT) für die Initialisierung von Micro Focus Enterprise Server zur Verfügung.	1. Connect zu Ihrer Micro Focus Enterprise EC2 Server-Instance her, indem Sie den Anweisungen in Schritt 2: Connect zu Ihrer Instance herstellen in der EC2 Amazon-Dokumentation folgen. 2. **Note** Kopieren Sie CICS Print Exit (DFHUPRNT) aus dem ausführbaren LRS VPSX/MFI-Ordner (benanntVPSX_MFI_R2) an den Speicherort der Micro Focus Enterprise Server-Instance. EC2 Für 32-Bit-Systeme lautet der Speicherort. `C:\Program Files (x86) \Micro Focus\Enterprise Server\bin` Für 64-Bit-Systeme lautet der Standort`C:\Program Files (x86) \Micro Focus`	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`\Enterprise Server\bin64 .`: Die `DFHUPRNT_64.dll` Datei muss `DFHUPRNT.dll` beim Kopieren umbenannt werden. Stellen Sie sicher, dass Micro Focus Enterprise Server CICS Print Exit (DFHUPRNT) erkannt hat 1. Stoppen und starten Sie Micro Focus Enterprise Server. 2. Öffnen Sie im Administrationsbereich von Micro Focus Enterprise Server die Optionen Monitor, Logs, Console logs. 3. Suchen Sie in den Konsolenprotokollen nach der folgenden Meldung: „3270 printer user exit DFHUPRNT successfully installed successfully.“	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie die Terminal-ID (TERMIDs) des CICS-Druckers als Micro Focus Enterprise Server.	Aktivieren Sie den 3270-Druck in Micro Focus Enterprise Server 1. Öffnen Sie im Administrationsbereich von Micro Focus Enterprise Server die Optionen CICS, Resources, By Group. 2. Wählen Sie im linken Navigationsbereich SIT (System Initialization Table) und dann BNKCICV. 3. Scrollen Sie im Bereich Allgemein nach unten zu 3270, und aktivieren Sie dann das Kontrollkästchen 3270 Print. Definieren Sie das Terminal des CICS-Druckers in Micro Focus Enterprise Server 1. Öffnen Sie im Administrationsbereich von Micro Focus Enterprise Server die Optionen CICS, Resources, By Type. 2. Wählen Sie im linken Navigationsbereich Term und anschließend Neu aus. Das Formular „Terminalressource erstellen“ wird geöffnet.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Geben Sie unter Name den Namen der LRS-Druckwarteschlange ein. (Hinweis: Dieses Muster verwendet „P275“ als Terminal-ID und LRS VPSX-Druckwarteschlange des CICS-Druckers.) 4. Geben Sie als Gruppe BANKTERM ein. 5. Geben Sie für Automatische Installation — Modell den Wert NEIN ein. 6. Geben Sie für Terminal Identifiers — Terminal type den DFHPRT32Wert ein. 7. Geben Sie als Netzname den Wert ein VTAMP275. 8. Aktivieren Sie für Terminaln utzung das Kontrollk ästchen In Betrieb. 9. Scrollen Sie zum Seitenanf ang und wählen Sie dann Speichern aus. 10. Wählen Sie Installieren aus. In einer Popup-Meldung wird eine Meldung über eine erfolgreiche Installation angezeigt.	

Richten Sie Drucker und Druckbenutzer in Micro Focus Enterprise Server und LRS VPSX/MFI ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Druckwartschlange im LRS VPSX.	1. Connect zu Ihrer LRS EC2 VPSX/MFI-Instance her, indem Sie den Anweisungen in Schritt 2: Connect zu Ihrer Instance herstellen in der Amazon-Dokumentation folgen. EC2 2. Öffnen Sie das VPSX-Webinterface über das Windows-Startmenü. 3. Wählen Sie im Navigationsbereich Drucker aus. 4. Wählen Sie Hinzufügen und dann Drucker hinzufügen. 5. Geben Sie auf der Seite Druckerkonfiguration P275 als Druckername ein. 6. Geben Sie für VPSX ID ein. VPS1 7. Wählen Sie für CommTypeTCPIP/LRSQ aus. 8. Geben Sie für Host/IP-Adresse die IP-Adresse des physischen Druckers ein, den Sie hinzufügen möchten. 9. Geben Sie unter Gerät den Namen Ihres Geräts ein.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	10. Wählen Sie entweder Windows-Treiber oder Linux/Mac-Treiber. 11. Wählen Sie Hinzufügen aus. **Note** Die Druckerwarteschlange muss dem in Micro Focus Enterprise TERMIDs Server erstellten Druck entsprechen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Druckbenutzer in LRS VPSX/MFI.	1. Connect zu Ihrer LRS EC2 VPSX/MFI-Instance her, indem Sie den Anweisungen in Schritt 2: Connect zu Ihrer Instance herstellen in der Amazon-Dokumentation folgen. EC2 2. Öffnen Sie das VPSX-Webinterface über das Windows-Startmenü. 3. Wählen Sie im Navigationsbereich Sicherheit und dann Benutzer aus. 4. Wählen Sie in der Spalte Benutzername die Option admin und dann Kopieren aus. 5. Geben Sie im Fenster Benutzerprofilverwaltung für Benutzername einen Benutzernamen ein (z. B. PrintUser). 6. Geben Sie unter Beschreibung eine kurze Beschreibung ein (z. B. Benutzer für Testdruck). 7. Wählen Sie Aktualisieren. Dadurch wird ein Druckbenutzer erstellt (z. B. PrintUser). 8. Wählen Sie im Navigationsbereich unter Benutzer	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den neuen Benutzer aus, den Sie erstellt haben. 9. Wählen Sie im Befehlsmenü die Option Sicherheit aus. 10. Wählen Sie auf der Seite Sicherheitsregeln alle zutreffenden Optionen für Druckersicherheit und Jobsicherheit aus und klicken Sie dann auf Speichern. 11. Um Ihren neuen Druckbenutzer zur Administratorgruppe hinzuzufügen, wechseln Sie zum Navigationsbereich, wählen Sie Sicherheit und dann Konfigurieren aus. 12. Fügen Sie im Fenster Sicherheitskonfiguration Ihren neuen Druckbenutzer zur Administratorspalte hinzu.	

Richten Sie die Druckauthentifizierung und -autorisierung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine von AWS verwaltete Microsoft AD-Domain mit Benutzern und Gruppen.	1. Erstellen Sie ein Active Directory auf AWS Managed Microsoft AD, indem Sie den Anweisungen unter Erstellen Sie Ihr	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	AWS Managed Microsoft AD-Verzeichnis in der AWS Directory Service Service-Dokumentation folgen. 2. Stellen Sie eine EC2 Instance (Active Directory -Manager) bereit und installieren Sie Active Directory-Tools zur Verwaltung Ihres AWS Managed Microsoft AD. Folgen Sie dazu den Anweisungen in Schritt 3: Bereitstellen einer EC2 Instanz zur Verwaltung Ihres AWS Managed Microsoft AD in der AWS Directory Service Service-Dokumentation. 3. **Note** Connect zu Ihrer EC2 Instance her, indem Sie den Anweisungen unter Schritt 2: Connect zu Ihrer Instance herstellen in der EC2 Amazon-Dokumentation folgen. : Wenn Sie eine Verbindung mit der EC2 Instance herstellen, geben	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie Ihre Administr atoranmeldedaten (für das Verzeichn is, das Sie in Schritt 1 erstellt haben) in das Windows-S icherheitsfenster ein. 4. Wählen Sie im Windows-S tartmenü unter Windows-V erwaltungstools die Option Active Directory-Benutzer und -Computer aus. 5. Erstellen Sie einen Druckbenutzer in der Active Directory-Domäne, indem Sie die Schritte unter Benutzer erstellen in der Dokumentation zum AWS-Verzeichnisdienst befolgen.	
Verbinden Sie LRS VPSX/MFI mit einer von AWS EC2 verwalteten Microsoft AD-Domain.	Verbinden Sie LRS VPSX/MFI EC2 automatisch (AWS Knowledge Center-Do kumentation) oder manuell (AWS Directory Service-Dokumentation) mit Ihrer AWS Managed Microsoft AD-Domain.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfiguration und Integration von LRS/DIS mit AWS Managed Microsoft AD.	1. Connect zu Ihrer LRS EC2 VPSX/MFI-Instance her, indem Sie den Anweisungen in Schritt 2: Connect zu Ihrer Instance herstellen in der Amazon-Dokumentation folgen. EC2 2. Öffnen Sie im Windows-Startmenü das VPSX-Webinterface. 3. Wählen Sie im Navigationsbereich Sicherheit und dann Konfigurieren aus. 4. Wählen Sie auf der Seite Sicherheitskonfiguration im Abschnitt Sicherheitsparameter für Sicherheitstyp die Option Intern aus. 5. Geben Sie Ihre Einstellungen für die restlichen Optionen im Abschnitt Sicherheitsparameter ein. 6. Öffnen Sie den Ordner LRS Output Management im Microsoft Windows-Startmenü, wählen Sie Serverstart und dann Serverstopp aus. 7. Melden Sie sich mit Ihrem Active Directory-Benutzernamen und -Passwort bei LRS VPSX/MFI an.	Cloud-Architekt

Testen Sie einen Online-Druck-Workflow

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initiieren Sie über die Micro Focus ACCT Demo-App eine Online-Druckanfrage.	1. **Note** Öffnen Sie den TN327 0-Termina l-Emulator in Ihrer Micro Focus Enterprise EC2 Server-Instanz. (: Dieses Muster verwendet 3270 Terminalemulatoren .) 2. Connect zum TN327 0-Terminal-Emulator (Rumba) her. Verwenden Sie als Hostnamenadresse 127.0.0.1. Verwenden Sie für Telnet-Port 9270. 3. Nachdem Sie eine Verbindung zum 3270-Bild schirm hergestellt haben, drücken Sie CTL+SHIFT +Z, um den Bildschirm zu löschen. 4. Um die ACCT-Demo-Anwendung zu starten, geben Sie im leeren Bildschirm ACCT ein. Dadurch wird der Hauptbild schirm der Anwendung ACCT Demo Online	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(CICS) geöffnet. Hinweis: Der Hauptbildschirm enthält Menüoptionen wie Kontodatei, Suchen nach Namen, Enter, Anforderungstyp, Konto und Drucker. 5. Um eine Druckanfrage über die ACCT Demo Online (CICS) -Anwendung einzureichen, geben Sie P in das Feld Anforderungstyp, 11111 in das Kontofeld und P275 in das Druckerfeld ein. Achten Sie darauf, den Wert im Druckerfeld auf den Wert der Terminal-ID des CICS-Druckers einzustellen. 6. Drücken Sie die Eingabetaste. Die Meldung „Print Request Scheduled“ wird am unteren Bildschirmrand angezeigt. Dadurch wird bestätigt, dass aus der ACCT-Demo-Anwendung eine Online-Druckanfrage generiert und zur Druckverarbeitung an LRS VPS/MFI gesendet wurde.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Druckausgabe in LRS VPSX/MFI.	1. Connect zu Ihrer LRS EC2 VPSX/MFI-Instance her, indem Sie den Anweisungen in Schritt 2: Connect zu Ihrer Instance herstellen in der Amazon-Dokumentation folgen. EC2 2. Öffnen Sie im Windows-Startmenü das VPSX-Webinterface. 3. Wählen Sie im Navigationsbereich Drucker und dann Ausgabewarteschlange aus. Suchen Sie die P275-Druckwartesch lange, die Sie zuvor für den Online-Druck erstellt haben. 4. Wählen Sie für die Druckerwarteschlange (P275) in der Spalte Spool-ID die Spool-ID für den Auftrag in der Druckerwarteschlange aus. 5. Wählen Sie auf der Registerkarte Aktionen in der Spalte BEFEHL die Option Durchsuchen. Sie können jetzt die Druckausgabe eines Kontoauszugs mit Spalten für Kontonummer, NACHNAME, VORNAME, ADRESSE,	Testingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	TELEFON, Nr. sehen. Ausgestellte Karten, Ausstellungsdatum, Betrag und Saldo. Ein Beispiel für dieses Muster finden Sie im Anhang online_print_output.	

Zugehörige Ressourcen

- Modernisierung der LRS-Leistung (LRS-Dokumentation)
- VTAM-Netzwerkkonzepte (IBM-Dokumentation)
- Zusammenfassung der LU-Typen (Logical Unit) (IBM-Dokumentation)
- ANSI und Maschinenwagensteuerungen (IBM-Dokumentation)
- Unterstützung von Mainframe-Workloads für Unternehmen auf AWS mit Micro Focus (AWS-Partnernetzwerk-Blog)
- Erstellen Sie ein Micro Focus Enterprise Server PAC mit Amazon EC2 Auto Scaling und Systems Manager (Dokumentation zu AWS Prescriptive Guidance)
- AFP-Datenstream (Advanced Function Presentation) (IBM-Dokumentation)
- Line Conditioned Data Stream (LCDS) (Compart-Dokumentation)

Zusätzliche Informationen

Überlegungen

Während Ihrer Modernisierung können Sie eine Vielzahl von Konfigurationen für Mainframe-Online-Prozesse und die damit generierte Leistung in Betracht ziehen. Die Mainframe-Plattform wurde von allen Kunden und Anbietern, die sie verwenden, an spezielle Anforderungen angepasst, die sich direkt auf den Druck auswirken. Beispielsweise kann Ihre aktuelle Plattform IBM Advanced Function Presentation (AFP) oder den Xerox Line Condition Data Stream (LCDS) in den aktuellen Arbeitsablauf integrieren. Darüber hinaus können Mainframe-Wagen-Steuerzeichen und Kanalbefehle das Aussehen der gedruckten Seite beeinflussen und erfordern möglicherweise eine besondere Behandlung. Im Rahmen der Planung der Modernisierung empfehlen wir Ihnen, die Konfigurationen in Ihrer spezifischen Druckumgebung zu bewerten und zu verstehen.

Erfassung von Druckdaten

In diesem Abschnitt werden die Methoden zur CICS-Anwendungsprogrammierung zusammengefasst, die Sie in einer IBM-Mainframe-Umgebung zum Drucken verwenden können. VPSX/MFI components provide techniques to allow the same application programs to create data in the same way. The following table describes how each application programming method is supported in a modernized CICS application running in AWS and Micro Focus Enterprise Server with an LRS VPSX/MFILRS-Druckserver.

Methode	Beschreibung	Support der Methode in einer modernisierten Umgebung
FÜHRUNGSKRÄFTE SENDEN TEXT... oder EXEC CICS SEND MAP..	Diese CICS- und VTAM-Methoden sind für die Erstellung und Bereitstellung von 3270/SCS-Druckdatenströmen an LUTYPE0,, und Druckgeräte verantwortlich. LUTYPE1 LUTYPE3	Eine Micro Focus Online Print Exit (DFHUPRNT) - Anwendungsprogrammschnittstelle (API) ermöglicht die Verarbeitung von Druckdaten, indem Druckdatenströme mit einer dieser Methoden erstellt werden. VPSX/MFI when 3270/SCS
FÜHRUNGSKRÄFTE SENDEN TEXT... oder EXEC CICS SEND MAP.. (mit IBM Mainframe-Software von Drittanbietern)	Die CICS- und VTAM-Methoden sind für die Erstellung und Bereitstellung von 3270/SCS-Druckdatenströmen an LUTYPE0,, und Druckgeräte verantwortlich. LUTYPE1 LUTYPE3 Softwareprodukte von Drittanbietern fangen die Druckdaten ab, konvertieren die Daten in Standarddruckformatdaten mit einem ASA/MCH-Steuerzeichen und platzieren die Daten auf dem JES-Spool, damit sie von Mainframe-basierte	Eine Micro Focus Online Print Exit (DFHUPRNT) - API ermöglicht die Verarbeitung von Druckdaten, indem VPSX/MFI when 3270/SCS Druckdatenströme mit einer dieser Methoden erstellt werden.

	n Drucksystemen verarbeit et werden können, die JES verwenden.	
EXECIT CICS SPOOLOPEN	Diese Methode wird von CICS-Anwendungsprogrammen verwendet, um Daten direkt in den JES-Spool zu schreiben . Die Daten stehen dann für die Verarbeitung durch Mainframe-basierte Drucksyst eme zur Verfügung, die JES verwenden.	Micro Focus Enterprise Server spoolt die Daten in den Enterprise Server-Spool, wo sie vom VPSX/MFI Batch Print Exit (LRSPRTE6) verarbeitet werden können, der die Daten auf VPSX spoolt.
DRS/API	Eine von LRS bereitgestellte programmatische Schnittst elle wird zum Schreiben von Druckdaten in JES verwendet.	VPSX/MFI bietet eine Ersatzschnittstelle, die die Druckdaten direkt an VPSX weiterleitet.

Zustandsprüfungen der Druckerflotte

LRS VPSX/MFI (LRS LoadX) kann tiefgreifende Zustandsprüfungen durchführen, einschließlich Geräteverwaltung und Betriebsoptimierung. Die Geräteverwaltung kann Fehler in einem Druckergerät erkennen und die Druckanforderung an einen fehlerfreien Drucker weiterleiten. Weitere Informationen zu umfassenden Integritätsprüfungen für Druckerflotten finden Sie in der LRS-Dokumentation, die in Ihrer Produktlizenz enthalten ist.

Authentifizierung und Autorisierung drucken

LRS/DIS enables LRS applications to authenticate user IDs and passwords by using Microsoft Active Directory or an LDAP server. In addition to basic print authorization, LRS/DISkann in den folgenden Anwendungsfällen auch detaillierte Drucksicherheitskontrollen anwenden:

- Steuert, wer den Druckerauftrag durchsuchen kann.
- Verwaltet die Navigationsebene der Aufträge anderer Benutzer.
- Operative Aufgaben verwalten. Zum Beispiel Sicherheitsfunktionen auf Befehlsebene wie „Sperren/Freigeben“, „Löschen“, „Ändern“, „Kopieren“ und „Umleiten“. Die Sicherheit kann entweder anhand

der Benutzer-ID oder der Gruppe eingerichtet werden (ähnlich wie bei der AD-Gruppe oder der LDAP-Gruppe).

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Verschieben Sie Mainframe-Dateien mit Transfer Family direkt nach Amazon S3

Erstellt von Luis Gustavo Dantas (AWS)

Übersicht

Im Rahmen der Modernisierung können Sie sich der Herausforderung stellen, Dateien zwischen Ihren lokalen Servern und der Amazon Web Services (AWS) Cloud zu übertragen. Die Übertragung von Daten von Mainframes kann eine große Herausforderung sein, da Mainframes in der Regel nicht auf moderne Datenspeicher wie Amazon Simple Storage Service (Amazon S3), Amazon Elastic Block Store (Amazon EBS) oder Amazon Elastic File System (Amazon EFS) zugreifen können.

Viele Kunden verwenden Intermediate-Staging-Ressourcen wie lokale Linux-, Unix- oder Windows-Server, um Dateien in die AWS-Cloud zu übertragen. Sie können diese indirekte Methode vermeiden, indem Sie AWS Transfer Family mit dem Secure Shell (SSH) File Transfer Protocol (SFTP) verwenden, um Mainframe-Dateien direkt auf Amazon S3 hochzuladen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine virtuelle private Cloud (VPC) mit einem Subnetz, das über Ihre Legacy-Plattform erreichbar ist
- Ein Transfer Family Family-Endpunkt für Ihre VPC
- Mainframe-VSAM-Dateien (Virtual Storage Access Method) wurden in sequentielle Dateien mit fester Länge konvertiert (IBM-Dokumentation)

Einschränkungen

- SFTP überträgt Dateien standardmäßig im Binärmodus, was bedeutet, dass Dateien unter Beibehaltung der EBCDIC-Kodierung auf Amazon S3 hochgeladen werden. Wenn Ihre Datei keine binären oder gepackten Daten enthält, können Sie den Unterbefehl sftp ascii (IBM-Dokumentation) verwenden, um Ihre Dateien während der Übertragung in Text zu konvertieren.
- Sie müssen Mainframe-Dateien (AWS Prescriptive Guidance) entpacken, die gepackte und binäre Inhalte enthalten, um diese Dateien in Ihrer Zielumgebung verwenden zu können.

- Amazon S3 S3-Objekte können eine Größe von mindestens 0 Byte bis zu einem Maximum von 5 TB haben. Weitere Informationen zu den Funktionen von Amazon S3 finden Sie unter Amazon S3 FAQs.

Architektur

Quelltechnologie-Stack

- Sprache zur Jobkontrolle (JCL)
- z/OS Unix-Shell und ISPF
- SFTP
- VSAM und Flatfiles

Zieltechnologie-Stack

- Transfer Family
- Amazon S3
- Amazon Virtual Private Cloud (Amazon VPC)

Zielarchitektur

Das folgende Diagramm zeigt eine Referenzarchitektur für die Verwendung von Transfer Family mit SFTP, um Mainframe-Dateien direkt in einen S3-Bucket hochzuladen.

Das Diagramm zeigt den folgenden Workflow:

1. Sie verwenden einen JCL-Job, um Ihre Mainframe-Dateien über Direct Connect vom Legacy-Mainframe in die AWS-Cloud zu übertragen.
2. Direct Connect ermöglicht es Ihrem Netzwerkverkehr, im globalen AWS-Netzwerk zu bleiben und das öffentliche Internet zu umgehen. Direct Connect verbessert auch die Netzwerkgeschwindigkeit, angefangen bei 50 Mbit/s bis hin zur Skalierung auf bis zu 100 Gbit/s.
3. Der VPC-Endpunkt ermöglicht Verbindungen zwischen Ihren VPC-Ressourcen und den unterstützten Diensten, ohne das öffentliche Internet zu nutzen. Der Zugriff auf Transfer Family und Amazon S3 ermöglicht eine hohe Verfügbarkeit, da er über die elastischen Netzwerkschnittstellen erfolgt, die sich in zwei privaten Subnetzen und Availability Zones befinden.

4. Transfer Family authentifiziert Benutzer und verwendet SFTP, um Ihre Dateien aus der Legacy-Umgebung zu empfangen und in einen S3-Bucket zu verschieben.

Automatisierung und Skalierung

Nachdem der Transfer Family Family-Service eingerichtet wurde, können Sie eine unbegrenzte Anzahl von Dateien vom Mainframe auf Amazon S3 übertragen, indem Sie einen JCL-Job als SFTP-Client verwenden. Sie können die Dateiübertragung auch automatisieren, indem Sie einen Mainframe-Batch-Job-Scheduler verwenden, um die SFTP-Jobs auszuführen, wenn Sie bereit sind, die Mainframe-Dateien zu übertragen.

Tools

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.
- Mit der AWS Transfer Family können Sie Ihre wiederkehrenden business-to-business Dateiübertragungen an Amazon S3 und Amazon EFS mithilfe der Protokolle SFTP, FTPS und FTP sicher skalieren.

Epen

Erstellen Sie den S3-Bucket und die Zugriffsrichtlinie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den S3-Bucket.	Erstellen Sie einen S3-Bucket, um die Dateien zu hosten, die Sie aus Ihrer Legacy-Umgebung übertragen.	Allgemeines AWS
Erstellen Sie die IAM-Rolle und -Richtlinie.	Transfer Family verwendet Ihre AWS Identity and Access Management (IAM) -Rolle,	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	um Zugriff auf den S3-Bucket zu gewähren, den Sie zuvor erstellt haben. Erstellen Sie eine IAM-Rolle, die die folgende IAM-Richtlinie umfasst: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "UserFolderListing", "Action": [ "s3:ListBucket", "s3:GetBucketLocation" ], "Effect": "Allow", "Resource": [ "arn:aws:s3:::<your-bucket-name>" ] }, { "Sid": "HomeDirObjectAccess", "Effect": "Allow", "Action": [ "s3:PutObject",`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"s3:GetObjectAcl",
	"s3:GetObject",
	"s3:DeleteObjectVersion",
	"s3:DeleteObject",
	"s3:PutObjectAcl",
	"s3:GetObjectVersion"
	],
	"Resource":
	"arn:aws:s3:::<your-bucket-name>/*"
	}
	]
	}</pre>
	Note
	Sie müssen den Anwendungsfall Transfer auswählen , wenn Sie die IAM-Rolle erstellen.	

Definieren Sie den Transferservice

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den SFTP-Server.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Transfer Family Family-Konsole und	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wählen Sie dann Server erstellen aus. 2. Wählen Sie nur SFTP (SSH File Transfer Protocol) — Dateiübertragung über das Secure Shell-Protokoll und wählen Sie dann Weiter. 3. Wählen Sie für Identity Provider die Option Service managed und dann Next aus. 4. Wählen Sie als Endpunkttyp die Option VPC Hosted aus. 5. Wählen Sie für Access die Option Intern aus. 6. Wählen Sie unter VPC Ihre VPC aus. 7. Wählen Sie im Abschnitt Availability Zones Ihre Availability Zones und Subnetze aus. 8. Wählen Sie im Abschnitt Sicherheitsgruppen Ihre Sicherheitsgruppe aus und klicken Sie dann auf Weiter. 9. Wählen Sie für Domain Amazon S3 und dann Weiter aus. 10. Behalten Sie die Standardoptionen auf der Seite Zusätzliche Details konfigurieren bei und wählen Sie dann Weiter.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	11. Wählen Sie Create Server (Server erstellen) aus. **Note** Weitere Informationen zur Einrichtung eines SFTP-Servers finden Sie unter Erstellen eines SFTP-fähigen Servers (AWS Transfer Family Family-Benutzerhandbuch).	
Holen Sie sich die Serveradresse.	1. Öffnen Sie die Transfer Family Family-Konsole und wählen Sie Ihre Server-ID in der Spalte Server-ID aus. 2. Wählen Sie im Abschnitt Endpunktdetails für Endpunkttyp die Endpunkt-ID aus. Dadurch gelangen Sie zur Amazon VPC-Konsole. 3. Suchen Sie auf der Registerkarte Details der Amazon VPC-Konsole nach den DNS-Namen neben DNS-Namen.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das SFTP-Client-Schlüsselpaar.	Erstellen Sie ein SSH-Schlüsselpaar für Microsoft Windows oder macOS/Linux/UNIX.	Allgemeines AWS, SSH

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den SFTP-Benutzer.	1. Öffnen Sie die Transfer Family Family-Konsole, wählen Sie im Navigationsbereich Server und wählen Sie dann Ihren Server aus. 2. Wählen Sie in der Spalte Server-ID die Server-ID für Ihren Server aus und klicken Sie dann auf Benutzer hinzufügen. 3. Geben Sie für Username einen Benutzernamen ein, der Ihrem SSH-Schlüsselpaar-Benutzernamen entspricht. 4. Wählen Sie unter Rolle die IAM-Rolle aus, die Sie zuvor erstellt haben. 5. Wählen Sie für das Home-Verzeichnis den S3-Bucket aus, den Sie zuvor erstellt haben. 6. Geben Sie für öffentliche SSH-Schlüssel das key pair ein, das Sie zuvor erstellt haben. 7. Wählen Sie Hinzufügen aus.	Allgemeines AWS

Übertragen Sie die Mainframe-Datei

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Senden Sie den privaten SSH-Schlüssel an den Mainframe.	Verwenden Sie SFTP oder SCP, um den privaten SSH-Schlüssel an die Legacy-Umgebung zu senden.
	
	SFTP-Beispiel:
	
	`sftp [USERNAME@mainframeIP]`
	`[password]`
	`cd [/u/USERNAME]`
	`put [your-key-pair-file]`
	
	SCP-Beispiel:
	
	`scp [your-key-pair-file] [USERNAME@MainframeIP]:/[u/USERNAME]`
	
	Als Nächstes speichern Sie den SSH-Schlüssel im z/OS Unix-Dateisystem unter dem Benutzernamen, der später den Dateiübertragungs-Batchjob ausführen wird (z. B.). `/u/CONTROLM`
	
	Note
	Weitere Informationen zur z/OS Unix-Shell finden Sie unter Eine Einführung in die z/
		Mainframe, z/OS Unix-Shell, FTP, SCP

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	OS-Shells (IBM-Dokumentation).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den JCL-SFTP-Client.	Da Mainframes keinen systemeigenen SFTP-Client haben, müssen Sie das BPXBATCH-Hilfsprogramm verwenden, um den SFTP-Client von der z/OS Unix-Shell aus auszuführen.
	
	Erstellen Sie im ISPF-Editor den JCL-SFTP-Client. Zum Beispiel:
	
	`//JOBNAM JOB ...`
	`//************`
	`******************`
	`******************`
	`******************`
	`****`
	`//SFTP EXEC PGM=BPXBATCH,REGION=0M`
	`//STDPARM DD *`
	`SH cp "//'MAINFRAME.FILE.NAME'" filename.txt;`
	`echo 'put filename.txt' > uplcmd;`
	`sftp -b uplcmd -i ssh_private_key_file ssh_username@<transfer service ip or DNS>;`
	`//SYSPRINT DD SYSOUT=*`
	`//STDOUT DD SYSOUT=*`
	`//STDENV DD *`
	`//STDERR DD SYSOUT=*`
		JCL, Mainframe, z/OS Unix-Shell

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Weitere Informationen zur Ausführung eines Befehls in der z/OS Unix-Shell finden Sie unter The BPXBATCH utility (IBM-Dokumentation). Weitere Informationen zum Erstellen oder Bearbeiten von JCL-Jobs in z/OS finden Sie unter Was ist ISPF? und Der ISPF-Editor (IBM-Dokumentation).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den JCL-SFTP-Client aus.	1. Geben Sie im ISPF-Edit or SUB ein und drücken Sie dann die EINGABETASTE, nachdem der JCL-Job erstellt wurde. 2. Überwachen Sie die Batch-Job-Aktivität des Mainframes zur Dateiübertragung in SDSF. **Note** Weitere Informationen zur Überprüfung der Aktivität von Batch-Jobs finden Sie im z/OS SDSF User's Guide (IBM-Dokumentation).	Mainframe, JCL, ISPF

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie die Dateiübertragung.	1. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon S3 S3-Konsole und wählen Sie dann im Navigationsbereich Buckets aus. 2. Wählen Sie den Bucket aus, der Ihrer Transfer Family zugeordnet ist. 3. Suchen Sie auf der Registerkarte „Objekte“ im Bereich „Objekte“ nach der Datei, die Sie vom Mainframe übertragen haben.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Automatisieren Sie den JCL-SFTP-Client.	Verwenden Sie den Job-Scheduler, um den JCL-SFTP-Client automatisch auszulösen. **Note** Sie können Mainframe-Job-Scheduler wie BMC Control-M oder CA Workload Automation verwenden, um Batch-Jobs für Dateiübertragungen auf der Grundlage von Zeit und anderen Abhängigkeiten von Batch-Jobs zu automatisieren.	Jobplaner

Zugehörige Ressourcen

- So funktioniert die AWS Transfer Family
- Mainframe-Modernisierung mit AWS

Sicherer und optimierter Benutzerzugriff in einer Db2-Verbunddatenbank auf AWS mithilfe vertrauenswürdiger Kontexte

Erstellt von Sai Parthasaradhi (AWS)

Übersicht

Viele Unternehmen migrieren ihre älteren Mainframe-Workloads zu Amazon Web Services (AWS). Diese Migration beinhaltet die Umstellung von IBM Db2 for z/OS-Datenbanken auf Db2 für Linux, Unix und Windows (LUW) auf Amazon Elastic Compute Cloud (Amazon). EC2 Während einer schrittweisen Migration von lokal zu AWS müssen Benutzer möglicherweise auf Daten in IBM Db2 z/OS und in Db2 LUW auf Amazon zugreifen, EC2 bis alle Anwendungen und Datenbanken vollständig auf Db2 LUW migriert sind. In solchen Szenarien für den Fernzugriff auf Daten kann die Benutzerauthentifizierung eine Herausforderung sein, da verschiedene Plattformen unterschiedliche Authentifizierungsmechanismen verwenden.

Dieses Muster beschreibt, wie Sie einen Verbundserver auf Db2 für LUW mit Db2 for z/OS als Remote-Datenbank einrichten. Das Muster verwendet einen vertrauenswürdigen Kontext, um die Identität eines Benutzers von Db2 LUW an Db2 z/OS weiterzugeben, ohne sich in der entfernten Datenbank erneut authentifizieren zu müssen. Weitere Informationen zu vertrauenswürdigen Kontexten finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Db2-Instance, die auf einer EC2 Amazon-Instance läuft
- Eine Remote-Datenbank von Db2 for z/OS, die lokal ausgeführt wird
- Das lokale Netzwerk, das über AWS Site-to-SiteVPN oder AWS AWS Direct Connect verbunden ist

Architektur

Zielarchitektur

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS-Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Mit AWS Site-to-Site VPN können Sie den Datenverkehr zwischen Instances, die Sie auf AWS starten, und Ihrem eigenen Remote-Netzwerk weiterleiten.

Andere Tools

- db2cli ist der Db2-Befehl für die interaktive Befehlszeilenschnittstelle (CLI).

Epen

Aktivieren Sie den Verbund in der Db2-LUW-Datenbank, die auf AWS ausgeführt wird

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie den Verbund auf der DB2 LUW-DB.	Führen Sie den folgenden Befehl aus, um den Verbund auf DB2 LUW zu aktivieren. `update dbm cfg using federated YES`	DBA
Starten Sie die Datenbank neu.	Führen Sie den folgenden Befehl aus, um die Datenbank neu zu starten. `db2stop force; db2start;`	DBA

Katalogisieren Sie die entfernte Datenbank

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Katalogisieren Sie das Remote-Db2 z/OS-Subs ystem.	Verwenden Sie den folgenden Beispielbefehl, um die entfernte Db2 z/OS-Date nbank auf Db2 LUW zu katalogisieren, die auf AWS ausgeführt wird. `catalog TCPIP NODE tcpnode REMOTE mainframehost SERVER mainframeport`	DBA
Katalogisieren Sie die entfernte Datenbank.	Verwenden Sie den folgenden Beispielbefehl, um die entfernte Datenbank zu katalogisieren. `catalog db dbnam1 as ndbnam1 at node tcpnode`	DBA

Erstellen Sie die Remoteserver-Definition

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sammeln Sie Benutzera nmeldeinformationen für die entfernte Db2 z/OS-Date nbank.	Bevor Sie mit den nächsten Schritten fortfahren, sammeln Sie die folgenden Informati onen: • Name des Db2 z/OS-Subs ystems — Der katalogis ierte Db2 z/OS-Name auf der LUW aus dem vorherige	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	n Schritt (zum Beispiel) `ndbnam1` • Db2 z/OS-Version — Die Version des Db2 z/OS-Subsystems (zum Beispiel) `12` • Db2 z/OS-Benutzer-ID — Der Benutzer mit der BIND-Berechtigung, die nur zum Erstellen der Serverdefinition benötigt wird (zum Beispiel) `dbuser1` • Db2 z/OS-Passwort — Das Passwort für `dbuser1` (zum Beispiel) `dbpasswd` • Db2 z/OS-Proxybenutzer — Die ID des Proxybenutzers, die verwendet wird, um eine vertrauenswürdige Verbindung herzustellen (z. B.) `zproxy` • Db2 z/OS Proxy-Passwort — Das Passwort für den `zproxy` Benutzer (zum Beispiel) `zproxy`	
Erstellen Sie den DRDA-Wrapper.	Führen Sie den folgenden Befehl aus, um den DRDA-Wrapper zu erstellen. `CREATE WRAPPER DRDA;`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Serverdef inition.	Führen Sie den folgenden Beispielbefehl aus, um die Serverdefinition zu erstellen. `CREATE SERVER ndbserver TYPE DB2/ZOS VERSION 12 WRAPPER DRDA AUTHORIZATION "dbuser1" PASSWORD "dbpasswd " OPTIONS ( DBNAME 'ndbnam1',FED_PROX Y_USER 'ZPROXY' );` In dieser Definition wird der Proxybenutzer `FED_PR0XY _USER` angegeben, der für den Aufbau vertrauen swürdiger Verbindungen zur Db2 z/OS-Datenbank verwendet wird. Die Benutzer-ID und das Kennwort für die Autorisierung sind nur für die Erstellung des Remoteser verobjekts in der Db2 LUW-Datenbank erforderlich. Sie werden später während der Laufzeit nicht verwendet.	DBA

Benutzerzuordnungen erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Benutzerz uordnung für den Proxybenu tzer.	Führen Sie den folgenden Befehl aus, um eine Benutzerz	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	uordnung für den Proxybenutzer zu erstellen. `CREATE USER MAPPING FOR ZPROXY SERVER ndbserver OPTIONS (REMOTE_AUTHID 'ZPROXY', REMOTE_PASSWORD 'zproxy');`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Benutzerzuordnungen für jeden Benutzer auf Db2 LUW.	Erstellen Sie Benutzerzuordnungen für alle Benutzer in der Db2 LUW-Datenbank auf AWS, die über den Proxybenutzer auf Remote-Daten zugreifen müssen. Führen Sie den folgenden Befehl aus, um die Benutzerzuordnungen zu erstellen. `CREATE USER MAPPING FOR PERSON1 SERVER ndbserver OPTIONS (REMOTE_AUTHID 'USERZID', USE_TRUSTED_CONTEXT 'Y');` Die Anweisung gibt an, dass ein Benutzer auf Db2 LUW (`PERSON1`) eine vertrauenswürdige Verbindung zur entfernten Db2 z/OS-Datenbank () herstellen kann. `USE_TRUSTED_CONTEXT 'Y'` Nachdem die Verbindung über den Proxybenutzer hergestellt wurde, kann der Benutzer mithilfe der Db2 z/OS-Benutzer-ID () auf die Daten zugreifen. `REMOTE_AUTHID 'USERZID'`	DBA

Erstellen Sie das vertrauenswürdige Kontextobjekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das vertrauen swürdige Kontextobjekt.	Verwenden Sie den folgenden Beispielbefehl, um das vertrauenswürdige Kontextob jekt in der entfernten Db2 z/ OS-Datenbank zu erstellen. `CREATE TRUSTED CONTEXT CTX_LUW_ZOS BASED UPON CONNECTIO N USING SYSTEM AUTHID ZPROXY ATTRIBUTES ( ADDRESS '10.10.10.10' ) NO DEFAULT ROLE ENABLE WITH USE FOR PUBLIC WITHOUT AUTHENTIC ATION;` In dieser Definition `CTX_LUW_ZOS` steht ein beliebiger Name für das vertrauenswürdige Kontextob jekt. Das Objekt enthält die Proxy-Benutzer-ID und die IP-Adresse des Servers, von dem die vertrauenswürdige Verbindung ausgehen muss. In diesem Beispiel ist der Server die Db2-LUW-D atenbank auf AWS. Sie können den Domainnam en anstelle der IP-Adresse verwenden. Die Klausel `WITH`	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`USE FOR PUBLIC WITHOUT AUTHENTICATION` gibt an, dass das Wechseln der Benutzer-ID bei einer vertrauenswürdigen Verbindung für jede Benutzer-ID zulässig ist. Ein Passwort muss nicht angegeben werden.	

Zugehörige Ressourcen

- IBM Resource Access Control Facility (RACF)
- IBM Db2 LUW-Verbund
- Vertrauenswürdige Kontexte

Zusätzliche Informationen

Vertrauenswürdige Db2-Kontexte

Ein vertrauenswürdiger Kontext ist ein Db2-Datenbankobjekt, das eine Vertrauensstellung zwischen einem Verbundserver und einem entfernten Datenbankserver definiert. Um eine vertrauenswürdige Beziehung zu definieren, spezifiziert der vertrauenswürdige Kontext Vertrauensattribute. Es gibt drei Arten von Vertrauensattributen:

- Die Systemautorisierungs-ID, die die erste Datenbankverbindungsanforderung stellt
- Die IP-Adresse oder der Domainname, von dem aus die Verbindung hergestellt wird
- Die Verschlüsselungseinstellung für die Datenkommunikation zwischen dem Datenbankserver und dem Datenbankclient

Eine vertrauenswürdige Verbindung wird hergestellt, wenn alle Attribute einer Verbindungsanforderung mit den Attributen übereinstimmen, die in einem vertrauenswürdigen Kontextobjekt angegeben sind, das auf dem Server definiert ist. Es gibt zwei Arten von vertrauenswürdigen Verbindungen: implizite und explizite. Nachdem eine implizite vertrauenswürdige Verbindung hergestellt wurde, erbt ein Benutzer eine Rolle, die ihm außerhalb des Geltungsbereichs

dieser vertrauenswürdigen Verbindungsdefinition nicht zur Verfügung steht. Nachdem eine explizite vertrauenswürdige Verbindung hergestellt wurde, können Benutzer auf dieselbe physische Verbindung mit oder ohne Authentifizierung umgeschaltet werden. Darüber hinaus können Db2-Benutzern Rollen zugewiesen werden, die Rechte spezifizieren, die nur innerhalb der vertrauenswürdigen Verbindung verwendet werden dürfen. Dieses Muster verwendet eine explizite vertrauenswürdige Verbindung.

Vertrauenswürdiger Kontext in diesem Muster

Nachdem das Muster vollständig ist, greift LUW PERSON1 auf Db2 mithilfe eines föderierten vertrauenswürdigen Kontextes auf Remotedaten von Db2 z/OS zu. Die Verbindung für PERSON1 wird über einen Proxybenutzer hergestellt, wenn die Verbindung von der IP-Adresse oder dem Domänennamen stammt, der in der vertrauenswürdigen Kontextdefinition angegeben ist. Nachdem die Verbindung hergestellt wurde, PERSON1 wird die entsprechende Db2 z/OS-Benutzer-ID ohne erneute Authentifizierung geändert, und der Benutzer kann auf Grundlage der für diesen Benutzer eingerichteten Db2-Berechtigungen auf die Daten oder Objekte zugreifen.

Vorteile verbundener vertrauenswürdiger Kontexte

- Bei diesem Ansatz wird das Prinzip der geringsten Rechte beibehalten, indem die Verwendung einer gemeinsamen Benutzer-ID oder Anwendungs-ID vermieden wird, für die eine Obermenge aller von allen Benutzern benötigten Rechte erforderlich wäre.
- Die tatsächliche Identität des Benutzers, der die Transaktion sowohl in der Verbunddatenbank als auch in der Remote-Datenbank durchführt, ist immer bekannt und kann überprüft werden.
- Die Leistung verbessert sich, da die physische Verbindung von allen Benutzern wiederverwendet wird, ohne dass sich der Verbundserver erneut authentifizieren muss.

Übertragung umfangreicher Db2 z/OS-Daten in CSV-Dateien nach Amazon S3

Erstellt von Bruno Sahinoglu (AWS), Ivan Schuster (AWS) und Abhijit Kshirsagar (AWS)

Übersicht

Ein Mainframe ist in vielen Unternehmen immer noch ein Aufzeichnungssystem, das eine riesige Menge an Daten enthält, darunter Stammdateneinheiten mit Aufzeichnungen über aktuelle und historische Geschäftstransaktionen. Es ist oft isoliert und die verteilten Systeme innerhalb desselben Unternehmens können nur schwer darauf zugreifen. Mit dem Aufkommen der Cloud-Technologie und der Demokratisierung von Big Data sind Unternehmen daran interessiert, die in den Mainframe-Daten verborgenen Erkenntnisse zu nutzen, um neue Geschäftsmöglichkeiten zu entwickeln.

Mit diesem Ziel möchten Unternehmen ihre Mainframe-Db2-Daten für ihre Amazon Web Services (AWS) Cloud-Umgebung öffnen. Die geschäftlichen Gründe sind vielfältig und die Übertragungsmethoden unterscheiden sich von Fall zu Fall. Möglicherweise ziehen Sie es vor, Ihre Anwendung direkt mit dem Mainframe zu verbinden, oder Sie ziehen es vor, Ihre Daten nahezu in Echtzeit zu replizieren. Wenn der Anwendungsfall darin besteht, ein Data Warehouse oder einen Data Lake zu speisen, ist das Vorhandensein einer up-to-date Kopie kein Problem mehr, und das in diesem Muster beschriebene Verfahren könnte ausreichend sein, insbesondere wenn Sie Lizenzkosten für Produkte von Drittanbietern vermeiden möchten. Ein weiterer Anwendungsfall könnte die Mainframe-Datenübertragung für ein Migrationsprojekt sein. In einem Migrationsszenario sind Daten für die Durchführung der funktionalen Äquivalenztests erforderlich. Der in diesem Beitrag beschriebene Ansatz ist eine kostengünstige Möglichkeit, die Db2-Daten in die AWS-Cloud-Umgebung zu übertragen.

Da Amazon Simple Storage Service (Amazon S3) einer der am stärksten integrierten AWS-Services ist, können Sie von dort aus auf die Daten zugreifen und mithilfe anderer AWS-Services wie Amazon Athena, AWS Lambda-Funktionen oder Amazon direkt Erkenntnisse gewinnen. QuickSight Sie können die Daten auch mithilfe von AWS Glue oder AWS Database Migration Service (AWS DMS) in Amazon Aurora oder Amazon DynamoDB laden. Vor diesem Hintergrund wird hier beschrieben, wie Db2-Daten in CSV-Dateien im ASCII-Format auf dem Mainframe entladen und die Dateien nach Amazon S3 übertragen werden.

Zu diesem Zweck wurden Mainframe-Skripte entwickelt, die bei der Generierung von Jobsteuerungssprachen (JCLs) helfen, mit denen Sie so viele Db2-Tabellen entladen und übertragen können, wie Sie benötigen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein Benutzer des IBM z/OS-Betriebssystems mit der Berechtigung, Restructured Extended Executor (REXX) - und JCL-Skripts auszuführen.
- Zugriff auf z/OS Unix System Services (USS) zur Generierung von privaten und öffentlichen SSH-Schlüsseln (Secure Shell).
- Ein beschreibbarer S3-Bucket. Weitere Informationen finden Sie unter Erstellen Sie Ihren ersten S3-Bucket in der Amazon S3 S3-Dokumentation.
- Ein SSH File Transfer Protocol (SFTP) -fähiger Server der AWS Transfer Family, der Service Managed als Identitätsanbieter und Amazon S3 als AWS-Speicherservice verwendet. Weitere Informationen finden Sie unter Erstellen eines SFTP-fähigen Servers in der Dokumentation zur AWS Transfer-Familie.

Einschränkungen

- Dieser Ansatz ist nicht für die Datensynchronisierung nahezu in Echtzeit oder in Echtzeit geeignet.
- Daten können nur von Db2 z/OS nach Amazon S3 verschoben werden, nicht umgekehrt.

Architektur

Quelltechnologie-Stack

- Mainframe, auf dem Db2 auf z/OS läuft

Zieltechnologie-Stack

- AWS Transfer Family
- Amazon S3
- Amazon Athena
- Amazon QuickSight
- AWS Glue
- Amazon Relational Database Service (Amazon RDS)
- Amazon Aurora

- Amazon Redshift

Quell- und Zielarchitektur

Das folgende Diagramm zeigt den Prozess zum Generieren, Extrahieren und Übertragen von Db2 z/OS-Daten im ASCII-CSV-Format in einen S3-Bucket.

1. Eine Liste von Tabellen wird für die Datenmigration aus dem Db2-Katalog ausgewählt.
2. Die Liste wird verwendet, um die Generierung von Entladejobs mit den numerischen Spalten und Datenspalten im externen Format voranzutreiben.
3. Die Daten werden dann mithilfe der AWS Transfer Family an Amazon S3 übertragen.
4. Ein AWS Glue-Auftrag zum Extrahieren, Transformieren und Laden (ETL) kann die Daten transformieren und im angegebenen Format in einen verarbeiteten Bucket laden, oder AWS Glue kann die Daten direkt in die Datenbank einspeisen.
5. Amazon Athena und Amazon QuickSight können verwendet werden, um die Daten abzufragen und zu rendern, um Analysen voranzutreiben.

Das folgende Diagramm zeigt einen logischen Ablauf des gesamten Prozesses.

1. Die erste JCL mit dem Namen TABNAME verwendet das Db2-Hilfsprogramm DSNTIAUL, um die Liste der Tabellen zu extrahieren und zu generieren, die Sie aus Db2 entladen möchten. Um Ihre Tabellen auszuwählen, müssen Sie die SQL-Eingabe manuell anpassen, um Filterkriterien auszuwählen und hinzuzufügen, die ein oder mehrere Db2-Schemas enthalten.
2. Die zweite JCL, REXXEXEC genannt, verwendet ein JCL-Skelett und das REXX-Programm, das zur Verfügung gestellt wird, um die vom JCL TABNAME erstellte Tabellenliste zu verarbeiten und eine JCL pro Tabellennamen zu generieren. Jede JCL enthält einen Schritt zum Entladen der Tabelle und einen weiteren Schritt zum Senden der Datei an den S3-Bucket mithilfe des SFTP-Protokolls.
3. Der letzte Schritt besteht darin, die JCL auszuführen, um die Tabelle zu entladen, und die Datei an AWS zu übertragen. Der gesamte Prozess kann mithilfe eines Schedulers vor Ort oder auf AWS automatisiert werden.

Tools

AWS-Services

- Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon Simple Storage Service (Amazon S3) analysieren können.
- Amazon Aurora ist eine vollständig verwaltete relationale Datenbank-Engine, die für die Cloud entwickelt wurde und mit MySQL und PostgreSQL kompatibel ist.
- AWS Glue ist ein vollständig verwalteter Service zum Extrahieren, Transformieren und Laden (ETL). Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben.
- Amazon QuickSight ist ein Business Intelligence (BI) -Service auf Cloud-Ebene, mit dem Sie Ihre Daten in einem einzigen Dashboard visualisieren, analysieren und melden können.
- Amazon Redshift ist ein verwalteter Data-Warehouse-Service im Petabyte-Bereich in der AWS-Cloud.
- Amazon Relational Database Service (Amazon RDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank in der AWS-Cloud.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Transfer Family ist ein sicherer Übertragungsservice, mit dem Sie Dateien in und aus AWS-Speicherservices übertragen können.

Mainframe-Tools

- Das SSH File Transfer Protocol (SFTP) ist ein sicheres Dateiübertragungsprotokoll, das die Fernanmeldung bei und die Dateiübertragung zwischen Servern ermöglicht. SSH bietet Sicherheit, indem es den gesamten Datenverkehr verschlüsselt.
- DSNTIAUL ist ein von IBM bereitgestelltes Beispielprogramm zum Entladen von Daten.
- DSNUTILB ist ein von IBM bereitgestelltes Batchprogramm für Dienstprogramme zum Entladen von Daten mit verschiedenen Optionen aus DSNTIAUL.
- z/OS OpenSSH ist ein Port von Open Source Software SSH, der auf dem Unix System Service unter dem IBM Betriebssystem z/OS läuft. SSH ist ein sicheres, verschlüsseltes Verbindungsprogramm zwischen zwei Computern, die in einem TCP/IP-Netzwerk laufen. Es bietet mehrere Dienstprogramme, darunter ssh-keygen.

- Das REXX-Skript (Restructured Extended Executor) wird verwendet, um die JCL-Generierung mit den Schritten Db2 Unload und SFTP zu automatisieren.

Code

Der Code für dieses Muster ist im unloaddb2-Repository verfügbar. GitHub

Bewährte Methoden

Beim ersten Entladen JCLs sollten die generierten Daten die gesamten Tabellendaten entladen.

Führen Sie nach dem ersten vollständigen Entladen inkrementelle Entladungen durch, um die Leistung zu verbessern und Kosten zu sparen. Aktualisieren Sie die SQL-Abfrage im JCL-Deck der Vorlage, um alle Änderungen am Entladevorgang zu berücksichtigen.

Sie können das Schema manuell oder mithilfe eines Skripts auf Lambda mit dem Db2-SYSPUNCH als Eingabe konvertieren. Für einen industriellen Prozess ist das AWS Schema Conversion Tool (SCT) die bevorzugte Option.

Verwenden Sie schließlich einen Mainframe-basierten Scheduler oder einen Scheduler auf AWS mit einem Agenten auf dem Mainframe, um den gesamten Prozess zu verwalten und zu automatisieren.

Epen

Richten Sie den S3-Bucket ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den S3-Bucket.	Anweisungen finden Sie unter Erstellen Sie Ihren ersten S3-Bucket.	Allgemeines AWS

Richten Sie den Transfer Family Family-Server ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen SFTP-fähigen Server.	Gehen Sie wie folgt vor, um einen SFTP-Server auf der	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	AWS Transfer Family Family-Konsole zu öffnen und zu erstellen: 1. Aktivieren Sie auf der Seite Protokolle auswählen das Kontrollkästchen SFTP (SSH File Transfer Protocol) — Dateiüber tragung über Secure Shell. 2. Wählen Sie für den Identität sanbieter die Option Service managed aus. 3. Wählen Sie für den Endpunkt Öffentlich zugänglich aus. 4. Wählen Sie für die Domain Amazon S3 aus. 5. Behalten Sie auf der Seite Zusätzliche Details konfiguri eren die Standardeinstellun gen bei. 6. Erstellen Sie den Server.	
Erstellen Sie eine IAM-Rolle für Transfer Family.	Um eine AWS Identity and Access Management (IAM) -Rolle für Transfer Family für den Zugriff auf Amazon S3 zu erstellen, folgen Sie den Anweisungen unter Erstellen einer IAM-Rolle und -Richtlin ie.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie einen vom Amazon S3 S3-Dienst verwalteten Benutzer hinzu.	Um den vom Service verwalteten Amazon S3 S3-Benutzer hinzuzufügen, folgen Sie den Anweisungen in der AWS-Dokumentation und verwenden Sie Ihre Mainframe-Benutzer-ID.	Allgemeines AWS

Sichern Sie das Kommunikationsprotokoll

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den SSH-Schlüssel.	Führen Sie in Ihrer Mainframe-USS-Umgebung den folgenden Befehl aus. `ssh-keygen -t rsa` **Note** Wenn Sie zur Eingabe einer Passphrase aufgefordert werden, lassen Sie sie leer.	Mainframe-Entwickler
Weisen Sie dem SSH-Ordner und den Schlüsseldateien die richtigen Autorisierungsstufen zu.	Standardmäßig werden die öffentlichen und privaten Schlüssel im Benutzerverzeichnis `/u/home/username/.ssh` gespeichert. Sie müssen den Schlüsseldateien die Autorisierung 644	Mainframe-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	und dem Ordner die Autorisierung 700 erteilen.
	
	`chmod 644 .ssh/id_rsa`
	`chmod 700 .ssh`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kopieren Sie den Inhalt des öffentlichen Schlüssels auf Ihren vom Amazon S3 S3-Dienst verwalteten Benutzer.	Um den von USS generierten Inhalt des öffentlichen Schlüssels zu kopieren, öffnen Sie die AWS Transfer Family Family-Konsole. 1. Klicken Sie im Navigationsbereich auf Servers (Server). 2. Wählen Sie den Bezeichner in der Spalte Server-ID aus, um die Serverdetails zu sehen 3. Wählen Sie unter Benutzer einen Benutzernamen aus, um die Benutzerdetails anzuzeigen 4. Wählen Sie unter Öffentliche SSH-Schlüssel die Option Öffentlichen SSH-Schlüssel hinzufügen aus, um den öffentlichen Schlüssel einem Benutzer hinzuzufügen. Geben Sie für den öffentlichen SSH-Schlüssel Ihren öffentlichen Schlüssel ein. Ihr Schlüssel wird vom Dienst validiert, bevor Sie Ihren neuen Benutzer hinzufügen können. 5. Wählen Sie Schlüssel hinzufügen.	Mainframe-Entwickler

Generieren Sie das JCLs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie die im Geltungsbereich enthaltene Db2-Tabellenliste.	Geben Sie Eingabe-SQL ein, um eine Liste der Tabellen zu erstellen, die für die Datenmigration vorgesehe n sind. In diesem Schritt müssen Sie Auswahlkr iterien angeben, indem Sie die DB2-Katalogtabelle SYSIBM.SYSTABLES mithilfe einer SQL WHERE-Klausel abfragen. Filter können so angepasst werden, dass sie ein bestimmtes Schema oder Tabellennamen enthalten, die mit einem bestimmten Präfix beginnen oder auf einem Zeitstempel für das inkrement elle Entladen basieren. Die Ausgabe wird in einem physikalischen sequentie llen Datensatz (PS) auf dem Mainframe erfasst. Dieser Datensatz dient als Eingabe für die nächste Phase der JCL-Generierung. Bevor Sie den JCL-TABNA MEN verwenden (Sie können ihn bei Bedarf umbenenne n), nehmen Sie die folgenden Änderungen vor:	Mainframe-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. <Jobcard>Ersetzen Sie es durch eine Jobklasse und einen Benutzer, der autorisiert ist, Db2-Diens tprogramme auszuführen. 2. Ersetzen Sie < HLQ1 > oder passen Sie die Namen der Ausgabe-Datasets an Ihre Site-Standards an. 3. Aktualisieren Sie den STEPLIB-Stack von PDSEs (partitionierter Datensatz erweitert) gemäß den Standards Ihrer Website. Das Beispiel in diesem Muster verwendet die IBM-Standardeinstellungen. 4. Ersetzen Sie den PLAN-Namen und die LIB durch Ihre installationsspezi fischen Werte. 5. Ersetzen Sie <Schema>u nd <Prefix>durch Ihre Auswahlkriterien für den Db2-Katalog. 6. Speichern Sie die resultier ende JCL in einer PDS-Bibliothek (partitionierter Datensatz). 7. Reichen Sie die JCL ein. Job zum Extrahieren der DB2-Tabellenliste	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<Jobcard>
	//*
	//* UNLOAD ALL THE TABLE
	 NAMES FOR A PARTICULAR
	 SCHEMA
	//*
	//STEP01 EXEC PGM=IEFBR
	14
	//*
	//DD1 DD DISP=(MOD
	,DELETE,DELETE),
	// UNIT=SYSDA,
	// SPACE=(1000,
	(1,1)),
	// DSN=<HLQ1
	>.DSN81210.TABLIST
	//*
	//DD2 DD DISP=(MOD
	,DELETE,DELETE),
	// UNIT=SYSDA,
	// SPACE=(1000,
	(1,1)),
	// DSN=<HLQ1
	>.DSN81210.SYSPUNCH
	//*
	//UNLOAD EXEC PGM=IKJEF
	T01,DYNAMNBR=20
	//SYSTSPRT DD
	 SYSOUT=*
	//STEPLIB DD
	 DISP=SHR,DSN=DSNC1
	0.DBCG.SDSNEXIT
	// DD DISP=SHR,
	DSN=DSNC10.SDSNLOAD
	// DD DISP=SHR,
	DSN=CEE.SCEERUN
	// DD DISP=SHR,
	DSN=DSNC10.DBCG.RU
	NLIB.LOAD
	//SYSTSIN DD *
	  DSN SYSTEM(DBCG)	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> RUN PROGRAM(D
	SNTIAUL) PLAN(DSNT
	IB12) PARMS('SQL') -
	       LIB('DSNC
	10.DBCG.RUNLIB.LOAD')
	  END
	//SYSPRINT DD SYSOUT=*
	//*
	//SYSUDUMP DD SYSOUT=*
	//*
	//SYSREC00 DD DISP=(NEW
	,CATLG,DELETE),
	// UNIT=SYSD
	A,SPACE=(32760,(10
	00,500)),
	// DSN=<HLQ1
	>.DSN81210.TABLIST
	//*
	//SYSPUNCH DD DISP=(NEW
	,CATLG,DELETE),
	// UNIT=SYSD
	A,SPACE=(32760,(10
	00,500)),
	// VOL=SER=S
	CR03,RECFM=FB,LREC
	L=120,BLKSIZE=12
	// DSN=<HLQ1
	>.DSN81210.SYSPUNCH
	//*
	//SYSIN DD *
	   SELECT CHAR(CREA
	TOR), CHAR(NAME)
	     FROM SYSIBM.SY
	STABLES
	    WHERE OWNER =
	 '<Schema>'
	      AND NAME LIKE
	 '<Prefix>%'
	      AND TYPE = 'T';
	/*</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die JCL-Vorlagen.	Die mit diesem Muster bereitgestellten JCL-Vorlagen enthalten eine generische Job-Card und Bibliotheksnamen. Die meisten Mainframe-Websites werden jedoch ihre eigenen Benennung sstandards für Datensatz namen, Bibliotheksnamen und Jobkarten haben. Beispiels weise kann eine bestimmte Jobklasse erforderlich sein, um Db2-Jobs auszuführen. Das Job Entry Subsystem implementiert JES2 und JES3 kann zusätzliche Änderungen auferlegen. Standard-Ladebibli otheken haben möglicher weise einen anderen ersten Qualifier als `SYS1` den IBM-Standard. Passen Sie die Vorlagen daher so an, dass sie Ihre standortspezifischen Standards berücksichtigen, bevor Sie sie ausführen. Nehmen Sie die folgenden Änderungen am Grundgerüst JCL UNLDSKEL vor: 1. Ändern Sie die Job-Card mit einer Jobklasse und einem Benutzer, die autorisiert sind, Db2-Diens tprogramme auszuführen.	Mainframe-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Passen Sie die Namen der Ausgabe-Datasets an Ihre Site-Standards an. 3. Aktualisieren Sie den STEPLIB-Stack von PDSEs gemäß Ihren Site-Stan dards. Das Beispiel in diesem Muster verwendet die IBM-Standardeinste llungen. 4. Ersetzen Sie es durch <DSN> den Namen und die Korrelations-ID Ihres Db2-Subsystems. 5. Speichern Sie die resultier ende JCL in einer PDS-Bibliothek, die Teil Ihres ISPSLIB-Stacks ist, der Standard-Skeleton-Vorlagenbibliothek für ISPF. Entladen und SFTP-JCL-Skelett `//&USRPFX.U JOB (DB2UNLOAD),'JOB', CLASS=A,MSGCLASS=A, //  TIME=1440 ,NOTIFY=&USRPFX //* DELETE DATASETS //STEP01  EXEC PGM=IEFBR14 //DD01  DD DISP=(MOD ,DELETE,DELETE), //  UNIT=SYSD A,`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`//  SPACE=(TRK,(1,1)),`
	`// DSN=&USRPFX..DB2.PUNCH.&JOBNAME`
	`//DD02  DD DISP=(MOD,DELETE,DELETE),`
	`//  UNIT=SYSDA,`
	`//  SPACE=(TRK,(1,1)),`
	`// DSN=&USRPFX..DB2.UNLOAD.&JOBNAME`
	`//*`
	`//* RUNNING DB2 EXTRACTION BATCH JOB FOR AWS DEMO`
	`//*`
	`//UNLD01  EXEC PGM=DSNUTILB,REGION=0M,`
	`// PARM='<DSN>,UNLOAD'`
	`//STEPLIB  DD DISP=SHR,DSN=DSNC10.DBCG.SDSNEXIT`
	`//  DD  DISP=SHR,DSN=DSNC10.SDSNLOAD`
	`//SYSPRINT DD  SYSOUT=*`
	`//UTPRINT  DD  SYSOUT=*`
	`//SYSOUT  DD  SYSOUT=*`
	`//SYSPUN01 DD DISP=(NEW,CATLG,DELETE),`
	`//  SPACE=(CYL,(1,1),RLSE),`
	`// DSN=&USRPFX..DB2.PUNCH.&JOBNAME`
	`//SYSREC01 DD DISP=(NEW,CATLG,DELETE),`
	`// SPACE=(CYL,(10,50),RLSE),	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`// DSN=&USRPFX..DB2.U`
	`NLOAD.&JOBNAME`
	`//SYSPRINT DD SYSOUT=*`
	`//SYSIN DD *`
	`UNLOAD`
	`DELIMITED COLDEL ','`
	`FROM TABLE &TABNAME`
	`UNLDDN SYSREC01`
	`PUNCHDDN SYSPUN01`
	`SHRLEVEL CHANGE`
	`ISOLATION UR;`
	`/*`
	`//*`
	`//* FTP TO AMAZON S3`
	`BACKED FTP SERVER IF`
	`UNLOAD WAS SUCCESSFUL`
	`//*`
	`//SFTP EXEC PGM=BPXBA`
	`TCH,COND=(4,LE),RE`
	`GION=0M`
	`//STDPARM DD *`
	`SH cp "//'&USRP`
	`FX..DB2.UNLOAD.&JO`
	`BNAME'"`
	`&TABNAME..csv;`
	`echo "ascii`
	`" >> uplcmd;`
	`echo "PUT &TABNAME.`
	`.csv " >>>> uplcmd;`
	`sftp -b uplcmd -i .ssh/`
	`id_rsa &FTPUSER.`
	`@&FTPSITE;`
	`rm &TABNAME..csv;`
	`//SYSPRINT DD SYSOUT=*`
	`//STDOUT DD SYSOUT=*`
	`//STDENV DD *`
	`//STDERR DD SYSOUT=*`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie die Mass Unload JCL.	Dieser Schritt beinhaltet die Ausführung eines REXX-Skripts in einer ISPF-Umgebung mithilfe von JCL. Geben Sie die Liste der im ersten Schritt erstellten Tabellen im Gültigkeitsbereich als Eingabe für die Massengenerierung von JCL anhand des Namens an. `TABLIST DD` Die JCL generiert eine neue JCL pro Tabellennamen in einem benutzerdefinierten partitionierten Datensatz, der anhand des Namens angegeben wird. `ISPFILE DD` Ordnen Sie diese Bibliothek vorher zu. Jede neue JCL besteht aus zwei Schritten: einem Schritt zum Entladen der Db2-Tabelle in eine Datei und einem Schritt zum Senden der Datei an den S3-Bucket. Nehmen Sie die folgenden Änderungen in der JCL REXXEXEC vor (Sie können den Namen ändern): 1. `Job card user ID`Ersetzen Sie es durch eine Mainframe-Benutzer-ID, die über Entladeberechtigungen für die Tabellen verfügt. Ersetzen	Mainframe-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	SieSYSPROC,, ISPPLIB ISPSLIBISPMLIB, und geben Sie den ISPTLIB <HLQ1> Wert ein oder passen Sie sie an, DSN damit sie den Standards Ihrer Website entsprechen. Um Ihre installationsspezifischen Werte herauszufinden, verwenden Sie den Befehl. TSO ISRDDN 2. <MFUSER>Ersetzen Sie ihn durch eine Benutzer-ID, die in Ihrer Installation über Rechte zur Ausführung von Jobs verfügt. 3. <FTPUSER> Ersetzen Sie es durch eine Benutzer-ID, die in Ihrer Installation über die USS- und FTP-Rechte verfügt. Es wird davon ausgegangen, dass sich diese Benutzer-ID und ihre SSH-Sicherheitsschlüssel im entsprechenden Unix Systems Services-Verzeichnis auf dem Mainframe befinden. 4. <AWS TransferFamily IP>Ersetzen Sie es durch die IP-Adresse der AWS Transfer Family oder den Domainnamen. Diese	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Adresse wird für den SFTP-Schritt verwendet.
	5. Reichen Sie die JCL ein, nachdem Sie die Standardunterkunft vor Ort beantragt und das REXX-Programm wie unten beschrieben aktualisiert haben.
	
	Auftrag zur Massengenerierung von JCL
	
	`//RUNREXX JOB (CREATEJCL),'RUNS ISPF TABLIST',`
	`CLASS=A,MSGCLASS=A,`
	`//         TIME=1440`
	`,NOTIFY=&SYSUID`
	`//* Most of the values`
	`  required can be updated`
	`  to your site specific`
	`//* values using the`
	`  command 'TSO ISRDDN' in`
	`  your ISPF session.`
	`//* Update all the lines`
	`  tagged with //update`
	`  marker to desired`
	`//* site specific`
	`  values.`
	`//ISPF EXEC PGM=IKJEF`
	`T01,REGION=2048K,D`
	`YNAMNBR=25`
	`//SYSPROC   DD`
	`  DISP=SHR,DSN=USER.`
	`Z23D.CLIST`
	`//SYSEXEC   DD`
	`  DISP=SHR,DSN=<HLQ1`
	`>.TEST.REXXLIB`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`//ISPPLIB DD DISP=SHR,DSN=ISP.SISPPENU`
	`//ISPSLIB DD DISP=SHR,DSN=ISP.SISPSENU`
	`// DD DISP=SHR,DSN=<HLQ1>.TEST.ISPSLIB`
	`//ISPMLIB DD DSN=ISP.SISPMENU,DISP=SHR`
	`//ISPTLIB DD DDNAME=ISPTABL`
	`// DD DSN=ISP.SISPTENU,DISP=SHR`
	`//ISPTABL DD LIKE=ISP.SISPTENU,UNIT=VIO`
	`//ISPPROF DD LIKE=ISP.SISPTENU,UNIT=VIO`
	`//ISPLOG DD SYSOUT=*,RECFM=VA,LRECL=125`
	`//SYSPRINT DD SYSOUT=*`
	`//SYSTSPRT DD SYSOUT=*`
	`//SYSUDUMP DD SYSOUT=*`
	`//SYSDBOUT DD SYSOUT=*`
	`//SYSTSPRT DD SYSOUT=*`
	`//SYSUDUMP DD SYSOUT=*`
	`//SYSDBOUT DD SYSOUT=*`
	`//SYSHELP DD DSN=SYS1.HELP,DISP=SHR`
	`//SYSOUT DD SYSOUT=*`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>//* Input list of
	tablenames
	//TABLIST DD
	DISP=SHR,DSN=<HLQ1
	>.DSN81210.TABLIST
	//* Output pds
	//ISPFILE DD
	DISP=SHR,DSN=<HLQ1
	>.TEST.JOBGEN
	//SYSTSIN DD *
	ISPSTART CMD(ZSTEPS
	<MFUSER> <FTPUSER> <AWS
	TransferFamily IP>)
	/*</pre>
	Bevor Sie das REXX-Skript verwenden, nehmen Sie die folgenden Änderungen vor:
	1. Speichern Sie das REXX-Skript in einer PDS-Bibliothek, die unter dem SYSEXEC Stack in der JCL REXXEXEC definiert ist, die im vorherigen Schritt bearbeitet wurde, mit ZSTEPS als Mitgliedsnamen. Wenn Sie es umbenennen möchten, sollten Sie die JCL entsprechend Ihren Bedürfnissen aktualisieren.
	2. Dieses Skript verwendet die Trace-Option, um zusätzliche Informationen zu drucken, falls Fehler auftreten. Sie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	können stattdessen nach den TSO Anweisungen EXECIOISPEXEC, und Fehlerbehandlungscode hinzufügen und die Trace-Zeile entfernen. 3. Dieses Skript generiert Elementnamen mithilfe der L0Dnnnnn Benennung skonvention, die bis zu 100.000 Mitglieder unterstützen kann. Wenn Sie mehr als 100.000 Tabellen haben, verwenden Sie ein kürzeres Präfix und passen Sie die Zahlen in der tempjob Anweisung an. STEPS REX-Skript `/*REXX - - -

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"EXECIO * DISKR
	TABLIST (STEM LINE.
	FINIS"
	DO I = 1 TO LINE.0
	Say I
	suffix = I
	Say LINE.i
	Parse var LINE.i
	schema table rest
	tabname =
	schema !! "." !! table
	Say tabname
	tempjob= "LOD" !!
	RIGHT("0000" !! i, 5)
	jobname=tempjob
	Say tempjob
	ADDRESS ISPEXEC
	"FTOPEN "
	ADDRESS ISPEXEC
	"FTINCL UNLDSKEL"
	/* member will be
	saved in ISPDSN library
	allocated in JCL */
	ADDRESS ISPEXEC
	"FTCLOSE NAME("tem
	pjob")"
	END
	
	ADDRESS TSO "FREE
	F(TABLIST) "
	ADDRESS TSO "FREE
	F(ISPFILE) "
	
	exit 0</pre>	

Führen Sie das aus JCLs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den Schritt Db2 Unload aus.	Nach der JCL-Generierung werden Sie über so viele Tabellen verfügen, JCLs wie Sie haben, die entladen werden müssen. In dieser Geschichte werden die Struktur und die wichtigst en Schritte anhand eines von JCL generierten Beispiels erklärt. Von Ihrer Seite aus ist keine Aktion erforderlich. Die folgenden Informationen dienen nur als Referenz. Wenn Sie JCLs die im vorherigen Schritt generiert en Daten einreichen möchten, fahren Sie mit dem Abschnitt LODnnnnn JCLs Aufgabe einreichen fort. Wenn Sie Db2-Daten mithilfe einer JCL mit dem von IBM bereitgestellten Hilfsprog ramm DSNUTILB Db2 entladen, müssen Sie sicherstellen, dass die entladenen Daten keine komprimierten numerischen Daten enthalten. Verwenden Sie dazu den DSNUTILB-Parameter. `DELIMITED`	Mainframe-Entwickler, Systemingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Der `DELIMITED` Parameter unterstützt das Entladen der Daten im CSV-Format, indem er ein Zeichen als Trennzeichen und doppelte Anführungszeichen für das Textfeld hinzufügt, die Auffüllung in der VARCHAR-Spalte entfernt und alle numerischen Felder, einschließlich der DATE-Felder, in ein EXTERNES FORMAT konvertiert. Das folgende Beispiel zeigt, wie der Entladeschritt in der generierten JCL aussieht, wobei das Komma als Trennzeichen verwendet wird. `UNLOAD DELIMITED COLDEL ',' FROM TABLE SCHEMA_NAME.TBNAME UNLDDN SYSREC01 PUNCHDDN SYSPUN01 SHRLEVEL CHANGE ISOLATION UR;`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den SFTP-Schritt aus.	Um das SFTP-Protokoll von einer JCL aus zu verwenden, verwenden Sie das BPXBATCH-Hilfsprogramm. Das SFTP-Hilfsprogramm kann nicht direkt auf die MVS-Datensätze zugreifen. Sie können den Befehl copy (`cp`) verwenden, um die sequenzielle Datei in das USS-Verzeichnis `&USRPFX..DB2.UNLOAD.&JOBNAME` zu kopieren, wo sie gespeichert wird. `&TABNAME..csv` Führen Sie den `sftp` Befehl mit dem privaten Schlüssel (`id_rsa`) und der RACF-Benutzer-ID als Benutzernamen aus, um eine Verbindung mit der IP-Adresse der AWS Transfer Family herzustellen. `SH cp "//'&USRPFX..DB2.UNLOAD.&JOBNAME'" &TABNAME..csv; echo "ascii " >> uplcmd; echo "PUT &TABNAME..csv " >>>> uplcmd; sftp -b uplcmd -i .ssh/id_rsa &FTPUSER.@&FTP_TF_SITE;`	Mainframe-Entwickler, Systemingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`rm &TABNAME..csv;`	
Reichen Sie das LODnnnnn JCLs ein.	Die vorherige JCL hat alle LODnnnnn JCL-Tabellen generiert, die entladen, in CSV umgewandelt und in den S3-Bucket übertragen werden müssen. Führen Sie den `submit` Befehl für alle aus JCLs , die generiert wurden.	Mainframe-Entwickler, Systemingenieur

Zugehörige Ressourcen

Weitere Informationen zu den verschiedenen in diesem Dokument verwendeten Tools und Lösungen finden Sie im Folgenden:

- z/OS OpenSSH-Benutzerhandbuch
- Db2 z/OS — Beispiel für UNLOAD-Steueranweisungen
- Db2 z/OS — Entladen von durch Trennzeichen getrennten Dateien
- Transfer Family — Erstellen Sie einen SFTP-fähigen Server
- Transfer Family — Arbeit mit dienstverwalteten Benutzern

Zusätzliche Informationen

Nachdem Sie Ihre Db2-Daten auf Amazon S3 gespeichert haben, haben Sie viele Möglichkeiten, neue Erkenntnisse zu gewinnen. Da Amazon S3 in AWS-Datenanalyse-Services integriert ist, können Sie diese Daten frei verwenden oder auf der verteilten Seite verfügbar machen. Sie können z. B. Folgendes tun:

- Erstellen Sie einen Data Lake auf Amazon S3 und gewinnen Sie wertvolle Erkenntnisse mithilfe query-in-place von Analyse- und Machine-Learning-Tools, ohne die Daten verschieben zu müssen.

- Initiieren Sie eine Lambda-Funktion, indem Sie einen Verarbeitungsworkflow nach dem Upload einrichten, der in die AWS Transfer Family integriert ist.
- Entwickeln Sie neue Microservices für den Zugriff auf Daten in Amazon S3 oder in einer vollständig verwalteten Datenbank mithilfe von AWS Glue, einem serverlosen Datenintegrationsservice, der es einfach macht, Daten für Analysen, maschinelles Lernen und Anwendungsentwicklung zu entdecken, aufzubereiten und zu kombinieren.

In einem Anwendungsfall für die Migration können Sie, da Sie beliebige Daten vom Mainframe auf S3 übertragen können, wie folgt vorgehen:

- Mit Amazon S3 Glacier und S3 Glacier Deep Archive können Sie die physische Infrastruktur außer Betrieb nehmen und eine kostengünstige Datenarchivierungsstrategie entwickeln.
- Entwickeln Sie skalierbare, langlebige und sichere Sicherungs- und Wiederherstellungslösungen mit Amazon S3 und anderen AWS-Services wie S3 Glacier und Amazon Elastic File System (Amazon EFS), um bestehende lokale Funktionen zu erweitern oder zu ersetzen.

Mehr Muster

- Stellen Sie die Security Automations for AWS WAF Solution mithilfe von Terraform bereit
- Replizieren Sie Mainframe-Datenbanken mithilfe von Precisely Connect nach AWS

Verwaltung

Themen

- Kostenmanagement
- Datenverarbeitung in Hochleistung
- Hybride Cloud
- Management & Governance
- Nachrichtenübermittlung und Kommunikation

Kostenmanagement

Themen

- Erstellen Sie mit dem AWS Cost Explorer detaillierte Kosten- und Nutzungsberichte für AWS Glue-Jobs
- Erstellen Sie mit dem AWS Cost Explorer detaillierte Kosten- und Nutzungsberichte für Amazon EMR-Cluster
- Mehr Muster

Erstellen Sie mit dem AWS Cost Explorer detaillierte Kosten- und Nutzungsberichte für AWS Glue-Jobs

Erstellt von Parijat Bhide (AWS) und Aromal Raj Jayarajan (AWS)

Übersicht

Dieses Muster zeigt, wie Sie die Nutzungskosten von AWS Glue Glue-Datenintegrationsaufträgen verfolgen können, indem Sie benutzerdefinierte Kostenzuweisungs-Tags konfigurieren. Sie können diese Tags verwenden, um detaillierte Kosten- und Nutzungsberichte im AWS Cost Explorer für Jobs in mehreren Dimensionen zu erstellen. Sie können beispielsweise die Nutzungskosten auf Team-, Projekt- oder Kostenstellenebene verfolgen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein oder mehrere AWS Glue Glue-Jobs, für die benutzerdefinierte Tags aktiviert sind

Architektur

Zieltechnologie-Stack

- AWS Glue
- AWS Cost Explorer

Das folgende Diagramm zeigt, wie Sie Tags anwenden können, um die Nutzungskosten für AWS Glue Glue-Jobs nachzuverfolgen.

Das Diagramm zeigt den folgenden Workflow:

1. Ein Dateningenieur oder AWS-Administrator erstellt benutzerdefinierte Kostenzuweisungs-Tags für die AWS Glue-Jobs.
2. Ein AWS-Administrator aktiviert die Tags.
3. Die Tags melden Metadaten an AWS Cost Explorer.

Tools

- AWS Glue ist ein vollständig verwalteter Service zum Extrahieren, Transformieren und Laden (ETL). Er hilft Ihnen dabei, Daten zuverlässig zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben.
- Mit AWS Cost Explorer können Sie Ihre AWS-Kosten und -Nutzung anzeigen und analysieren.

Epen

Erstellen und aktivieren Sie Tags für Ihre AWS Glue Glue-Jobs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie benutzerdefinierte Kostenzuweisungs-Tags für Ihre AWS Glue Glue-Jobs.	So fügen Sie Tags zu einem vorhandenen AWS Glue Glue-Job hinzu 1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die AWS Glue-Konsole. 2. Wählen Sie im linken Navigationsbereich unter ETL die Option Jobs aus. 3. Wählen Sie im Bereich „Ihre Jobs“ den Namen des Jobs aus, den Sie taggen möchten. 4. Wählen Sie die Registerkarte Job details (Auftragsdetails) aus. Erweitern Sie dann den Bereich Erweiterte Eigenschaften. 5. Wählen Sie für Tags die Option Neues Tag hinzufügen aus.	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Geben Sie unter Schlüssel einen Namen für Ihr Tag ein. 7. (Optional) Geben Sie unter Wert einen Wert ein, den Sie dem Schlüssel zuordnen möchten. 8. (Optional) Wiederholen Sie die Schritte 5 bis 7 für jedes Tag, das Sie für den Job erstellen möchten. 9. Wählen Sie Speichern. So fügen Sie Tags zu einem neuen AWS Glue Glue-Job hinzu 1. Erstellen Sie einen neuen AWS Glue Glue-Job auf der Grundlage Ihrer Anwendungsfallanfo rderungen. Anweisungen finden Sie unter Arbeiten mit Aufträgen auf der AWS Glue Glue-Konsole im AWS Glue Glue-Entwicklerhan dbuch. 2. Wenn Sie die Einstellu ngen für die Auftragsd etails konfigurieren, folgen Sie den Schritten 4-9 im Abschnitt So fügen Sie Tags zu einem vorhanden	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en AWS Glue Glue-Job hinzu. **Note** Weitere Informationen finden Sie unter AWS-Tags in AWS Glue im AWS Glue Developer Guide.	
Aktivieren Sie die benutzerdefinierten Tags für die Kostenzuweisung.	Folgen Sie den Anweisungen unter Aktivierung von benutzerdefinierten Kostenzuweisungs-Tags im AWS-Abrechnungsbenutzerhandbuch.	AWS-Administrator

Erstellen Sie Kosten- und Nutzungsberichte für Ihre AWS Glue Glue-Jobs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Kosten- und Nutzungsberichte für Ihre AWS Glue Glue-Jobs mithilfe von Tag-Filtern in AWS Cost Explorer.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS Cost Management-Konsole. 2. Wählen Sie im linken Navigationsbereich Berichte aus. 3. Wählen Sie Neuen Bericht erstellen aus. 4. Wählen Sie unter Berichtstyp auswählen die Option	Allgemein AWS, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Kosten und Nutzung (empfohlen) aus. Wählen Sie dann Bericht erstellen aus. 5. Wählen Sie für Filter die Option Service aus. Das Drop-down-Menü „Service“ wird angezeigt. 6. Aktivieren Sie die Kontrollk ästchen neben Glue. Wählen Sie dann Filter anwenden aus. 7. Wählen Sie für Filter die Option Tag aus. Das Drop-down-Menü „Tag“ wird angezeigt. 8. Wählen Sie Team. Aktiviere n Sie dann die Kontrollk ästchen neben den Teams, denen Sie Tags zugewiese n haben. Schließe alle Teams aus, denen du keine Tags zugewiesen hast. Wählen Sie dann Filter anwenden aus. 9. Wählen Sie oben im Diagramm die Option Tag aus. Wählen Sie dann die Tags für die AWS Glue Glue-Jobs aus, für die Sie einen Bericht erstellen möchten. 10. Wählen Sie oben im Diagramm die Dropdownl	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	iste Letzte 3 Monate aus und wählen Sie den Zeitraum aus, den der Bericht abdecken soll. Wählen Sie dann das Drop-down-Menü „Monatlich “ und wählen Sie aus, wie die Einzelposten im Bericht basierend auf dem Zeitrahmen aggregiert werden sollen. 11. Wählen Sie Save as (Speichern unter) aus. Geben Sie dann einen Titel für Ihren Bericht ein. 12. Wählen Sie Bericht speichern. Weitere Informationen finden Sie unter Erkunden Ihrer Daten mit Cost Explorer im AWS Cost Management-Benutzerhandbuch.	

Erstellen Sie mit dem AWS Cost Explorer detaillierte Kosten- und Nutzungsberichte für Amazon EMR-Cluster

Erstellt von Parijat Bhide (AWS) und Aromal Raj Jayarajan (AWS)

Übersicht

Dieses Muster zeigt, wie Sie die Nutzungskosten von Amazon EMR-Clustern verfolgen können, indem Sie benutzerdefinierte Kostenzuweisungs-Tags konfigurieren. Sie können diese Tags verwenden, um detaillierte Kosten- und Nutzungsberichte in AWS Cost Explorer für Cluster in mehreren Dimensionen zu erstellen. Sie können beispielsweise die Nutzungskosten auf Team-, Projekt- oder Kostenstellenebene verfolgen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein oder mehrere EMR-Cluster, für die benutzerdefinierte Tags aktiviert sind

Architektur

Zieltechnologie-Stack

- Amazon EMR
- AWS Cost Explorer

Zielarchitektur

Das folgende Diagramm zeigt, wie Sie Tags anwenden können, um die Nutzungskosten für bestimmte Amazon EMR-Cluster nachzuverfolgen.

Das Diagramm zeigt den folgenden Workflow:

1. Ein Dateningenieur oder AWS-Administrator erstellt benutzerdefinierte Kostenzuweisungs-Tags für die Amazon EMR-Cluster.
2. Ein AWS-Administrator aktiviert die Tags.
3. Die Tags melden Metadaten an AWS Cost Explorer.

Tools

Tools

- Amazon EMR ist eine verwaltete Cluster-Plattform, die die Ausführung von Big-Data-Frameworks auf AWS vereinfacht, um große Datenmengen zu verarbeiten und zu analysieren.
- Mit AWS Cost Explorer können Sie Ihre AWS-Kosten und -Nutzung anzeigen und analysieren.

Epen

Erstellen und aktivieren Sie Tags für Ihre Amazon EMR-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie benutzerd efinierte Kostenzuweisungs-Tags für Ihre Amazon EMR-Cluster.	So fügen Sie Tags zu einem vorhandenen Amazon EMR-Cluster hinzu Folgen Sie den Anweisungen unter Hinzufügen von Tags zu einem vorhandenen Cluster im Amazon EMR Managemen t Guide. So fügen Sie Tags zu einem neuen Amazon EMR-Cluster hinzu Folgen Sie den Anweisungen unter Hinzufügen von Tags zu einem neuen Cluster im Amazon EMR Management Guide. Weitere Informationen zur Einrichtung eines Amazon EMR-Clusters finden Sie unter Planen und Konfigurieren von	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Clustern im Amazon EMR Management Guide.	
Aktivieren Sie die benutzerdefinierten Tags für die Kostenzuweisung.	Folgen Sie den Anweisungen unter Aktivierung von benutzerdefinierten Kostenzuweisungs-Tags im AWS-Abrechnungsbenutzerhandbuch.	AWS-Administrator

Erstellen Sie Kosten- und Nutzungsberichte für Ihre Amazon EMR-Cluster

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Kosten- und Nutzungsberichte für Ihre Amazon EMR-Cluster mithilfe von Tag-Filtern in AWS Cost Explorer.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS Cost Management-Konsole. 2. Wählen Sie im linken Navigationsbereich Berichte aus. 3. Wählen Sie Neuen Bericht erstellen aus. 4. Wählen Sie unter Berichtstyp auswählen die Option Kosten und Nutzung (empfohlen) aus. Wählen Sie dann Bericht erstellen aus. 5. Wählen Sie für Filter die Option Service aus. Das Drop-down-Menü Service wird angezeigt.	Allgemein AWS, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Aktivieren Sie die Kontrollkästchen neben EMR (Elastic MapReduce) und EC2-Instances (Elastic Compute Cloud — Compute). Wählen Sie dann Filter anwenden. 7. Wählen Sie für Filter die Option Tag aus. Das Drop-down-Menü „Tag“ wird angezeigt. 8. Wählen Sie Team. Aktivieren Sie dann die Kontrollkästchen neben den Teams, denen Sie Tags zugewiesen haben. Schließe alle Teams aus, denen du keine Tags zugewiesen hast. Wählen Sie dann Filter anwenden aus. 9. Wählen Sie oben im Diagramm die Option Tag aus. Wählen Sie dann die Tags für die Amazon EMR-Cluster aus, für die Sie einen Bericht erstellen möchten. 10. Wählen Sie oben im Diagramm die Dropdownliste Letzte 3 Monate und wählen Sie den Zeitraum aus, den der Bericht abdecken soll. Wählen Sie dann das Drop-down-Menü	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	„Monatlich“ und wählen Sie aus, wie die Einzelposten im Bericht basierend auf dem Zeitrahmen aggregiert werden sollen. 11. Wählen Sie Save as (Speichern unter) aus. Geben Sie dann einen Titel für Ihren Bericht ein. 12. Wählen Sie Bericht speichern. Weitere Informationen finden Sie unter Erkunden Ihrer Daten mit Cost Explorer im AWS Cost Management-Benutzerhandbuch.	

Mehr Muster

- Automatisieren Sie den AWS Infrastrukturbetrieb mithilfe von Amazon Bedrock
- Automatische Inventarisierung von AWS Ressourcen für mehrere Konten und Regionen
- Automatisieren Sie die Erstellung von AppStream 2.0-Ressourcen mit AWS CloudFormation
- Automatisches Archivieren von Elementen in Amazon S3 mithilfe von DynamoDB TTL
- Automatisches Stoppen und Starten einer Amazon RDS-DB-Instance mithilfe von AWS Systems Manager Maintenance Windows
- Erstellen Sie detaillierte Kosten- und Nutzungsberichte für Amazon RDS und Amazon Aurora
- Löschen Sie ungenutzte Amazon EBS-Volumes mit AWS Config und AWS Systems Manager
- Schätzung der Speicherkosten für eine Amazon DynamoDB-Tabelle
- Schätzen Sie die Kosten einer DynamoDB-Tabelle für On-Demand-Kapazität
- Richten Sie ereignisgesteuertes Auto Scaling in Amazon EKS mithilfe von Amazon EKS Pod Identity und KEDA ein
- Koordinieren Sie die Ressourcenabhängigkeit und die Aufgabenausführung mithilfe des AWS Fargate WaitCondition Hook-Konstrukts

Datenverarbeitung in Hochleistung

Themen

- Stellen Sie mithilfe von Terraform und DRA ein Lustre-Dateisystem für die Hochleistungsdatenverarbeitung bereit
- Richten Sie ein Grafana-Monitoring-Dashboard für AWS ein ParallelCluster
- Richten Sie mithilfe von NICE EnginFrame und NICE DCV Session Manager eine auto skalierende virtuelle Desktop-Infrastruktur ein

Stellen Sie mithilfe von Terraform und DRA ein Lustre-Dateisystem für die Hochleistungsdatenverarbeitung bereit

Erstellt von Arun Bagal (AWS) und Ishwar Chauthaiwale (AWS)

Übersicht

Dieses Muster stellt automatisch ein Lustre-Dateisystem bereit AWS und integriert es mit Amazon Elastic Compute Cloud (Amazon EC2) und Amazon Simple Storage Service (Amazon S3).

Mit dieser Lösung können Sie schnell eine High Performance Computing (HPC) -Umgebung mit integriertem Speicher, Rechenressourcen und Amazon S3 S3-Datenzugriff einrichten. Es kombiniert die Speicherfunktionen von Lustre mit den flexiblen Rechenoptionen von Amazon EC2 und dem skalierbaren Objektspeicher in Amazon S3, sodass Sie datenintensive Workloads in den Bereichen maschinelles Lernen, HPC und Big-Data-Analysen bewältigen können.

Das Muster verwendet ein HashiCorp Terraform-Modul und Amazon FSx for Lustre, um den folgenden Prozess zu optimieren:

- Bereitstellung eines Lustre-Dateisystems
- Einrichtung einer Data Repository Association (DRA) zwischen FSx for Lustre und einem S3-Bucket, um das Lustre-Dateisystem mit Amazon S3 S3-Objekten zu verknüpfen
- Eine Instanz erstellen EC2
- Mounten des Lustre-Dateisystems mit dem Amazon S3-verknüpften DRA auf der Instance EC2

Zu den Vorteilen dieser Lösung gehören:

- Modularer Aufbau. Sie können die einzelnen Komponenten dieser Lösung einfach warten und aktualisieren.
- Skalierbarkeit. Sie können schnell konsistente Umgebungen in unseren AWS-Konten Regionen bereitstellen.
- Flexibilität. Sie können die Bereitstellung an Ihre spezifischen Bedürfnisse anpassen.
- Bewährte Verfahren. Dieses Muster verwendet vorkonfigurierte Module, die AWS bewährten Methoden folgen.

Weitere Informationen zu Lustre-Dateisystemen finden Sie auf der Lustre-Website.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Eine IAM-Richtlinie AWS Identity and Access Management (Least Privilege) (siehe Anweisungen)

Einschränkungen

FSx for Lustre beschränkt das Lustre-Dateisystem auf eine einzige Availability Zone, was problematisch sein kann, wenn Sie hohe Verfügbarkeitsanforderungen haben. Wenn die Availability Zone, die das Dateisystem enthält, ausfällt, ist der Zugriff auf das Dateisystem bis zur Wiederherstellung verloren. Um eine hohe Verfügbarkeit zu erreichen, können Sie DRA verwenden, um das Lustre-Dateisystem mit Amazon S3 zu verknüpfen und Daten zwischen Availability Zones zu übertragen.

Produktversionen

- Terraform Version 1.9.3 oder höher
- HashiCorp AWS-Provider-Version 4.0.0 oder höher

Architektur

Das folgende Diagramm zeigt die Architektur für FSx für Lustre und die ergänzende Architektur AWS-Services in. AWS Cloud

Die Architektur umfasst Folgendes:

- Ein S3-Bucket wird als langlebiger, skalierbarer und kostengünstiger Speicherort für Daten verwendet. Die Integration zwischen FSx for Lustre und Amazon S3 bietet ein leistungsstarkes Dateisystem, das nahtlos mit Amazon S3 verknüpft ist.
- FSx for Lustre betreibt und verwaltet das Lustre-Dateisystem.
- Amazon CloudWatch Logs sammelt und überwacht Protokolldaten aus dem Dateisystem. Diese Protokolle bieten Einblicke in die Leistung, den Zustand und die Aktivität Ihres Lustre-Dateisystems.
- Amazon EC2 wird verwendet, um mithilfe des Open-Source-Lustre-Clients auf Lustre-Dateisysteme zuzugreifen. EC2 Instanzen können auf Dateisysteme von anderen Availability Zones innerhalb

derselben Virtual Private Cloud (VPC) zugreifen. Die Netzwerkkonfiguration ermöglicht den Zugriff über Subnetze innerhalb der VPC. Nachdem das Lustre-Dateisystem auf der Instanz bereitgestellt wurde, können Sie mit den Dateien und Verzeichnissen arbeiten, als würden Sie ein lokales Dateisystem verwenden.

- AWS Key Management Service (AWS KMS) erhöht die Sicherheit des Dateisystems, indem Daten im Ruhezustand verschlüsselt werden.

Automatisierung und Skalierung

Terraform erleichtert die Bereitstellung, Verwaltung und Skalierung Ihrer Lustre-Dateisysteme in mehreren Umgebungen. FSx Bei Lustre hat ein einzelnes Dateisystem Größenbeschränkungen, sodass Sie möglicherweise horizontal skalieren müssen, indem Sie mehrere Dateisysteme erstellen. Sie können Terraform verwenden, um je nach Ihren Workload-Anforderungen mehrere Lustre-Dateisysteme bereitzustellen.

Tools

AWS-Services

- Amazon CloudWatch Logs hilft Ihnen dabei, die Protokolle all Ihrer Systeme und Anwendungen zu zentralisieren, AWS-Services sodass Sie sie überwachen und sicher archivieren können.
- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon FSx for Lustre macht es einfach und kostengünstig, ein leistungsstarkes Lustre-Dateisystem zu starten, auszuführen und zu skalieren.
- AWS Key Management Service (AWS KMS) hilft Ihnen dabei, kryptografische Schlüssel zu erstellen und zu kontrollieren, um Ihre Daten zu schützen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub Provision FSx for Lustre Filesystem using Terraform verfügbar.

Bewährte Methoden

- Die folgenden Variablen definieren das Lustre-Dateisystem. Stellen Sie sicher, dass Sie diese entsprechend Ihrer Umgebung korrekt konfigurieren, wie im Abschnitt Epics beschrieben.
  - `storage_capacity`— Die Speicherkapazität des Lustre-Dateisystems, in. GiBs Die Mindest- und Standardeinstellung ist 1200 GiB.
  - `deployment_type`— Der Bereitstellungstyp für das Lustre-Dateisystem. Eine Erläuterung der beiden Optionen `PERSISTENT_1` und `PERSISTENT_2` (Standard) finden Sie in der Dokumentation FSx zu Lustre.
  - `per_unit_storage_throughput`— Der Lese- und Schreibdurchsatz in MBs pro Sekunde pro TiB.
  - `subnet_id`— Die ID des privaten Subnetzes, in dem Sie Lustre bereitstellen FSx möchten.
  - `vpc_id`— Die ID Ihrer virtuellen privaten Cloud, AWS in der Sie Lustre bereitstellen FSx möchten.
  - `data_repository_path`— Der Pfad zum S3-Bucket, der mit dem Lustre-Dateisystem verknüpft wird.
  - `iam_instance_profile`— Das IAM-Instance-Profil, das zum Starten der EC2 Instance verwendet werden soll.
  - `kms_key_id`— Der Amazon-Ressourcenname (ARN) des AWS KMS Schlüssels, der für die Datenverschlüsselung verwendet wird.
- Stellen Sie mithilfe der `vpc_id` Variablen und den korrekten Netzwerkzugriff und die korrekte Platzierung innerhalb der `security_group` VPC sicher.
- Führen Sie den `terraform plan` Befehl wie im Abschnitt Epics beschrieben aus, um eine Vorschau der Änderungen anzuzeigen und sie zu überprüfen, bevor Sie sie übernehmen. Dies hilft dabei catch potenzielle Probleme zu erkennen und stellt sicher, dass Sie wissen, was bereitgestellt wird.
- Verwenden Sie den `terraform validate` Befehl, wie im Abschnitt Epics beschrieben, um nach Syntaxfehlern zu suchen und um zu bestätigen, dass Ihre Konfiguration korrekt ist.

Epen

So richten Sie Ihre Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Terraform.	Folgen Sie den Anweisungen in der Terraform-Dokumentation, um Terraform auf Ihrem lokalen Computer zu installieren.	AWS DevOps, DevOps Ingenieur
Richten Sie AWS Anmeldeinformationen ein.	Folgen Sie den Anweisungen in der AWS Dokumentation, um das Profil AWS Command Line Interface (AWS CLI) für das Konto einzurichten.	AWS DevOps, DevOps Ingenieur
Klonen Sie das GitHub Repository.	Um das GitHub Repository zu klonen, führen Sie den folgenden Befehl aus: `git clone https://github.com/aws-samples/provision-fsx-lustre-with-terraform.git`	AWS DevOps, DevOps Ingenieur

Konfiguration und Bereitstellung FSx für Lustre

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Bereitstellungskonfiguration.	1. Navigieren Sie im geklonten Repository auf Ihrem lokalen Computer zu dem `fsx_deployment` Verzeichnis:	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`cd fsx_deployment` 2. Öffnen Sie die `terraform.tfvars` Datei und aktualisieren Sie die Werte der folgenden Variablen: • `vpc_id` • `subnet_id` • `data_repository_path` • `iam_instance_profile` • `kms_key_id` Eine Beschreibung dieser Variablen finden Sie im Abschnitt Bewährte Methoden. 3. Öffnen Sie im selben Verzeichnis die `locals.tf` Datei und aktualisieren Sie die CIDR-Bereiche für die Variablen `fsx_inress` und die `fsx_egress` Sicherheitsgruppe. 4. Öffnen Sie bei Bedarf die `variables.tf` Datei und aktualisieren Sie die Standardwerte dieser Variablen: • `storage_capacity` • `deployment_type`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `per_unit_storage_throughput` Eine Beschreibung dieser Variablen finden Sie im Abschnitt Bewährte Methoden.	
Initialisieren Sie die Terraform-Umgebung.	Um Ihre Umgebung für die Ausführung des `fsx_deployment` Terraform-Moduls zu initialisieren, führen Sie Folgendes aus: `terraform init`	AWS DevOps, DevOps Ingenieur
Validieren Sie die Terraform-Syntax.	Führen Sie Folgendes aus, um nach Syntaxfehlern zu suchen und zu bestätigen, dass Ihre Konfiguration korrekt ist: `terraform validate`	AWS DevOps, DevOps Ingenieur
Validieren Sie die Terraform-Konfiguration.	Führen Sie Folgendes aus, um einen Terraform-Ausführungsplan zu erstellen und eine Vorschau der Bereitstellung anzuzeigen: `terraform plan -var-file terraform.tfvars`	AWS DevOps, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie das Terraform-Modul bereit.	Führen Sie Folgendes aus, um die FSx for Lustre-Ressourcen bereitzustellen: `terraform apply -var-file terraform.tfvars`	AWS DevOps, DevOps Ingenieur

AWS Ressourcen bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

AWS Ressourcen entfernen.	Nachdem Sie Ihre FSx for Lustre-Umgebung nicht mehr genutzt haben, können Sie die von Terraform bereitgestellten AWS Ressourcen entfernen, um unnötige Kosten zu vermeiden. Das im Code-Repository bereitgestellte Terraform-Modul automatisiert diese Bereinigung.
	1. Navigieren Sie in Ihrem lokalen Repository zum Verzeichnis: `fsx_deployment`
	`cd fsx_deployment`
	2. Führen Sie den Befehl aus:
	`terraform destroy -var-file terraform.tfvars`
		AWS DevOps, DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
FSx für Lustre gibt Fehler zurück.	Hilfe bei Problemen mit FSx Lustre finden Sie unter Fehlerbehebung bei Amazon FSx for Lustre in der FSx for Lustre-Dokumentation.

Zugehörige Ressourcen

- Amazon FSx for Lustre mithilfe von Terraform erstellen (AWS Anbieterreferenz in der Terraform-Dokumentation)
- Erste Schritte mit Amazon FSx for Lustre (FSx für Lustre-Dokumentation)
- AWS Blogbeiträge über Amazon FSx for Lustre

Richten Sie ein Grafana-Monitoring-Dashboard für AWS ein ParallelCluster

Erstellt von Dario La Porta (AWS) und William Lu (AWS)

Übersicht

AWS ParallelCluster unterstützt Sie bei der Bereitstellung und Verwaltung von HPC-Clustern (High Performance Computing). Es unterstützt die Open-Source-Job-Scheduler AWS Batch und Slurm. Obwohl AWS CloudWatch für die Protokollierung und Metriken in Amazon integriert ParallelCluster ist, bietet es kein Monitoring-Dashboard für die Arbeitslast.

Das Grafana-Dashboard für AWS ParallelCluster (GitHub) ist ein Überwachungs-Dashboard für AWS ParallelCluster. Es bietet Einblicke in den Job Scheduler und detaillierte Überwachungsmetriken auf Betriebssystemebene (OS). Weitere Informationen zu den in dieser Lösung enthaltenen Dashboards finden Sie unter Beispiel-Dashboards im Repository. GitHub Diese Metriken helfen Ihnen dabei, den HPC-Workload und seine Leistung besser zu verstehen. Der Dashboard-Code wird jedoch nicht für die neuesten Versionen von AWS ParallelCluster oder die Open-Source-Pakete aktualisiert, die in der Lösung verwendet werden. Dieses Muster verbessert die Lösung und bietet die folgenden Vorteile:

- Unterstützt AWS ParallelCluster v3
- Verwendet die neueste Version von Open-Source-Paketen, darunter Prometheus, Grafana, Prometheus Slurm Exporter und NVIDIA DCGM-Exporter
- Erhöht die Anzahl der CPU-Kerne und die Anzahl der CPU-Kerne, die von den Slurm-Jobs verwendet werden GPUs
- Fügt ein Dashboard zur Jobüberwachung hinzu
- Verbessert das Dashboard zur GPU-Knotenüberwachung für Knoten mit 4 oder 8 Grafikprozessoren (GPUs)

Diese Version der erweiterten Lösung wurde in der HPC-Produktionsumgebung eines AWS-Kunden implementiert und verifiziert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- AWS ParallelCluster CLI, installiert und konfiguriert.

- Eine unterstützte Netzwerkkonfiguration für AWS ParallelCluster. Dieses Muster verwendet die AWS-Konfiguration ParallelCluster mit zwei Subnetzen, was ein öffentliches Subnetz, ein privates Subnetz, ein Internet-Gateway und ein NAT-Gateway erfordert.
- Alle ParallelCluster AWS-Clusterknoten müssen über Internetzugang verfügen. Dies ist erforderlich, damit die Installationsskripte die Open-Source-Software und die Docker-Images herunterladen können.
- Ein key pair in Amazon Elastic Compute Cloud (Amazon EC2). Ressourcen, die über dieses key pair verfügen, haben Secure Shell (SSH) -Zugriff auf den Hauptknoten.

Einschränkungen

- Dieses Muster wurde entwickelt, um Ubuntu 20.04 LTS zu unterstützen. Wenn Sie eine andere Version von Ubuntu oder Amazon Linux oder CentOS verwenden, müssen Sie die mit dieser Lösung bereitgestellten Skripts ändern. Diese Änderungen sind in diesem Muster nicht enthalten.

Produktversionen

- Ubuntu 20.04 LTS
- ParallelCluster 3.X

Überlegungen zur Abrechnung und zu den Kosten

- Die nach diesem Muster bereitgestellte Lösung fällt nicht unter das kostenlose Kontingent. Für Amazon EC2, Amazon FSx for Lustre, das NAT-Gateway in Amazon VPC und Amazon Route 53 fallen Gebühren an.

Architektur

Zielarchitektur

Das folgende Diagramm zeigt, wie ein Benutzer auf das Monitoring-Dashboard für AWS ParallelCluster auf dem Hauptknoten zugreifen kann. Auf dem Hauptknoten werden NICE DCV, Prometheus, Grafana, Prometheus Slurm Exporter, Prometheus Node Exporter und NGINX Open Source ausgeführt. Auf den Rechenknoten wird der Prometheus Node Exporter ausgeführt, und sie führen auch den NVIDIA DCGM-Exporter aus, wenn der Knoten enthält. GPUs Der Hauptknoten ruft Informationen von den Rechenknoten ab und zeigt diese Daten im Grafana-Dashboard an.

In den meisten Fällen ist der Hauptknoten nicht stark ausgelastet, da der Job-Scheduler keine nennenswerte Menge an CPU oder Arbeitsspeicher benötigt. Benutzer greifen mithilfe von SSL auf Port 443 auf das Dashboard auf dem Hauptknoten zu.

Alle autorisierten Zuschauer können die Monitoring-Dashboards anonym einsehen. Nur der Grafana-Administrator kann Dashboards ändern. Sie konfigurieren in der `aws-parallelcluster-monitoring/docker-compose/docker-compose.head.yml` Datei ein Passwort für den Grafana-Administrator.

Tools

AWS-Services

- NICE DCV ist ein leistungsstarkes Remote-Display-Protokoll, mit dem Sie Remote-Desktops und Anwendungsstreaming von jeder Cloud oder jedem Rechenzentrum auf jedes Gerät unter unterschiedlichen Netzwerkbedingungen bereitstellen können.
- AWS ParallelCluster unterstützt Sie bei der Bereitstellung und Verwaltung von HPC-Clustern (High Performance Computing). Es unterstützt die Open-Source-Job-Scheduler AWS Batch und Slurm.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten.

Andere Tools

- Docker ist eine Reihe von Platform-as-a-Service (PaaS) -Produkten, die Virtualisierung auf Betriebssystemebene nutzen, um Software in Containern bereitzustellen.
- Grafana ist eine Open-Source-Software, mit der Sie Metriken, Protokolle und Traces abfragen, visualisieren, darauf hinweisen und untersuchen können.
- NGINX Open Source ist ein Open-Source-Webserver und Reverse-Proxy.
- NVIDIA Data Center GPU Manager (DCGM) ist eine Suite von Tools zur Verwaltung und Überwachung von NVIDIA-Grafikprozessoren (GPUs) für Rechenzentren in Clusterumgebungen. In diesem Muster verwenden Sie den DCGM-Exporter, mit dem Sie GPU-Metriken aus Prometheus exportieren können.

- Prometheus ist ein Open-Source-Toolkit zur Systemüberwachung, das seine Metriken als Zeitreihendaten mit zugehörigen Schlüssel-Wert-Paaren sammelt und speichert, die als Labels bezeichnet werden. In diesem Muster verwenden Sie auch Prometheus Slurm Exporter, um Metriken zu sammeln und zu exportieren, und Sie verwenden Prometheus Node Exporter, um Metriken aus den Rechenknoten zu exportieren.
- Ubuntu ist ein Linux-basiertes Open-Source-Betriebssystem, das für Unternehmensserver, Desktops, Cloud-Umgebungen und IoT entwickelt wurde.

Code-Repository

Der Code für dieses Muster ist im GitHub pcluster-monitoring-dashboardRepository verfügbar.

Epen

Erstellen Sie die erforderlichen Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Erstellen Sie einen Amazon-S3-Bucket. Sie verwenden diesen Bucket, um die Konfigurationsskripten zu speichern. Anweisungen finden Sie in der Amazon S3 S3-Dokumentation unter Bucket erstellen.	Allgemeines AWS
Klonen Sie das Repository	Klonen Sie das GitHub pcluster-monitoring-dashboardRepo, indem Sie den folgenden Befehl ausführen. `git clone https://github.com/aws-samples/parallelcluster-monitoring-dashboard.git`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Admin-Passwort.	1. Wählen Sie den `aws-parallelcluster-monitoring` Ordner aus, wählen Sie den `docker-compose` Ordner aus und öffnen Sie dann die Datei docker-compose.head.yml. 2. Ersetzen Sie die `GF_SECURITY_ADMIN_PASSWORD` Variable durch ein Passwort Ihrer Wahl. `Grafana4PC!` Dies ist das Administratorkennwort, mit dem Sie das Grafana-Konto verwalten. 3. Speichern und schließen Sie die Datei docker-compose.head.yml.	Linux-Shell-Skripting
Kopieren Sie die erforderlichen Dateien in den S3-Bucket.	Kopieren Sie das Skript post_install.sh und den aws-parallelcluster-monitoringOrdner in den S3-Bucket, den Sie erstellt haben. Anweisungen finden Sie in der Amazon S3 S3-Dokumentation unter Hochladen von Objekten.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie eine zusätzliche Sicherheitsgruppe für den Hauptknoten.	1. Erstellen Sie eine Sicherheitsgruppe für den Hauptknoten. Diese Sicherheitsgruppe ermöglicht eingehenden Datenverkehr zu den Überwachungs-Dashboards auf dem Hauptknoten. Anweisungen finden Sie unter Erstellen einer Sicherheitsgruppe in der Amazon VPC-Dokumentation. 2. Fügen Sie der Sicherheitsgruppe eine Regel für eingehenden Datenverkehr hinzu. Anweisungen finden Sie unter Regeln zu einer Sicherheitsgruppe hinzufügen in der Amazon VPC-Dokumentation. Verwenden Sie die folgenden Parameter für die Regel: • Typ — HTTPS • Protokoll — TCP • Portbereich — 443 • Quelle — Geben Sie Ihre IP-Adresse ein • Beschreibung — Erlauben Sie Benutzern den Zugriff auf das Monitoring-Dashboard	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie eine IAM-Richtlinie für den Hauptknoten.	Erstellen Sie eine identitätsbasierte Richtlinie für den Hauptknoten. Diese Richtlinie ermöglicht es dem Knoten, Metrikdaten von Amazon CloudWatch abzurufen. Das GitHub Repo enthält eine Beispielrichtlinie. Anweisungen finden Sie unter Erstellen von IAM-Richtlinien in der Dokumentation zu AWS Identity and Access Management (IAM).	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie eine IAM-Richtlinie für die Rechenknoten.	Erstellen Sie eine identitätsbasierte Richtlinie für die Rechenknoten. Diese Richtlinie ermöglicht es dem Knoten, die Tags zu erstellen, die die Job-ID und den Job-Besitzer enthalten. Das GitHub Repo enthält eine Beispielrichtlinie. Anweisungen finden Sie in der IAM-Dokumentation unter Erstellen von IAM-Richtlinien. Wenn Sie die bereitgestellte Beispieldatei verwenden, ersetzen Sie die folgenden Werte: • <REGION>— Die AWS-Region, in der der Cluster gehostet wird • <ACCOUNT_ID>— Die AWS-Konto-ID	AWS-Administrator

Den Cluster erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die bereitgestellte Cluster-Vorlagendatei.	Erstellen Sie den ParallelCluster AWS-Cluster. Verwenden Sie die bereitgestellte CloudFormation AWS-Vorlagendatei cluster.yaml als Ausgangspunkt für die Erstellung des Clusters.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ersetzen Sie die folgenden Werte in der bereitgestellten Vorlage: • <REGION>— Die AWS-Region, in der der Cluster gehostet wird. • <HEADNODE_SUBNET>— Das öffentliche Subnetz der VPC. • <ADDITIONAL_HEAD_NODE_SG>— Der Name der Sicherheitsgruppe, die Sie für den Hauptknoten erstellt haben. • <KEY_NAME>— Geben Sie den Namen eines vorhandenen EC2 Amazon-Schlüsselpaars key pair. Ressourcen, die über dieses key pair verfügen, haben Secure Shell (SSH) -Zugriff auf den Hauptknoten. • <ALLOWED_IPS>— Geben Sie den CIDR-formatierten IP-Adressbereich ein, über den SSH-Verbindungen zum Hauptknoten hergestellt werden können. • <ADDITIONAL_HEAD_NODE_POLICY>— Geben Sie den Namen der IAM-Richtlinie ein, die Sie für den Hauptknoten erstellt haben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• <BUCKET_NAME>— Geben Sie den Namen des S3-Buckets ein, den Sie erstellt haben. • <COMPUTE_SUBNET>— Geben Sie den Namen des privaten Subnetzes in der VPC ein. • <ADDITIONAL_COMPUTE_NODE_POLICY>— Geben Sie den Namen der IAM-Richtlinie ein, die Sie für den Compute-Knoten erstellt haben.	
Erstellen Sie den -Cluster.	Geben Sie in der ParallelCluster AWS-CLI den folgenden Befehl ein. Dadurch wird die CloudFormation Vorlage bereitgestellt und der Cluster erstellt. Weitere Informationen zu diesem Befehl finden Sie unter pcluster create-cluster in der AWS-Dokumentation. ParallelCluster `pcluster create-cluster -n <cluster_name> -c cluster.yaml`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überwachen Sie die Cluster-Erstellung.	Geben Sie den folgenden Befehl ein, um die Clustererstellung zu überwachen. Weitere Informationen zu diesem Befehl finden Sie unter pcluster describe-cluster in der AWS-Dokumentation. ParallelCluster `pcluster describe-cluster -n <cluster_name>`	AWS-Administrator

Verwendung der Grafana-Dashboards

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Zugang zum Grafana-Portal.	1. Geben Sie den folgenden Befehl ein, um die öffentliche IP-Adresse des Hauptknotens abzurufen. `pcluster describe-cluster -n <cluster_name> --query headNode.publicIpAddress` 2. Navigieren Sie in einem Webbrowser zur folgenden URL, um auf das Grafana-Dashboard zuzugreifen. https://<head_node_public_ip_address>	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie auf der Grafana-Startseite das 4-eckige Dashboard-Symbol im linken Menü und wählen Sie dann Allgemein. Dies zeigt eine Liste der konfiguri erten Dashboards. Die folgenden Dashboards sind in Grafana verfügbar: • Cluster-Kosten — Enthält Informationen zu den Kosten des Clusters • Cluster-Protokolle — Enthält Informationen zu den Protokollen des Clusters • Compute-Knotendeta ils — Enthält Informati onen über die Nutzungss tatistiken der Rechenkno ten • Liste der Rechenkno ten — Enthält die Liste der Rechenknoten des Clusters • GPU-Knoten — Enthält Informationen zur Nutzungsstatistik der GPU-Knoten • Jobdetails — Enthält Informationen über die Auslastung der Jobressourcen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Details zum Hauptknoten — Enthält Informationen zur Nutzungsstatistik des Hauptknotens • ParallelCluster Zusammenfassung — Enthält Informationen zur Cluster-Nutzung	

Bereinigen Sie die Lösung, um die damit verbundenen Kosten zu vermeiden

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie den Cluster.	Geben Sie den folgenden Befehl ein, um den Cluster zu löschen. Weitere Informationen zu diesem Befehl finden Sie unter pcluster delete-cluster in der AWS-Dokumentation. ParallelCluster `pcluster delete-cluster -n <cluster_name>`	AWS-Administrator
Löschen Sie die IAM-Richtlinien.	Löschen Sie die Richtlinien, die Sie für den Hauptknoten und den Rechenknoten erstellt haben. Weitere Informationen zum Löschen von Richtlinien finden Sie unter Löschen von IAM-Richtlinien in der IAM-Dokumentation.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die Sicherhei tsgruppe und die Sicherhei tsregel.	Löschen Sie die Sicherhei tsgruppe, die Sie für den Hauptknoten erstellt haben. Weitere Informationen finden Sie unter Löschen von Sicherheitsgruppenregeln und Löschen einer Sicherhei tsgruppe in der Amazon VPC-Dokumentation.	AWS-Administrator
Löschen Sie den S3-Bucket.	Löschen Sie den S3-Bucket , den Sie zum Speichern der Konfigurationsskripten erstellt haben. Weitere Informationen finden Sie unter Löschen eines Buckets in der Amazon S3 S3-Dokumentation.	Allgemeines AWS

Fehlerbehebung

Problem	Lösung
Auf den Hauptknoten kann im Browser nicht zugegriffen werden.	Überprüfen Sie die Sicherheitsgruppe und vergewissern Sie sich, dass der eingehende Port 443 geöffnet ist.
Grafana öffnet nicht.	Suchen Sie auf dem Hauptknoten im Container -Log nach`docker logs Grafana`.
Einige Metriken enthalten keine Daten.	Überprüfen Sie auf dem Hauptknoten die Container-Logs aller Container.

Zugehörige Ressourcen

AWS-Dokumentation

- IAM-Richtlinien für Amazon EC2

Andere AWS-Ressourcen

- AWS ParallelCluster
- Überwachungs-Dashboard für AWS ParallelCluster (AWS-Blogbeitrag)

Sonstige Ressourcen

- Prometheus-Überwachungssystem
- Grafana

Richten Sie mithilfe von NICE EnginFrame und NICE DCV Session Manager eine auto skalierende virtuelle Desktop-Infrastruktur ein

Erstellt von Dario La Porta (AWS) und Salvatore Maccarone (AWS)

Übersicht

NICE DCV ist ein leistungsstarkes Remote-Display-Protokoll, mit dem Sie Remote-Desktops und -anwendungen über unterschiedliche Netzwerkbedingungen von jeder Cloud oder jedem Rechenzentrum auf jedes Gerät streamen können. Mit NICE DCV und Amazon Elastic Compute Cloud (Amazon EC2) können Sie grafikintensive Anwendungen remote auf EC2 Amazon-Instances ausführen und deren Benutzeroberflächen auf einfachere Remote-Client-Computer streamen. Dadurch werden teure dedizierte Workstations und die Übertragung großer Datenmengen zwischen der Cloud und den Client-Computern überflüssig.

Dieses Muster richtet eine voll funktionsfähige, automatisch skalierende virtuelle Desktop-Infrastruktur (VDI) für Linux und Windows ein, auf die über eine webbasierte Benutzeroberfläche zugegriffen werden kann. Die VDI-Lösung bietet Anwendern aus der Forschung und Entwicklung (F&E) eine zugängliche und leistungsstarke Benutzeroberfläche, über die sie grafikintensive Analyseanfragen einreichen und Ergebnisse aus der Ferne überprüfen können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver. AWS-Konto
- Administratorrechte und eine Reihe von Zugriffsschlüsseln.
- AWS Cloud Development Kit (AWS CDK) Toolkit, installiert und konfiguriert. Weitere Informationen finden Sie unter Installieren der AWS CDK.
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert für Ihren AWS-Konto. Weitere Informationen finden Sie unter Installieren oder Aktualisierung auf die neueste Version von AWS CLI.
- Python, installiert und konfiguriert. Weitere Informationen finden Sie unter Quellversionen (Python-Website).
- Eine oder mehrere virtuelle private Clouds (VPCs) sind verfügbar.
- Zwei oder mehr Elastic IP-Adressen verfügbar. Weitere Informationen zum Standardlimit finden Sie unter Elastic IP Address Limit.

- Richten Sie für die EC2 Linux-Amazon-Instances ein Secure Shell (SSH) -Schlüsselpaar key pair. Weitere Informationen finden Sie unter Schlüsselpaare und Linux-Instances.

Produktversionen

- AWS CDK Version 2.26.0 oder höher
- Python Version 3.8 oder höher

Architektur

Zielarchitektur

Die folgende Abbildung zeigt die verschiedenen Komponenten dieser VDI-Lösung. Der Benutzer interagiert mit NICE EnginFrame , um EC2 Amazon-Instances gemäß den Amazon EC2 Auto Scaling Scaling-Gruppen für Windows- und Linux-NICE-DCV-Instances zu starten.

Automatisierung und Skalierung

Der in diesem Muster enthaltene Code erstellt eine benutzerdefinierte VPC, öffentliche und private Subnetze, ein Internet-Gateway, ein NAT-Gateway, einen Application Load Balancer, Sicherheitsgruppen und AWS Identity and Access Management (IAM) -Richtlinien. AWS CloudFormation wird auch verwendet, um die Flotte von Linux- und Windows-NICE-DCV-Servern zu erstellen.

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK)ist ein Softwareentwicklungs-Framework, das Ihnen hilft, AWS Cloud Infrastruktur im Code zu definieren und bereitzustellen.
- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend AWS-Konten zu verwalten.
- NICE DCV ist ein leistungsstarkes Remote-Display-Protokoll, mit dem Sie Remote-Desktops und Anwendungsstreaming von jeder Cloud oder jedem Rechenzentrum auf jedes Gerät unter unterschiedlichen Netzwerkbedingungen bereitstellen können. In diesem Muster bietet es ein

bandbreiteneffizientes Erlebnis, bei dem 3D-Grafiken aus der Ferne (High Performance Computing, HPC) gestreamt werden.

- NICE DCV Session Manager hilft Ihnen, den Lebenszyklus von NICE DCV-Sitzungen auf einer Flotte von NICE DCV-Servern zu erstellen und zu verwalten.
- NICE EnginFrame ist ein fortschrittliches Frontend-Webinterface für den Zugriff auf technische und wissenschaftliche Anwendungen in der Cloud.

Code-Repository

Der Code für dieses Muster ist in der Auto Scaling VDI-Lösung mit NICE EnginFrame und dem NICE DCV Session Manager-Repository verfügbar.

Epen

Stellen Sie die virtuelle Desktop-Infrastruktur bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Klonen Sie das Repository, das den Code enthält: `git clone https://github.com/aws-samples/elastic-vdi-infrastructure.git`	Cloud-Architekt

Installieren Sie die erforderlichen AWS CDK Bibliotheken.	Installieren Sie die AWS CDK Bibliotheken:
	`cd elastic-vdi-infrastructure`
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	`pip3 install -r requirements.txt`
		Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Parameter.	1. Öffnen Sie die Datei app.py in einem Texteditor Ihrer Wahl. 2. Ersetzen Sie den `CHANGE_ME` Wert für die folgenden erforderlichen Parameter: • `region`— Das Ziel AWS-Region. Eine vollständige Liste finden Sie hier: AWS-Regionen. • `account`— Die ID des Ziels AWS-Konto. Weitere Informationen finden Sie unter Ihre AWS-Konto ID finden. • `key_name`— Das key pair, das für den Zugriff auf die EC2 Linux-Amazon-Instances verwendet wird. 3. (Optional) Ändern Sie die Werte für die folgenden Parameter, um die Lösung an Ihre Umgebung anzupassen: • `ec2_type_enginframe` — Der EnginFrame Instanztyp • `ec2_type_broker` — Der Instanztyp des Session Manager Brokers	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `ebs_enginframe_size` — Die Größe des Amazon Elastic Block Store (Amazon EBS) - Volumes für die Instance EnginFrame • `ebs_broker_size` — Die Größe des Amazon EBS-Volumes für die Session Manager Broker-Instance • `TagName and TagValue`— Das Abrechnungs-Tag für die Ressourcen • `efadmin_uid` — Die eindeutige Kennung des EnginFrame Administratorbenutzers (efadmin) • `linux_shared_storage_size` — OpenZFS-Größe in Gibibytes (GiB) • `Shared_Storage_Linux` — Der Einhängepunkt des gemeinsam genutzten Speichers • `Enginframe_installer` — Der Download-Link für EnginFrame • `Session_Manager_Broker_Installer` — Der Download-Link für	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den Session Manager Broker 4. Speichern und schließen Sie die Datei app.py.	

Stellen Sie die Lösung bereit.	Führen Sie die folgenden Befehle nacheinander aus:
	`cdk bootstrap`
	`cdk deploy Assets-Stack Parameters-Stack`
	`cdk deploy Elastic-Vdi-Infrastructure`
	Wenn die Bereitstellung abgeschlossen ist, werden die folgenden beiden Ausgaben zurückgegeben:
	• `Elastic-Vdi-Infrastructure.EnginFrameURL` — Die HTTPS-Adresse des EnginFrame Portals
	• `Elastic-Vdi-InfrastruSecretEFadminPassword` — Der Amazon-Ressourcenname (ARN) des Secrets, das das Passwort für den Benutzer efadmin enthält
	Notieren Sie sich diese Werte. Sie verwenden sie später in diesem Muster.
		Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Flotte von Linux-Servern bereit.	1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die CloudFormation Konsole. 2. Wählen Sie Stack erstellen und dann Mit neuen Ressourcen aus. 3. Wählen Sie im Ordner cloudformation_files die Datei .yaml aus. dcv-linux-fleet 4. Definieren Sie auf der Seite „Stack-Details angeben“ die folgenden Parameter: • Stackname — Der Name des Stacks. • DcvFleet— Der Name der NICE DCV-Flotte. Lassen Sie diesen Wert nicht leer und verwenden Sie keine Leerzeichen. • InstanceType— Der Instance-Typ der Flotte. • RootVolumeSize— Die Größe des Root-Volumes der EC2 Linux-Amazon-Instance. • MinSize— Die Mindestan zahl von Knoten, die verfügbar sein sollten und auf denen keine DCV-Sitzung ausgeführ t werden sollte. Wenn	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie beispielsweise eingeben2, beginnt die Lösung mit 2 Knoten. Wenn ein Benutzer eine Sitzung erstellt, verringer t sich die Anzahl der verfügbaren Knoten auf1, und die Lösung erstellt einen weiteren Knoten, um das Minimum beizubehalten. • MaxSize— Die maximale Anzahl von Knoten in der Flotte. Benutzer können keine neuen Sitzungen starten, wenn das Maximum erreicht wurde. • BillingTagName— Der Tagname, der für die Abrechnung verwendet wird. Dieser Tag-Name muss sich von dem für den Windows-Stack verwendeten untersche iden. • BillingTagValue— Der Tag-Wert, der für die Abrechnung verwendet wird. 5. Schließen Sie den Assistent en zur Stack-Erstellung ab und wählen Sie dann Submit, um mit der	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Erstellung des Stacks zu beginnen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Flotte von Windows-Servern bereit.	1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die CloudFormation Konsole. 2. Wählen Sie Stack erstellen und dann Mit neuen Ressourcen aus. 3. Wählen Sie im Ordner cloudformation_files die Datei .yaml aus. dcv-windows-fleet 4. Definieren Sie auf der Seite „Stack-Details angeben“ die folgenden Parameter: • Stackname — Der Name des Stacks. • DcvFleet— Der Name der NICE DCV-Flotte. Lassen Sie diesen Wert nicht leer und verwenden Sie keine Leerzeichen. • InstanceType— Der Instance-Typ der Flotte. • RootVolumeSize— Die Größe des Root-Volumes der EC2 Windows-Amazon-Instance. • MinSize— Die Mindestanzahl von Knoten, die verfügbar sein sollten und auf denen keine DCV-Sitzung ausgeführt werden darf.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• MaxSize— Die maximale Anzahl von Knoten in der Flotte. • BillingTagName— Der Tagname, der für die Abrechnung verwendet wird. Dieser Tag-Name muss sich von dem für den Linux-Stack verwendeten untersche iden. • BillingTagValue— Der Tag-Wert, der für die Abrechnung verwendet wird. 5. Schließen Sie den Assistent en zur Stack-Erstellung ab und wählen Sie dann Submit, um mit der Erstellung des Stacks zu beginnen.	

Greifen Sie auf die bereitgestellte Umgebung zu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie das EnginFrame Administratorkennwort ab.	Das EnginFrame Administr atorkonto hat den Namen efadmin, und das Passwort ist geheim gespeichert. AWS Secrets Manager Der ARN des Secrets wird dynamisch generiert und ist in	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Ausgabe der AWS CDK Bereitstellung sichtbar. 1. Im vorherigen Epos finden Sie in der Geschichte Deploy the Solution unter der `Elastic-Vdi-Infrastructure.SecretEFadminPassword` Ausgabe den ARN des generierten Geheimnisses. 2. Führen Sie einen der folgenden Schritte aus, um das Geheimnis abzurufen: • Verwenden Sie die Secrets Manager Manager-Konsole. Weitere Informationen finden Sie unter Secrets abrufen. • Geben Sie den get-secret-value -Befehl ein. `aws secretsmanager get-secret-value \ --secret-id <secret_arn> \ --query SecretString \ --output text`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Greifen Sie auf das EnginFrame Portal zu.	1. Im vorherigen Epos finden Sie in der Story Deploy the Solution unter der `Elastic-Vdi-Infrastructure.EnginFrameURL` Ausgabe die HTTPS-Adresse des EnginFrame Portals. 2. Geben Sie in einem Webbrowser die HTTPS-Adresse des Portals ein. 3. Geben Sie die Anmeldeinformationen für den Benutzer efadmin ein.	Cloud-Architekt
Starten Sie eine Windows-Sitzung.	1. Wählen Sie im EnginFrame Portal im Menü Windows Desktop. 2. Wenn Sie aufgefordert werden, sich als Windows-Administrator anzumelden, geben Sie dasselbe Passwort ein, das Sie für den Benutzer efadmin verwendet haben. 3. Vergewissern Sie sich, dass die Windows-Sitzung erfolgreich gestartet wurde.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie eine Linux-Sitzung.	1. Wählen Sie im EnginFrame Portal im Menü Linux Desktop. 2. Wenn Sie aufgefordert werden, sich anzumelden, geben Sie die Anmeldeinformationen für den Benutzer efadmin ein. 3. Vergewissern Sie sich, dass die Linux-Sitzung erfolgreich gestartet wurde.	Cloud-Architekt

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Lösche die Stapel.	Löschen Sie in der CloudFormation Konsole die Stacks für die Windows- und Linux-Serverflotten. Weitere Informationen finden Sie unter Löschen eines Stacks.	Cloud-Architekt
Löschen Sie die Infrastruktur.	Löschen Sie die bereitgestellte Infrastruktur mithilfe des folgenden AWS CDK Befehls: `cdk destroy --all`	Cloud-Architekt

Fehlerbehebung

Problem	Lösung
Die Bereitstellung wurde nicht abgeschlossen, da sie unterbrochen wurde.	Folgen Sie den Anweisungen im Clean-up-Epic und wiederholen Sie dann dieses Muster, um die Umgebung erneut bereitzustellen.

Zugehörige Ressourcen

- NICE DCV
- NETT EnginFrame

Hybride Cloud

Themen

- Konfiguration einer Rechenzentrumserweiterung für VMware Cloud on AWS mithilfe des Hybrid Linked Mode
- Konfigurieren Sie VMware vRealize Automation für die Bereitstellung VMs in der VMware Cloud auf AWS
- Integrieren Sie VMware vRealize Network Insight mit VMware Cloud on AWS
- Migrieren VMs Sie mithilfe von HCX OS Assisted Migration zur VMware Cloud auf AWS
- Senden Sie mithilfe von VMware Aria Operations AWS for Logs Logs von VMware Cloud on an Splunk
- Richten Sie mithilfe von AWS CDK eine CI/CD-Pipeline für Hybrid-Workloads auf Amazon ECS Anywhere ein und GitLab
- Mehr Muster

Konfiguration einer Rechenzentrumserweiterung für VMware Cloud on AWS mithilfe des Hybrid Linked Mode

Erstellt von Deepak Kumar (AWS)

Übersicht

> Hinweis: Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Vertriebspartnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

Dieses Muster beschreibt, wie Sie den Hybrid Linked Mode verwenden können, um Inventare in einem lokalen Rechenzentrum und einem softwaredefinierten VMware Cloud-on-AWS-Rechenzentrum (SDDC) mithilfe einer einzigen vSphere Client-Schnittstelle anzuzeigen und zu verwalten. VMware

Durch die Konfiguration des Hybrid Linked Mode können Sie Ihre lokalen virtuellen Maschinen (VMs) und Anwendungen zum Cloud-SDDC migrieren. Ihre IT-Teams können dann Ihre cloudbasierten Ressourcen mit vertrauten VMware Tools verwalten, ohne dass neue Tools erforderlich sind. Mithilfe der VMware Cloud Gateway Appliance können Sie auch einen konsistenten Betrieb und eine vereinfachte Verwaltung sicherstellen.

Dieses Muster bietet zwei Optionen für die Konfiguration des Hybrid Linked Mode, Sie können jedoch jeweils nur eine Option verwenden. Die erste Option installiert die Cloud Gateway Appliance und verwendet sie, um eine Verbindung vom lokalen vCenter Server zum Cloud-SDDC herzustellen. Die zweite Option konfiguriert den Hybrid Linked Mode vom Cloud-SDDC aus.

Voraussetzungen und Einschränkungen

Voraussetzungen (beide Optionen)

- Ein vorhandenes lokales Rechenzentrum und ein Cloud-SDDC.
- Eine bestehende Verbindung zwischen dem lokalen Rechenzentrum und dem Cloud-SDDC, die AWS Direct Connect, ein VPN oder beides verwendet.
- Das lokale Rechenzentrum und das Cloud-SDDC werden mit dem Network Time Protocol (NTP) oder einer anderen autoritativen Zeitquelle synchronisiert.

- Die maximale Latenz einer Round-Trip-Zeit zwischen dem lokalen Rechenzentrum und dem Cloud-SDDC beträgt nicht mehr als 100 ms.
- Cloud-Administratoren mit Zugriff auf Ihre lokale Umgebung.
- Der vollqualifizierte Domänenname (FQDN) des vCenter Servers muss in eine private IP-Adresse aufgelöst werden.

Voraussetzungen für Option 1

- Die lokale Umgebung sollte auf vSphere 6.5.0d oder höher ausgeführt werden.
- Die Cloud Gateway Appliance und der vCenter Server können über AWS Direct Connect, ein VPN oder beides kommunizieren.
- Die Cloud Gateway Appliance erfüllt die Hardwareanforderungen.
- Die Firewall-Ports sind geöffnet.

Voraussetzungen für Option 2

- Der lokale vCenter Server wird auf vSphere 6.0 Update 3 oder höher oder auf vSphere 6.5.0d oder höher ausgeführt.
- Anmeldeinformationen sind für die lokale vSphere Single Sign-On (SSO) -Domäne verfügbar.
- Benutzer in der lokalen Umgebung haben nur Lesezugriff auf den Basis-DN (Basis-DN).
- Der lokale DNS-Server (Domain Name System) ist für Management Gateway konfiguriert. VMware
- Implementieren Sie Netzwerkverbindungstests mit dem VMware Connectivity Validator.
- Die Firewall-Ports sind geöffnet.

Einschränkungen

- Der hybride verknüpfte Modus kann nur eine lokale vCenter Server Enhanced Linked Mode-Domäne verbinden.
- Der hybride verknüpfte Modus unterstützt nur lokale vCenter Server, auf denen Version 6.7 oder höher ausgeführt wird.

Architektur

Das folgende Diagramm zeigt beide Optionen für die Konfiguration des verknüpften Hybrid-Modus.

Migration verschiedener Workload-Typen im Hybrid Linked Mode

Der Hybrid Linked Mode unterstützt die Migration von Workloads zwischen einem lokalen Rechenzentrum und einem Cloud-SDDC, indem entweder eine Cold-Migration oder eine Live-Migration mit vSphere vMotion verwendet wird. VMware Zu den Faktoren, die bei der Auswahl der Migrationsmethode berücksichtigt werden müssen, gehören der Typ und die Version des virtuellen Switches, der Verbindungstyp zum Cloud-SDDC und die Version der virtuellen Hardware.

Eine Cold-Migration ist für VMs diese Art von Ausfallzeit angemessen. Sie können sie herunterfahren VMs, migrieren und dann wieder einschalten. Die Migration dauert schneller, da der aktive Speicher nicht kopiert werden muss. Wir empfehlen die Verwendung einer Cold-Migration für Anwendungen, die Ausfallzeiten in Kauf nehmen (z. B. Tier-3-Anwendungen oder Entwicklungs- und Test-Workloads). Wenn es VMs nicht zu Ausfallzeiten kommt, sollten Sie eine Live-Migration mit vMotion für Ihre geschäftskritischen Anwendungen in Betracht ziehen.

Das folgende Diagramm bietet einen Überblick über die verschiedenen Arten der Workload-Migration im Hybrid Linked Mode.

Tools

- VMware Cloud on AWS ist ein integriertes Cloud-Angebot, das gemeinsam von AWS und entwickelt wurde VMware.
- VMware Cloud Gateway Appliance ermöglicht eine Reihe von Hybrid-Cloud-Anwendungsfällen, bei denen lokale Ressourcen mit Cloud-Ressourcen verbunden werden.
- VMware VMwareDie Virtualisierungsplattform von vSphere verwandelt Rechenzentren in aggregierte Computerinfrastrukturen, die CPU-, Speicher- und Netzwerkressourcen umfassen.

Epen

Option 1 — Verwenden Sie den verknüpften Hybrid-Modus mit der Cloud Gateway-Appliance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Cloud Gateway-Appliance.	1. Melden Sie sich bei der VMware Cloud on AWS-	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Konsole an und laden Sie die Cloud Gateway Appliance herunter. 2. Installieren Sie die Cloud Gateway Appliance in Ihrer lokalen Umgebung mit den folgenden zwei Schritten: • Wählen Sie Start, um die Cloud Gateway Appliance zu konfigurieren und dann bereitzustellen. • Konfigurieren Sie den verknüpften Hybrid-Mo dus. Weitere Informationen und detaillierte Schritte finden Sie in der VMware Dokumenta tion unter Konfiguration des Hybrid Linked Mode mithilfe der vCenter Cloud Gateway Appliance.	

Option 2 — Verwenden Sie den verknüpften Hybrid-Modus aus dem Cloud-SDDC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den verknüpften Hybrid-Modus über das Cloud-SDDC.	1. Melden Sie sich bei der VMware Cloud on AWS-Konsole an und überprüfe n Sie mit dem Connectiv ity Validator alle erforderl ichen Netzwerkverbindung	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en. Weitere Informati onen dazu finden Sie in der Dokumentation unter Überprüfen der Netzwerkk onnektivität für den VMware Hybrid Linked Mode. 2. Melden Sie sich beim vSphere Client des Cloud-SDDC an, wählen Sie Menü, dann Administration und dann Domains aus. 3. Wählen Sie im Abschnitt Hybrid Cloud Linked Domains aus und stellen Sie dann eine Verbindung zu Ihrem lokalen vCenter Server her. 4. Fügen Sie der Cloud-SDD C Lightweight Directory Access Protocol (LDAP) -Domäne eine Identität squelle hinzu. Weitere Informationen dazu finden Sie in der Dokumentation unter Hinzufügen einer Identitätsquelle zur SDDC-LDAP-Domäne. VMware	

Zugehörige Ressourcen

- Konfiguration des verknüpften Hybrid-Modus
- Konfiguration des hybriden verknüpften Modus für die VMware Cloud auf AWS

Konfigurieren Sie VMware vRealize Automation für die Bereitstellung VMs in der VMware Cloud auf AWS

Erstellt von Deepak Kumar (AWS)

Übersicht

> Hinweis: Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

VMware vRealize Automation ist eine Automatisierungssoftware, mit der Sie IT-Ressourcen anfordern und verwalten können. Wenn Sie sich für die Konfiguration von vRealize Automation mit VMware Cloud on AWS entscheiden, können Sie die Bereitstellung von virtuellen Maschinen (VMs), Anwendungen und IT-Services in mehreren Rechenzentren und Cloud-Umgebungen automatisieren.

Ihre IT-Teams können dann Katalogelemente erstellen, um die Servicebereitstellung und die Betriebsfunktionen zu konfigurieren, die Ihre Benutzer anfordern und mit ihren vorhandenen vRealize Automation-Tools verwenden können. Sie können auch Ihre IT-Agilität und Effizienz verbessern, indem Sie VMware Cloud on AWS mit vRealize Automation Cloud Assembly integrieren.

Dieses Muster beschreibt, wie VMware vRealize Automation so konfiguriert wird, dass Funktionen in VMware Cloud on AWS automatisch erstellt VMs oder angewendet werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein vorhandenes lokales Rechenzentrum und ein softwaredefiniertes VMware Cloud-on-AWS-Rechenzentrum (SDDC). Weitere Informationen zum Cloud-SDCC finden Sie in der Dokumentation unter Über softwaredefinierte Rechenzentren. VMware
- Eine bestehende Verbindung zwischen dem lokalen Rechenzentrum und dem Cloud-SDDC, die AWS Direct Connect, ein VPN (routen- oder richtlinienbasiert) oder beides verwendet.
- Das lokale Rechenzentrum und das Cloud-SDDC werden mit dem Network Time Protocol (NTP) oder einer anderen autoritativen Zeitquelle synchronisiert.
- Die maximale Latenz einer Round-Trip-Zeit zwischen dem lokalen Rechenzentrum und dem Cloud-SDDC beträgt nicht mehr als 100 ms.

- Der vollqualifizierte Domänenname (FQDN) des vCenter Servers muss in eine private IP-Adresse aufgelöst werden.
- Cloud-SDDC-Benutzer mit Zugriff auf Ihre lokale Umgebung.
- Zugriff auf Organisationsinhaber in der vRealize Automation Cloud Assembly-Dienstrolle.
- Endbenutzer mit der Berechtigung in vRealize Automation Service Broker, den Dienst zu nutzen.
- Der CIDR-Bereich (Classless Inter-Domain Routing) des lokalen Rechenzentrums muss für die Generierung von API-Token aus der VMware Cloud on AWS-Konsole geöffnet sein. Die folgende Liste enthält die Mindestrollen, die für die Generierung von API-Token erforderlich sind:
  - Mitglied der Organisation
  - Inhaber der Organisation
  - Servicerollen — VMware Cloud auf AWS
  - Administrator
  - NSX Cloud-Administrator
  - NSX-Cloud-Auditor

Weitere Informationen dazu finden Sie unter Konnektivitätsoptionen für VMware Cloud on AWS im SDDCs AWS-Partnernetzwerk-Blog.

Einschränkungen

- Sie können nur 20 VMware Cloud-Konten mit öffentlichen Endpoints in einem vRealize Automation konfigurieren. Weitere Informationen dazu finden Sie in der Dokumentation unter Maxima für Skalierbarkeit und Parallelität. VMware

Produktversionen

- vRealize Automation Version 8.x oder höher
- VMware vRealize Identity Manager Version 3.x oder höher
- VMware vRealize Suite Lifecycle Manager Version 8.x oder höher

Architektur

Das folgende Diagramm zeigt die vRealize Automation-Services, die die Infrastruktur sowohl von lokalen als auch von VMware Cloud-on-AWS-Umgebungen nutzen können.

VMware Cloud Assembly-Komponenten

VMware Cloud Assembly ist eine Kernkomponente von vRealize Automation und Sie können damit Ressourcen bereitstellen, bereitstellen VMs und berechnen. In der folgenden Tabelle werden VMware Cloud Assembly-Komponenten beschrieben, die für die Bereitstellung in VMware Cloud VMs on AWS konfiguriert werden müssen.

Komponenten	Definition
Cloud-Konto	Das Cloud-Konto enthält Verbindungsdetails (z. B. Servername, Benutzername und Passwort, Zugriffsschlüssel und API-Token). VMware Cloud Assembly verwendet das Cloud-Konto, um eine Bestandsaufnahme Ihrer Ressourcen zu erstellen.
Cloud-Zonen	Cloud-Zonen identifizieren Ressourcengrenzen im Cloud-Konto (z. B. AWS-Regionen und das Cloud-SDDC). Cloud-Zonen verknüpfen Rechenressourcen mit dem Cloud Assembly-Projekt.
Projekte	Ein Projekt ist eine logische Einheit, die aus Benutzern und Ressourcen wie Cloud-Zon en besteht. Es besteht auch aus Ressource nkontingenten und VM-Benennungsrichtlinien, die beim Erstellen der VM verwendet werden.
Zuordnungen von Geschmacksrichtungen	Flavor-Mapping liefert Informationen über die Kapazität der VM (z. B. Anzahl CPUs und Menge des Speichers), die in der Cloud-Vor lage verwendet wird.
Image-Zuordnungen	Die Image-Mapping ordnet die VMware vSphere-VM-Vorlage und das Amazon Web Services (AWS) -Image zu, die in der Cloud-Vor lage verwendet werden. Weitere Informationen dazu finden Sie in der Dokumentation unter

	Weitere Informationen zu Image-Zuordnungen in vRealize Automation. VMware
Netzwerkprofil	Das Netzwerkprofil steuert die Platzierungsentscheidung, bei der bei der VM-Bereitstellung ein Netzwerk ausgewählt wird.
Speicherprofil	Das Speicherprofil steuert die Entscheidung über die Platzierung und Auswahl des Speichers bei der VM-Bereitstellung.
Cloud-Vorlagen	VMware Cloud-Vorlagen sind ein wichtiger Bestandteil von vRealize Automation, da sie die Bereitstellung und Orchestrierung der Cloud-Infrastruktur definieren. Die Cloud-Vorlagen sind Spezifikationen für die Ressourcen und beinhalten den Ressourcentyp, die Ressource neigenschaften und die von Benutzern zu erfassenden Eingaben.

Tools

- VMware vRealize Automation — vRealize Automation ist eine Plattform zur Infrastrukturautomatisierung mit ereignisgesteuerter Statusverwaltung und Compliance. Sie wurde entwickelt, um Unternehmen bei der Steuerung und Sicherung von Self-Service-Clouds, Multi-Cloud-Automatisierung mit Governance und basierter Infrastrukturbereitstellung zu unterstützen. DevOps
- VMware Cloud on AWS — VMware Cloud on AWS ist ein integriertes Cloud-Angebot, das gemeinsam von AWS und entwickelt wurde VMware.

Epen

Generieren Sie die API-Token

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie die API-Token von Ihrem VMware Cloud on AWS-Konto aus.	1. Melden Sie sich bei der VMware Cloud Console an. 2. Wählen Sie in der VMware Cloud Services-Symbolliei ste Mein Konto und dann API-Token aus. 3. Geben Sie einen Namen für Ihr API-Token ein, geben Sie die erforderl iche Lebensdauer an und definieren Sie die Bereiche für das Token. 4. Aktivieren Sie das Kontrollk ästchen ID öffnen und wählen Sie dann Generate aus. 5. Notieren Sie sich die Anmeldeinformationen des API-Tokens. Weitere Informationen dazu finden Sie in der VMware Dokumentation unter Wie generiere ich API-Token.	Cloud-Administrator

Installieren Sie vRealize Automation in Ihrem lokalen Rechenzentrum

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die erforderliche Software herunter.	Laden Sie die VMware vRealize Suite-ISO-Datei von My VMware Portal herunter. Dieses Paket enthält vRealize Suite Lifecycle Manager, VMware Identity Manager und vRealize Automation.	Cloud-Administrator
Installieren Sie die -Software.	Installieren Sie die Software und stellen Sie eine Verbindung zu Ihrem Cloud-SDCC her, indem Sie den Anweisungen unter Installation von vRealize Suite Lifecycle Manager mit Easy Installer for vRealize Automation und VMware Identity Manager in der Dokumentation folgen. VMware **Important** Stellen Sie sicher, dass Folgendes für Ihre Installation verfügbar ist: • Das lokale VMware vCenter Server-Setup und die Anmeldeinformationen	Cloud-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Die Netzwerkdetails für die vRealize Automation-IP und das Subnetz • Der vRealize Automation-Lizenzschlüssel	

VMware Cloud on AWS mit VMware Cloud Assembly Connect

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie Ihre Cloud-Konten.	1. Öffnen Sie in der VMware Cloud-Konsole den Tab Infrastruktur, wählen Sie Verwalten — Cloud-Konten und dann Cloud-Konten hinzufügen. 2. Wählen Sie VMware Cloud on AWS als Typ. 3. Fügen Sie die API-Token-Informationen ein, die Sie zuvor aufgezeichnet haben. Dadurch werden alle verfügbaren Clouds SDDCs in Ihrer VMware Cloud on AWS-Organisation aufgefüllt. 4. Wählen Sie das erforderliche Cloud-SDCC aus und geben Sie dann den vCenter-Benutzernamen und das Kennwort für das SDDC ein.	Cloud-Architekt, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Nachdem Sie erfolgreich authentifiziert wurden, können Sie das integrierte VMware Cloud on AWS-Konto mit dem Status OK anzeigen. Weitere Informationen dazu finden Sie in der VMware Dokumentation unter Erstellen eines VMware Cloud on AWS-Cloud-Kontos in vRealize Automation.	
Konfigurieren Sie das Projekt.	1. Öffnen Sie in der VMware Cloud Console den Tab Projekte und wählen Sie dann Neues Projekt aus. 2. Geben Sie den Namen Ihres Projekts ein. 3. Öffnen Sie die Registerkarte Cloud-Zonen und wählen Sie das VMware Standard-Cloud-on-AWS-Cloud-Konto aus.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Cloud-Zone konfigurieren.	1. Öffnen Sie in der VMware Cloud-Konsole Cloud-Zonen und wählen Sie die Cloud-Zone für Ihr SDDC-Rechenzentrum aus. 2. Standardmäßig hat `cloudadmin@vmc.local` (dies ist die standardmäßige lokale Benutzer-ID für das vCenter des Cloud-SDDC) nur Zugriff auf die Bereitstellung in der. `Compute-ResourcePool` 3. Öffnen Sie die Registerkarte Compute unter Cloud Zones und wählen Sie dann Compute- aus. ResourcePool	Cloud-Administrator
Konfigurieren Sie das Flavor-Mapping.	1. Öffnen Sie die Registerkarte Flavor Mappings und erstellen Sie ein neues Flavor-Mapping. 2. Geben Sie den Flavor-Namen ein, wählen Sie das VMware Cloud on AWS-Konto aus und geben Sie dann die Anzahl von vCPUs und die Speicherm enge an.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Image-Zuordnung.	1. Öffnen Sie Image Mappings und erstellen Sie ein neues Image-Mapping. 2. Geben Sie den Bildnamen ein. 3. Wählen Sie das VMware Cloud on AWS-Konto und stellen Sie die erforderl ichen Cloud-Kontovorlagen bereit.	Cloud-Administrator
Netzwerkprofil konfigurieren.	1. Öffnen Sie das Netzwerkp rofil und erstellen Sie ein neues Netzwerkprofil. 2. Geben Sie den Namen des Netzwerkprofils ein. 3. Öffnen Sie die Registerk arte Netzwerk und wählen Sie das vorhandene Netzwerk aus, das Sie für die Bereitstellung verwenden möchten.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie das Speicherprofil.	1. Öffnen Sie das Speicherprofil und wählen Sie Neues Speicherprofil. 2. Geben Sie den Namen des Speicherprofils ein. 3. Erstellen Sie im Abschnitt Richtlinien eine neue Richtlinie. 4. Wählen Sie Workload Datastore aus. Hat standardmäßig `cloudadmin@vmc.local` nur Zugriff auf die Bereitstellung im Datenspeicher des Workloads.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die Cloud-Vorlage.	1. Öffnen Sie die Registerkarte „Design“, wählen Sie „Cloud-Vorlagen“ und dann „Neu von“ und „Leere Leinwand“. 2. Geben Sie den Namen und die Beschreibung der Cloud-Vorlage an. 3. Wählen Sie das Projekt aus, das Sie zuvor erstellt haben. 4. Ziehen Sie von der Entwurfsseite für Cloud-Template-Ressourcen die Komponenten entsprechend Ihren Anforderungen auf die leere Arbeitsfläche. 5. Wählen Sie Test, um die Vorlage zu testen und etwaige Probleme zu beheben. 6. Wählen Sie Deployment aus und geben Sie den Namen der Deployment ein VMs. Weitere Informationen dazu finden Sie in der VMware Dokumentation unter Erstellen einer einfachen Cloud-Vorlage.	Cloud-Administrator

Zugehörige Ressourcen

- Connect vRealize Automation Version 8.x mit Ihrem SDDC:
- Stellen Sie ein SDDC aus der VMware Cloud auf der AWS-Konsole bereit
- Integration von AWS Direct Connect mit der VMware Cloud auf AWS

Integrieren Sie VMware vRealize Network Insight mit VMware Cloud on AWS

Erstellt von Deepak Kumar (AWS), Piotr Pitera (AWS) und Sachin Trivedi (AWS)

Übersicht

> Hinweis: Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von oder seinen Channel-Partnern weiterverkauft. AWS Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

Dieses Muster beschreibt, wie Sie VMware vRealize Network Insight in VMware Cloud on integrieren AWS und den Verkehrsfluss von Ihren virtuellen Maschinen überprüfen. Diese Integration hilft Ihnen auch bei der Planung von Anwendungsmigrationen zu VMware Cloud on. AWS

vRealize Network Insight bietet Einblick in Ihre Netzwerkinfrastruktur. Es bietet Netzwerküberwachungs- und Analysefunktionen, um die Sicherheit zu verbessern, Migrationsrisiken zu minimieren und die Leistung zu optimieren. Sie können dieses Tool verwenden, um den Datenfluss von Ihren virtuellen Maschinen zu überwachen und empfohlene Sicherheitsregeln auf der Grundlage des beobachteten Datenverkehrs einzusehen. Weitere Informationen zu vRealize Network Insight finden Sie in der VMware Dokumentation.

VMware Cloud on AWS ist ein pay-as-you-go (On-Demand-Dienst), der es Unternehmen jeder Größe ermöglicht, Workloads in VMware vSphere-basierten Cloud-Umgebungen auszuführen, indem sie eine Vielzahl von verwenden. AWS-Services Sie können mit mindestens 2 Hosts pro SDDC-Cluster beginnen und in Ihrer Produktionsumgebung auf bis zu 16 Hosts pro Cluster skalieren. Weitere Informationen finden Sie auf der VMware Cloud AWS on-Website. Weitere Informationen SDDCs finden Sie in der VMware Dokumentation unter Über softwaredefinierte Rechenzentren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- VMware Cloud auf AWS SDDC, bereitgestellt

Einschränkungen

- Bekannte Einschränkungen finden Sie in der VMware Dokumentation.

Produktversionen

- vRealize Network Insight Version 5.0.0
- VMware Cloud auf AWS SDDC Version 1.24

Architektur

Quelltechnologie-Stack

- vRealize Network Insight

Zieltechnologie-Stack

- VMware Cloud an AWS

Zielarchitektur

Das folgende Diagramm zeigt die Konnektivität zwischen VMware Cloud on AWS und vRealize Network Insight vor Ort.

Tools

- VMware Cloud on AWS ist ein integriertes Cloud-Angebot, das gemeinsam von AWS und entwickelt wurde VMware.
- VMware vRealize Network Insight ist ein Überwachungs- und Analysetool, das Einblicke in die Netzwerkinfrastruktur für die Sicherheitsplanung und Fehlerbehebung bietet.

Epen

Richten Sie Ihre Umgebung für vRealize Network Insight ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein VMware Benutzerkonto.	Erstellen Sie ein VMware Benutzerkonto oder melden Sie sich mit Ihrem bestehend en VMware Konto an.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Um ein neues Konto zu eröffnen: 1. Eröffnen Sie ein VMware Customer Connect-Konto, indem Sie das Registrierungsformular ausfüllen. Neue Benutzer erhalten eine E-Mail, um ihre Konten zu aktivieren. 2. Geben Sie den Authentifizierungscode aus der E-Mail ein. 3. Loggen Sie sich bei Customer Connect ein.	
Laden Sie die OVA-Dateien für vRealize Network Insight herunter.	Laden Sie die OVA-Dateien für vRealize Network Insight herunter:. 1. Navigieren Sie zur VMware Produkt-Download-Seite unter https://my.vmware.com/group/vmware/home. 2. Suchen Sie nach vRealize Network Insight. 3. Laden Sie die neuesten Plattform- und Collector-OVA-Dateien von vRealize Network Insight Version 5.0.0 herunter.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie vRealize Network Insight bereit.	Anweisungen zur Bereitstellung finden Sie in der VMware Dokumentation.	Cloud-Administrator

Fügen Sie eine Datenquelle und einen Collector hinzu

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie eine Datenquelle hinzu.	1. Melden Sie sich bei vRealize Network Insight an. 2. Wählen Sie Einstellungen, Konten und Datenquellen, Quelle hinzufügen. 3. Wählen Sie für Typ die Option On-Premise vCenter Server aus. Weitere Informationen finden Sie in der VMware -Dokumentation.	Cloud-Administrator
Richten Sie einen Collector für die Datenquelle ein.	Anweisungen finden Sie in der VMware Dokumentation.	Cloud-Administrator

Analysieren Sie Anwendungsabhängigkeiten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine -Anwendung.	Wenn Sie noch keine Anwendung in vRealize Network Insight haben, folgen Sie den Schritten in der	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	VMware Dokumentation, um eine zu erstellen.	
Entdecken und analysieren Sie Ihre Anwendung.	1. Verwenden Sie vRealize Network Insight, um Ihre Anwendung zu ermitteln . Anweisungen finden Sie in der VMware Dokumentation. 2. Analysieren Sie Ihre Anwendung. Anweisungen finden Sie in der VMware Dokumentation.	Cloud-Administrator

Zugehörige Ressourcen

- Bereitstellen eines VMware SDDC auf AWS mithilfe von VMware Cloud on AWS (AWS Prescriptive Guidance)
- Konfigurieren Sie eine Rechenzentrumserweiterung für VMware Cloud On AWS mithilfe des Hybrid Linked Mode (Prescriptive Guidance)AWS
- Migrieren Sie VMware SDDC AWS unter Verwendung von VMware HCX (Prescriptive Guidance) zur VMware CloudAWS
- VMware Dokumentation zu vRealize Network Insight (Website) VMware

Migrieren VMs Sie mithilfe von HCX OS Assisted Migration zur VMware Cloud auf AWS

Erstellt von Deepak Kumar (AWS) und Himanshu Gupta (AWS)

Übersicht

> Hinweis: Ab dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von oder seinen Channel-Partnern weiterverkauft. AWS Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

Dieses Muster beschreibt, wie eine virtuelle Maschine (VM) mithilfe von OS Assisted Migration (OSAM) von einer Nicht-vSphere-Umgebung zu VMware Cloud on Amazon Web Services (AWS) migriert wird.

OSAM ist Teil der VMware Hybrid Cloud Extension (HCX), die in VMware Cloud on AWS enthalten ist. Sie können OSAM verwenden, um eine Nicht-vSphere-Umgebung wie VMware KVM oder Hyper-V zu Cloud on AWS zu migrieren. VMware OSAM verwendet Sentinel-Software, die Sie auf einer Windows- oder Linux-Gast-VM installieren, um die Replikation der VM aus Ihrer lokalen Umgebung in ein softwaredefiniertes Rechenzentrum (SDDC) in der Cloud auf AWS zu unterstützen. VMware

Dieses Muster erklärt, wie Sie OSAM aktivieren, Sentinel-Software auf einer Windows-VM installieren, eine Verbindung herstellen und sich bei einer HCX Sentinel Gateway (SGW) -Appliance am Quellstandort registrieren und eine Weiterleitungsverbindung mit einer HCX Sentinel Data Receiver (SDR) -Appliance am Zielstandort herstellen, um die Migration zu initiieren.

Weitere Informationen zu OSAM finden Sie in der Dokumentation. VMware

Voraussetzungen und Einschränkungen

Voraussetzungen

- Installieren Sie HCX in Ihren Quell- und Zielumgebungen. Informationen zu den HCX-Voraussetzungen finden Sie unter Migrieren von VMware SDDC zu VMware Cloud on AWS using VMware HCX in der AWS Prescriptive Guidance Guidance-Dokumentation.
- Informationen zu den Voraussetzungen für OSAM finden Sie in der Installationscheckliste in der Dokumentation. VMware

- Informationen zu den OSAM-Ports finden Sie unter VMware HCX-Port-Anforderungen auf der Website VMware Ports and Protocols.

Einschränkungen

- VMware HCX 4.2.0-Konfigurationsgrenzen
- Überlegungen zur OSAM-Bereitstellung
- Unterstützte Gastbetriebssysteme
- Überlegungen zum Gastbetriebssystem

Produktversionen

- VMware HCX 4.2.0
- VMware SDDC 1.12

Architektur

Das folgende Diagramm zeigt, wie HCX OSAM mit der Sentinel-Software zusammenarbeitet, um Nicht-vSphere VMs aus Ihrer lokalen Umgebung in Cloud on AWS zu replizieren. VMware

OSAM besteht aus drei Komponenten:

- Die Sentinel Gateway (SGW) -Appliance, die zur Verbindung und Weiterleitung von Workloads und Anwendungen in der quellenbasierten Umgebung verwendet wird VMware
- Der Sentinel Data Receiver (SDR), der in der VMware Ziel-Cloud-on-AWS-Umgebung verwendet wird, um migrierte Workloads von der Quelle zu empfangen
- Sentinel-Software, die auf jeder Gast-VM installiert sein muss, die Sie migrieren möchten

OSAM verwendet die Sentinel-Software, die auf Windows- oder Linux-Gastsystemen installiert ist, VMs um die Replikation einer lokalen VM auf ein SDDC zu unterstützen. VMware Die Sentinel-Software, die Sie auf dem Gast installieren, VMs sammelt die Systemkonfigurationen von der Gast-VM und unterstützt Sie bei der Datenreplikation. Diese Informationen werden auch verwendet, um das Inventar der Gäste VMs für die Migration zu erstellen und helfen dabei, die Festplatten auf der Replikat-VM für Replikations- und Migrationszwecke vorzubereiten.

Tools

- VMware HCX 4.2.0
- VMware Cloud auf AWS SDDC

Epen

HCX konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie HCX Cloud und HCX Connector bereit.	Folgen Sie den Anweisung en unter HCX Connector- und HCX Cloud-Installationen in der Dokumentation. VMware	Cloud-Administrator, Systemadministrator

OSAM konfigurieren und migrieren VMs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie HCX Sentinel.	So installieren Sie Sentinel unter Linux: 1. Wählen Sie im vCenter Server für den HCX Connector Interconnect, Multi-Site Service Mesh, Sentinel Management aus. 2. Wählen Sie Linux-Paket herunterladen. 3. Installieren Sie den Sentinel-Agenten auf einem Linux-Computer. Weitere Informationen finden Sie in der Dokumentation	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	unter Herunterladen und Installieren der HCX Sentinel Agent-Software. VMware	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Migrieren VMs.	Gehen Sie wie folgt VMs vor, um Ihre eigenen Gruppen (sogenannte Mobilität sgruppen) zu migrieren: 1. Wählen Sie im vSphere Client im HCX-Plug-In Dienste, Migration aus. 2. Wählen Sie Migrate (Migrieren). 3. Wählen Sie Non vSphere Inventory, Remotever bindungen aus. Daraufhin wird die Liste angezeigt VMs , auf der Sie HCX Sentinel installiert haben. 4. Geben Sie unter Gruppenname den Namen der Mobilitätsgruppe ein, die Sie für die erstellen möchten. VMs 5. Wählen VMs Sie die aus, die Sie migrieren möchten, und klicken Sie dann auf Hinzufügen, um sie der Mobilitätsgruppe hinzuzufü gen. 6. Für jede VM: a. Wählen Sie den Ziel-Compute-Container aus. b. Wählen Sie den Zielspeic her aus.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	c. Wählen Sie das Migrationsprofil aus. d. Wählen Sie den Zielordner aus. 7. Um den Migrationsprozess zu starten, wählen Sie Go. HCX validiert Ihre VM-Auswahl, bevor die Migration beginnt. Weitere Informationen finden Sie in der Dokumentation unter Migration virtueller Maschinen mit Mobilitätsgruppen und Überwachung und Schätzung der Migration mit Mobilitätsgruppen. VMware	

Zugehörige Ressourcen

VMware Dokumentation:

- VMware HCX-Benutzerhandbuch
- Installieren Sie die Checkliste B — HCX mit einer VMC SDDC-Zielumgebung
- VMware HCX in der VMware Cloud auf AWS
- HCX OS-unterstützte Migration für die VMware Cloud auf AWS
- VMware HCX 4.2.1 Versionshinweise

Senden Sie mithilfe von VMware Aria Operations AWS for Logs Logs von VMware Cloud on an Splunk

Erstellt von Deepak Kumar (AWS) und Piotr Pitera (AWS)

Übersicht

> Hinweis: Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

Dieses Muster beschreibt, wie VMware AWS Cloud-on-Ereignisse oder -Protokolle mithilfe von VMware Aria Operations for Logs an ein Syslog oder einen HTTP-Endpunkt wie Splunk weitergeleitet werden.

VMware Aria Operations for Logs ist ein Tool zur Protokollanalyse, das eine verbesserte Transparenz und eine beschleunigte Fehlerbehebung in der VMware Cloud-on-Umgebung bietet. AWS Sie können dieses Tool so konfigurieren, dass entweder alle oder ein Teil der Protokolle oder Ereignisse in der VMware Cloud AWS an einen Syslog- oder HTTP-Endpunkt gesendet werden. Der Endpunkt kann entweder ein Software-as-a-Service (SaaS) -Endpunkt oder ein lokaler Endpunkt wie Splunk sein. (Dieses Muster enthält die Anweisungen für Splunk.) Weitere Informationen zu VMware Aria Operations for Logs finden Sie in der VMware Dokumentation.

VMware Cloud on AWS ist ein pay-as-you-go (On-Demand-Dienst), der es Unternehmen jeder Größe ermöglicht, Workloads in VMware vSphere-basierten Cloud-Umgebungen auszuführen, indem sie eine Vielzahl von verwenden. AWS-Services Sie können mit mindestens 2 Hosts pro SDDC-Cluster (Software-Defined Data Center) beginnen und in Ihrer Produktionsumgebung auf bis zu 16 Hosts pro Cluster skalieren. Weitere Informationen finden Sie auf der VMware Cloud on-Website. AWS Weitere Informationen SDDCs finden Sie in der VMware Dokumentation unter Über softwaredefinierte Rechenzentren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Splunk, vor Ort konfiguriert

Einschränkungen

Sie können sich für ein kostenloses Testabonnement für VMware Aria Operations for Logs anmelden. Dieses Abonnement ist 30 Tage gültig und hat die folgenden Einschränkungen:

- Maximale Größe der Protokolle, die Sie weiterleiten können: 50 GB Protokolle pro Tag
- Maximale Anzahl von Konfigurationen für die Protokollweiterleitung, die Sie erstellen können: 10
- Maximale Anzahl von Konfigurationen für die Protokollweiterleitung, die Sie aktivieren können: 5

Um auf alle Servicefunktionen zugreifen zu können, müssen Sie ein Upgrade auf ein Premium-Abonnement durchführen.

Weitere Informationen zu Test- und Premium-Abonnements finden Sie in der VMware Dokumentation unter VMware Aria Operations for Logs (SaaS) -Abonnements und Abrechnung. Weitere Informationen zu Nutzungsbeschränkungen finden Sie in der VMware Dokumentation unter Nutzungsbeschränkungen für Funktionen.

Produktversionen

- VMware Cloud auf AWS SDDC Version 1.24
- VMware Aria-Operationen für Logs Version 8.10
- Lokale Version 9.x von Splunk

Architektur

Quelltechnologie-Stack

- VMware Cloud an AWS
- VMware Aria-Operationen für Logs

Zieltechnologie-Stack

- Splunk vor Ort

Zielarchitektur

Das folgende Diagramm zeigt die Konnektivität zwischen einem Unternehmensrechenzentrum und VMware Aria Operations for Logs in VMware Cloud on AWS.

Tools

- VMware Cloud on AWS ist ein integriertes Cloud-Angebot, das gemeinsam von AWS und entwickelt wurde VMware.
- VMware Aria Operations for Logs ist ein Tool zur Protokollanalyse und Fehlerbehebung für VMware Cloud on AWS.

Epen

Stellen Sie ein SDDC bereit und aktivieren Sie VMware Aria Operation for Logs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie eine VMware Cloud auf AWS SDDC bereit.	Folgen Sie den Anweisung en unter Bereitstellen eines VMware SDDC auf mithilfe AWS von VMware Cloud on AWS in Prescriptive Guidance. AWS	Cloud-Architekt, Cloud-Adm inistrator
Melden Sie sich für VMware Aria Operations for Logs an.	Anweisungen finden Sie in der VMware Dokumentation.	Cloud-Architekt

Stellen Sie einen Cloud-Proxy bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie einen Cloud-Proxy bereit.	Um Logs an eine lokale Instanz von Splunk weiterzul eiten, müssen Sie einen Cloud-Proxy für VMware Aria Operations for Logs hinzufüge n. Dieser Proxy empfängt Informationen vom lokalen Rechenzentrum und sendet	Cloud-Administrator, Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	sie zur Analyse an VMware Aria Operations for Logs. So laden Sie den Cloud-Proxy herunter und installieren ihn: 1. Stellen Sie sicher, dass die Ports 443, 22 und 514 zwischen Ihrer lokalen Umgebung und VMware Cloud on geöffnet sind. AWS Für zusätzliche Ports können Sie 1514/TCP oder 6514/TCP verwenden . Weitere Informationen zu Ports finden Sie in der Dokumentation unter VMware Aria Operations for Logs Firewall-Empfehlungen. VMware 2. Melden Sie sich bei VMware Aria Operations für Logs an. 3. Wählen Sie auf der Startseite im Widget Add Collector aus. 4. Kopieren Sie auf dem Bildschirm Cloud Proxy Virtual Appliance den Token-Schlüssel. Sie müssen diesen Schlüssel innerhalb von 24 Stunden verwenden, um die folgenden Schritte abzuschließen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Wählen Sie den Download-Link für die OVA-Datei. 6. Navigieren Sie zum VMware vSphere Web Client, wählen Sie Ihren Cluster aus und wählen Sie dann OVF-Vorlage bereitstellen aus. 7. Wenn Sie zur Eingabe des Schlüssels aufgefordert werden, fügen Sie den Token-Schlüssel ein, den Sie in Schritt 4 kopiert haben. 8. Wählen Sie Fertig stellen, um den Cloud-Proxy zu installieren.	

Leiten Sie Logs an einen lokalen Splunk-Endpunkt weiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Protokollweiterleitung.	Um Logs an den Splunk-Endpunkt weiterzuleiten: 1. Melden Sie sich bei VMware Aria Operations für Logs an. 2. Navigieren Sie zu Log Management. 3. Wählen Sie Log Forwarding.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie Neue Konfiguration und nehmen Sie die folgenden Einstellungen vor: • Geben Sie einen Namen für die Konfiguration der Protokollweiterleitung ein. • Wählen Sie als Ziel die Option On Premises aus. • Wählen Sie für Cloud Proxy den Cloud-Proxy aus, den Sie zuvor installiert haben. • Wählen Sie als Endpunkttyp die Option TCP aus. • Geben Sie für Endpunkt-URL Ihre lokale Splunk-URL im folgenden Format ein: `tcp://x.x.x.x (your Splunk IP address):514` • (Optional) Für Tags können Sie Tag-Namen und -Werte angeben, um das Abfragen zu erleichtern. • Wählen Sie „Auf alle Protokolle anwenden“ oder „Auf bestimmte Protokolle anwenden“. Wenn Sie alle VMware	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Cloud on AWS-Logs an Splunk senden möchten, wählen Sie Apply to all logs. 5. Wählen Sie Überprüfen. 6. Wählen Sie Speichern. Weitere Informationen finden Sie in der Dokumentation unter Logs from VMware Aria Operations weiterleiten für Logs. VMware	

Zugehörige Ressourcen

- VMware Cloud auf der AWS Website
- Über softwaredefinierte Rechenzentren (VMware Dokumentation)
- Stellen Sie mithilfe AWS von VMware Cloud on ein VMware SDDC bereit (Prescriptive Guidance AWS)AWS
- Migrieren Sie Workloads mithilfe AWS VMware von HCX (Prescriptive Guidance) in die VMware CloudAWS
- Konfigurieren Sie eine Rechenzentrumserweiterung auf VMware Cloud On AWS mithilfe des Hybrid Linked Mode (Prescriptive Guidance)AWS

Richten Sie mithilfe von AWS CDK eine CI/CD-Pipeline für Hybrid-Workloads auf Amazon ECS Anywhere ein und GitLab

Erstellt von Dr. Rahul Sharad Gaikwad (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen.

Amazon ECS Anywhere ist eine Erweiterung des Amazon Elastic Container Service (Amazon ECS). Es bietet Unterstützung für die Registrierung einer externen Instanz, z. B. eines lokalen Servers oder einer virtuellen Maschine (VM), in Ihrem Amazon ECS-Cluster. Diese Funktion hilft, Kosten zu senken und komplexe lokale Container-Orchestrierung und -Operationen zu minimieren. Sie können ECS Anywhere verwenden, um Containeranwendungen sowohl in lokalen als auch in Cloud-Umgebungen bereitzustellen und auszuführen. Dadurch entfällt für Ihr Team die Notwendigkeit, mehrere Bereiche und Fähigkeiten zu erlernen oder komplexe Software eigenständig zu verwalten.

Dieses Muster beschreibt einen step-by-step Ansatz zur Bereitstellung eines Amazon ECS-Clusters mit Amazon ECS Anywhere Anywhere-Instances mithilfe von Amazon Web Services (AWS) Cloud Development Kit (AWS CDK) -Stacks. Anschließend verwenden Sie AWS CodePipeline , um eine Pipeline für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) einzurichten. Anschließend replizieren Sie Ihr GitLab Code-Repository auf AWS CodeCommit und stellen Ihre containerisierte Anwendung auf dem Amazon ECS-Cluster bereit.

Dieses Muster soll denjenigen helfen, die eine lokale Infrastruktur verwenden, um Containeranwendungen auszuführen und die Anwendungscodebasis GitLab zu verwalten. Sie können diese Workloads mithilfe von AWS-Cloud-Services verwalten, ohne Ihre bestehende lokale Infrastruktur zu stören.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine Container-Anwendung, die auf einer lokalen Infrastruktur ausgeführt wird.
- Ein GitLab Repository, in dem Sie Ihre Anwendungscodebasis verwalten. Weitere Informationen finden Sie unter Repository (GitLab).

- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert. Weitere Informationen finden Sie unter Installation oder Aktualisierung der neuesten Version der AWS-CLI (AWS-CLI-Dokumentation).
- AWS CDK Toolkit, global installiert und konfiguriert. Weitere Informationen finden Sie unter Installieren des AWS-CDK (AWS-CDK-Dokumentation).
- npm, installiert und konfiguriert für das AWS-CDK in. TypeScript Weitere Informationen finden Sie unter Node.js und npm herunterladen und installieren (npm-Dokumentation).

Einschränkungen

- Einschränkungen und Überlegungen finden Sie unter Externe Instances (Amazon ECS Anywhere) in der Amazon ECS-Dokumentation.

Produktversionen

- AWS CDK Toolkit Version 2.27.0 oder höher
- npm Version 7.20.3 oder höher
- Node.js Version 16.6.1 oder höher

Architektur

Zieltechnologie-Stack

- AWS-CDK
- AWS CloudFormation
- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- Amazon ECS Anywhere
- Amazon Elastic Container Registry (Amazon ECR)
- AWS Identity and Access Management (IAM)
- AWS-Systemmanager
- GitLab Repositorium

Zielarchitektur

Dieses Diagramm stellt zwei primäre Workflows dar, die in diesem Muster beschrieben werden, nämlich die Bereitstellung des Amazon ECS-Clusters und die Einrichtung der CI/CD pipeline that sets up and deploys the CI/CD Pipeline, wie folgt:

1. Bereitstellung des Amazon ECS-Clusters
    a. Wenn Sie den ersten AWS-CDK-Stack bereitstellen, erstellt er einen CloudFormation Stack auf AWS.
    b. Dieser CloudFormation Stack stellt einen Amazon ECS-Cluster und zugehörige AWS-Ressourcen bereit.
    c. Um eine externe Instance bei einem Amazon ECS-Cluster zu registrieren, müssen Sie den AWS Systems Manager Agent (SSM Agent) auf Ihrer VM installieren und die VM als von AWS Systems Manager verwaltete Instance registrieren.
    d. Sie müssen auch den Amazon ECS-Container-Agenten und Docker auf Ihrer VM installieren, um sie als externe Instance beim Amazon ECS-Cluster zu registrieren.
    e. Wenn die externe Instance registriert und mit dem Amazon ECS-Cluster konfiguriert ist, kann sie mehrere Container auf Ihrer VM ausführen, die als externe Instance registriert ist.
    f. Der Amazon ECS-Cluster ist aktiv und kann die Anwendungs-Workloads über Container ausführen. Die Amazon ECS Anywhere Anywhere-Container-Instance wird in einer lokalen Umgebung ausgeführt, ist aber mit dem Amazon ECS-Cluster in der Cloud verknüpft.
2. Einrichtung und Bereitstellung der CI/CD-Pipeline
    a. Wenn Sie den zweiten AWS-CDK-Stack bereitstellen, erstellt er einen weiteren CloudFormation Stack auf AWS.
    b. Dieser CloudFormation Stack stellt eine Pipeline in CodePipeline und zugehörigen AWS-Ressourcen bereit.
    c. Sie übertragen Änderungen am Anwendungscode per Push und führen sie in ein lokales GitLab Repository zusammen.
    d. Das GitLab Repository wird automatisch in das Repository repliziert. CodeCommit
    e. Die Aktualisierungen des CodeCommit Repositorys werden automatisch gestartet. CodePipeline
    f. CodePipeline kopiert Code aus der CodeCommit integrierten implementierbaren Anwendung und erstellt sie. CodeBuild

g. CodePipeline erstellt ein Docker-Image der CodeBuild Build-Umgebung und überträgt es in das Amazon ECR-Repository.
h. CodePipeline initiiert CodeDeploy Aktionen, die das Container-Image aus dem Amazon ECR-Repo abrufen.
i. CodePipeline stellt das Container-Image auf dem Amazon ECS-Cluster bereit.

Automatisierung und Skalierung

Dieses Muster verwendet das AWS-CDK als Infrastructure-as-Code-Tool (IaC) zur Konfiguration und Bereitstellung dieser Architektur. AWS CDK unterstützt Sie bei der Orchestrierung der AWS-Ressourcen und der Einrichtung von Amazon ECS Anywhere und der CI/CD-Pipeline.

Tools

AWS-Services

- Das AWS Cloud Development Kit (AWS CDK) ist ein Softwareentwicklungs-Framework, das Sie bei der Definition und Bereitstellung der AWS-Cloud-Infrastruktur im Code unterstützt.
- AWS CodeCommit ist ein Versionskontrollservice, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodePipeline hilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Amazon Elastic Container Registry (Amazon ECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.
- Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, schneller Container-Management-Service, der das Ausführen, Beenden und Verwalten von Containern in einem Cluster vereinfacht. Dieses Muster verwendet auch Amazon ECS Anywhere, das Unterstützung für die Registrierung eines lokalen Servers oder einer VM in Ihrem Amazon ECS-Cluster bietet.

Andere Tools

- Node.js ist eine ereignisgesteuerte JavaScript Laufzeitumgebung, die für die Erstellung skalierbarer Netzwerkanwendungen entwickelt wurde.

- npm ist eine Softwareregistrierung, die in einer Node.js -Umgebung ausgeführt wird und verwendet wird, um Pakete gemeinsam zu nutzen oder auszuleihen und die Bereitstellung von privaten Paketen zu verwalten.
- Vagrant ist ein Open-Source-Hilfsprogramm für den Aufbau und die Wartung portabler virtueller Softwareentwicklungsumgebungen. Zu Demonstrationszwecken verwendet dieses Muster Vagrant, um eine lokale VM zu erstellen.

Code-Repository

Der Code für dieses Muster ist in der GitHub CI/CD-Pipeline für Amazon ECS Anywhere unter Verwendung des AWS CDK-Repositorys verfügbar.

Bewährte Methoden

Beachten Sie bei der Bereitstellung dieses Musters die folgenden bewährten Methoden:

- Bewährte Methoden für die Entwicklung und Bereitstellung einer Cloud-Infrastruktur mit dem AWS CDK
- Bewährte Methoden für die Entwicklung von Cloud-Anwendungen mit AWS CDK (AWS-Blogbeitrag)

Epen

Überprüfen Sie die AWS-CDK-Konfiguration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die AWS-CDK-Version.	Überprüfen Sie die Version des AWS CDK Toolkit, indem Sie den folgenden Befehl eingeben. `cdk --version` Für dieses Muster ist Version 2.27.0 oder höher erforderl ich. Wenn Sie eine frühere	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Version haben, folgen Sie den Anweisungen in der AWS CDK-Dokumentation, um sie zu aktualisieren.	
Überprüfen Sie die NPM-Version.	Überprüfen Sie die Version von npm, indem Sie den folgenden Befehl eingeben. `npm --version` Dieses Muster erfordert Version 7.20.3 oder höher. Wenn Sie eine frühere Version haben, folgen Sie den Anweisungen in der npm-Dokumentation, um sie zu aktualisieren.	DevOps Ingenieur

Richten Sie AWS-Anmeldeinformationen ein.	Richten Sie AWS-Anmeldeinformationen ein, indem Sie den `aws configure` Befehl eingeben und den Anweisungen folgen.
	`$aws configure`
	`AWS Access Key ID [None]: <your-access-key-ID>`
	`AWS Secret Access Key [None]: <your-secret-access-key>`
	`Default region name [None]: <your-Region-name>`
	`Default output format [None]:`
		DevOps Ingenieur

Bootstrap für die AWS-CDK-Umgebung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Klonen Sie das AWS-CDK-Code-Repository.	1. Klonen Sie die CI/CD-Pipeline für Amazon ECS Anywhere mithilfe des AWS CDK-Repositorys für dieses Muster, indem Sie den folgenden Befehl eingeben.
	`git clone https://github.com/aws-samples/amazon-ecs-anywhere-cicd-pipeline-cdk-sample.git`
	2. Navigieren Sie in das geklonte Verzeichnis, indem Sie den folgenden Befehl eingeben.
	`cd amazon-ecs-anywhere-cicd-pipeline-cdk-sample`
		DevOps Ingenieur

Bootstrapping für die Umwelt.	Stellen Sie die CloudFormation Vorlage für das Konto und die AWS-Region bereit, die Sie verwenden möchten, indem Sie den folgenden Befehl eingeben. `cdk bootstrap <account-number>/<Region>`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie unter Bootstrapping in der AWS CDK-Dokumentation.	

Aufbau und Bereitstellung der Infrastruktur für Amazon ECS Anywhere

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie die Paketabhängigkeiten und kompilieren Sie die TypeScript Dateien.	Installieren Sie die Paketabhängigkeiten und kompilieren Sie die TypeScript Dateien, indem Sie die folgenden Befehle eingeben.
	`$cd EcsAnywhereCdk`
	`$npm install`
	`$npm fund`
	Mit diesen Befehlen werden alle Pakete aus dem Beispiel-Repository installiert. Weitere Informationen finden Sie unter npm ci und npm install in der npm-Dokumentation. Wenn Sie bei der Eingabe dieser Befehle Fehler über fehlende Pakete erhalten, lesen Sie den Abschnitt zur Fehlerbehebung in diesem Muster.
		DevOps Ingenieur

Erstellen Sie das Projekt.	Geben Sie den folgenden Befehl ein, um den Projektcode zu erstellen. `npm run build`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen zum Erstellen und Bereitstellen des Projekts finden Sie unter Ihre erste AWS-CDK-App in der AWS-CDK-Dokumentation.	

Stellen Sie den Amazon ECS Anywhere Anywhere-Infrastruktur-Stack bereit.	1. Listen Sie die Stacks auf, indem Sie den folgenden Befehl eingeben.
	`$cdk list`
	2. Vergewissern Sie sich, dass die Ausgabe die `ECSAnywherePipelineStack` Stapel `EcsAnywhereInfraStack` und zurückgibt.
	3. Stellen Sie den `EcsAnywhereInfraStack` Stack bereit, indem Sie den folgenden Befehl eingeben.
	`$cdk deploy EcsAnywhereInfraStack`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Erstellung und Ausgabe des Stacks.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation/. 2. Wählen Sie auf der Seite Stacks den `EcsAnywhereInfraStack` Stack aus. 3. Vergewissern Sie sich, dass der Stack-Status entweder `CREATE_IN_PROGRESS` oder `CREATE_COMPLETE` lautet. Die Einrichtung des Amazon ECS-Clusters kann einige Zeit in Anspruch nehmen. Fahren Sie erst fort, wenn die Stack-Erstellung abgeschlossen ist.	DevOps Ingenieur

Richten Sie eine lokale VM ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie Ihre VM ein.	Erstellen Sie eine Vagrant-VM, indem Sie den `vagrant up` Befehl aus dem Stammverzeichnis eingeben, in dem sich Vagrantfile befindet. Weitere	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Informationen finden Sie in der Vagrant-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Registrieren Sie Ihre VM als externe Instanz.	1. Melden Sie sich mit dem `vagrant ssh` Befehl bei der Vagrant-VM an. Weitere Informationen finden Sie in der Vagrant-Dokumentation. 2. Installieren Sie AWS CLI auf der VM, indem Sie die AWS-CLI-Installationsanweisungen befolgen und die folgenden Befehle eingeben. `$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" \ > -o "awscliv2.zip" $sudo apt install unzip $unzip awscliv2.zip $sudo ./aws/install $aws configure AWS Access Key ID [None]: <your-access-key-ID> AWS Secret Access Key [None]: <your-secret-access-key> Default region name [None]: <your-Region-name> Default output format [None]:` 1. Erstellen Sie einen Aktivierungscode und eine ID, mit	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	denen Sie Ihre VM bei AWS Systems Manager registrieren und Ihre externe Instanz aktivieren können. Die Ausgabe dieses Befehls enthält die Werte für die Aktivierungs-ID und den Aktivierungscode.
	
	`aws ssm create-activation \ > --iam-role EcsAnywhereInstanceRole \ > | tee ssm-activation.json`
	
	Wenn Sie bei der Ausführung dieses Befehls eine Fehlermeldung erhalten, finden Sie weitere Informationen im Abschnitt Problembehandlung.
	2. Exportieren Sie die Aktivierungs-ID und die Codewerte.
	
	`export ACTIVATION_ID=<activation-ID> export ACTIVATION_CODE=<activation-code>`
	
	3. Laden Sie das Installationsskript auf Ihre VM herunter.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`curl --proto "https" -o "ecs-anywhere-install.sh" \ > "https://amazon-ecs-agent.s3.amazonaws.com/ecs-anywhere-install-latest.sh"`
	4. Führen Sie das Installationsskript auf Ihrer VM aus.
	`sudo bash ecs-anywhere-install.sh \ --cluster EcsAnywhereCluster \ --activation-id $ACTIVATION_ID \ --activation-code $ACTIVATION_CODE \ --region <region-name>`
	Dadurch wird Ihre VM als externe Amazon ECS Anywhere Anywhere-Instance eingerichtet und die Instance im Amazon ECS-Cluster registriert. Weitere Informationen finden Sie unter Registrierung einer externen Instance in einem Cluster in der Amazon ECS-Dokumentation. Wenn Sie Probleme haben, lesen Sie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den Abschnitt Fehlerbehebung.	

Überprüfen Sie den Status von Amazon ECS Anywhere und der externen VM.	Verwenden Sie die folgenden Befehle, um zu überprüfen, ob Ihre VM mit der Amazon ECS-Steuerebene verbunden ist und läuft.
	`$aws ssm describe-instance-information`
	`$aws ecs list-container-instances --cluster $CLUSTER_NAME`
		DevOps Ingenieur

Stellen Sie die CI/CD-Pipeline bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie einen Zweig im CodeCommit Repo.	Erstellen Sie einen Branch mit dem Namen `main` im CodeCommit Repo, indem Sie den ersten Commit für das Repository erstellen. Sie können der AWS-Dokumentation folgen, um einen Commit zu erstellen CodeCommit. Nachfolgend finden Sie einen Beispielbefehl.
	`aws codecommit put-file \`
	`--repository-name EcsAnywhereRepo \`
	`--branch-name main \`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--file-path README.md \ --file-content "Test" \ --name "Dev Ops" \ --email "devops@example.com" \ --commit-message "Adding README."`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie die Repo-Mirroring ein.	Sie können ein GitLab Repository von und zu externen Quellen spiegeln. Sie können auswählen, welches Repository als Quelle dient. Branches, Tags und Commits werden automatisch synchroni siert. Richten Sie einen Push-Mirror zwischen dem GitLab Repository, das Ihre Anwendung hostet, und dem CodeCommit Repository ein. Anweisungen finden Sie unter Einen Push-Mirror von GitLab bis einrichten CodeCommit (GitLab Dokumentation). **Note** Standardmäßig synchronisiert die Spiegelung das Repository automatis ch. Wenn Sie die Repositorys manuell aktualisieren möchten, finden Sie weitere Informationen unter Einen Mirror aktualisi eren (Dokument ation)GitLab .	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den CI/CD-Pipeline-Stack bereit.	Stellen Sie den `EcsAnywherePipelineStack` Stack bereit, indem Sie den folgenden Befehl eingeben. `$cdk  deploy EcsAnywherePipelineStack`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die CI/CD-Pipeline.	1. Nehmen Sie Änderungen am Anwendungscode vor und übertragen Sie ihn in das lokale GitLab Quell-Repository. Weitere Informationen finden Sie unter Push-Optionen (GitLab Dokumentation). Bearbeiten Sie beispielsweise die `../application/index.html` Datei, um den Versionswert der Anwendung zu aktualisieren. 2. Wenn der Code in das CodeCommit Repository repliziert wird, wird die CI/CD-Pipeline gestartet. Führen Sie eine der folgenden Aktionen aus: • Wenn Sie die automatische Spiegelung verwenden, um das Repository mit dem GitLab Repo zu synchronisieren, fahren Sie mit dem nächsten CodeCommit Schritt fort. • Wenn Sie die manuelle Spiegelung verwenden, übertragen Sie die Änderungen am Anwendungscode in das CodeCommit	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Repository, indem Sie den Anweisungen unter Einen Spiegel aktualisieren (Dokumentation) folgen. GitLab 3. Geben Sie auf Ihrem lokalen Computer in einem Webbrowser http://localhost:80 ein. Dadurch wird die NGINX-Webseite geöffnet, da Port 80 in Vagrantfile an localhost weitergeleitet wird. Vergewissern Sie sich, dass Sie den Wert der aktualisierten Anwendungsversion anzeigen können. Dadurch werden die Pipeline und die Image-Bereitstellung validiert. 4. (Optional) Wenn Sie die Bereitstellung in der AWS-Managementkonsole überprüfen möchten, gehen Sie wie folgt vor: a. Öffnen Sie die Amazon ECS-Konsole unter https://console.aws.amazon.com/ecs/. b. Wählen Sie die zu verwendende Region in der Navigationsleiste aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	c. Klicken Sie im Navigationsbereich auf Cluster. d. Wählen Sie auf der Cluster-Seite den EcsAnywhereCluster Cluster aus. e. Wählen Sie Aufgabendefinitionen. f. Vergewissern Sie sich, dass der Container läuft.	

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Bereinigen und löschen Sie die Ressourcen.	Nachdem Sie dieses Muster durchgegangen sind, sollten Sie die von Ihnen erstellten proof-of-concept Ressourcen entfernen. Geben Sie zum Aufräumen die folgenden Befehle ein.
	`$cdk destroy EcsAnywherePipelineStack`
	`$cdk destroy EcsAnywhereInfraStack`
		DevOps Ingenieur

Fehlerbehebung

Problem	Lösung

Fehler bezüglich fehlender Pakete bei der Installation von Paketabhängigkeiten.	Geben Sie einen der folgenden Befehle ein, um fehlende Pakete zu beheben.
	`$npm ci`
	or
	`$npm install -g @aws-cdk/<package_name>`

Wenn Sie den `aws ssm create-activation` Befehl auf der VM ausführen, erhalten Sie die folgende Fehlermeldung. `An error occurred (ValidationException) when calling the CreateActivation operation: Nonexistent role or missing ssm service principal in trust policy: arn:aws:iam::000000000000:role/EcsAnywhereInstanceRole`	Der `EcsAnywhereInfraStack` Stack ist nicht vollständig bereitgestellt, und die IAM-Rolle, die für die Ausführung dieses Befehls erforderlich ist, wurde noch nicht erstellt. Überprüfen Sie den Stack-Status in der CloudFormation Konsole. Versuchen Sie den Befehl erneut, nachdem sich der Status auf `CREATE_COMPLETE` geändert hat.

Eine Amazon ECS-Zustandsprüfung wird zurückgegeben`UNHEALTHY` , und der folgende Fehler wird im Abschnitt Services des Clusters in der Amazon ECS-Konsole angezeigt.
`service EcsAnywhereService was unable to place a task because no container instance met all of its requirements. Reason: No Container Instances were found in your cluster.`
	Starten Sie den Amazon ECS-Agenten auf Ihrer Vagrant-VM neu, indem Sie die folgenden Befehle eingeben.
	`$vagrant ssh`
	`$sudo systemctl restart ecs`
	`$sudo systemctl status ecs`

Zugehörige Ressourcen

- Amazon ECS Anywhere Anywhere-Marketingseite
- Dokumentation zu Amazon ECS Anywhere
- Amazon ECS Anywhere Anywhere-Demo (Video)
- Amazon ECS Anywhere Anywhere-Workshop-Beispiele (GitHub)
- Spiegelung von Repositorys (GitLab Dokumentation)

Mehr Muster

- Automatisieren Sie die Einrichtung von regionsübergreifendem Peering mit AWS Transit Gateway
- Verwalten Sie lokale Containeranwendungen, indem Sie Amazon ECS Anywhere mit dem AWS CDK einrichten
- Migrieren Sie Hadoop-Daten mithilfe WANdisco LiveData von Migrator zu Amazon S3
- Migrieren Sie VMware VMs mit HCX Automation mithilfe von PowerCLI
- Ändern Sie HTTP-Header, wenn Sie von F5 zu einem Application Load Balancer auf AWS migrieren
- Rehosten Sie lokale Workloads in der AWS-Cloud: Migrationscheckliste
- Verwenden Sie BMC Discovery-Abfragen, um Migrationsdaten für die Migrationsplanung zu extrahieren

Management & Governance

Themen

- Identifizieren und benachrichtigen Sie, wenn Amazon Data Firehose-Ressourcen nicht mit einem AWS KMS Schlüssel verschlüsselt sind
- Automatisieren Sie das Hinzufügen oder Aktualisieren von Windows-Registrierungseinträgen mit AWS Systems Manager
- Automatisches Erstellen eines RFC in AMS mit Python
- Automatisches Stoppen und Starten einer Amazon RDS-DB-Instance mithilfe von AWS Systems Manager Maintenance Windows
- Zentralisieren Sie die Verteilung von Softwarepaketen in AWS Organizations mithilfe von Terraform
- Konfigurieren Sie die Protokollierung für .NET-Anwendungen in Amazon CloudWatch Logs mithilfe von NLog
- Kopieren Sie AWS Service Catalog-Produkte zwischen verschiedenen AWS-Konten und AWS-Regionen
- Erstellen Sie eine RACI- oder RASCI-Matrix für ein Cloud-Betriebsmodell
- Erstellen Sie mithilfe der CloudWatch Amazon-Anomalieerkennung Alarme für benutzerdefinierte Metriken
- Erstellen Sie eine AWS Cloud9 Cloud9-IDE, die Amazon EBS-Volumes mit Standardverschlüsselung verwendet
- Automatisches Erstellen von Tag-basierten CloudWatch Amazon-Dashboards
- Dokumentieren Sie Ihr AWS-Landingzone-Design
- Verbessern Sie die Betriebsleistung, indem Sie Amazon DevOps Guru in mehreren AWS-Regionen, Konten und OUs mit dem AWS CDK aktivieren
- Implementieren Sie Account Factory for Terraform (AFT) mithilfe einer Bootstrap-Pipeline
- AWS Service Catalog-Produkte in mehreren AWS-Konten und AWS-Regionen verwalten
- Migrieren Sie ein AWS-Mitgliedskonto von AWS Organizations zu AWS Control Tower
- Überwachen Sie SAP RHEL Pacemaker-Cluster mithilfe von AWS-Services
- Überwachen Sie die Anwendungsaktivität mithilfe von CloudWatch Logs Insights
- Überwachen Sie die Nutzung eines gemeinsam genutzten Amazon Machine Image über mehrere AWS-Konten
- Benachrichtigungen für programmatische Kontoschließungen in AWS Organizations einrichten

- EBS-Snapshot-Details für Ihr AWS-Konto oder Ihre Organisation anzeigen
- Mehr Muster

Identifizieren und benachrichtigen Sie, wenn Amazon Data Firehose-Ressourcen nicht mit einem AWS KMS Schlüssel verschlüsselt sind

Erstellt von Ram Kandaswamy (AWS)

Übersicht

Aus Compliance-Gründen müssen einige Organisationen die Verschlüsselung für Datenlieferressourcen wie Amazon Data Firehose aktiviert haben. Dieses Muster zeigt eine Möglichkeit, Ressourcen zu überwachen, zu erkennen und zu benachrichtigen, wenn Ressourcen nicht den Vorschriften entsprechen.

Um die Verschlüsselungsanforderungen aufrechtzuerhalten, kann dieses Muster für die automatische Überwachung und Erkennung von Amazon Data Firehose-Lieferressourcen verwendet werden, die nicht mit einem AWS Key Management Service (AWS KMS) -Schlüssel verschlüsselt sind. AWS Die Lösung sendet Warnmeldungen und kann so erweitert werden, dass automatische Problembehebungen durchgeführt werden. Diese Lösung kann auf ein einzelnes Konto oder eine Umgebung mit mehreren Konten angewendet werden, z. B. auf eine Umgebung, die eine AWS landing zone verwendet oder. AWS Control Tower

Voraussetzungen und Einschränkungen

Voraussetzungen

- Amazon Data Firehose-Lieferstream
- Ausreichende Berechtigungen und Vertrautheit mit dem AWS CloudFormation, was bei dieser Infrastrukturautomatisierung verwendet wird

Einschränkungen

- Die Lösung funktioniert nicht in Echtzeit, da sie AWS CloudTrail Ereignisse zur Erkennung verwendet und es eine Verzögerung zwischen der Erstellung einer unverschlüsselten Ressource und dem Senden der Benachrichtigung gibt.

Architektur

Zieltechnologie-Stack

Die Lösung verwendet serverlose Technologie und die folgenden Dienste:

- AWS CloudTrail
- Amazon CloudWatch
- AWS Command Line Interface (AWS CLI)
- AWS Identity and Access Management (ICH BIN)
- Amazon Data Firehose
- AWS Lambda
- Amazon-Simple-Notification-Service (Amazon-SNS)

Zielarchitektur

Das Diagramm veranschaulicht diese Schritte:

1. Ein Benutzer erstellt oder ändert Amazon Data Firehose.
2. Ein CloudTrail Ereignis wurde erkannt und abgeglichen.
3. Lambda wird aufgerufen.
4. Ressourcen, die nicht den Vorschriften entsprechen, werden identifiziert.
5. E-Mail-Benachrichtigung wird gesendet.

Automatisierung und Skalierung

Sie können diese Lösung verwenden AWS CloudFormation StackSets , um diese Lösung mit einem einzigen Befehl auf mehrere Konten AWS-Regionen oder Konten anzuwenden.

Tools

- AWS CloudTrailist ein Programm AWS-Service , das Ihnen dabei hilft, Unternehmensführung, Compliance sowie Betriebs- und Risikoprüfungen Ihres Unternehmens zu ermöglichen AWS-Konto. Aktionen, die von einem Benutzer, einer Rolle oder einem ausgeführt AWS-Service werden, werden als Ereignisse in aufgezeichnet CloudTrail. Zu den Ereignissen gehören Aktionen AWS Management Console, die im Rahmen der API-Operationen AWS CLI AWS SDKs,, und ausgeführt wurden.
- Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS Ressourcen beschreiben, nahezu in Echtzeit.

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie mithilfe AWS-Services von Befehlen in Ihrer Befehlszeilen-Shell interagieren können.
- AWS Identity and Access Management (IAM) ist ein Webdienst, mit dem Sie den Zugriff auf AWS Ressourcen sicher kontrollieren können. Sie verwenden IAM, um zu steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzt) ist, Ressourcen zu nutzen.
- Amazon Data Firehose ist ein vollständig verwalteter Service für die Bereitstellung von Streaming-Daten in Echtzeit. Mit Firehose müssen Sie keine Anwendungen schreiben oder Ressourcen verwalten. Sie konfigurieren Ihre Datenproduzenten zum Senden von Daten an Firehose. Die Daten werden dann automatisch an das angegebene Ziel geliefert.
- AWS Lambdaist ein Rechendienst, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde. Sie zahlen nur für die Rechenzeit, die Sie tatsächlich verbrauchen — es fallen keine Gebühren an, wenn Ihr Code nicht ausgeführt wird.
- Amazon Simple Notification Service (Amazon SNS) ist ein verwalteter Service, der die Nachrichtenzustellung von Verlagen an Abonnenten (auch bekannt als Produzenten und Verbraucher) ermöglicht.

Epen

Setzen Sie Verschlüsselung zur Einhaltung gesetzlicher Vorschriften durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereitstellen AWS CloudFormation StackSets.	Verwenden Sie in der die `firehose-encryption-checker.yaml` Vorlage (im Anhang) AWS CLI, um das Stack-Set zu erstellen, indem Sie den folgenden Befehl ausführen. Geben Sie ein gültiges Amazon SNS SNS-Thema Amazon Resource Name (ARN) für den Parameter ein. Die Bereitstellung sollte erfolgrei	Cloud-Architekt, Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ch CloudWatch Event-Reg eln, die Lambda-Funktion und eine IAM-Rolle mit den erforderlichen Berechtigungen erstellen, wie in der Vorlage beschrieben. `aws cloudformation create-stack-set --stack-set-name my-stack-set -- template-body file:// firehose-encryption-checker.yaml`	
Erstellen Sie Stack-Instanzen.	Stacks können sowohl in einem Konto AWS-Regio nen Ihrer Wahl als auch in einem oder mehreren Konten erstellt werden. Führen Sie den folgenden Befehl aus, um Stack-Instances zu erstellen. Ersetzen Sie den Stackname n, die Kontonummern und die Regionen durch Ihre eigenen. `aws cloudformation create-stack-insta nces --stack-set- name my-stack-set --accounts 123456789 012 223456789012 -- regions us-east-1 us- east-2 us-west-1 us- west-2 --operation- preferences FailureTo leranceCount=1`	Cloud-Architekt, Systemadm inistrator

Zugehörige Ressourcen

- Arbeitet mit AWS CloudFormation StackSets
- Was ist Amazon CloudWatch Events?

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Automatisieren Sie das Hinzufügen oder Aktualisieren von Windows-Registrierungseinträgen mit AWS Systems Manager

Erstellt von Appasaheb Bagali (AWS)

Übersicht

AWS Systems Manager ist ein Fernverwaltungstool für Amazon Elastic Compute Cloud (Amazon EC2) -Instances. Systems Manager bietet Transparenz und Kontrolle über Ihre Infrastruktur auf Amazon Web Services. Dieses vielseitige Tool kann verwendet werden, um Änderungen an der Windows-Registrierung zu korrigieren, die im Bericht über Sicherheitslücken als Sicherheitslücken identifiziert wurden.

In diesem Muster werden die Schritte beschrieben, mit EC2 denen Sie Ihre Instanzen, auf denen das Windows-Betriebssystem ausgeführt wird, schützen können, indem Registrierungsänderungen automatisiert werden, die zum Schutz Ihrer Umgebung empfohlen werden. Das Muster verwendet den Befehl Run, um ein Command-Dokument auszuführen. Der Code ist angehängt, und ein Teil davon ist im Codeabschnitt enthalten.

Voraussetzungen und Einschränkungen

- Ein aktives AWS-Konto
- Berechtigungen für den Zugriff auf die EC2 Instanz und den Systems Manager

Architektur

Zieltechnologie-Stack

- Eine virtuelle private Cloud (VPC) mit zwei Subnetzen und einem NAT-Gateway (Network Address Translation)
- Ein Systems Manager Manager-Befehlsdokument zum Hinzufügen oder Aktualisieren des Registrierungsnamens und -werts
- Systems Manager Run Command, um das Command-Dokument auf den angegebenen EC2 Instanzen auszuführen

Zielarchitektur

Tools

Tools

- IAM-Richtlinien und -Rollen — AWS Identity and Access Management (IAM) ist ein Webservice, mit dem Sie den Zugriff auf AWS-Ressourcen sicher kontrollieren können. Sie verwenden IAM, um zu steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzt) ist, Ressourcen zu nutzen.
- Amazon Simple Storage Service — Amazon Simple Storage Service (Amazon S3) ist ein Speicher für das Internet. Der Service ist darauf ausgelegt, Cloud Computing für Entwickler zu erleichtern. In diesem Muster wird ein S3-Bucket zum Speichern der Systems Manager Manager-Protokolle verwendet.
- AWS Systems Manager — AWS Systems Manager ist ein AWS-Service, mit dem Sie Ihre Infrastruktur auf AWS anzeigen und steuern können. Systems Manager unterstützt Sie bei der Aufrechterhaltung von Sicherheit und Compliance, indem es Ihre verwalteten Instanzen scannt und festgestellte Richtlinienverstöße meldet (oder Korrekturmaßnahmen ergreift).
- AWS Systems Manager Command-Dokument — AWS Systems Manager Command-Dokumente werden von Run Command verwendet. Die meisten Befehlsdokumente werden auf allen Linux- und Windows Server-Betriebssystemen unterstützt, die von Systems Manager unterstützt werden.
- AWS Systems Manager Run Command — Mit AWS Systems Manager Run Command können Sie die Konfiguration Ihrer verwalteten Instances remote und sicher verwalten. Mit Run Command können Sie allgemeine Verwaltungsaufgaben automatisieren und einmalige Konfigurationsänderungen in großem Umfang durchführen.

Code

Sie können den folgenden Beispielcode verwenden, um einen Microsoft Windows-RegistrierungsnamenVersion, einen Registrierungspfad zu HKCU:\Software\ScriptingGuys\Scripts und einen Wert für hinzuzufügen oder zu aktualisieren2.

```
#Windows registry path which needs to add/update
$registryPath ='HKCU:\\Software\\ScriptingGuys\\Scripts'
#Windows registry Name  which needs to add/update
$Name = 'Version'
```

```
#Windows registry value  which needs to add/update
$value = 2
# Test-Path cmdlet to see if the registry key exists.
IF(!(Test-Path $registryPath))
        {
           New-Item -Path $registryPath -Force | Out-Null
           New-ItemProperty -Path $registryPath -Name $name -Value     $value ` -
PropertyType DWORD -                 Force | Out-        Null
        } ELSE {
                      New-ItemProperty -Path $registryPath -Name $name -Value $value `
 -PropertyType            DWORD        -Force | Out-Null
            }
echo 'Registry Path:'$registryPath
 echo 'Registry Name:'$registryPath
 echo 'Registry Value:'(Get-ItemProperty -Path $registryPath -Name $Name).version
```

Das vollständige Codebeispiel für das Systems Manager Manager-Befehlsdokument JavaScript Object Notation (JSON) ist beigefügt.

Epen

Richten Sie eine VPC ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC.	Erstellen Sie in der AWS-Managementkonsole eine VPC mit öffentlichen und privaten Subnetzen und einem NAT-Gateway. Weitere Informationen finden Sie in der AWS-Dokumentation.	Cloud-Administrator
Erstellen Sie Sicherhei tsgruppen.	Stellen Sie sicher, dass jede Sicherheitsgruppe den Zugriff für das Remote Desktop Protocol (RDP) von der Quell-IP-Adresse aus ermöglicht.	Cloud-Administrator

Erstellen Sie eine IAM-Richtlinie und eine IAM-Rolle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Richtlinie.	Erstellen Sie eine IAM-Richtlinie, die Zugriff auf Amazon S3 EC2, Amazon und Systems Manager bietet.	Cloud-Administrator
Erstellen Sie eine IAM-Rolle.	Erstellen Sie eine IAM-Rolle und fügen Sie die IAM-Richtlinie hinzu, die den Zugriff auf Amazon S3 EC2, Amazon und Systems Manager ermöglicht.	Cloud-Administrator

Führen Sie die Automatisierung aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Systems Manager Manager-Befehlsdokument.	Erstellen Sie ein Systems Manager Manager-Befehlsdokument, das die Microsoft Windows-Registrierungsänderungen bereitstellt, die hinzugefügt oder aktualisiert werden sollen.	Cloud-Administrator
Führen Sie den Run Command von Systems Manager aus.	Führen Sie den Systems Manager Run Command aus und wählen Sie das Befehlsdokument und die Systems Manager Manager-Zielinstanzen aus. Dadurch wird die Änderung der Microsoft Windows-Registrierung im ausgewählten Befehlsdo	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	kument auf die Zielinstanzen übertragen.	

Zugehörige Ressourcen

- AWS Systems Manager
- AWS Systems Manager Manager-Dokumente
- AWS Systems Manager Befehl ausführen

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Automatisches Erstellen eines RFC in AMS mit Python

Erstellt von Gnanasekaran Kailasam (AWS)

Übersicht

AWS Managed Services (AMS) hilft Ihnen dabei, Ihre Cloud-basierte Infrastruktur effizienter und sicherer zu betreiben, indem es Ihre Amazon Web Services (AWS) -Infrastruktur kontinuierlich verwaltet. Um eine Änderung an Ihrer verwalteten Umgebung vorzunehmen, müssen Sie einen neuen Änderungsantrag (RFC) erstellen und einreichen, der eine Change Type (CT) -ID für einen bestimmten Vorgang oder eine bestimmte Aktion enthält.

Die manuelle Erstellung eines RFC kann jedoch etwa fünf Minuten dauern, und Teams in Ihrer Organisation müssen möglicherweise RFCs täglich mehrere Anfragen einreichen. Dieses Muster hilft Ihnen, den RFC-Erstellungsprozess zu automatisieren, die Erstellungszeit für jeden RFC zu reduzieren und manuelle Fehler zu vermeiden.

Dieses Muster beschreibt, wie Sie mithilfe von Python-Code automatisch den `Stop EC2 instance` RFC erstellen, der Amazon Elastic Compute Cloud (Amazon EC2) -Instances in Ihrem AMS-Konto stoppt. Sie können dann den Ansatz dieses Musters und die Python-Automatisierung auf andere RFC-Typen anwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein AMS Advanced-Konto. Weitere Informationen dazu finden Sie in den AMS-Betriebsplänen in der AWS Managed Services Services-Dokumentation.
- Mindestens eine bestehende EC2 Instance in Ihrem AMS-Konto.
- Ein Verständnis dafür, wie man RFCs in AMS etwas erstellt und einreicht.
- Vertrautheit mit Python.

Einschränkungen

- Sie können es nur RFCs für Änderungen in Ihrem AMS-Konto verwenden. Ihr AWS-Konto verwendet unterschiedliche Verfahren für ähnliche Änderungen.

Architektur

Technologie-Stack

- AMS
- AWS-Befehlszeilenschnittstelle (AWS Command Line Interface, AWS CLI)
- AWS SDK für Python (Boto3)
- Python und die erforderlichen Pakete (JSON und Boto3)

Automatisierung und Skalierung

Dieses Muster enthält Beispielcode zur Automatisierung des `Stop EC2 instance` RFC, Sie können den Beispielcode und die Vorgehensweise dieses Musters jedoch auch für andere RFCs Zwecke verwenden.

Tools

- AWS Managed Services — AMS hilft Ihnen dabei, Ihre AWS-Infrastruktur effizienter und sicherer zu betreiben.
- AWS CLI — AWS Command Line Interface (AWS CLI) ist ein einheitliches Tool zur Verwaltung Ihrer AWS-Services. In AMS bietet die Change-Management-API Operationen zum Erstellen und Verwalten RFCs.
- AWS SDK for Python (Boto3) — Das SDK für Python macht es einfach, Ihre Python-Anwendung, -Bibliothek oder Ihr Skript in AWS-Services zu integrieren.

Code

Die `AMS Stop EC2 Instance.zip` Datei (angehängt) enthält den Python-Code zum Erstellen eines `Stop EC2 instance` RFC. Sie können diesen Code auch so konfigurieren, dass er einen einzelnen RFC für mehrere EC2 Instanzen sendet.

Epen

Option 1 — Umgebung für macOS oder Linux einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren und validieren Sie Python.	1. Öffnen Sie ein Terminalf enster und führen Sie den `brew install python3` Befehl aus. 2. Stellen Sie sicher, dass Python korrekt installie rt ist, indem `python --version` Sie den Befehl ausführen. 3. Überprüfen Sie, ob die Installation korrekt `pip` ist, indem `pip --version` Sie den Befehl ausführen.	AWS-Systemadministrator
Installieren Sie AWS CLI.	Führen Sie den `pip install awscli --upgrade –user` Befehl aus, um AWS CLI zu installieren.	AWS-Systemadministrator
Installieren Sie Boto3.	Führen Sie den `pip install boto3` Befehl aus, um Boto3 zu installieren.	AWS-Systemadministrator
Installieren Sie JSON.	Führen Sie den `pip install json` Befehl aus, um JSON zu installieren.	AWS-Systemadministrator
Richten Sie AMS CLI ein.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die AMS-Konso le und wählen Sie dann Dokumentation aus. Laden Sie	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die ZIP-Datei herunter, die die AMS-CLI enthält, entpacken Sie sie und installieren Sie sie dann auf Ihrem lokalen Computer. Nachdem Sie AMS CLI installiert haben, führen Sie den `aws amscm help` Befehl aus. Die Ausgabe enthält Informationen über den AMS-Change-Management-Proze ss.	

Option 2 — Umgebung für Windows einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren und validieren Sie Python.	1. Öffnen Sie die Seite Python-Versionen für Windows, laden Sie die neueste Version herunter und installieren Sie dann Python. 2. Stellen Sie sicher, dass Python korrekt installie rt ist, indem `python --version` Sie den Befehl ausführen. 3. Überprüfen Sie, ob die Installation korrekt `pip` ist, indem `pip --version` Sie den Befehl ausführen.	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie AWS CLI.	Führen Sie den `pip install awscli --upgrade –user` Befehl aus, um AWS CLI zu installieren.	AWS-Systemadministrator
Installieren Sie Boto3.	Führen Sie den `pip install boto3` Befehl aus, um Boto3 zu installieren.	AWS-Systemadministrator
Installieren Sie JSON.	Führen Sie den `pip install json` Befehl aus, um JSON zu installieren.	AWS-Systemadministrator
Richten Sie AMS CLI ein.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die AMS-Konsole und wählen Sie dann Dokumentation aus. Laden Sie die ZIP-Datei herunter, die die AMS-CLI enthält, entpacken Sie sie und installieren Sie sie dann auf Ihrem lokalen Computer. Nachdem Sie AMS CLI installiert haben, führen Sie den `aws amscm help` Befehl aus. Die Ausgabe enthält Informationen über den AMS-Change-Management-Prozess	AWS-Systemadministrator

Extrahieren Sie die CT-ID und die Ausführungsparameter für den RFC

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Extrahieren Sie die CT-ID, Version und Ausführungsparameter für den RFC.	Jeder RFC hat eine andere CT-ID, Version und Ausführungsparameter. Sie können diese Informationen mit einer der folgenden Optionen extrahieren: 1. Folgen Sie den Anweisungen im Abschnitt Finding a Request for Change (RFC) with the CLI in RFC-Anwendungsbeispielen aus der AWS Managed Services Services-Dokumentation. 2. Öffnen Sie einen vorhandenen RFC eines ähnlichen Typs oder erstellen Sie einen neuen RFC testweise über die AMS-Konsole. Verwenden Sie die CT-ID und die Ausführungsparameter des RFC. Weitere Informationen dazu finden Sie unter Suchen nach einem RFC mit der Konsole in der AWS Managed Services Services-Dokumentation.	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Um die Python-Automatisierung dieses Musters für andere anzupasse n RFCs, ersetzen Sie den CT-Typ und die Parameterwerte in der `ams_stop_ec2_instance` Python-Codedatei aus der `AMS Stop EC2 Instance.zip` Datei (angehängt) durch die Werte, die Sie extrahiert haben.	

Führen Sie die Python-Automatisierung aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie die Python-Au tomatisierung aus.	1. Laden Sie die `AMS Stop EC2 Instance.zip` Datei (angehängt) auf Ihren lokalen Computer herunter und extrahieren Sie die Datei. 2. Aktualisieren Sie `input_instances` mit Ihren EC2 Instanzin formationen.	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Öffnen Sie ein Terminal und navigieren Sie zum Pfad für Ihren extrahierten Code 4. Führen Sie den Befehl `pythonams_stop_ec2_instance.py` aus.	

Zugehörige Ressourcen

- Was sind Änderungstypen?
- CLI-Tutorial: Zweistufiger Stack mit hoher Verfügbarkeit (Linux/RHEL)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Automatisches Stoppen und Starten einer Amazon RDS-DB-Instance mithilfe von AWS Systems Manager Maintenance Windows

Erstellt von Ashita Dsilva (AWS)

Übersicht

Dieses Muster zeigt, wie eine Amazon Relational Database Service (Amazon RDS) -DB-Instance mithilfe von AWS Systems Manager Maintenance Windows nach einem bestimmten Zeitplan automatisch gestoppt und gestartet wird (z. B. das Herunterfahren einer DB-Instance außerhalb der Geschäftszeiten, um die Kosten zu senken).

AWS Systems Manager Automation stellt die Runbooks `AWS-StopRdsInstance` und `AWS-StartRdsInstance` Runbooks zum Stoppen und Starten von Amazon RDS-DB-Instances bereit. Das bedeutet, dass Sie keine benutzerdefinierte Logik mit AWS Lambda Funktionen schreiben oder eine Amazon CloudWatch Events-Regel erstellen müssen.

Systems Manager bietet zwei Funktionen für die Planung von Aufgaben: State Manager und Maintenance Windows. State Manager legt die erforderliche Statuskonfiguration für Ressourcen in Ihrem Amazon Web Services (AWS) -Konto einmalig oder nach einem bestimmten Zeitplan fest und verwaltet sie. Maintenance Windows führt während eines bestimmten Zeitfensters Aufgaben für die Ressourcen in Ihrem Konto aus. Sie können zwar den Ansatz dieses Musters mit State Manager oder Maintenance Windows verwenden, wir empfehlen jedoch, Maintenance Windows zu verwenden, da damit eine oder mehrere Aufgaben auf der Grundlage der zugewiesenen Priorität ausgeführt werden können und auch AWS Lambda Funktionen und AWS Step Functions Aufgaben ausgeführt werden können. Weitere Informationen zu State Manager und Maintenance Windows finden Sie unter Choising between State Manager und Maintenance Windows in der Systems Manager Manager-Dokumentation.

Dieses Muster enthält detaillierte Schritte zur Konfiguration von zwei separaten Wartungsfenstern, die Cron-Ausdrücke verwenden, um eine Amazon RDS-DB-Instance zu stoppen und dann zu starten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto.
- Eine bestehende Amazon RDS-DB-Instance, die Sie nach einem bestimmten Zeitplan beenden und starten möchten.

- Cron-Ausdrücke für Ihren gewünschten Zeitplan. Beispielsweise `cron(0 9 ? * MON-FRI *)` führt der Ausdruck die Aufgabe an jedem Montag, Dienstag, Mittwoch, Donnerstag und Freitag um 09:00 Uhr aus. Weitere Informationen finden Sie in der Systems Manager Manager-Dokumentation unter Cron- und Rate-Ausdrücke für Wartungsfenster.
- Vertrautheit mit Systems Manager.
- Berechtigungen zum Starten und Stoppen der RDS-Instanz. Weitere Informationen finden Sie im Abschnitt Epics.

Einschränkungen

- Eine Amazon RDS-DB-Instance kann für bis zu sieben Tage gleichzeitig gestoppt werden. Nach sieben Tagen wird die DB-Instance automatisch neu gestartet, um sicherzustellen, dass sie alle erforderlichen Wartungsupdates erhält.
- Sie können eine DB-Instance nicht stoppen, bei der es sich um eine Read Replica handelt oder die über eine Read Replica verfügt.
- Sie können eine Amazon RDS for SQL Server-DB-Instance in einer Multi-AZ-Konfiguration nicht stoppen.
- Servicekontingente gelten für Maintenance Windows und Systems Manager Automation. Weitere Informationen zu Servicekontingenten finden Sie in der Allgemeine AWS-Referenz Dokumentation unter AWS Systems Manager Endpunkte und Kontingente.
- Einige AWS-Services sind nicht in allen AWS-Regionen verfügbar. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie auf der Seite Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Architektur

Das folgende Diagramm zeigt den Workflow zum automatischen Stoppen und Starten einer Amazon RDS-DB-Instance.

Der Workflow umfasst die folgenden Schritte:

1. Erstellen Sie ein Wartungsfenster und verwenden Sie Cron-Ausdrücke, um den Stopp- und Startzeitplan für Ihre Amazon RDS-DB-Instances zu definieren.

2. Registrieren Sie mithilfe des `AWS-StartRdsInstance` Runbooks `AWS-StopRdsInstance` oder eine Systems Manager Automation-Task im Wartungsfenster.

3. Registrieren Sie ein Ziel für das Wartungsfenster, indem Sie eine tagbasierte Ressourcengruppe für Ihre Amazon RDS-DB-Instances verwenden.

Technologie-Stack

- AWS CloudFormation
- AWS Identity and Access Management (IAM)
- Amazon RDS
- Systems Manager

Automatisierung und Skalierung

Sie können mehrere Amazon RDS-DB-Instances gleichzeitig stoppen und starten, indem Sie die erforderlichen Amazon RDS-DB-Instances taggen, eine Ressourcengruppe erstellen, die alle markierten DB-Instances umfasst, und diese Ressourcengruppe als Ziel für das Wartungsfenster registrieren.

Tools

- AWS CloudFormationist ein Service, der Sie bei der Modellierung und Einrichtung Ihrer AWS Ressourcen unterstützt.
- AWS Identity and Access Management (IAM) ist ein Webservice, mit dem Sie den Zugriff auf AWS Ressourcen sicher kontrollieren können.
- Amazon Relational Database Service (Amazon RDS) ist ein Webservice, der die Einrichtung, den Betrieb und die Skalierung einer relationalen Datenbank in der erleichtert. AWS Cloud
- AWS Resource Groupshilft Ihnen, AWS Ressourcen in Gruppen zu organisieren, Ressourcen mit Tags zu versehen und Aufgaben für gruppierte Ressourcen zu verwalten, zu überwachen und zu automatisieren.
- AWS Systems Manageristeine AWS-Service , mit der Sie Ihre Infrastruktur anzeigen und steuern können AWS. Dieses Muster verwendet die folgenden Funktionen von Systems Manager:
  - AWS Systems Manager Die Automatisierung vereinfacht allgemeine Wartungs- und Bereitstellungsaufgaben von Amazon Elastic Compute Cloud (Amazon EC2) -Instances und anderen AWS Ressourcen.

- AWS Systems Manager Maintenance Windows hilft Ihnen dabei, einen Zeitplan für die Ausführung potenziell störender Aktionen an Ihren Instances zu definieren.

Epen

Erstellen und konfigurieren Sie die IAM-Servicerolle für Systems Manager Automation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die IAM-Servicerolle für Systems Manager Automation.	Melden Sie sich bei der an AWS Management Console und erstellen Sie eine Servicerolle für Systems Manager Automation. Sie können eine der folgenden beiden Methoden verwenden , um diese Servicerolle zu erstellen: • Wird verwendet AWS CloudFormation , um eine Servicerolle für Systems Manager Automation zu konfigurieren • Verwenden Sie IAM, um Rollen für Systems Manager Automation zu konfigurieren Der Systems Manager Automation-Workflow ruft Amazon RDS auf, indem er eine Servicerolle verwendet, um Start- und Stoppaktionen auf der Amazon RDS-DB-In stance durchzuführen.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Die Servicerolle muss mit der folgenden Inline-Richtlinie konfiguriert werden, die über Berechtigungen zum Starten und Stoppen der Amazon RDS-DB-Instance verfügt: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "RdsStartStop", "Effect": "Allow", "Action": [ "rds:StopDBInstance", "rds:StartDBInstance" ], "Resource": "<RDS_Instance_ARN>" }, { "Sid": "RdsDescribe", "Effect": "Allow", "Action": "rds:DescribeDBInstances", "Resource": "*" } ] }`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Stellen Sie sicher, dass Sie es `<RDS_Instance_ARN>` durch den Amazon Resource Name (ARN) Ihrer Amazon RDS-DB-Instance ersetzen. Wenn Sie mit der Verwendung von IAM-Richtlinien und -Rollen nicht vertraut sind, folgen Sie den Anweisungen im Abschnitt Lösungsübersicht des AWS Systems Manager Blogposts „Amazon RDS stop and start use“ planen. **Important** Stellen Sie sicher, dass Sie den ARN der Servicerolle aufzeichnen.	

Erstellen Sie eine Ressourcengruppe

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Kennzeichnen Sie die Amazon RDS-DB-Instances.	Öffnen Sie die Amazon RDS-Konsole und kennzeichnen Sie die Amazon RDS-DB-Instances, die Sie der Ressourcengruppe hinzufügen möchten. Ein Tag besteht aus Metadaten, die einer AWS Ressource zugewiesen	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	sind, und besteht aus einem Schlüssel-Wert-Paar. Wir empfehlen, Action als Tag-Schlüssel und StartStopals Wert zu verwenden. Weitere Informationen dazu finden Sie in der Amazon RDS-Dokumentation unter Hinzufügen, Auflisten und Entfernen von Tags.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Ressource ngruppe für Ihre markierten Amazon RDS-DB-Instances.	Öffnen Sie die AWS Resource Groups Konsole und erstellen Sie eine Ressourcengruppe auf der Grundlage des Tags, das Sie für Ihre Amazon RDS-DB-Instances erstellt haben. Stellen Sie sicher, dass Sie unter Gruppierungskriterien AWS: :RDS:: DBInstance als Ressourcentyp auswählen und dann das Schlüssel-Wert-Paar des Tags angeben (z. B. „Action-“). StartStop Dadurch wird sicherges tellt, dass der Service nur nach Amazon RDS-DB-In stances sucht und nicht nach anderen Ressourcen, die über dieses Tag verfügen. Stellen Sie sicher, dass Sie den Namen der Ressource ngruppe aufzeichnen. Weitere Informationen und detaillierte Schritte finden Sie in der AWS Resource Groups Dokumentation unter Erstellen einer tagbasierten Abfrage und Erstellen einer Gruppe.	AWS-Administrator

Konfigurieren Sie ein Wartungsfenster zum Stoppen der Amazon RDS-DB-Instances

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Wartungsfenster.	1. Öffnen Sie die Systems Manager Manager-Konsole, wählen Sie Maintenance Windows und anschließend Create a Maintenance Window aus. Geben Sie einen Namen für Ihr Wartungsfenster ein (z. B. "StopRdsInstance„), geben Sie eine Beschreibung ein und deaktivieren Sie dann die Option Nicht registrierte Ziele zulassen. 2. Wählen Sie Cron/Rate expression und geben Sie den Zeitplanausdruck an, um zu definieren, wann die Amazon RDS-DB-Instances gestoppt werden sollen. Geben Sie 1 für die Dauer und 0 für „Aufgaben beenden“ ein. Standardmäßig wird in der Zeitzone UTC angezeigt. Sie können die Zeitzone ändern, um das Wartungsfenster auf der Grundlage des in Ihrem Cron-Ausdruck definierten Zeitstempels zu starten. 3. Wählen Sie Create maintenance window (Wartungsfenster erstellen	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	) aus. Das System kehrt zur Seite des Wartungsfensters zurück, und der Status Ihres Wartungsfensters ist Aktiviert. ⚠ Important Die Aufgabe zum Stoppen der DB-Instance wird fast sofort ausgeführt, wenn sie initiiert wird, und erstreckt sich nicht über die gesamte Dauer des Wartungsfensters. Dieses Muster enthält die Mindestwerte für die Dauer und die Initiierung von Aufgaben beenden, da es sich dabei um die erforderlichen Parameter für ein Wartungsfenster handelt. Weitere Informationen und detaillierte Schritte finden Sie unter Erstellen eines Wartungsfensters (Konsole) in der Systems Manager Manager-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Weisen Sie dem Wartungsfenster ein Ziel zu.	1. Wählen Sie in der Systems Manager Manager-Konsole Maintenance Windows, dann Actions und anschließend Register targets aus. 2. Geben Sie im Bereich Ziele die Option Ressourcengruppe auswählen und wählen Sie dann den Namen einer vorhandenen Ressourcengruppe in Ihrem Konto aus. 3. Wählen Sie für Ressourcentypen AWS: :RDS:: DBInstance und wählen Sie dann Ziel registrieren aus. Weitere Informationen und detaillierte Schritte finden Sie unter Zuweisen von Zielen zu einem Wartungsfenster (Konsole) in der Systems Manager Manager-Dokumentation.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Weisen Sie dem Wartungsfenster eine Aufgabe zu.	1. Wählen Sie in der Systems Manager Manager-Konsole Maintenance Windows und dann Ihr Wartungsfenster aus. Wählen Sie Aktionen und anschließend Automatisierungsaufgabe registrieren aus. 2. Wählen Sie für Dokument die Option AWS- StopRdsInstance. 3. Wählen Sie im Abschnitt Ziele die Option Registrierte Zielgruppen auswählen und wählen Sie dann das Wartungsfensterziel aus, das Sie für das aktuelle Wartungsfenster registriert haben. 4. Geben Sie für die Ratensteuerung 100 Prozent für Parallelität und Fehlerschwellenwert an. Sie können die Werte für die Ratenkontrolle entsprechend Ihren Anforderungen an die Parallelität von Aufgaben und den Schwellenwert für Fehler ändern. Weitere Informationen dazu finden Sie in der Systems Manager Manager-Dokumentation	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	unter Über Parallelität und Fehlerschwellenwerte. 5. Lassen Sie dieses Feld im Abschnitt IAM-Servicerolle für Servicerolle leer oder erstellen Sie Ihre eigene benutzerdefinierte Rolle. Wenn Sie das Feld leer lassen, erstellt Systems Manager automatisch die serviceverknüpfte Rolle AWSServiceRoleForAmazonSSM und ordnet die Rolle dann der Aufgabe zu. Informationen zum Erstellen Ihrer eigenen benutzerdefinierten Rolle finden Sie unter Erstellen einer benutzerdefinierten Servicerolle für Wartungsfenster (Konsole) und ordnen Sie diese benutzerdefinierte Rolle dann der Aufgabe zu. 6. Geben Sie im Abschnitt Eingabeparameter die folgenden Parameter für das Runbook an: • InstanceId: `{{RESOURCE_ID}}` **Note** Denn ein Pseudo-Parameter	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wird verwendet InstanceId, um die Amazon RDS-DB-Ressourcen-ID aus dem ARN zu extrahieren. Weitere Informationen zu Pseudo-Parametern finden Sie unter Über Pseudo-Parameter in der Systems Manager Manager-Dokumentation. • AutomationAssumeRole: Geben Sie den ARN der Servicerolle an, die Sie für Systems Manager Automation erstellt haben. 7. Wählen Sie Automatisierungsaufgabe registrieren aus. ⚠ Important Die Option Servicerolle definiert die Servicerolle, die für das Wartungsfenster zur Ausführung von	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Aufgaben erforderl ich ist. Diese Rolle ist jedoch nicht identisch mit der Servicero lle, die Sie zuvor für Systems Manager Automation erstellt haben. Weitere Informationen und detaillierte Schritte finden Sie unter Zuweisen von Aufgaben zu einem Wartungsf enster (Konsole) in der Systems Manager Manager-D okumentation.	

Konfigurieren Sie ein Wartungsfenster zum Starten der Amazon RDS-DB-Instances

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie ein Wartungsfenster, um die Amazon RDS-DB-Instances zu starten.	Wiederholen Sie die Schritte aus dem Fenster Wartung konfigurieren, um die Amazon RDS-DB-Instances zu beenden. Epic, um ein weiteres Wartungsfenster zu konfigurieren, um die Amazon RDS-DB-Instances zu einem geplanten Zeitpunkt zu starten.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Important Sie müssen die folgenden Änderungen vornehmen, wenn Sie das Wartungsfenster für den Start der DB-Instances konfiguri eren: • Verwenden Sie einen neuen Namen für das Wartungsf enster (z. B. "StartRds Instance„). • Ersetzen Sie den Cron-Ausdruck durch den Cron-Ausdruck, den Sie zum Starten der DB-Instances verwenden möchten. • Ersetzen Sie das **`AWS-StopRdsInstance`** Runbook durch in Task. **`AWS-StartRdsInstan ce`**	

Zugehörige Ressourcen

- Verwenden Sie Dokumente von Systems Manager Automation, um Instanzen zu verwalten und Kosten außerhalb der Geschäftszeiten zu senken (AWS Blogbeitrag)

Zentralisieren Sie die Verteilung von Softwarepaketen in AWS Organizations mithilfe von Terraform

Erstellt von Pradip kumar Pandey (AWS), Aarti Rajput (AWS), Chintamani Aphale (AWS), T.V.R.L.Phani Kumar Dadi (AWS), Mayuri Shinde (AWS) und Pratap Kumar Nanda (AWS)

Übersicht

Unternehmen verwalten AWS-Konten häufig mehrere AWS-Regionen , die auf mehrere verteilt sind, um eine starke Isolationsbarriere zwischen Workloads zu schaffen. Um sicher und konform zu bleiben, installieren ihre Verwaltungsteams agentenbasierte Tools wie CrowdStrikeSentinelOne, oder TrendMicroTools für Sicherheitsscans sowie den CloudWatch Amazon-Agenten, den Datadog Agent oder AppDynamics Agenten für die Überwachung. Diese Teams stehen oft vor Herausforderungen, wenn sie die Verwaltung und Verteilung von Softwarepaketen in dieser großen Landschaft zentral automatisieren wollen.

Distributor, eine Funktion von AWS Systems Manager, automatisiert den Prozess der Paketierung und Veröffentlichung von Software auf verwalteten Microsoft Windows- und Linux-Instanzen in der Cloud und auf lokalen Servern über eine einzige, vereinfachte Oberfläche. Dieses Muster zeigt, wie Sie Terraform verwenden können, um den Prozess der Verwaltung der Softwareinstallation weiter zu vereinfachen und Skripts mit minimalem Aufwand für eine große Anzahl von Instanzen und Mitgliedskonten auszuführen. AWS Organizations

Diese Lösung funktioniert für Amazon-, Linux- und Windows-Instances, die von Systems Manager verwaltet werden.

Voraussetzungen und Einschränkungen

- Ein Distributor-Paket, das die zu installierende Software enthält
- Terraform Version 0.15.0 oder höher
- Amazon Elastic Compute Cloud (Amazon EC2) -Instances, die von Systems Manager verwaltet werden und über grundlegende Berechtigungen für den Zugriff auf Amazon Simple Storage Service (Amazon S3) im Zielkonto verfügen
- Eine landing zone für Ihre Organisation, die eingerichtet wird mit AWS Control Tower
- (Optional) Account Factory für Terraform (AFT)

Architektur

Einzelheiten zur Ressource

Dieses Muster verwendet Account Factory for Terraform (AFT), um alle erforderlichen AWS Ressourcen und die Code-Pipeline für die Bereitstellung der Ressourcen in einem Bereitstellungskonto zu erstellen. Die Code-Pipeline wird in zwei Repositorys ausgeführt:

- Die globale Anpassung enthält Terraform-Code, der auf allen bei AFT registrierten Konten ausgeführt wird.
- Kontoanpassungen enthalten Terraform-Code, der im Bereitstellungskonto ausgeführt wird.

Sie können diese Lösung auch ohne AFT bereitstellen, indem Sie Terraform-Befehle im Ordner für Kontoanpassungen ausführen.

Der Terraform-Code stellt die folgenden Ressourcen bereit:

- AWS Identity and Access Management (IAM) Rolle und Richtlinien
  - SystemsManager- AutomationExecutionRole gewährt dem Benutzer Berechtigungen zum Ausführen von Automatisierungen in den Zielkonten.
  - SystemsManager- AutomationAdministrationRole gewährt dem Benutzer Berechtigungen zum Ausführen von Automatisierungen in mehreren Konten und Organisationseinheiten ()OUs.
- Komprimierte Dateien und manifest.json für das Paket
  - In Systems Manager enthält ein Paket mindestens eine ZIP-Datei mit Software oder installierbaren Ressourcen.
  - Das JSON-Manifest enthält Verweise auf Ihre Paketcodedateien.
- S3-Bucket
  - Das verteilte Paket, das von der gesamten Organisation gemeinsam genutzt wird, wird sicher in einem Amazon S3 S3-Bucket gespeichert.
- AWS Systems Manager Dokumente (SSM-Dokumente)
  - `DistributeSoftwarePackage`enthält die Logik zur Verteilung des Softwarepakets an jede Zielinstanz in den Mitgliedskonten.
  - `AddSoftwarePackageToDistributor`enthält die Logik, um die installierbaren Software-Ressourcen zu verpacken und sie der Automatisierung hinzuzufügen, eine Funktion von AWS Systems Manager.
- Systems Manager -Zuordnung.

- Für die Bereitstellung der Lösung wird eine Systems Manager Manager-Zuordnung verwendet.

Architektur und Arbeitsablauf

Die Abbildung zeigt die folgenden Schritte:

1. Um die Lösung von einem zentralen Konto aus auszuführen, laden Sie Ihre Pakete oder Software zusammen mit den Bereitstellungsschritten in einen S3-Bucket hoch.
2. Ihr maßgeschneidertes Paket wird im Bereich Dokumente der Systems Manager Manager-Konsole auf der Registerkarte Mein Eigentum verfügbar.
3. State Manager, eine Funktion von Systems Manager, erstellt, plant und führt eine Zuordnung für das Paket in der gesamten Organisation aus. Die Zuordnung gibt an, dass das Softwarepaket auf einem verwalteten Knoten installiert und ausgeführt werden muss, bevor es auf dem Zielknoten installiert werden kann.
4. Die Assoziation weist Systems Manager an, das Paket auf dem Zielknoten zu installieren.
5. Für alle nachfolgenden Installationen oder Änderungen können Benutzer dieselbe Zuordnung regelmäßig oder manuell von einem einzigen Standort aus ausführen, um kontenübergreifende Bereitstellungen durchzuführen.
6. Bei Mitgliedskonten sendet Automation Bereitstellungsbefehle an den Distributor.
7. Der Distributor verteilt Softwarepakete auf mehrere Instanzen.

Diese Lösung verwendet das interne Verwaltungskonto AWS Organizations, aber Sie können auch ein Konto (delegierter Administrator) angeben, das dieses Konto im Namen der Organisation verwaltet.

Tools

AWS-Services

- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt. Dieses Muster verwendet Amazon S3, um das verteilte Paket zu zentralisieren und sicher zu speichern.
- AWS Systems Managerhilft Ihnen bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der AWS Cloud ausgeführt werden. Es vereinfacht das Anwendungs- und Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme

und hilft Ihnen, Ihre AWS Ressourcen sicher und in großem Umfang zu verwalten. Dieses Muster verwendet die folgenden Systems Manager Manager-Funktionen:

  - Der Distributor unterstützt Sie beim Paketieren und Veröffentlichen von Software auf verwalteten Systems Manager-Instanzen.
  - Die Automatisierung vereinfacht allgemeine Wartungs-, Bereitstellungs- und Problembehebungsaufgaben für viele AWS Dienste.
  - Documents führt Aktionen auf Ihren von Systems Manager verwalteten Instanzen in Ihrer Organisation und Ihren Konten durch.
- AWS Organizationsist ein Kontoverwaltungsservice, der Ihnen hilft, mehrere AWS Konten in einer Organisation zu konsolidieren, die Sie erstellen und zentral verwalten.

Andere Tools

- Terraform ist ein IaC-Tool (Infrastructure as Code) HashiCorp , mit dem Sie Cloud- und lokale Ressourcen erstellen und verwalten können.

Code-Repository

Die Anweisungen und der Code für dieses Muster sind im Repository für die GitHub zentralisierte Paketverteilung verfügbar.

Bewährte Methoden

- Um einer Assoziation Tags zuzuweisen, verwenden Sie die AWS Command Line Interface (AWS CLI) oder die AWS -Tools für PowerShell. Das Hinzufügen von Tags zu einer Zuordnung über die Systems-Manager-Konsole wird nicht unterstützt. Weitere Informationen finden Sie unter Tagging Systems Manager Manager-Ressourcen in der Systems Manager Manager-Dokumentation.
- Um eine Zuordnung mithilfe einer neuen Version eines Dokuments auszuführen, das von einem anderen Konto aus geteilt wurde, legen Sie die Dokumentversion auf `default` fest.
- Um nur den Zielknoten zu taggen, verwenden Sie einen Tag-Schlüssel. Wenn Sie Ihre Knoten mithilfe mehrerer Tag-Schlüssel als Ziel verwenden möchten, verwenden Sie die Option Resource Group.

Epen

Konfigurieren Sie Quelldateien und Konten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Klonen Sie das Repository	1. Klonen Sie das GitHub zentrale Repository für die Paketverteilung:
	`git clone https://github.com/aws-samples/aws-organization-centralised-package-distribution`
	2. Das Terraform-Code-Repository benötigt zwei Anpassungsordner, die von AFT verwaltet werden. Vergewissern Sie sich, dass Ihre lokale Kopie des Repositorys diese Ordner enthält:
	`$ cd centralised-package-distribution`
	`$ ls`
	`global-customization account-customization`
		DevOps Ingenieur

Aktualisieren Sie globale Variablen.	Aktualisieren Sie die folgenden Eingabeparameter in der `global-customization/variables.tf` Datei. Diese Variablen gelten für alle	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Konten, die von AFT erstellt und verwaltet werden. • `account_id` : Die ID des Kontos, auf dem die Distributor-Lösung bereitgestellt wird. • `aws_region` : Der AWS-Region Ort, an dem die Assoziation bereitgestellt wird.	
Kontovariablen aktualisieren.	Aktualisieren Sie die folgenden Eingabeparameter in der `account-customization/variables.tf` Datei. Diese Variablen gelten nur für bestimmte Konten, die von AFT erstellt und verwaltet werden. • `package_bucket_name` : Der Name des S3-Buckets, der die Paketvertrauensdatei enthält. • `package_name` : Der Name der Paketvertrauensdatei. • `package_version` : Die Paketversion des Installers.	DevOps Ingenieur

Passen Sie Parameter und Bereitstellungsdateien an

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Eingabeparameter für die State Manager-Zuordnung.	Aktualisieren Sie die folgenden Eingabepa rameter in der `account-c ustomization/assoc iation.tf` Datei, um den Status zu definieren, den Sie für Ihre Instances beibehalt en möchten. Sie können die Standardparameterwerte verwenden, wenn sie Ihren Anwendungsfall unterstützen. • `targetAccounts` : Die Organisationseinheit (OU) IDs innerhalb von AWS Organizations, die Konten mit den Ziel-Instances für die Verteilung darstellt. OU IDs beginnt mit „ou“. • `targetRegions` : Die AWS-Regionen (zum Beispiel „us-east-1″ oder“ ap-southeast-2“), auf der die Ziel-Instances ausgeführt werden. • `action`: Geben Sie an, ob das Paket installiert oder deinstalliert werden soll. • `installationType` : Einer der folgenden Installat ionstypen:	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `uninstall` : Das Paket ist deinstalliert. • `reinstall` : Die Anwendung wird offline geschaltet, bis der Neuinstallationsvorgang abgeschlossen ist. • `In-place update`: Die Anwendung ist verfügbar , solange neue oder aktualisierte Dateien zur Installation hinzugefügt werden. • `name`: Der Name des Pakets, das installiert oder deinstalliert werden soll. • `version`: Die Version des Pakets, das installiert oder deinstalliert werden soll. Wenn keine Version des Pakets installiert ist, gibt das System einen Fehler zurück. • `bucketName` : Der S3-Bucket-Name, unter dem das Paket bereitgestellt wurde. Dieser Bucket sollte nur aus den Paketen und der Manifestdatei bestehen. • `bucketPrefix` : Das S3-Präfix, in dem die Paket-Ass ets gespeichert sind. • `AutomationAssumeRo le` : Der Amazon-Re	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ssourcenname (ARN) von`SystemsManager-AutomationAdministrationRole` .	
Bereiten Sie die komprimierten Dateien und die `manifest.json` Datei für das Paket vor.	Dieses Muster enthält PowerShell installierbare Beispieldateien (.msi für Windows und .rpm für Linux) mit Installations- und Deinstallationsskripten im Ordner. `account-customization/package` 1. Ersetzen Sie die PowerShell installierbaren Dateien durch Ihre eigenen Dateien oder stellen Sie Ihre installierbare Datei, Installations- und Deinstallationsskripts und die Manifestdatei bereit, um ein Paket in dem `account-customization` Ordner in Ihrem Konto zu erstellen. 2. Passen Sie die `manifest.json` Standarddatei, die Terraform im `account-customization` Ordner generiert, Ihren Anforderungen entsprechend an.	DevOps Ingenieur

Führen Sie Terraform-Befehle aus, um Ressourcen bereitzustellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Initialisieren Sie die Terraform-Konfiguration.	Um die Lösung automatisch mit AFT bereitzustellen, senden Sie den Code an: AWS CodeCommit
	`$ git add *`
	`$ git commit -m "message"`
	`$ git push`
	Sie können diese Lösung auch ohne AFT bereitstellen, indem Sie einen Terraform-Befehl aus dem `account-customization` Ordner ausführen. Um das Arbeitsverzeichnis zu initialisieren, das die Terraform-Dateien enthält, führen Sie folgenden Befehl aus:
	`$ terraform init`
		DevOps Ingenieur

Änderungen in der Vorschau anzeigen.	Führen Sie den folgenden Befehl aus, um eine Vorschau der Änderungen anzuzeigen, die Terraform an der Infrastruktur vornehmen wird: `$ terraform plan` Dieser Befehl wertet die Terraform-Konfiguration aus,	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	um den gewünschten Status der deklarierten Ressourcen zu ermitteln. Außerdem wird der gewünschte Status mit der tatsächlichen Infrastru ktur verglichen, die innerhalb des Workspace bereitgestellt werden soll.	
Änderungen übernehmen.	Führen Sie den folgenden Befehl aus, um die Änderunge n zu implementieren, die Sie an den `variables.tf` Dateien vorgenommen haben: `$ terraform apply`	DevOps Ingenieur

Ressourcen validieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie die Erstellung von SSM-Dokumenten.	1. Wählen Sie in der Systems Manager Manager-K onsole im linken Navigatio nsbereich Dokumente aus. 2. Wählen Sie die Registerk arte Owned by me (In meinem Besitz) aus. Sie sollten die `AddSoftwa rePackageToDistrib utor` Pakete `Distribut`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`eSoftwarePackage` und sehen.	
Bestätigen Sie den erfolgreichen Einsatz von Automatisierungen.	1. Wählen Sie in der Systems Manager Manager-Konsole im linken Navigationsbereich Automation aus. 2. In der Liste der Automatisierungsausführungen sollten Sie die neuesten Versionen `DistributeSoftwarePackage` und `AddSoftwarePackageToDistributor` Bereitstellungen sehen. 3. Wählen Sie die Ausführungs-ID, um zu überprüfen, ob sie erfolgreich abgeschlossen wurden.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass das Paket für die ausgewählten Mitgliedskonten-Instanzen bereitgestellt wurde.	1. Wählen Sie in der Systems Manager Manager-Konsole im Navigationsbereich die Option Befehl ausführen aus. 2. Im Befehlsverlauf sehen Sie jeden Aufruf und seinen Status. 3. Wählen Sie eine beliebige Befehls-ID, um den Bereitstellungsverlauf für jede Zielinstanz anzuzeige n. 4. Wählen Sie die Instanz-ID und suchen Sie im Abschnitt Ausgabe nach der Distribution.	DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Die State Manager-Zuordnung ist fehlgesch lagen oder befindet sich im Status „Ausstehe nd“.	Informationen zur Fehlerbehebung finden Sie im AWS Knowledge Center.
Eine geplante Verknüpfung konnte nicht ausgeführt werden.	Ihre Zeitplanspezifikation ist möglicherweise ungültig. State Manager unterstützt derzeit nicht die Angabe von Monaten in Cron-Ausd rücken für Assoziationen. Verwenden Sie Cron- oder Rate-Ausdrücke, um den Zeitplan zu bestätigen.

Zugehörige Ressourcen

- Zentralisierte Paketverteilung (GitHub Repository)
- Account Factory für Terraform (AFT)
- Anwendungsfälle und bewährte Verfahren (Dokumentation)AWS Systems Manager

Konfigurieren Sie die Protokollierung für .NET-Anwendungen in Amazon CloudWatch Logs mithilfe von NLog

Erstellt von Bibhuti Sahu (AWS) und Rob Hill (AWS) (AWS)

Übersicht

Dieses Muster beschreibt, wie das NLog Open-Source-Logging-Framework verwendet wird, um die Nutzung von.NET-Anwendungen und Ereignisse in Amazon CloudWatch Logs zu protokollieren. In der CloudWatch Konsole können Sie die Protokollnachrichten der Anwendung nahezu in Echtzeit einsehen. Sie können auch Messwerte einrichten und Alarme so konfigurieren, dass Sie benachrichtigt werden, wenn ein Metrik-Schwellenwert überschritten wird. Mithilfe von CloudWatch Application Insights können Sie automatisierte oder benutzerdefinierte Dashboards anzeigen, die potenzielle Probleme für die überwachten Anwendungen aufzeigen. CloudWatch Application Insights soll Ihnen helfen, laufende Probleme mit Ihren Anwendungen und Ihrer Infrastruktur schnell zu isolieren.

Um Protokollnachrichten in CloudWatch Logs zu schreiben, fügen Sie das `AWS.Logger.NLog` NuGet Paket dem .NET-Projekt hinzu. Anschließend aktualisieren Sie die `NLog.config` Datei, um CloudWatch Logs als Ziel zu verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine.NET-Web- oder Konsolenanwendung, die:
  - Verwendet unterstützte.NET Framework- oder .NET Core-Versionen. Weitere Informationen finden Sie unter Produktversionen.
  - Wird verwendet NLog , um Protokolldaten an Application Insights zu senden.
- Berechtigungen zum Erstellen einer IAM-Rolle für einen AWS-Service. Weitere Informationen finden Sie unter Berechtigungen für Servicerollen.
- Berechtigungen zur Übergabe einer Rolle an einen AWS-Service. Weitere Informationen finden Sie unter Erteilen von Benutzerberechtigungen zur Übergabe einer Rolle an einen AWS-Service.

Produktversionen

- .NET Framework Version 3.5 oder höher
- .NET Core-Versionen 1.0.1, 2.0.0 oder höher

Architektur

Zieltechnologie-Stack

- NLog
- CloudWatch Amazon-Protokolle

Zielarchitektur

1. Die .NET-Anwendung schreibt Protokolldaten in das NLog Logging-Framework.
2. NLog schreibt die Protokolldaten in CloudWatch Logs.
3. Sie verwenden CloudWatch Alarme und benutzerdefinierte Dashboards, um die .NET-Anwendung zu überwachen.

Tools

AWS-Services

- Amazon CloudWatch Application Insights hilft Ihnen dabei, den Zustand Ihrer Anwendungen und der zugrunde liegenden AWS-Ressourcen zu beobachten.
- Amazon CloudWatch Logs hilft Ihnen dabei, die Protokolle all Ihrer Systeme, Anwendungen und AWS-Services zu zentralisieren, sodass Sie sie überwachen und sicher archivieren können.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Bei den AWS-Tools für PowerShell handelt es sich um eine Reihe von PowerShell Modulen, die Ihnen helfen, Operationen auf Ihren AWS-Ressourcen von der PowerShell Befehlszeile aus zu skripten.

Andere Tools

- Logger. NLogist ein NLog Ziel, das Protokolldaten in CloudWatch Logs aufzeichnet.

- NLogist ein Open-Source-Protokollierungsframework für .NET-Plattformen, mit dem Sie Protokolldaten in Ziele wie Datenbanken, Protokolldateien oder Konsolen schreiben können.
- PowerShellist ein Automatisierungs- und Konfigurationsverwaltungsprogramm von Microsoft, das unter Windows, Linux und macOS läuft.
- Visual Studio ist eine integrierte Entwicklungsumgebung (IDE), die Compiler, Tools zur Codevervollständigung, Grafikdesigner und andere Funktionen zur Unterstützung der Softwareentwicklung umfasst.

Bewährte Methoden

- Legen Sie eine Aufbewahrungsrichtlinie für die Zielprotokollgruppe fest. Dies muss außerhalb der NLog Konfiguration erfolgen. Standardmäßig werden Protokolldaten auf unbestimmte Zeit in CloudWatch Logs gespeichert.
- Halten Sie sich an die Best Practices für die Verwaltung von AWS-Zugriffsschlüsseln.

Epen

Richten Sie Zugriff und Tools ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Richtlinie.	Folgen Sie den Anweisungen unter Richtlinien mit dem JSON-Editor erstellen in der IAM-Dokumentation. Geben Sie die folgende JSON-Richtlinie ein, die über die geringsten Rechte verfügt, die erforderlich sind, damit CloudWatch Logs Logs Logs lesen und schreiben kann. `{ "Version": "2012-10-17", "Statement": [ {`	AWS-Administrator, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"Effect": "Allow", "Action": ["logs:CreateLogGroup", "logs:CreateLogStream", "logs:GetLogEvents", "logs:PutLogEvents", "logs:DescribeLogGroups", "logs:DescribeLogStreams", "logs:PutRetentionPolicy"], "Resource": ["*"] }] }	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine IAM-Rolle.	Folgen Sie den Anweisungen unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service in der IAM-Dokumentation. Wählen Sie die Richtlinie aus, die Sie zuvor erstellt haben. Dies ist die Rolle, die CloudWatch Logs bei der Durchführung von Protokollierungsaktionen einnimmt.	AWS-Administrator, AWS DevOps
Richten Sie AWS-Tools für ein PowerShell.	1. Folgen Sie den Anweisungen für Ihr Betriebssystem unter Installation der AWS-Tools für PowerShell. 2. Verwenden Sie die AWS-Tools für PowerShell Cmdlets, um Ihren Zugriffsschlüssel und Ihren geheimen Schlüssel in einem Profil zu speichern. Anweisungen finden Sie in der PowerShell Dokumentation unter Profile verwalten in den AWS-Tools.	Allgemeines AWS

Konfiguration NLog

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie das NuGet Paket.	1. Wählen Sie in Visual Studio Datei und dann Projekt oder Lösung öffnen aus.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie das Projekt aus, das Sie installieren möchten NLog. 3. Wählen Sie in Visual Studio Tools, NuGet Package Manager, Package Manager Console aus. 4. Installieren Sie das `AWS.Logger.NLog` NuGet Paket, indem Sie den folgenden Befehl eingeben. `Install-Package AWS.Logger.NLog -Version 3.1.0`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie das Logging-Ziel.	1. Öffnen Sie die `NLog.config` Datei. 2. Geben Sie für `type` das Ziel ein`AWSTarget` . 3. Geben Sie für `logGroup` das Ziel den Namen der Protokollgruppe ein, die Sie verwenden möchten. Wenn die Protokollgruppe noch nicht existiert, wird automatisch eine neue Protokollgruppe mit dem angegebenen Namen erstellt. 4. Geben Sie für das Ziel die AWS-Region ein`region`, in der CloudWatch Logs konfiguriert ist. 5. Geben Sie für das Ziel `profile` den Namen des Profils ein, das Sie zuvor zum Speichern des Zugriffsschlüssels und des geheimen Schlüssels erstellt haben. 6. Speichern und schließen Sie die Datei `NLog.config` . Eine Beispielkonfigurationsdatei finden Sie im Abschnitt Zusätzliche Informationen dieses Musters.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wenn Sie Ihre Anwendung ausführen, NLog werden die Protokollmeldungen geschrieben und an CloudWatch Logs gesendet.	

Validieren und überwachen Sie die Protokolle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Protokollierung.	Folgen Sie den Anweisungen unter An CloudWatch Protokolle gesendete Protokolldaten anzeigen in der Dokumentation zu den CloudWatch Protokollen. Stellen Sie sicher, dass Protokollereignisse für die .NET-Anwendung aufgezeichnet werden. Wenn keine Protokollereignisse aufgezeichnet werden, finden Sie weitere Informationen im Abschnitt Problembehandlung in diesem Muster.	Allgemeines AWS
Überwachen Sie den.NET-Anwendungsstapel.	Konfigurieren Sie die Überwachung nach CloudWatch Bedarf für Ihren Anwendungsfall. Sie können CloudWatch Logs Insights, CloudWatch Metrics Insights und CloudWatch Application Insights verwenden, um Ihren .NET-Workload zu	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	überwachen. Sie können auch Alarme so konfigurieren, dass Sie Benachrichtigungen erhalten können, und Sie können ein benutzerdefiniertes Dashboard zur Überwachung der Arbeitslast von einer einzigen Ansicht aus erstellen.	

Fehlerbehebung

Problem	Lösung
Protokolldaten werden nicht in CloudWatch Logs angezeigt.	Stellen Sie sicher, dass die IAM-Richtlinie mit der IAM-Rolle verknüpft ist, die CloudWatch Logs annimmt. Anweisungen dazu finden Sie im Abschnitt Zugriff und Tools einrichten im Abschnitt Epics.

Zugehörige Ressourcen

- Arbeiten mit Log-Gruppen und Log-Streams (CloudWatch Logs-Dokumentation)
- Amazon CloudWatch Logs und .NET Logging Frameworks (AWS-Blogbeitrag)

Zusätzliche Informationen

Im Folgenden finden Sie eine `NLog.config` Beispieldatei.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <configSections>
    <section name="nlog" type="NLog.Config.ConfigSectionHandler, NLog" />
  </configSections>
  <startup>
```

```
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.7.2" />
  </startup>
  <nlog>
    <extensions>
      <add assembly="NLog.AWS.Logger" />
    </extensions>
    <targets>
      <target name="aws" type="AWSTarget" logGroup="NLog.TestGroup" region="us-east-1"
 profile="demo"/>
    </targets>
    <rules>
      <logger name="*" minlevel="Info" writeTo="aws" />
    </rules>
  </nlog>
</configuration>
```

Kopieren Sie AWS Service Catalog-Produkte zwischen verschiedenen AWS-Konten und AWS-Regionen

Erstellt von Sachin Vighe (AWS) und Santosh Kale (AWS)

Übersicht

AWS Service Catalog ist ein regionaler Service. Das bedeutet, dass die Portfolios und Produkte von AWS Service Catalog nur in der AWS-Region sichtbar sind, in der sie erstellt wurden. Wenn Sie einen AWS Service Catalog-Hub in einer neuen Region einrichten, müssen Sie Ihre vorhandenen Produkte neu erstellen, was ein zeitaufwändiger Vorgang sein kann.

Der Ansatz dieses Musters trägt dazu bei, diesen Prozess zu vereinfachen, indem beschrieben wird, wie Produkte von einem AWS Service Catalog-Hub in einem AWS-Quellkonto oder einer AWS-Quellregion auf einen neuen Hub in einem Zielkonto oder einer Zielregion kopiert werden. Weitere Informationen zum Hub-and-Spoke-Modell von AWS Service Catalog finden Sie unter Hub-and-Spoke-Modell von AWS Service Catalog: So automatisieren Sie die Bereitstellung und Verwaltung von AWS Service Catalog für viele Konten im AWS Management and Governance-Blog.

Das Muster enthält auch die separaten Codepakete, die zum Kopieren von AWS Service Catalog-Produkten zwischen Konten oder in andere Regionen erforderlich sind. Durch die Verwendung dieses Musters kann Ihr Unternehmen Zeit sparen, bestehende und frühere Produktversionen in einem neuen AWS Service Catalog-Hub verfügbar machen, das Risiko manueller Fehler minimieren und den Ansatz auf mehrere Konten oder Regionen skalieren.

> **Note**
>
> Der Abschnitt Epics dieses Musters bietet zwei Optionen zum Kopieren von Produkten. Sie können Option 1 verwenden, um Produkte zwischen Konten zu kopieren, oder Option 2 wählen, um Produkte zwischen Regionen zu kopieren.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Bestehende AWS Service Catalog-Produkte in einem Quellkonto oder einer Region.
- Ein vorhandener AWS Service Catalog-Hub in einem Zielkonto oder einer Zielregion.

- Wenn Sie Produkte zwischen Konten kopieren möchten, müssen Sie das AWS Service Catalog-Portfolio, das die Produkte enthält, teilen und dann in Ihr Zielkonto importieren. Weitere Informationen dazu finden Sie unter Teilen und Importieren von Portfolios in der AWS-Servicekatalog-Dokumentation.

Einschränkungen

- AWS Service Catalog-Produkte, die Sie zwischen Regionen oder Konten kopieren möchten, dürfen nicht zu mehr als einem Portfolio gehören.

Architektur

Das folgende Diagramm zeigt das Kopieren von AWS Service Catalog-Produkten von einem Quellkonto in ein Zielkonto.

Das folgende Diagramm zeigt das Kopieren von AWS Service Catalog-Produkten von einer Quellregion in eine Zielregion.

Technologie-Stack

- Amazon CloudWatch
- AWS Identity and Access Management (IAM)
- AWS Lambda
- AWS Service Catalog

Automatisierung und Skalierung

Sie können den Ansatz dieses Musters skalieren, indem Sie eine Lambda-Funktion verwenden, die je nach der Anzahl der eingegangenen Anfragen oder der Anzahl der AWS Service Catalog-Produkte, die Sie kopieren müssen, skaliert werden kann. Weitere Informationen dazu finden Sie unter Lambda-Funktionsskalierung in der AWS Lambda Lambda-Dokumentation.

Tools

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Mit AWS Service Catalog können Sie Kataloge von IT-Services, die für AWS zugelassen sind, zentral verwalten. Endbenutzer können schnell nur die jeweils benötigten genehmigten IT-Services bereitstellen, wobei die Einschränkungen Ihrer Organisation berücksichtigt werden.

Code

Sie können das `cross-account-copy` Paket (angehängt) verwenden, um AWS Service Catalog-Produkte zwischen Konten zu kopieren, oder das `cross-region-copy` Paket (angehängt), um Produkte zwischen Regionen zu kopieren.

Das `cross-account-copy` Paket enthält die folgenden Dateien:

- `copyconf.properties`— Die Konfigurationsdatei, die die Regions- und AWS-Konto-ID-Parameter für das Kopieren von Produkten zwischen Konten enthält.
- `scProductCopyLambda.py`— Die Python-Funktion zum Kopieren von Produkten zwischen Konten.
- `createDestAccountRole.sh`— Das Skript zum Erstellen einer IAM-Rolle im Zielkonto.
- `createSrcAccountRole.sh`— Das Skript zum Erstellen einer IAM-Rolle im Quellkonto.
- `copyProduct.sh`— Das Skript zum Erstellen und Aufrufen der Lambda-Funktion zum Kopieren von Produkten zwischen Konten.

Das `cross-region-copy` Paket enthält die folgenden Dateien:

- `copyconf.properties`— Die Konfigurationsdatei, die die Regions- und AWS-Konto-ID-Parameter für das Kopieren von Produkten zwischen Regionen enthält.
- `scProductCopyLambda.py`— Die Python-Funktion zum Kopieren von Produkten zwischen Regionen.
- `copyProduct.sh`— Das Skript zum Erstellen einer IAM-Rolle und zum Erstellen und Aufrufen der Lambda-Funktion zum Kopieren von Produkten zwischen Regionen.

Epen

Option 1 — AWS Service Catalog-Produkte kontenübergreifend kopieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Konfigurationsdatei.	1. Laden Sie das `cross-account-copy` Paket (angehängt) auf Ihren lokalen Computer herunter. 2. Aktualisieren Sie die `copyconf.properties` Konfigurationsdatei mit den folgenden Werten: • `srcRegion` — Geben Sie die Quellregion an, in der die Produkte enthalten sind. • `destRegion` — Geben Sie die Zielregion für die Produkte an. • `sourceAccountId` — Geben Sie die AWS-Konto-ID für Ihr Quellkonto an. • `destAccountId` — Geben Sie die AWS-Konto-ID für Ihr Zielkonto an.	AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator
Konfigurieren Sie Ihre Anmeldeinformationen für AWS CLI im Zielkonto.	Konfigurieren Sie Ihre Anmeldeinformationen für den Zugriff auf AWS CLI in Ihrem Zielkonto, indem Sie den `aws configure` Befehl	AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	ausführen und die folgenden Werte angeben:
	
	`$aws configure`
	`AWS Access Key ID`
	` [None]: <your_acc`
	`ess_key_id>`
	`AWS Secret Access Key`
	` [None]: <your_sec`
	`ret_access_key>`
	`Default region name`
	` [None]: Region`
	`Default output format`
	` [None]:`
	
	Weitere Informationen dazu finden Sie in der Dokumentation zur AWS-Befehlszeilenschnittstelle unter Grundlagen der Konfiguration.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie Ihre Anmeldeinformationen für AWS CLI im Quellkonto.	Konfigurieren Sie Ihre Anmeldeinformationen für den Zugriff auf AWS CLI in Ihrem Quellkonto, indem Sie den `aws configure` Befehl ausführen und die folgenden Werte angeben:
	`$aws configure`
	`AWS Access Key ID [None]: <your_access_key_id>`
	`AWS Secret Access Key [None]: <your_secret_access_key>`
	`Default region name [None]: Region`
	`Default output format [None]:`
	Weitere Informationen dazu finden Sie in der Dokumentation zur AWS-Befehlszeilenschnittstelle unter Grundlagen der Konfiguration.
		AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Lambda-Ausführungsrolle in Ihrem Zielkonto.	Führen Sie das `createDestAccountRole.sh` Skript in Ihrem Zielkonto aus. Das Skript implementiert die folgenden Aktionen: • Erstellt eine Lambda-Ausführungsrolle in Ihrem Zielkonto • Erstellt die IAM-Richtlinie für die Lambda-Ausführungsrolle und fügt sie an	AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator
Erstellen Sie die kontoüber greifende IAM-Rolle in Ihrem Quellkonto.	Führen Sie das `createSrcAccountRole.sh` Skript in Ihrem Quellkonto aus. Das Skript implementiert die folgenden Aktionen: • Erstellt eine kontoüber greifende IAM-Rolle in Ihrem Quellkonto, die von der Lambda-Ausführungsrolle im Zielkonto übernommen wird, um Produkte zu kopieren • Erstellt eine IAM-Richtlinie für die kontoübergreifende Rolle in Ihrem Quellkonto und fügt sie an	AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das CopyProduct-Skript im Zielkonto aus.	Führen Sie das `copyProduct.sh` Skript in Ihrem Zielkonto aus. Das Skript implementiert die folgenden Aktionen: • Erzeugt und ruft die Lambda-Funktion auf, um Produkte vom Quellkonto in das Zielkonto zu kopieren	AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator

Option 2 — AWS Service Catalog-Produkte von einer Quellregion in eine Zielregion kopieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Konfigurationsdatei.	1. Laden Sie das `cross-region-copy` Paket (angehängt) auf Ihren lokalen Computer herunter. 2. Aktualisieren Sie die `copyconf.properties` Konfigurationsdatei mit den folgenden Werten: • `srcRegion` — Geben Sie die Quellregion an, in der die Produkte enthalten sind. • `destRegion` — Geben Sie die Zielregion für die Produkte an. • `accountId` — Geben Sie Ihre AWS-Konto-ID an.	AWS-Systemadministrator, Cloud-Administrator, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie Ihre Anmeldeinformationen für AWS CLI.	Konfigurieren Sie Ihre Anmeldeinformationen für den Zugriff auf AWS CLI in Ihrer Umgebung, indem Sie den `aws configure` Befehl ausführen und die folgenden Werte angeben:
	`$aws configure`
	`AWS Access Key ID [None]: <your_access_key_id>`
	`AWS Secret Access Key [None]: <your_secret_access_key>`
	`Default region name [None]: Region`
	`Default output format [None]:`
	Weitere Informationen dazu finden Sie in der Dokumentation zur AWS-Befehlszeilenschnittstelle unter Grundlagen der Konfiguration.
		AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das CopyProduct-Skript aus.	Führen Sie das `copyProduct.sh` Skript in Ihrer Zielregion aus. Das Skript implementiert die folgenden Aktionen: • Erzeugt eine Lambda-Ausführungsrolle • Erstellt die IAM-Richtlinie für die Lambda-Ausführungsrolle und fügt sie an • Erzeugt und ruft die Lambda-Funktion auf, um Produkte aus der Quellregion in die Zielregion zu kopieren	AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator

Zugehörige Ressourcen

- Eine Lambda-Ausführungsrolle erstellen (AWS Lambda Lambda-Dokumentation)
- Eine Lambda-Funktion erstellen (AWS Lambda Lambda-Dokumentation)
- AWS-Servicekatalog-API-Referenz
- Dokumentation zum AWS Service Catalog

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Erstellen Sie eine RACI- oder RASCI-Matrix für ein Cloud-Betriebsmodell

Erstellt von Teddy Germade (AWS), Jerome Descreux (AWS), Josselin LE MINEUR (AWS) und Florian Leroux (AWS)

Übersicht

Das Cloud Center of Excellence (CCoE) oder CEE (Cloud Enablement Engine) ist ein kompetentes und verantwortungsbewusstes Team, das sich auf die Betriebsbereitschaft für die Cloud konzentriert. Ihr Hauptaugenmerk liegt auf der Umstellung der Informations-IT-Organisation von einem lokalen Betriebsmodell auf ein Cloud-Betriebsmodell. Das CCo E sollte ein funktionsübergreifendes Team sein, das Vertreter aus den Bereichen Infrastruktur, Anwendungen, Betrieb und Sicherheit umfasst.

Eine der Schlüsselkomponenten eines Cloud-Betriebsmodells ist eine RACI-Matrix oder RASCI-Matrix. Dies wird verwendet, um die Rollen und Verantwortlichkeiten für alle Parteien zu definieren, die an Migrationsaktivitäten und Cloud-Operationen beteiligt sind. Der Matrixname leitet sich von den in der Matrix definierten Zuständigkeitstypen ab: verantwortlich (R), rechenschaftspflichtig (A), unterstützend (S), konsultiert (C) und informiert (I). Die Art der Unterstützung ist optional. Wenn Sie sie einbeziehen, wird sie als RASCI-Matrix bezeichnet, und wenn Sie sie ausschließen, wird sie als RACI-Matrix bezeichnet.

Wenn Sie mit der beigefügten Vorlage beginnen, kann Ihr CCo E-Team eine RACI- oder RASCI-Matrix für Ihre Organisation erstellen. Die Vorlage enthält Teams, Rollen und Aufgaben, die in Cloud-Betriebsmodellen üblich sind. Die Grundlage dieser Matrix bilden die Aufgaben im Zusammenhang mit der Betriebsintegration und den CCo E-Funktionen. Sie können diese Vorlage jedoch an die Anforderungen der Struktur und des Anwendungsfalls Ihres Unternehmens anpassen.

Der Implementierung einer RACI-Matrix sind keine Grenzen gesetzt. Dieser Ansatz funktioniert für große Organisationen, Start-ups und alles dazwischen. In kleinen Organisationen kann dieselbe Ressource mehrere Rollen übernehmen.

Epen

Erstelle die Matrix

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die wichtigst en Interessengruppen.	Identifizieren Sie wichtige Service- und Teammanag	Projektmanager

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	er, die mit den strategis chen Zielen Ihres Cloud-Bet riebsmodells verknüpft sind.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Passen Sie die Matrixvorlage an.	Laden Sie die Vorlage im Abschnitt Anlagen herunter und aktualisieren Sie dann die RACI- oder RASCI-Matrix wie folgt:
	• Aktualisieren Sie im Arbeitsblatt Cloud Teams die CCo E-Stream-Namen, Teamnamen und Teambeschreibungen nach Bedarf für Ihre Organisation.
	• Aktualisieren Sie im Arbeitsblatt Cloud-Rollen die Rollen, Teamnamen und Rollenbeschreibungen nach Bedarf für Ihre Organisation.
	• Aktualisieren Sie auf dem RASCI-Arbeitsblatt Folgendes nach Bedarf für Ihre Organisation:
	  • Aktualisieren Sie in Zeile 1 und Spalte A die CCo E-Streams.
	  • Aktualisieren Sie in Zeile 2 die Teamnamen.
	  • Aktualisieren Sie in Zeile 3 die Rollennamen.
	  • Aktualisieren Sie in den Spalten D und E die allgemeinen Felder und Aktivitäten, die Sie in
		Projektmanager

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ihr RASCI-Diagramm aufnehmen möchten.	
Planen Sie Besprechungen.	1. Kommunizieren Sie die RASCI-Ziele allen Beteiligten. 2. Planen Sie ein oder mehrere Treffen, sodass ein bevollmächtigter Vertreter jedes Teams teilnehmen kann.	Projektmanager

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vervollständigen Sie die Matrix.	Gehen Sie in der Besprechung mit allen Beteiligten wie folgt vor: 1. Vergewissern Sie sich, dass ein Vertreter jedes Teams anwesend ist. Die Teilnahme des Teams ist verpflichtend, damit Sie jeder Aufgabe die Zuständig keitstypen genau zuordnen können. 2. Erkundigen Sie sich mit den Teilnehmern darüber, was eine RASCI-Matrix ist und welche Ziele verfolgt werden. 3. Besprechen Sie das Modell der gemeinsam en Verantwortung mit den Teilnehmern, damit sie den Umfang der Verantwor tung ihrer Organisation für die Sicherheit in der Cloud verstehen. 4. Füllen Sie auf dem RASCI-Arbeitsblatt für jede Aufgabe oder Aktivität die Spalten F bis AN aus, um die folgenden Zuständig keitstypen zuzuweisen: • Verantwortlich (R) — Diese Rolle ist für die Ausführung der Arbeiten	Projektmanager

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zur Erledigung der Aufgabe verantwortlich. • Rechenschaftspflichtig (A) — Diese Rolle ist dafür verantwortlich, dass die Aufgabe erledigt wird. Diese Rolle ist auch dafür verantwortlich, sicherzustellen, dass die Voraussetzungen erfüllt sind, und die Aufgabe an die Verantwortlichen zu delegieren. • Support (S) — Diese Rolle hilft den Verantwortlichen, die Aufgabe zu erledigen. Dieser Zuständigkeitstyp ist optional, und Sie können ihn ausschließen, um eine traditionellere RACI-Matrix zu erstellen. • Konsultiert (C) — Diese Rolle sollte konsultiert werden, um Meinungen oder Fachwissen zu der jeweiligen Aufgabe einzuholen. Je nach Aufgabe ist diese Art von Verantwortung möglicher weise nicht erforderlich. • Informiert (I) — Diese Rolle sollte über den Fortschritt der Aufgabe	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	auf dem Laufenden gehalten und benachric htigt werden, wenn die Aufgabe abgeschlossen ist. • Leer — Diese Rolle ist nicht an der Aktivität oder Aufgabe beteiligt.	
Teilen Sie die RASCI-Matrix.	Wenn die RACI- oder RASCI-Matrix vollständig ist, lassen Sie sie von der Unternehm ensleitung genehmigen. Speichern Sie sie in einem gemeinsam genutzten Repository oder an einem zentralen Ort, wo alle Beteiligt en darauf zugreifen können. Wir empfehlen, Standardp rozesse zur Dokumente nkontrolle zu verwenden , um Änderungen an der Matrix aufzuzeichnen und zu genehmigen.	Projektmanager

Zugehörige Ressourcen

- AWS-Modell mit geteilter Verantwortung

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Erstellen Sie mithilfe der CloudWatch Amazon-Anomalieerkennung Alarme für benutzerdefinierte Metriken

Erstellt von Ram Kandaswamy (AWS) und Raheem Jiwani (AWS)

Übersicht

In der Amazon Web Services (AWS) Cloud können Sie Amazon verwenden, um Alarme CloudWatch zu erstellen, die Messwerte überwachen und Benachrichtigungen senden oder automatisch Änderungen vornehmen, wenn ein Schwellenwert überschritten wird.

Um zu vermeiden, dass Sie durch statische Schwellenwerte eingeschränkt werden, können Sie Alarme erstellen, die auf vergangenen Mustern basieren und Sie benachrichtigen, wenn bestimmte Messwerte außerhalb des normalen Betriebsfensters liegen. Sie könnten beispielsweise die Antwortzeiten Ihrer API von Amazon API Gateway aus überwachen und Benachrichtigungen über Anomalien erhalten, die Sie daran hindern, ein Service Level Agreement (SLA) einzuhalten.

Dieses Muster beschreibt, wie die CloudWatch Anomalieerkennung für benutzerdefinierte Metriken verwendet wird. Das Muster zeigt Ihnen, wie Sie eine benutzerdefinierte Metrik in Amazon CloudWatch Logs Insights erstellen oder eine benutzerdefinierte Metrik mit einer AWS Lambda Lambda-Funktion veröffentlichen und anschließend die Anomalieerkennung einrichten und Benachrichtigungen mit Amazon Simple Notification Service (Amazon SNS) erstellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein vorhandenes SNS-Thema, das für das Senden von E-Mail-Benachrichtigungen konfiguriert ist. Weitere Informationen dazu finden Sie unter Erste Schritte mit Amazon SNS in der Amazon SNS SNS-Dokumentation.
- Eine bestehende Anwendung, konfiguriert mit CloudWatch Logs.

Einschränkungen

- CloudWatch Metriken unterstützen keine Millisekunden-Zeitintervalle. Weitere Informationen zur Granularität regulärer und benutzerdefinierter Metriken finden Sie auf Amazon CloudWatch FAQs.

Architektur

Das Diagramm zeigt den folgenden Workflow:

1. Protokolle, die Metriken verwenden, die von CloudWatch Logs erstellt und aktualisiert wurden, werden gestreamt. CloudWatch
2. Ein Alarm wird auf der Grundlage von Schwellenwerten ausgelöst und sendet eine Warnung an ein SNS-Thema.
3. Amazon SNS sendet Ihnen eine E-Mail-Benachrichtigung.

Technologie-Stack

- CloudWatch
- AWS Lambda
- Amazon SNS

Tools

- Amazon CloudWatch bietet eine zuverlässige, skalierbare und flexible Überwachungslösung.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitzustellen oder zu verwalten.
- Amazon Simple Notification Service (Amazon SNS) ist ein verwalteter Service, der die Nachrichtenzustellung von Verlagen an Abonnenten ermöglicht.

Epen

Richten Sie die Anomalieerkennung für eine benutzerdefinierte Metrik ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 1 — Erstellen Sie eine benutzerdefinierte Metrik mit einer Lambda-Funktion.	Laden Sie die `lambda_function.py` Datei (angehängt) herunter und ersetzen Sie dann die `lambda_function.py`	DevOps Ingenieur, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Beispieldatei im aws-lambda-developer-guideRepository in der AWS-Dokumentation GitHub. Dadurch erhalten Sie eine Lambda-Beispielfunktion, die benutzerdefinierte Metriken an CloudWatch Logs sendet. Die Lambda-Funktion verwendet die Boto3-API für die Integration. CloudWatch Nachdem Sie die Lambda-Funktion ausgeführt haben, können Sie sich bei der AWS-Managementkonsole anmelden, die CloudWatch Konsole öffnen und die veröffentlichte Metrik ist in Ihrem veröffentlichten Namespace verfügbar.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 2 — Erstellen Sie benutzerdefinierte Metriken aus CloudWatch Protokoll gruppen.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die CloudWatc h Konsole und wählen Sie dann Protokollgruppen aus. Wählen Sie die Protokoll gruppe aus, für die Sie eine Metrik erstellen möchten. Wählen Sie Aktionen und dann Metrikfilter erstellen aus. Geben Sie unter Filtermuster das Filtermuster ein, das Sie verwenden möchten. Weitere Informationen finden Sie in der CloudWatch Dokumentation unter Filter- und Mustersyn tax. Um Ihr Filtermuster zu testen, geben Sie unter Testmuste r ein oder mehrere Protokoll ereignisse ein. Jedes Protokoll ereignis muss innerhalb einer einzelnen Zeile liegen, da Zeilenumbrüche verwendet werden, um Protokollereigniss e im Anzeigebereich Log event messages (Ereignis meldungen protokollieren) zu trennen. Nachdem Sie das Muster getestet haben, können Sie unter Metrikdetails einen Namen und einen Wert für Ihre Metrik eingeben.	DevOps Ingenieur, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen und Schritte zum Erstellen einer benutzerdefinierten Metrik finden Sie in der CloudWatch Dokumentation unter Erstellen eines Metrikfilters für eine Protokollgruppe.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Alarm für Ihre benutzerdefinierte Metrik.	Wählen Sie auf der CloudWatch Konsole Alarme und dann Create Alarm aus. Wählen Sie Metrik auswählen und geben Sie den Namen der Metrik, die Sie zuvor erstellt haben, in das Suchfeld ein. Wählen Sie die Registerkarte Graphische Metriken und konfigurieren Sie die Optionen entsprechend Ihren Anforderungen. Wählen Sie unter Bedingungen die Option Anomalieerkennung statt Statische Schwellenwerte aus. Dies zeigt Ihnen ein Band, das auf zwei standardmäßigen Standardabweichungen basiert. Sie können Schwellenwerte einrichten und diese an Ihre Anforderungen anpassen. Wählen Sie Weiter aus. **Note** Das Band ist dynamisch und hängt von der Qualität der Datenpunkte ab. Wenn Sie mit der Aggregation weiterer Daten beginnen, werden das Band und	DevOps Ingenieur, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Schwellenwerte automatisch aktualisi ert.	
Richten Sie SNS-Benac hrichtigungen ein.	Wählen Sie unter Benachric htigung das SNS-Thema aus, das benachrichtigt werden soll, wenn sich der Alarm im `ALARM` Status, `OK` Status oder `INSUFFICIENT_DATA` Status befindet. Um zu erreichen, dass der Alarm mehrere Benachric htigungen für den gleichen Alarmstatus oder für verschied ene Statuswerte sendet, wählen Sie Benachrichtigung hinzufügen. Wählen Sie Weiter aus. Geben Sie einen Namen und eine Beschreib ung für den Alarm ein. Der Name darf nur ASCII-Zei chen enthalten. Wählen Sie anschließend Weiter. Vergewissern Sie sich unter Vorschau und Erstellen, dass die Informationen und Bedingungen korrekt sind, und wählen Sie dann Alarm erstellen aus.	DevOps Ingenieur, AWS DevOps

Zugehörige Ressourcen

- Veröffentlichen von benutzerdefinierten Metriken auf CloudWatch
- Verwenden der CloudWatch Erkennung von Anomalien
- Alarmereignisse und Amazon EventBridge
- Was sind die besten Methoden, die Sie bei der Übertragung benutzerdefinierter Metriken auf Cloud Watch beachten sollten? (Video)
- Einführung in CloudWatch Application Insights (Video)
- Erkennen Sie Anomalien mit CloudWatch (Video)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Erstellen Sie eine AWS Cloud9 Cloud9-IDE, die Amazon EBS-Volumes mit Standardverschlüsselung verwendet

Erstellt von Janardhan Malyala (AWS) und Dhrubajyoti Mukherjee (AWS)

Übersicht

Hinweis AWS Cloud9 : ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS Cloud9 können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Sie können standardmäßig Verschlüsselung verwenden, um die Verschlüsselung Ihrer Amazon Elastic Block Store (Amazon EBS) -Volumes und Snapshot-Kopien in der Amazon Web Services (AWS) -Cloud zu erzwingen.

Sie können eine integrierte Entwicklungsumgebung (IDE) von AWS Cloud9 erstellen, die standardmäßig verschlüsselte EBS-Volumes verwendet. Die serviceverknüpfte Rolle AWS Identity and Access Management (IAM) für AWS Cloud9 erfordert jedoch Zugriff auf den AWS Key Management Service (AWS KMS) -Schlüssel für diese EBS-Volumes. Wenn kein Zugriff bereitgestellt wird, kann die AWS Cloud9 Cloud9-IDE möglicherweise nicht gestartet werden, und das Debuggen kann schwierig sein.

Dieses Muster enthält die Schritte zum Hinzufügen der serviceverknüpften Rolle für AWS Cloud9 zum AWS-KMS-Schlüssel, der von Ihren EBS-Volumes verwendet wird. Das in diesem Muster beschriebene Setup hilft Ihnen dabei, erfolgreich eine IDE zu erstellen und zu starten, die standardmäßig EBS-Volumes mit Verschlüsselung verwendet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Die Standardverschlüsselung ist für EBS-Volumes aktiviert. Weitere Informationen zur Standardverschlüsselung finden Sie unter Amazon EBS-Verschlüsselung in der Dokumentation zu Amazon Elastic Compute Cloud (Amazon EC2).
- Ein vorhandener, vom Kunden verwalteter KMS-Schlüssel zur Verschlüsselung Ihrer EBS-Volumes.

> **Note**
>
> Sie müssen die serviceverknüpfte Rolle für AWS Cloud9 nicht erstellen. Wenn Sie eine AWS Cloud9-Entwicklungsumgebung erstellen, erstellt AWS Cloud9 die serviceverknüpfte Rolle für Sie.

Architektur

Technologie-Stack

- AWS Cloud9
- IAM
- AWS KMS

Tools

- AWS Cloud9 ist eine integrierte Entwicklungsumgebung (IDE), die Sie beim Codieren, Erstellen, Ausführen, Testen und Debuggen von Software unterstützt. Es hilft Ihnen auch dabei, Software in der AWS-Cloud zu veröffentlichen.
- Amazon Elastic Block Store (Amazon EBS) bietet Speichervolumes auf Blockebene zur Verwendung mit Amazon Elastic Compute Cloud (Amazon EC2) -Instances.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie kontrollieren, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Key Management Service (AWS KMS) unterstützt Sie bei der Erstellung und Kontrolle kryptografischer Schlüssel, um Ihre Daten zu schützen.

Epen

Suchen Sie den Standardwert für den Verschlüsselungsschlüssel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Notieren Sie sich den Standardwert des Verschlüs	Melden Sie sich bei der AWS-Managementkonsole an und	Cloud-Architekt, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
selungsschlüssels für die EBS-Volumes.	öffnen Sie die EC2 Amazon-Konsole. Wählen Sie EC2 Dashboard und dann unter Kontoattribute die Option Datenschutz und Sicherheit aus. Kopieren Sie im Bereich EBS-Verschlüsselung den Wert im Feld Standardv erschlüsselungsschlüssel und notieren Sie ihn.	

Zugriff auf den AWS-KMS-Schlüssel bereitstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gewähren Sie AWS Cloud9 Zugriff auf den KMS-Schlüssel für EBS-Volumes.	1. Öffnen Sie die AWS KMS KMS-Konsole und wählen Sie dann Customer managed keys aus. Wählen Sie den AWS-KMS-S chlüssel aus, der für die Amazon EBS-Versc hlüsselung verwendet wird, und wählen Sie dann Schlüssel anzeigen aus. 2. Vergewissern Sie sich auf der Registerkarte Schlüssel richtlinie, dass Sie die Textform der Schlüssel richtlinie sehen können. Wenn Sie das Textformular nicht sehen können, wählen Sie Zur Richtlinienansicht wechseln.	Cloud-Architekt, Ingenieur DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie Bearbeiten aus. Fügen Sie der Richtlinie den Code im Abschnitt Zusätzliche Informationen hinzu und wählen Sie dann Änderungen speichern aus. Die Richtlinienänderungen ermöglichen es der serviceverknüpften Rolle für AWS Cloud9,`AWSServiceRoleForAWSCloud9` , auf den Schlüssel zuzugreifen. Weitere Informationen zur Aktualisierung einer Schlüsselrichtlinie finden Sie unter So ändern Sie eine Schlüsselrichtlinie (AWS KMS KMS-Dokumentation). **Important** Die serviceverknüpfte Rolle für AWS Cloud9 wird automatisch erstellt, wenn Sie Ihre erste IDE starten. Weitere Informationen finden Sie unter Erstellen einer serviceverknüpften Rolle in der AWS	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Cloud9 Cloud9-Do kumentation.	

Erstellen und starten Sie die IDE

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen und starten Sie die AWS Cloud9 IDE.	Öffnen Sie die AWS Cloud9 Cloud9-Konsole und wählen Sie Umgebung erstellen. Konfigurieren Sie die IDE gemäß Ihren Anforderu ngen, indem Sie die Schritte unter Erstellen einer EC2 Umgebung in der AWS Cloud9 Cloud9-Dokumentation befolgen.	Cloud-Architekt, Ingenieur DevOps

Zugehörige Ressourcen

- Von AWS Cloud9 verwendete EBS-Volumes verschlüsseln
- Eine serviceverknüpfte Rolle für AWS Cloud9 erstellen
- Erstellen Sie eine EC2 Umgebung in AWS Cloud9

Zusätzliche Informationen

Wichtige Aktualisierungen der AWS KMS KMS-Richtlinien

Ersetzen Sie <aws_accountid> durch Ihre AWS-Konto-ID.

```
{
            "Sid": "Allow use of the key",
            "Effect": "Allow",
```

```
            "Principal": {
                "AWS": "arn:aws:iam::<aws_accountid>:role/aws-service-role/
cloud9.amazonaws.com/AWSServiceRoleForAWSCloud9"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow attachment of persistent resources",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<aws_accountid>:role/aws-service-role/
cloud9.amazonaws.com/AWSServiceRoleForAWSCloud9"
            },
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        }
```

Verwendung eines kontoübergreifenden Schlüssels

Wenn Sie einen kontoübergreifenden KMS-Schlüssel verwenden möchten, müssen Sie einen Grant in Kombination mit der KMS-Schlüsselrichtlinie verwenden. Dies ermöglicht den kontoübergreifenden Zugriff auf den Schlüssel. Führen Sie in demselben Konto, mit dem Sie die Cloud9-Umgebung erstellt haben, den folgenden Befehl im Terminal aus.

```
aws kms create-grant \
 --region <Region where Cloud9 environment is created> \
 --key-id <The cross-account KMS key ARN> \
```

```
--grantee-principal arn:aws:iam::<The account where Cloud9 environment is
created>:role/aws-service-role/cloud9.amazonaws.com/AWSServiceRoleForAWSCloud9 \
--operations "Encrypt" "Decrypt" "ReEncryptFrom" "ReEncryptTo" "GenerateDataKey"
"GenerateDataKeyWithoutPlaintext" "DescribeKey" "CreateGrant"
```

Nachdem Sie diesen Befehl ausgeführt haben, können Sie Cloud9-Umgebungen erstellen, indem Sie die EBS-Verschlüsselung mit einem Schlüssel in einem anderen Konto verwenden.

Automatisches Erstellen von Tag-basierten CloudWatch Amazon-Dashboards

Erstellt von Janak Vadaria (AWS), RAJNEESH TYAGI (AWS) und Vinodkumar Mandalapu (AWS)

Übersicht

Das manuelle Erstellen verschiedener CloudWatch Amazon-Dashboards kann zeitaufwändig sein, insbesondere wenn Sie mehrere Ressourcen erstellen und aktualisieren müssen, um Ihre Umgebung automatisch zu skalieren. Eine Lösung, die Ihre CloudWatch Dashboards automatisch erstellt und aktualisiert, kann Ihnen Zeit sparen. Dieses Muster hilft Ihnen bei der Implementierung einer vollautomatischen AWS Cloud Development Kit (AWS CDK) Pipeline, die CloudWatch Dashboards für Ihre AWS Ressourcen auf der Grundlage von Tag-Änderungsereignissen erstellt und aktualisiert, um Golden Signals-Metriken anzuzeigen.

Im Bereich Site Reliability Engineering (SRE) bezieht sich Golden Signals auf einen umfassenden Satz von Kennzahlen, die einen umfassenden Überblick über einen Service aus Nutzer- oder Verbrauchersicht bieten. Diese Metriken bestehen aus Latenz, Traffic, Fehlern und Sättigung. Weitere Informationen finden Sie unter Was ist Site Reliability Engineering (SRE)? auf der AWS Website.

Die durch dieses Muster bereitgestellte Lösung ist ereignisgesteuert. Nach der Bereitstellung überwacht es kontinuierlich die Tag-Änderungsereignisse und aktualisiert die CloudWatch Dashboards und Alarme automatisch.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert
- Voraussetzungen für die AWS CDK Version 2
- Eine Bootstrap-Umgebung auf AWS
- Python versie 3
- AWS SDK for Python (Boto3), installiert
- Node.js Version 18 oder höher
- Node Package Manager (npm), installiert und konfiguriert für AWS CDK

- Mittlere Vertrautheit (Stufe 200) mit dem und AWS CDK AWS CodePipeline

Einschränkungen

Diese Lösung erstellt derzeit automatisierte Dashboards nur für die folgenden AWS-Services:

- Amazon Relational Database Service (Amazon RDS)
- AWS Auto Scaling
- Amazon-Simple-Notification-Service (Amazon-SNS)
- Amazon-DynamoDB
- AWS Lambda

Architektur

Zieltechnologie-Stack

- CloudWatch Dashboards
- CloudWatch Alarme

Zielarchitektur

1. Ein AWS Tag-Änderungsereignis für die konfigurierten Anwendungs-Tags oder Codeänderungen initiiert eine Pipeline AWS CodePipeline zur Erstellung und Bereitstellung aktualisierter Dashboards. CloudWatch
2. AWS CodeBuild führt ein Python-Skript aus, um die Ressourcen zu finden, für die Tags konfiguriert sind, und speichert die Ressource IDs in einer lokalen Datei in einer CodeBuild Umgebung.
3. CodeBuild führt cdk synth aus, um AWS CloudFormation Vorlagen zu generieren, die CloudWatch Dashboards und Alarme bereitstellen.
4. CodePipeline stellt die AWS CloudFormation Vorlagen in der angegebenen Region bereit. AWS-Konto
5. Wenn der AWS CloudFormation Stack erfolgreich bereitgestellt wurde, können Sie sich die CloudWatch Dashboards und Alarme ansehen.

Automatisierung und Skalierung

Diese Lösung wurde mithilfe von automatisiert AWS CDK. Sie finden den Code im CloudWatch Repository GitHub Golden Signals Dashboards auf Amazon. Für zusätzliche Skalierung und zur Erstellung benutzerdefinierter Dashboards können Sie mehrere Tag-Schlüssel und -Werte konfigurieren.

Tools

Amazon-Dienste

- Amazon EventBridge ist ein serverloser Event-Bus-Service, der Ihnen hilft, Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen zu verbinden, darunter AWS Lambda Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen. AWS-Konten
- AWS CodePipelinehilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.
- AWS CodeBuildist ein vollständig verwalteter Build-Service, der Ihnen hilft, Quellcode zu kompilieren, Komponententests durchzuführen und Artefakte zu erstellen, die sofort einsatzbereit sind.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Bewährte Methoden

Als bewährte Sicherheitsmethode können Sie Verschlüsselung und Authentifizierung für die Quell-Repositorys verwenden, die eine Verbindung zu Ihren Pipelines herstellen. Weitere bewährte Methoden finden Sie in der Dokumentation unter CodePipeline Bewährte Methoden und Anwendungsfälle. CodePipeline

Epen

Konfigurieren und implementieren Sie die Beispielanwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren und implementieren Sie die Beispielanwendung.	1. Klonen Sie das GitHub Beispielcode-Repository mit dem folgenden Befehl: `git clone https://github.com/aws-samples/golden-signals-dashboards-sample-app` 2. Navigieren Sie zum geklonten Repository auf Ihrem Computer und öffnen Sie die `src/project-settings.ts` Datei mit einem Editor Ihrer Wahl. 3. Ändern Sie den `projectSettings` konstanten Wert entsprechend Ihren AWS Ressourcen-Tags und Anwendungszuordnungen. 4. Legen Sie die `AWS_ACCOUNT` `GS_DASHBOARD_INSTANCE` Umgebungsvariablen `AWS_REGION` , und fest: • Stellen `AWS_ACCOUNT` Sie die Konto-ID Ihres AWS Kontos ein.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wählen `AWS_REGION` Sie die Region aus, in der Sie die Beispielanwendung bereitstellen möchten. • Stellen Sie `GS_DASHBOARD_INSTANCE` `dev` dies `test` je nach Entwicklungsumgebung auf`prod`, oder ein. (Wir empfehlen `test` das in diesem Muster beschriebene Testverfahren.) 5. Richten Sie das AWS CLI mit Ihren AWS Anmeldeinformationen ein. Weitere Informationen finden Sie in der AWS CLI Dokumentation unter Einrichten und Anzeigen von Konfigurationseinstellungen mithilfe von Befehlen. 6. Führen Sie den folgenden Befehl aus, um die Golden Signals Dashboard-Beispielanwendung bereitzustellen: `sh deploy.sh`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Automatisches Erstellen von Dashboards und Alarmen.	Nachdem Sie die Beispielanwendung bereitgestellt haben, können Sie alle Ressourcen, die diese Lösung unterstützt, mit den erwarteten Tag-Werten erstellen. Dadurch werden automatisch die angegebenen Dashboards und Alarme erstellt. Um diese Lösung zu testen, erstellen Sie eine AWS Lambda Funktion: 1. Melden Sie sich in dem AWS Management Console Bereich an, in AWS-Region dem Sie die Beispielanwendung bereitgestellt haben. 2. Öffnen Sie die Lambda-Konsole unter https://console.aws.amazon.com/lambda/. 3. Wählen Sie Funktion erstellen und geben Sie dann einen Funktionsnamen ein. 4. Wählen Sie im Bereich Erweiterte Einstellungen die Option Tags aktivieren und dann Neues Tag hinzufügen aus. Geben Sie	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den folgenden Schlüssel und Wert ein: • Schlüssel: `AutoDashboard` • Wert: `True` 5. Wählen Sie Funktion erstellen. Die Lambda-Funktion startet sofort eine CodePipeline, die die Dashboards und Alarme für diese bestimmte Lambda-Funktion automatisch erstellt. 6. Um die automatisierten Dashboards und Alarme anzuzeigen, öffnen Sie die Konsole unter. CloudWatch https://console.aws.amazon.com/cloudwatch/ Sie können die benutzerdefinierten Dashboards und Alarme für die Funktion anzeigen, die Sie in der `projectSettings` Konstante angegeben haben (standardmäßig APP1-lambda). 7. Wählen Sie das Dashboard für die Lambda-Funktion aus, um zusätzliche automatisierte Dashboards anzuzeigen, die im Rahmen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dieser Lösung erstellt wurden. 8. Wiederholen Sie diese Schritte für andere Dienste wie Amazon RDS, Amazon SNS und DynamoDB AWS Auto Scaling, um die zugehörigen Dashboards zu generieren. Ein Beispiel für Amazon RDS finden Sie im Abschnitt Zusätzliche Informationen.	

Entfernen Sie die Beispielanwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entferne das `golden-signals-dashboard` Konstrukt.	1. Um alle von der Beispielanwendung erstellten AWS CloudFormation Stacks zu entfernen, müssen Sie die `GS_DASHBOARD_INSTANCE` Umgebungsvariablen `AWS_ACCOUNT` `AWS_REGION` , und neu konfigurieren. Für den `destroy.sh` Befehl sind diese Konfigurationen erforderlich. • `AWS_ACCOUNT` ist die Konto-ID Ihres AWS Kontos. • `AWS_REGION` ist die Region, in der Sie Ihre	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Beispielanwendung bereitgestellt haben. • `GS_DASHBOARD_INSTANCE` basiert`dev`,`test`, oder`prod`, auf Ihren vorherigen Einstellungen. 2. AWS CLI Mit Ihren AWS Anmeldeinformationen einrichten. 3. Führen Sie den folgenden Befehl aus, um die Beispielanwendung und alle zugehörigen AWS CloudFormation Stacks zu entfernen: `sh destroy.sh`	

Fehlerbehebung

Problem	Lösung
Der Python-Befehl wurde nicht gefunden (bezieht `findresources.sh` sich auf Zeile 8).	Überprüfen Sie die Version Ihrer Python-Installation. Wenn Sie Python Version 3 installiert haben, `python` ersetzen `python3` Sie es durch Zeile 8 der `resources.sh` Datei und führen Sie den `sh deploy.sh` Befehl erneut aus, um die Lösung bereitzustellen.

Zugehörige Ressourcen

- Bootstrapping (Dokumentation)AWS CDK

- Benannte Profile verwenden (Dokumentation)AWS CLI
- AWS CDK Werkstatt

Zusätzliche Informationen

Die folgende Abbildung zeigt ein Beispiel-Dashboard für Amazon RDS, das als Teil dieser Lösung erstellt wurde.

Dokumentieren Sie Ihr AWS-Landingzone-Design

Erstellt von Michael Daehnert (AWS), Florian Langer (AWS) und Michael Lodemann (AWS)

Übersicht

Eine landing zone ist eine gut strukturierte Umgebung mit mehreren Konten, die auf bewährten Methoden für Sicherheit und Compliance basiert. Es ist der unternehmensweite Container, der all Ihre Organisationseinheiten (OUs) AWS-Konten, Benutzer und andere Ressourcen enthält. Eine landing zone kann skaliert werden, um den Bedürfnissen eines Unternehmens jeder Größe gerecht zu werden. AWS bietet zwei Optionen für die Erstellung Ihrer landing zone: eine servicebasierte landing zone mithilfe AWS Control Toweroder eine benutzerdefinierte landing zone, die Sie erstellen. Für jede Option ist ein anderer AWS Wissensstand erforderlich.

AWS wurde entwickelt AWS Control Tower , um Ihnen zu helfen, Zeit zu sparen, indem Sie die Einrichtung einer landing zone automatisieren. AWS Control Tower wird von Ihnen verwaltet AWS und verwendet bewährte Verfahren und Richtlinien, um Sie bei der Erstellung Ihrer grundlegenden Umgebung zu unterstützen. AWS Control Tower verwendet integrierte Dienste wie AWS Service Catalogund AWS Organizations, um Konten in Ihrer landing zone bereitzustellen und den Zugriff auf diese Konten zu verwalten.

AWS Landezonenprojekte unterscheiden sich in Bezug auf Anforderungen, Implementierungsdetails und operative Maßnahmen. Es gibt Anpassungsaspekte, die bei jeder Landezonenimplementierung berücksichtigt werden müssen. Dies beinhaltet (ist aber nicht beschränkt auf), wie das Zugriffsmanagement gehandhabt wird, welcher Technologie-Stack verwendet wird und welche Überwachungsanforderungen für operative Exzellenz gelten. Dieses Muster bietet eine Vorlage, mit der Sie Ihr Landezonenprojekt dokumentieren können. Mithilfe der Vorlage können Sie Ihr Projekt schneller dokumentieren und Ihren Entwicklungs- und Betriebsteams helfen, Ihre landing zone zu verstehen.

Voraussetzungen und Einschränkungen

Einschränkungen

Dieses Muster beschreibt nicht, was eine landing zone ist oder wie sie implementiert wird. Weitere Informationen zu diesen Themen finden Sie im Abschnitt Verwandte Ressourcen.

Epen

Erstellen Sie das Entwurfsdokument

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die wichtigsten Interessengruppen.	Identifizieren Sie wichtige Service- und Teammanager, die mit Ihrer landing zone verbunden sind.	Projektmanager
Passen Sie die Vorlage an.	Laden Sie die Vorlage im Bereich Anlagen herunter und aktualisieren Sie die Vorlage dann wie folgt: 1. Entfernen Sie alle Abschnitte, die nicht für die landing zone oder die Prozesse Ihres Unternehmens gelten. 2. Fügen Sie alle Abschnitte hinzu, die für Ihre Organisation einzigartig sind.	Projektmanager
Füllen Sie die Vorlage aus.	Füllen Sie die Vorlage in Besprechungen mit den Beteiligten oder mithilfe eines write-and-review Prozesses wie folgt aus: 1. Verwenden Sie die Anleitungen und Informationen in den blauen Feldern, um die einzelnen Abschnitte auszufüllen. 2. Ersetzen oder entfernen Sie alle gelben Felder durch	Projektmanager

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	benutzerdefinierte Werte für Ihre Organisation. 3. Ersetzen oder entfernen Sie alle Bildfelder durch Ihre benutzerdefinierte Architektur oder Flussdiagramme. 4. Füllen Sie den Abschnitt Revisionsverlauf und Mitwirkende der Vorlage aus.	
Teilen Sie das Entwurfsdokument.	Wenn Ihre Entwurfsdokumentation für die landing zone vollständig ist, speichern Sie sie in einem gemeinsam genutzten Repository oder an einem zentralen Ort, wo alle Beteiligten darauf zugreifen können. Wir empfehlen, dass Sie Standardprozesse zur Dokumentenkontrolle verwenden, um Änderungen am Konstruktionsdokument aufzuzeichnen und zu genehmigen.	Projektmanager

Zugehörige Ressourcen

- AWS Control Tower Dokumentation
  - Plane deine AWS Control Tower landing zone
  - AWS Strategie für mehrere Konten für Ihre AWS Control Tower landing zone
  - Administrative Tipps für die Einrichtung der landing zone
  - Erwartungen an die Konfiguration der landing zone

- Anpassungen für AWS Control Tower (AWS Lösungsbibliothek)
- Einrichtung einer sicheren und skalierbaren AWS Umgebung mit mehreren Konten (AWS Prescriptive Guidance)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Verbessern Sie die Betriebsleistung, indem Sie Amazon DevOps Guru in mehreren AWS-Regionen, Konten und OUs mit dem AWS CDK aktivieren

Erstellt von Dr. Rahul Sharad Gaikwad (AWS)

Übersicht

Dieses Muster zeigt die Schritte zur Aktivierung des Amazon DevOps Guru-Service in mehreren Amazon Web Services (AWS) -Regionen, Konten und Organisationseinheiten (OUs) mithilfe des AWS Cloud Development Kit (AWS CDK) in TypeScript. Sie können AWS CDK-Stacks verwenden, um AWS CloudFormation StackSets vom (primären) AWS-Administratorkonto aus bereitzustellen, um Amazon DevOps Guru für mehrere Konten zu aktivieren, anstatt sich bei jedem Konto anzumelden und DevOps Guru für jedes Konto einzeln zu aktivieren.

Amazon DevOps Guru bietet Funktionen für künstliche Intelligenz (AIOps), mit denen Sie die Verfügbarkeit Ihrer Anwendungen verbessern und betriebliche Probleme schneller lösen können. DevOps Guru reduziert Ihren manuellen Aufwand, indem es Empfehlungen anwendet, die auf maschinellem Lernen (ML) basieren, ohne dass ML-Kenntnisse erforderlich sind. DevOps Guru analysiert Ihre Ressourcen und Betriebsdaten. Wenn es Anomalien feststellt, bietet es Kennzahlen, Ereignisse und Empfehlungen, die Ihnen helfen, das Problem zu lösen.

Dieses Muster beschreibt drei Bereitstellungsoptionen für die Aktivierung von Amazon DevOps Guru:

- Für alle Stack-Ressourcen in mehreren Konten und Regionen
- Für alle Stack-Ressourcen auf OUs
- Für bestimmte Stack-Ressourcen über mehrere Konten und Regionen

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert. (Weitere Informationen finden Sie unter Installation, Aktualisierung und Deinstallation der AWS-CLI in der AWS-CLI-Dokumentation.)
- AWS CDK Toolkit, installiert und konfiguriert. (Siehe AWS CDK Toolkit in der AWS CDK-Dokumentation.)

- Node Package Manager (npm), installiert und konfiguriert für das AWS-CDK in. TypeScript (Weitere Informationen finden Sie unter Node.js und npm herunterladen und installieren in der npm-Dokumentation.)
- Python3 wurde installiert und konfiguriert, um ein Python-Skript auszuführen, um Datenverkehr in die serverlose Beispielanwendung einzuschleusen. (Siehe Python-Setup und -Verwendung in der Python-Dokumentation.)
- Pip, installiert und konfiguriert, um die Python-Anforderungsbibliothek zu installieren. (Weitere Informationen finden Sie in den Pip-Installationsanweisungen auf der PyPI Website.)

Produktversionen

- AWS CDK Toolkit Version 1.107.0 oder höher
- npm Version 7.9.0 oder höher
- Node.js Version 15.3.0 oder höher

Architektur

Technologien

Die Architektur für dieses Muster umfasst die folgenden Dienste:

- DevOps Amazon-Guru
- AWS CloudFormation
- Amazon API Gateway
- AWS Lambda
- Amazon-DynamoDB
- Amazon CloudWatch
- AWS CloudTrail

AWS-CDK-Stapel

Das Muster verwendet die folgenden AWS-CDK-Stacks:

- `CdkStackSetAdminRole`— Erstellt eine Administratorrolle für AWS Identity and Access Management (IAM), um eine Vertrauensbeziehung zwischen dem Administrator und den Zielkonten herzustellen.

- `CdkStackSetExecRole`— Erstellt eine IAM-Rolle, um dem Administratorkonto zu vertrauen.
- `CdkDevopsGuruStackMultiAccReg`— Aktiviert DevOps Guru in mehreren AWS-Regionen und Konten für alle Stacks und richtet Amazon Simple Notification Service (Amazon SNS) - Benachrichtigungen ein.
- `CdkDevopsGuruStackMultiAccRegSpecStacks`— Aktiviert DevOps Guru in mehreren AWS-Regionen und Konten für bestimmte Stacks und richtet Amazon SNS SNS-Benachrichtigungen ein.
- `CdkDevopsguruStackOrgUnit`— Aktiviert DevOps Guru Across OUs und richtet Amazon SNS SNS-Benachrichtigungen ein.
- `CdkInfrastructureStack`— Stellt serverlose Beispielanwendungskomponenten wie API Gateway, Lambda und DynamoDB im Administratorkonto bereit, um die Fehlerinjektion und die Generierung von Erkenntnissen zu demonstrieren.

Beispiel für eine Anwendungsarchitektur

Das folgende Diagramm zeigt die Architektur einer serverlosen Beispielanwendung, die in mehreren Konten und Regionen bereitgestellt wurde. Das Muster verwendet das Administratorkonto, um alle AWS-CDK-Stacks bereitzustellen. Es verwendet auch das Administratorkonto als eines der Zielkonten für die Einrichtung DevOps von Guru.

1. Wenn DevOps Guru aktiviert ist, erstellt es zunächst eine Baseline-Analyse für das Verhalten der einzelnen Ressourcen und nimmt dann Betriebsdaten aus CloudWatch den bereitgestellten Kennzahlen auf.
2. Wenn es eine Anomalie erkennt, korreliert es diese mit den Ereignissen aus CloudTrail und generiert daraus Erkenntnisse.
3. Die Erkenntnisse liefern eine korrelierte Abfolge von Ereignissen sowie vorgeschriebene Empfehlungen, die es dem Betreiber ermöglichen, die verursachende Ressource zu identifizieren.
4. Amazon SNS sendet Benachrichtigungen an den Betreiber.

Automatisierung und Skalierung

Das mit diesem Muster bereitgestellte GitHub Repository verwendet das AWS-CDK als Infrastructure-as-Code-Tool (IaC), um die Konfiguration für diese Architektur zu erstellen. AWS CDK hilft Ihnen dabei, Ressourcen zu orchestrieren und DevOps Guru für mehrere AWS-Konten, Regionen und zu aktivieren. OUs

Tools

AWS-Services

- AWS CDK — Das AWS Cloud Development Kit (AWS CDK) hilft Ihnen dabei, Ihre Cloud-Infrastruktur als Code in einer der fünf unterstützten Programmiersprachen zu definieren: TypeScript,, Python JavaScript, Java und C#.
- AWS CLI — Die AWS-Befehlszeilenschnittstelle (AWS CLI) ist ein einheitliches Tool, das eine konsistente Befehlszeilenschnittstelle für die Interaktion mit AWS-Services und -Ressourcen bietet.

Code

Der Quellcode für dieses Muster ist im Amazon DevOps Guru CDK Samples-Repository verfügbar. GitHub Der AWS-CDK-Code ist TypeScript eingeschrieben. Folgen Sie den Anweisungen im nächsten Abschnitt, um das Repository zu klonen und zu verwenden.

> **Important**
>
> Einige der Geschichten in diesem Muster enthalten AWS CDK- und AWS CLI-Befehlsbeispiele, die für Unix, Linux und macOS formatiert sind. Ersetzen Sie unter Windows das Fortsetzungszeichen mit dem umgekehrten Schrägstrich (\) am Ende jeder Zeile durch ein Caret-Zeichen (^).

Epen

Bereiten Sie die AWS-Ressourcen für die Bereitstellung vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie benannte AWS-Profile.	Richten Sie Ihre benannten AWS-Profile wie folgt ein, um Stacks in einer Umgebung mit mehreren Konten bereitzus tellen. Für das Administratorkonto:	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`$aws configure --profile administrator`
	`AWS Access Key ID [****]: <your-administrator-access-key-ID>`
	`AWS Secret Access Key [****]: <your-administrator-secret-access-key>`
	`Default region name [None]: <your-administrator-region>`
	`Default output format [None]: json`
	
	Für das Zielkonto:
	
	`$aws configure --profile target`
	`AWS Access Key ID [****: <your-target-access-key-ID>`
	`AWS Secret Access Key [****]: <your-target-secret-access-key>`
	`Default region name [None]: <your-target-region>`
	`Default output format [None]: json`
	
	Weitere Informationen finden Sie unter Verwenden von benannten Profilen in der AWS-CLI-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die AWS-Profilkonfigurationen.	(Optional) Sie können Ihre AWS-Profilkonfigurationen in den `config` Dateien `credentials` und überprüfen, indem Sie den Anweisungen unter Konfigurationseinstellungen einrichten und anzeigen in der AWS-CLI-Dokumentation folgen.	DevOps Ingenieur
Überprüfen Sie die AWS-CDK-Version.	Überprüfen Sie die Version des AWS CDK Toolkit, indem Sie den folgenden Befehl ausführen: `$cdk --version` Für dieses Muster ist Version 1.107.0 oder höher erforderlich. Wenn Sie eine frühere Version von AWS CDK haben, folgen Sie den Anweisungen in der AWS CDK-Dokumentation, um sie zu aktualisieren.	DevOps Ingenieur
Klonen Sie den Projektcode.	Klonen Sie das GitHub Repository für dieses Muster mit dem folgenden Befehl: `$git clone https://github.com/aws-samples/amazon-devopsguru-cdk-samples.git`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Installieren Sie die Paketabhängigkeiten und kompilieren Sie die TypeScript Dateien.	Installieren Sie die Paketabhängigkeiten und kompilieren Sie die TypeScript Dateien, indem Sie die folgenden Befehle ausführen:
	`$cd amazon-devopsguru-cdk-samples`
	`$npm install`
	`$npm fund`
	Mit diesen Befehlen werden alle Pakete aus dem Beispiel-Repository installiert.
	Important
	Wenn Sie eine Fehlermeldung über fehlende Pakete erhalten, verwenden Sie einen der folgenden Befehle:
	`$npm ci`
	–oder–
	`$npm install -g @aws-cdk/<package-name>`
	Die Liste der Paketnamen und Versionen finden Sie im `Dependencies` Abschnitt
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der `/amazon-devopsguru-cdk-samples/package.json` Datei. Weitere Informationen finden Sie unter npm ci und npm install in der npm-Dokumentation.	

Erstellen (synthetisieren) Sie die AWS-CDK-Stacks

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie eine E-Mail-Adresse für Amazon SNS SNS-Benachrichtigungen.	Gehen Sie wie folgt vor, um eine E-Mail-Adresse für Amazon SNS SNS-Benachrichtigungen anzugeben: 1. Bearbeiten Sie die Dateien `/amazon-devopsguru-cdk-samples/lib/cdk-devopsguru-multi-acc-reg-stack.ts` und `/amazon-devopsguru-cdk-samples/lib/cdk-devopsguru-org-uni-stack.ts` . 2. Aktualisieren Sie im `Subscription` Abschnitt `DevOpsGuruTopic` , den `Endpoint` Parameter mit Ihrer E-Mail-Adresse. 3. Speichern und schließen Sie die Dateien.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den Projektcode.	Erstellen Sie den Projektcode und synthetisieren Sie die Stacks, indem Sie den folgenden Befehl ausführen:
	`npm run build && cdk synth`
	Die Ausgabe sollte folgender maßen oder ähnlich aussehen:
	`$npm run build && cdk synth`
	`> cdk-devopsguru@0.1.0 build`
	`> tsc`
	`Successfully synthesized to ~/amazon-devopsguru-cdk-samples/cdk.out`
	`Supply a stack id (CdkDevopsGuruStackMultiAccReg,CdkDevopsGuruStackMultiAccRegSpecStacks, CdkDevopsguruStackOrgUnit, CdkInfrastructureStack, CdkStackSetAdminRole, CdkStackSetExecRole) to display its template.`
	Weitere Informationen und Schritte finden Sie unter Ihre erste AWS-CDK-App in der AWS-CDK-Dokumentation.
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Listet die AWS CDK-Stacks auf.	Führen Sie den folgenden Befehl aus, um alle AWS-CDK-Stacks aufzulisten:
	`$cdk list`
	Der Befehl zeigt die folgende Liste an:
	`CdkDevopsGuruStack`
	`MultiAccReg`
	`CdkDevopsGuruSt`
	`ackMultiAccRegSpec`
	`Stacks`
	`CdkDevopsguruStackOr`
	`gUnit`
	`CdkInfrastructureStac`
	`k`
	`CdkStackSetAdminRole`
	`CdkStackSetExecRole`
		DevOps Ingenieur

Option 1 — Aktivieren Sie DevOps Guru für alle Stack-Ressourcen über mehrere Konten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die AWS CDK-Stacks für die Erstellung von IAM-Rollen bereit.	Dieses Muster verwendet AWS CloudFormation StackSets, um Stack-Ope rationen über mehrere Konten hinweg durchzuführen. Wenn Sie Ihr erstes Stack-Set erstellen, müssen Sie die folgenden IAM-Rollen erstellen, um die erforderl	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ichen Berechtigungen in Ihren AWS-Konten einzurichten: • `AWSCloudFormationStackSetAdministrationRole` • `AWSCloudFormationStackSetExecutionRole` **Note** Die Rollen müssen genau diese Namen haben. 1. Erstellen Sie die `AWSCloudFormationStackSetAdministrationRole` IAM-Rolle im Administratorkonto (primär), indem Sie den folgenden CLI-Befehl ausführen: `$cdk deploy CdkStackSetAdminRole --profile administrator` 2. Erstellen Sie die `AWSCloudFormationStackSetExecutionRole` IAM-Rolle in allen Zielkonten, auf denen Sie die Stack-Instances	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	ausführen möchten. Führen Sie die folgenden CLI-Befehle aus, um diese Rolle zu erstellen:
	
	`$cdk deploy CdkStackSetExecRole \`
	`  --parameters AdministratorAccountId=<administrator-account-ID> \`
	`  --profile administrator`
	
	`$cdk deploy CdkStackSetExecRole \`
	`  --parameters AdministratorAccountId=<administrator-account-ID> \`
	`  --profile target`
	
	Weitere Informationen finden Sie in der CloudFormation AWS-Dokumentation unter Gewähren selbstverwalteter Berechtigungen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie den AWS CDK-Stack bereit, um DevOps Guru für mehrere Konten zu aktivieren.	Der AWS `CdkDevopsGuruStackMultiAccReg` CDK-Stack erstellt StackSets zur Bereitstellung von Stack-Instances über mehrere Konten und Regionen hinweg. Führen Sie den folgenden CLI-Befehl mit den angegebenen Parametern aus, um den Stack bereitzustellen:
	`$cdk deploy CdkDevopsGuruStackMultiAccReg \`
	`  --profile administrator \`
	`  --parameters AdministratorAccountId=<administrator-account-ID> \`
	`  --parameters TargetAccountId=<target-account-ID> \`
	`  --parameters RegionIds="<region-1>,<region-2>"`
	Derzeit ist Amazon DevOps Guru in den AWS-Regionen verfügbar, die in den häufig gestellten Fragen zu DevOps Guru aufgeführt sind.
		DevOps Ingenieur

Option 2 — Aktivieren Sie DevOps Guru für alle Stack-Ressourcen OUs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Organisationseinheit extrahieren IDs.	Identifizieren Sie auf der AWS Organizations IDs Organizations-Konsole die Organisationseinheiten, in denen Sie DevOps Guru aktivieren möchten.	DevOps Ingenieur
Aktivieren Sie vom Service verwaltete Berechtigungen für OUs.	Wenn Sie AWS Organizations für die Kontoverwaltung verwenden, müssen Sie service-verwaltete Berechtigungen gewähren, um DevOps Guru zu aktivieren. Anstatt die IAM-Rollen manuell zu erstellen, verwenden Sie organisationsbasierte Rollen mit vertrauenswürdigem Zugriff und serviceverknüpften Rollen (). SLRs	DevOps Ingenieur

Stellen Sie den AWS CDK-Stack bereit, um DevOps Guru Across OUs zu aktivieren.	Der `CdkDevopsguruStackOrgUnit` AWS-CDK-Stack ermöglicht den gesamten DevOps OUs Guru-Service. Um den Stack bereitzustellen, führen Sie den folgenden Befehl mit den angegebenen Parametern aus:
	`$cdk deploy CdkDevopsguruStackOrgUnit \`
	`  --profile administrator \`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--parameters RegionIds="<region-1>,<region-2>" \ --parameters OrganizationalUnitIds="<OU-1>,<OU-2>"`	

Option 3 — Aktivieren Sie DevOps Guru für bestimmte Stack-Ressourcen über mehrere Konten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die AWS CDK-Stacks für die Erstellung von IAM-Rollen bereit.	Wenn Sie die in der ersten Option aufgeführten erforderlichen IAM-Rollen noch nicht erstellt haben, tun Sie dies zuerst: 1. Erstellen Sie die `AWSCloudFormationStackSetAdministrationRole` IAM-Rolle im Administratorkonto (primär), indem Sie den folgenden CLI-Befehl ausführen: `$cdk deploy CdkStackSetAdminRole --profile administrator` 2. Erstellen Sie die `AWSCloudFormationStackSetExecutionRole` IAM-Rolle in allen Zielkonten, auf denen Sie die Stack-Instances ausführen möchten. Führen	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Sie die CLI-Befehle aus, um diese Rolle zu erstellen:
	
	`$cdk deploy CdkStackSetExecRole \ --parameters AdministratorAccountId=<administrator-account-ID> \ --profile administrator`
	
	`$cdk deploy CdkStackSetExecRole \ --parameters AdministratorAccountId=<administrator-account-ID> \ --profile target`
	
	Weitere Informationen finden Sie in der CloudFormation AWS-Dokumentation unter Gewähren selbstverwalteter Berechtigungen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie vorhandene Stapel.	Wenn Sie bereits die erste Option verwendet haben, um DevOps Guru für alle Stack-Ressourcen zu aktivieren, können Sie den alten Stack mit dem folgenden Befehl löschen: `$cdk destroy CdkDevopsGuruStackMultiAccReg --profile administrator` Sie können den `RegionIds` Parameter auch ändern, wenn Sie den Stack erneut bereitstellen, um den Fehler Stacks already exist zu vermeiden.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie den AWS CDK-Stack mit einer Stack-Liste.	1. Bearbeiten Sie die `/amazon-devopsguru-cdk-samples/lib/cdk-devopsguru-multi-acc-reg-spec-stack.ts` -Datei. 2. Führen Sie unter `Resources CloudFormation` ,`StackNames` , die Stacks auf, für die Sie Guru aktivieren DevOps möchten. Zu Demonstrationszwecken gibt der Parameter den `CdkInfrastructureStack` Stack an. Sie können diesen Eintrag jedoch nach Ihren Anforderungen bearbeiten. 3. Speichern und schließen Sie die Datei. 4. Um die Stack-Vorlage zu synthetisieren und zu aktualisieren, führen Sie folgenden Befehl aus: `$cdk synth`	Dateningenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den AWS CDK-Stack bereit, um DevOps Guru für bestimmte Stack-Ressourcen über mehrere Konten hinweg zu aktivieren.	Der AWS `CdkDevopsGuruStackMultiAccRegSpecStacks` CDK-Stack ermöglicht DevOps Guru für bestimmte Stack-Ressourcen über mehrere Konten hinweg. Führen Sie den folgenden Befehl aus, um den Stack bereitzustellen: `$cdk deploy CdkDevopsGuruStackMultiAccRegSpecStacks \ --profile administrator \ --parameters AdministratorAccountId=<administrator-account-ID> \ --parameters TargetAccountId=<target-account-ID> \ --parameters RegionIds="<region-1>,<region-2>"` **Note** Wenn Sie diesen Stack bereits für Option 1 bereitgestellt haben, ändern Sie den `RegionIds` Parameter (stellen Sie sicher, dass Sie aus verfügbaren Regionen wählen), um den	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Fehler Stacks already exist zu vermeiden.	

Stellen Sie den AWS CDK-Infrastruktur-Stack bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie das Beispiel für einen serverlosen Infrastru kturstapel bereit.	Der `CdkInfrastructureS tack` AWS-CDK-Stack stellt serverlose Komponenten wie API Gateway, Lambda und eine DynamoDB-Tabelle bereit, um die Erkenntnisse von Guru zu demonstrieren. DevOps Führen Sie den folgenden Befehl aus, um den Stack bereitzustellen: `$cdk deploy CdkInfras tructureStack -- profile administrator`	DevOps Ingenieur
Fügen Sie Beispieldatensätze in DynamoDB ein.	Führen Sie den folgenden Befehl aus, um die DynamoDB-Tabelle mit Beispieldatensätzen zu füllen. Geben Sie den richtigen Pfad für das Skript an. `populate-shops-dynamodb-tab le.json` `$aws dynamodb batch-wri te-item \`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`--request-items file://scripts/populate-shops-dynamodb-table.json \ --profile administrator`
	
	Die Ausgabe des Befehls sieht wie folgt aus:
	
	`{ "UnprocessedItems": {} }`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Überprüfen Sie die eingefügten Datensätze in DynamoDB.	Um zu überprüfen, ob die DynamoDB-Tabelle die Beispieldatensätze aus der `populate-shops-dynamodb-table.json` Datei enthält, greifen Sie auf die URL für die `ListRestApiEndpointMonitorOperator` API zu, die als Ausgabe des AWS-CDK-Stacks veröffentlicht wird. Sie finden diese URL auch auf der Registerkarte Outputs der CloudFormation AWS-Konsole für den `CdkInfrastructureStack` Stack. Die AWS-CDK-Ausgabe würde wie folgt aussehen:
	
	`CdkInfrastructureStack.CreateRestApiMonitorOperatorEndpointD1D00045 = https://oure17c5vob.execute-api.<your-region>.amazonaws.com/prod/`
	
	`CdkInfrastructureStack.ListRestApiMonitorOperatorEndpointABBDB8D8 = https://cdff8icfrn4.execute-api.<your-region>.amazonaws.com/prod/`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Warten Sie, bis die Ressourcen das Baselining abgeschlossen haben.	Dieser serverlose Stack hat einige Ressourcen. Wir empfehlen, dass Sie 2 Stunden warten, bevor Sie die nächsten Schritte ausführen. Wenn Sie diesen Stack in einer Produktionsumgebung bereitgestellt haben, kann es bis zu 24 Stunden dauern, bis das Baselining abgeschlossen ist. Dies hängt von der Anzahl der Ressourcen ab, die Sie in DevOps Guru für die Überwachung ausgewählt haben.	DevOps Ingenieur

Generieren Sie Einblicke in DevOps Guru

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie den AWS CDK-Infrastruktur-Stack.	Um DevOps Guru Insights auszuprobieren, können Sie einige Konfigurationsänderungen vornehmen, um ein typisches Betriebsproblem zu reproduzieren. 1. Bearbeiten Sie die `/amazon-devopsguru-cdk-samples/lib/infrastructure-stack.ts` -Datei. 2. Ändern Sie in `DDB Table` diesem Abschnitt die	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Lesekapazität für die DynamoDB-Tabelle von 5 auf 1.
	3. Speichern und schließen Sie die Datei.
	4. Führen Sie die folgenden Befehle aus, um den aktualisierten AWS CDK-Infrastruktur-Stack zu synthetisieren und bereitzustellen:
	`$cdk synth`
	`$cdk deploy CdkInfrastructureStack --profile administrator`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie HTTP-Anfragen in die API ein.	Fügen Sie eingehenden Datenverkehr in Form von HTTP-Anfragen in die API ein: `ListRestApiMonitor0peratorEndpointxxxx` 1. Bearbeiten Sie das Python-Skript `/amazon-devopsguru-cdk-samples/scripts/sendAPIRequest.py` . 2. Aktualisieren Sie die `url` Variable mit dem API-Link für `ListRestApiMonitorOperatorEndpointxxxx` . Sie finden diese URL in der Ausgabe des Befehls AWS CDK deploy oder in der AWS Cloudformation-Konsole auf der Registerkarte Outputs für den Stack. 3. Speichern und schließen Sie die Datei. 4. Führen Sie das Python-Skript mit dem folgenden Befehl aus: `$python sendAPIRequest.py` 5. Stellen Sie sicher, dass Sie den Statuscode 200 erhalten.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Möglicherweise müssen Sie das Skript über mehrere (vorzugsweise vier) Terminals ausführen, um eine hohe Datenverk ehrsrate zu erreichen. 7. Nachdem das Skript etwa 10 Minuten in einer Schleife ausgeführt wurde, können Sie auf der DevOps Guru-Konsole einen Einblick in die Betriebsabläufe erhalten.	
Sehen Sie sich DevOps Guru Insights an.	Unter Standardbedingungen zeigt das DevOps Guru-Dash board im Zähler für laufende Einblicke Null an. Wenn es eine Anomalie erkennt, gibt es eine Warnung in Form eines Einblicks aus. Wählen Sie im Navigationsbereich Insights aus, um die Details der Anomalie anzuzeigen, einschließlich einer Übersicht , aggregierter Kennzahlen, relevanter Ereignisse und Empfehlungen. Weitere Informationen zur Überprüfu ng von Erkenntnissen finden Sie im Blogbeitrag Gewinnen betrieblicher Erkenntnisse AIOps mit Amazon DevOps Guru.	DevOps Ingenieur

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Ressourcen bereinigen und löschen.	Nachdem Sie dieses Muster durchgegangen sind, sollten Sie die Ressourcen, die Sie erstellt haben, entfernen, um weitere Kosten zu vermeiden . Führen Sie die folgenden Befehle aus:
	`$cdk destroy CdkDevopsGuruStackMultiAccRegprofile administrator`
	`$cdk destroy CdkDevopsguruStackOrgUnit --profile administrator`
	`$cdk destroy CdkDevopsGuruStackMultiAccRegSpecStacks --profile administrator`
	`$cdk destroy CdkInfrastructureStack --profile administrator`
	`$cdk destroy CdkStackSetAdminRole --profile administrator`
	`$cdk destroy CdkStackSetExecRole --profile administrator`
	`$cdk destroy CdkStackSetExecRole --profile target`
		DevOps Ingenieur

Zugehörige Ressourcen

- AIOps Mit Amazon DevOps Guru betriebliche Einblicke gewinnen

- Einfache Konfiguration von Amazon DevOps Guru für mehrere Konten und Regionen mit AWS CloudFormation StackSets
- DevOps Guru-Workshop

Implementieren Sie Account Factory for Terraform (AFT) mithilfe einer Bootstrap-Pipeline

Erstellt von Vinicius Elias (AWS) und Edgar Costa Filho (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Dieses Muster bietet eine einfache und sichere Methode für die Bereitstellung von AWS Control Tower Account Factory for Terraform (AFT) über das Verwaltungskonto von. AWS Organizations Der Kern der Lösung ist eine AWS CloudFormation Vorlage, die die AFT-Konfiguration automatisiert, indem eine Terraform-Pipeline erstellt wird, die so strukturiert ist, dass sie für die erste Bereitstellung oder nachfolgende Updates leicht angepasst werden kann.

Sicherheit und Datenintegrität haben bei uns oberste Priorität. AWS Daher wird die Terraform-Statusdatei, eine wichtige Komponente, die den Status der verwalteten Infrastruktur und Konfigurationen verfolgt, sicher in einem Amazon Simple Storage Service (Amazon S3) -Bucket gespeichert. Dieser Bucket ist mit verschiedenen Sicherheitsmaßnahmen konfiguriert, darunter serverseitige Verschlüsselung und Richtlinien zur Blockierung des öffentlichen Zugriffs, um sicherzustellen, dass Ihr Terraform-Status vor unbefugtem Zugriff und Datenschutzverletzungen geschützt ist.

Das Verwaltungskonto orchestriert und überwacht die gesamte Umgebung, sodass es sich um eine wichtige Ressource in der Umgebung handelt. AWS Control Tower Dieses Muster folgt AWS bewährten Methoden und stellt sicher, dass der Bereitstellungsprozess nicht nur effizient ist, sondern auch den Sicherheits- und Governance-Standards entspricht, um eine umfassende, sichere und effiziente Möglichkeit zur Bereitstellung von AFT in Ihrer Umgebung zu bieten. AWS

Weitere Informationen zu AFT finden Sie in der AWS Control Tower Dokumentation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine einfache Umgebung mit AWS mehreren Konten mit mindestens den folgenden Konten: Verwaltungskonto, Protokollarchivkonto, Auditkonto und einem zusätzlichen Konto für die AFT-Verwaltung.

- Eine etablierte AWS Control Tower Umgebung. Das Verwaltungskonto sollte ordnungsgemäß konfiguriert sein, da die CloudFormation Vorlage darin bereitgestellt wird.
- Die erforderlichen Berechtigungen im AWS Verwaltungskonto. Sie benötigen ausreichende Berechtigungen, um Ressourcen wie S3-Buckets, AWS Lambda Funktionen, AWS Identity and Access Management (IAM-) Rollen und Projekte zu erstellen und AWS CodePipeline zu verwalten.
- Vertrautheit mit Terraform. Es ist wichtig, die Kernkonzepte und den Arbeitsablauf von Terraform zu verstehen, da die Bereitstellung die Generierung und Verwaltung von Terraform-Konfigurationen beinhaltet.

Einschränkungen

- Beachten Sie die AWS Ressourcenkontingente in Ihrem Konto. Durch die Bereitstellung werden möglicherweise mehrere Ressourcen erstellt, und das Erreichen von Dienstkontingenten könnte den Bereitstellungsprozess behindern.
- Die Vorlage wurde für bestimmte Versionen von Terraform und entwickelt. AWS-Services Für das Aktualisieren oder Ändern von Versionen sind möglicherweise Änderungen an der Vorlage erforderlich.
- Die Vorlage unterstützt keine Dienste des selbstverwalteten Versionskontrollsystems (VCS) wie GitHub Enterprise.

Produktversionen

- Terraform Version 1.6.6 oder höher
- AFT Version 1.11 oder höher

Architektur

Zieltechnologie-Stack

- AWS CloudFormation
- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- Amazon EventBridge
- IAM

- AWS Lambda
- Amazon S3

Zielarchitektur

Das folgende Diagramm veranschaulicht die Implementierung, die in diesem Muster beschrieben wird.

Der Workflow besteht aus drei Hauptaufgaben: dem Erstellen der Ressourcen, dem Generieren des Inhalts und dem Ausführen der Pipeline.

Die Ressourcen erstellen

Die mit diesem Muster bereitgestellte CloudFormation Vorlage erstellt und richtet alle erforderlichen Ressourcen ein, abhängig von den Parametern, die Sie bei der Bereitstellung der Vorlage auswählen. Die Vorlage erstellt mindestens die folgenden Ressourcen:

- Eine CodePipeline Pipeline zur Implementierung des AFT
- Ein S3-Bucket zum Speichern der Terraform-Statusdatei, die der AFT-Implementierung zugeordnet ist
- Zwei CodeBuild Projekte zur Implementierung des Terraform-Plans und zur Anwendung von Befehlen in verschiedenen Phasen der Pipeline
- IAM-Rollen für und Dienste CodeBuild CodePipeline
- Ein zweiter S3-Bucket zum Speichern von Pipeline-Laufzeitartefakten

Je nach ausgewähltem VCS-Anbieter (CodeCommit oder externem VCS) erstellt die Vorlage die folgenden Ressourcen.

- CodeCommit:
  - Ein CodeCommit Repository zum Speichern des AFT Terraform-Bootstrap-Codes
  - Eine EventBridge Regel zum Erfassen von CodeCommit Repository-Änderungen in der Filiale `main`
  - Eine weitere IAM-Rolle für die Regel EventBridge
- Für jeden anderen externen VCS-Anbieter, wie zum Beispiel: GitHub
  - Eine Verbindung AWS CodeConnections

Wenn Sie CodeCommit als VCS-Anbieter auswählen und den `Generate AFT Files` Parameter auf festlegen, erstellt die Vorlage außerdem die folgenden zusätzlichen Ressourcen`true`, um den Inhalt zu generieren:

- Ein S3-Bucket zum Speichern des generierten Inhalts und zur Verwendung als Quelle für das Repository CodeCommit
- Eine Lambda-Funktion, um die angegebenen Parameter zu verarbeiten und den entsprechenden Inhalt zu generieren
- Eine IAM-Funktion zum Ausführen der Lambda-Funktion
- Eine CloudFormation benutzerdefinierte Ressource, die die Lambda-Funktion ausführt, wenn die Vorlage bereitgestellt wird

Der Inhalt wird generiert

Um die AFT-Bootstrap-Dateien und deren Inhalt zu generieren, verwendet die Lösung eine Lambda-Funktion und einen S3-Bucket. Die Funktion erstellt einen Ordner im Bucket und anschließend zwei Dateien innerhalb des Ordners: `main.tf` und. `backend.tf` Die Funktion verarbeitet auch die angegebenen CloudFormation Parameter und füllt diese Dateien mit vordefiniertem Code, wodurch die jeweiligen Parameterwerte ersetzt werden.

Den Code, der als Vorlage für die Generierung der Dateien verwendet wird, finden Sie im GitHub Repository der Lösung. Im Grunde werden die Dateien wie folgt generiert.

main.tf

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory?
ref=<aft_version>"

  # Required variables
  ct_management_account_id  = "<ct_management_account_id>"
  log_archive_account_id    = "<log_archive_account_id>"
  audit_account_id          = "<audit_account_id>"
  aft_management_account_id = "<aft_management_account_id>"
  ct_home_region            = "<ct_home_region>"

  # Optional variables
  tf_backend_secondary_region = "<tf_backend_secondary_region>"
  aft_metrics_reporting       = "<false|true>"
```

```
  # AFT Feature flags
  aft_feature_cloudtrail_data_events      = "<false|true>"
  aft_feature_enterprise_support          = "<false|true>"
  aft_feature_delete_default_vpcs_enabled = "<false|true>"

  # Terraform variables
  terraform_version      = "<terraform_version>"
  terraform_distribution = "<terraform_distribution>"

  # VCS variables (if you have chosen an external VCS)
  vcs_provider                                = "<github|githubenterprise|gitlab|
gitlabselfmanaged|bitbucket>"
  account_request_repo_name                   = "<org-name>/aft-account-request"
  account_customizations_repo_name            = "<org-name>/aft-account-
customizations"
  account_provisioning_customizations_repo_name = "<org-name>/aft-account-provisioning-
customizations"
  global_customizations_repo_name             = "<org-name>/aft-global-
customizations"

}
```

Backend.tf

```
terraform {
  backend "s3" {
    region = "<aft-main-region>"
    bucket = "<s3-bucket-name>"
    key    = "aft-setup.tfstate"
  }
}
```

Wenn Sie den `Generate AFT Files` Parameter während der CodeCommit Repository-Erstellung auf setzen`true`, verwendet die Vorlage den S3-Bucket mit dem generierten Inhalt als Quelle für den `main` Branch, um das Repository automatisch zu füllen.

Die Pipeline ausführen

Nachdem die Ressourcen erstellt und die Bootstrap-Dateien konfiguriert wurden, wird die Pipeline ausgeführt. In der ersten Phase (Source) wird der Quellcode aus dem Hauptzweig des Repositorys abgerufen, und in der zweiten Phase (Build) wird der Befehl Terraform Plan ausgeführt und die zu überprüfenden Ergebnisse generiert. In der dritten Phase (Genehmigung) wartet die Pipeline auf eine

manuelle Aktion, um die letzte Phase (Deploy) zu genehmigen oder abzulehnen. In der letzten Phase führt die Pipeline den `apply` Terraform-Befehl aus, indem sie das Ergebnis des vorherigen `plan` Terraform-Befehls als Eingabe verwendet. Schließlich werden eine kontoübergreifende Rolle und die Berechtigungen im Verwaltungskonto verwendet, um die AFT-Ressourcen im AFT-Verwaltungskonto zu erstellen.

> **Note**
>
> Wenn Sie einen externen VCS-Anbieter auswählen, müssen Sie die Verbindung mit den Anmeldeinformationen Ihres VCS-Anbieters autorisieren. Um die Einrichtung abzuschließen, folgen Sie den Schritten unter Aktualisieren einer ausstehenden Verbindung in der Dokumentation zur AWS Developer Tools-Konsole.

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend AWS-Konten zu verwalten.
- AWS CodeBuildist ein vollständig verwalteter Build-Service, der Ihnen hilft, Quellcode zu kompilieren, Komponententests durchzuführen und Artefakte zu erstellen, die sofort einsatzbereit sind.
- AWS CodeCommitist ein Versionskontrolldienst, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS CodePipelinehilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.
- AWS CodeConnectionsermöglicht AWS Ressourcen und Dienste, z. B. CodePipeline die Verbindung zu externen Code-Repositorys wie GitHub.
- AWS Lambdaist ein Rechendienst, der Ihren Code als Reaktion auf Ereignisse ausführt und Rechenressourcen automatisch verwaltet. So können Sie schnell eine moderne, serverlose Anwendung für die Produktion erstellen.
- AWS SDK für Python (Boto3)ist ein Softwareentwicklungskit, mit dem Sie Ihre Python-Anwendung, -Bibliothek oder Ihr Skript integrieren können AWS-Services.

Andere Tools

- Terraform ist ein Infrastructure-as-Code-Tool (IaC), mit dem Sie Infrastrukturen sicher und effizient erstellen, ändern und versionieren können. Dazu gehören Komponenten auf niedriger Ebene wie Recheninstanzen, Speicher und Netzwerke sowie Komponenten auf hoher Ebene wie DNS-Einträge und SaaS-Funktionen.
- Python ist eine leicht zu erlernende, leistungsstarke Programmiersprache. Sie verfügt über effiziente Datenstrukturen auf hoher Ebene und bietet einen einfachen, aber effektiven Ansatz für objektorientierte Programmierung.

Code-Repository

Der Code für dieses Muster ist im GitHub AFT-Bootstrap-Pipeline-Repository verfügbar.

Das offizielle AFT-Repository finden Sie unter AWS Control Tower Account Factory for Terraform in. GitHub

Bewährte Methoden

Wenn Sie AFT mithilfe der bereitgestellten CloudFormation Vorlage bereitstellen, empfehlen wir Ihnen, bewährte Methoden zu befolgen, um eine sichere, effiziente und erfolgreiche Implementierung zu gewährleisten. Zu den wichtigsten Richtlinien und Empfehlungen für die Implementierung und den Betrieb des AFT gehören die folgenden.

- Gründliche Überprüfung der Parameter: Prüfen Sie jeden Parameter in der CloudFormation Vorlage sorgfältig und verstehen Sie ihn. Eine genaue Parameterkonfiguration ist entscheidend für die korrekte Einrichtung und Funktion von AFT.
- Regelmäßige Vorlagenaktualisierungen: Halten Sie die Vorlage mit den neuesten AWS Funktionen und Terraform-Versionen auf dem neuesten Stand. Regelmäßige Updates helfen Ihnen dabei, neue Funktionen zu nutzen und die Sicherheit zu gewährleisten.
- Versionierung: Legen Sie die Version Ihres AFT-Moduls fest und verwenden Sie, wenn möglich, eine separate AFT-Bereitstellung zum Testen.
- Umfang: Verwenden Sie AFT nur, um Infrastruktur-Leitplanken und Anpassungen bereitzustellen. Verwenden Sie es nicht, um Ihre Anwendung bereitzustellen.
- Linting und Validierung: Die AFT-Pipeline erfordert eine verknüpfte und validierte Terraform-Konfiguration. Führen Sie Lint, Validation und Test aus, bevor Sie die Konfiguration in die AFT-Repositorys übertragen.

- Terraform-Module: Erstellen Sie wiederverwendbaren Terraform-Code als Module und geben Sie immer die Terraform- und AWS Provider-Versionen an, die den Anforderungen Ihres Unternehmens entsprechen.

Epen

Richten Sie die Umgebung ein und konfigurieren Sie sie AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereite die AWS Control Tower Umgebung vor.	Richten Sie sie AWS Control Tower in Ihrer AWS Umgebung ein und konfiguri eren Sie sie, um eine zentrale Verwaltung und Steuerung für Sie zu gewährleisten AWS-Konten. Weitere Informationen finden Sie AWS Control Tower in der AWS Control Tower Dokumentation unter Erste Schritte mit.	Cloud-Administrator
Starten Sie das AFT-Verwa ltungskonto.	Verwenden Sie die AWS Control Tower Account Factory, um ein neues Konto AWS-Konto zu eröffnen, das als Ihr AFT-Verwaltungskon to dient. Weitere Informati onen finden Sie in der AWS Control Tower Dokumentation unter Konten mit AWS Service Catalog Account Factory bereitstellen.	Cloud-Administrator

Stellen Sie die CloudFormation Vorlage im Verwaltungskonto bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die CloudFormation Vorlage.	In diesem Epic stellen Sie die mit dieser Lösung bereitgestellte CloudFormation Vorlage bereit, um die AFT-Bootstrap-Pipeline in Ihrem AWS Verwaltungskonto einzurichten. Die Pipeline stellt die AFT-Lösung in dem AFT-Verwaltungskonto bereit, das Sie im vorherigen Epic eingerichtet haben. Schritt 1: Öffnen Sie die Konsole AWS CloudFormation • Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS CloudFormation Konsole. Vergewissern Sie sich, dass Sie in der richtigen AWS Control Tower Hauptregion tätig sind. Schritt 2: Erstellen Sie einen neuen Stack 1. Wählen Sie, ob Sie einen neuen Stapel erstellen möchten. 2. Wählen Sie die Option zum Hochladen einer Vorlagendatei und laden Sie die	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	CloudFormation Vorlage hoch, die mit diesem Muster bereitgestellt wurde. Schritt 3: Konfigurieren Sie die Stack-Parameter • `VCS Provider`: Wählen Sie den zu verwendenden Anbieter für das Versionsk ontrollsystem (VCS) aus. Sie können ein externes VCS auswählen GitHub, z. B. oder verwenden, CodeCommit wenn Ihr Konto den Dienst nutzen darf. • `Repository Name` : Geben Sie den Repository-Namen zum Speichern des AFT-Bootstrap-Moduls an. Verwenden Sie für externe VCS-Anbieter den vollständ igen Pfad, einschließlich des Organisationsnamens (z. B.`my-github-org/my-r epo`). • `Branch Name`: Geben Sie den Quell-Repository-Zweig an. • `CodeBuild Docker Image`: Wählen Sie die Datei aus, die als CodeBuild	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Docker-Basisimage verwendet werden soll.
	• Wenn Sie den VCS-Anbieter auf eine andere Option als einstellen CodeCommit, fahren Sie mit Schritt 8 fort.
	
	Schritt 4: Entscheiden Sie sich für die Dateigenerierung
	• Wenn Sie es CodeCommit als Ihren VCS-Anbieter ausgewählt haben, können Sie den `Generate AFT Files` Parameter verwenden, um die Generierung von AFT-Standardbereitstellungsdateien zu steuern. Stellen Sie diesen Parameter wie folgt ein:
	  • `true`um automatisch AFT-Bereitstellungsdateien im angegebenen Repository zu erstellen und zu speichern.
	  • `false`wenn Sie die Dateierstellung manuell durchführen möchten oder die Dateien bereits vorhanden sind.
	• Wenn Sie ausgewählt haben`false`, fahren Sie mit Schritt 8 fort. Andernfal	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	ls führen Sie zuerst die Schritte 5—7 aus.
	
	Schritt 5: Füllen Sie die AWS Control Tower AFT-Konto informationen aus
	
	• Wenn Sie den `Generate AFT Files` Parameter auf einstellen`true`, geben Sie die folgenden AWS Control Tower und die kontospez ifischen AFT-Informationen ein.
	  • `Log Archive Account ID`: Die ID der Log Archive-Konto-ID in. AWS Control Tower
	  • `Audit Account ID`: Die ID des Audit-Kontos in AWS Control Tower.
	  • `AFT Management Account ID`: Die ID des AFT-Verwaltungskontos, das Sie im ersten Epic erstellt haben.
	  • `AFT Main Region`und`AFT Secondary Region`: Der Haupt- und der Sekundärcode AWS-Regionen für den AFT-Einsatz.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Schritt 6: AFT-Optionen konfigurieren
	• Richten Sie die Berichter stattung über Metriken ein:
	  • `AFT Enable Metrics Reporting` : Aktiviert oder deaktiviert die Berichterstattung über AFT-Metriken. Weitere Informationen finden Sie in der AWS Control Tower Dokumentation unter Betriebskennzahlen.
	• Legen Sie die AFT-Funkt ionsoptionen fest:
	  • `Enable AFT CloudTrail Data Events`: Aktiviert CloudTrail Datenerei gnisse in allen von AFT verwalteten Konten. Weitere Informationen finden Sie in der AWS Control Tower Dokumenta tion unter AWS CloudTrail Datenereignisse.
	  • `Enable AFT Enterprise Support` : Aktivieren Sie Enterpris e Support in allen von AFT verwalteten Konten. Weitere Informationen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	finden Sie in der AWS Control Tower Dokumentation unter AWS Enterprise Support Plan. • `Enable AFT Delete Default VPC`: Löscht alles nur VPCs im AFT-Verwaltungskonto. Weitere Informationen finden Sie in der AWS Control Tower Dokumentation unter Löschen der AWS Standard-VPC. Schritt 7: Versionen angeben • `AFT Terraform Version`: Wählen Sie die Version von Terraform aus, die in AFT-Pipelines verwendet werden soll. • `AFT Version`: Definieren Sie die AFT-Version für die Bereitstellung. Behalten Sie die Standardeinstellung (`latest`) bei, um die aktuellste AFT-Version zu verwenden. Schritt 8: Überprüfen und erstellen Sie den Stapel • Überprüfen Sie alle Parameter und Einstellu	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ngen. Wenn alles in Ordnung ist, fahren Sie mit der Erstellung des Stacks fort. Schritt 9: Überwachen Sie die Stack-Erstellung • AWS CloudFormation stellt die von Ihnen definierten Ressourcen bereit und konfiguriert sie. Überwache n Sie den Prozess der Stack-Erstellung auf der CloudFormation Konsole. Dieser Vorgang kann mehrere Minuten dauern. Schritt 10: Überprüfen Sie die Bereitstellung • Wenn der Stack-Status CREATE_COMPLETE anzeigt, stellen Sie sicher, dass alle Ressourcen korrekt erstellt wurden. • Notieren Sie sich den Wert im Abschnitt Ausgaben. `TerraformBackendBu cketName`	

Füllen und validieren Sie das AFT-Bootstrap-Repository und die Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 1: Füllen Sie das AFT-Bootstrap-Repository für ein externes VCS auf.	Wenn Sie den VCS-Anbieter auf ein externes VCS (nicht auf CodeCommit) einstellen, gehen Sie wie folgt vor. (Optional) Nachdem Sie die CloudFormation Vorlage bereitgestellt haben, können Sie den Inhalt im neu erstellte n AFT-Bootstrap-Repository auffüllen oder überprüfen und testen, ob die Pipeline erfolgreich ausgeführt wurde. Schritt 1: Aktualisieren Sie die Verbindung 1. Wählen Sie auf der CodePipeline Konsole im Navigationsbereich Einstellungen, Verbindun gen aus. 2. Wählen Sie die `aft-vcs-connection` Verbindun g aus. Sie sollte sich im `Pending` Status befinden. 3. Wählen Sie Ausstehen de Verbindung aktualisi eren und folgen Sie den Anweisungen unter Ausstehende Verbindun g aktualisieren in der	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Dokumentation zur Developer Tools-Konsole.
	4. Wenn sich die Verbindung im `Available` Status befindet, fahren Sie mit dem nächsten Schritt fort.
	
	Schritt 2: Füllen Sie das Repository
	
	1. Verwenden Sie Ihre externen VCS-Anmeldeinformationen, um das Repository, das Sie in der Vorlage angegeben haben, auf Ihren lokalen Computer zu klonen. Wenn Sie den Standardnamen beibehalten haben, wird das Repository aufgerufen`aft-setup` .
	2. Erstellen Sie im Repository einen Ordner namens`terraform` , der zwei leere Dateien enthält: `backend.tf` und`main.tf`.
	3. Öffnen Sie die `backend.tf` Datei und fügen Sie diesen Codeausschnitt hinzu:
	
	`terraform {`
	`  backend "s3" {`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> region = "<aft-main-region>"
	    bucket = "<s3-bucket-name>"
	    key = "aft-setup"
	  }
	}</pre>
	In der Datei:
	• `<aft-main-region>`Durch die AFT-Hauptregion ersetzen. Dies sollte mit der AWS Control Tower Hauptregion übereinstimmen.
	• `<s3-bucket-name>`Ersetzen Sie es durch den Namen des Terraform-Backend-Buckets. Sie finden dies in der `Terraform BackendBucketName` Ausgabe, die mit der zuvor bereitgestellten CloudFormation Vorlage generiert wurde.
	4. Öffnen Sie die `main.tf` Datei und verwenden Sie eines der im AFT-Repository verfügbaren Beispiele, um AFT bereitzustellen. Sie können beispielsweise mit Ihrem bevorzugten VCS-Anbie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ter (CodeCommit, GitHub, oder Bitbucket) zusammena rbeiten oder die AFT-VPC anpassen. Weitere AFT-Eingabeoptionen finden Sie in der README-Datei im AFT-Repository. Schritt 2: Bestätigen Sie Ihre Änderungen und übertragen Sie sie • Nachdem Sie den Ordner und die Dateien erstellt und gefüllt haben, bestätige n Sie Ihre Änderungen und laden Sie den Code in das Repository hoch. Die Pipeline wird automatisch gestartet, durchläuft die Phasen Source und Build und wartet dann vor der Bereitstellungsphase auf eine Genehmigungsaktion.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Option 2: Füllen Sie das AFT-Bootstrap-Repository für aus. CodeCommit	Wenn Sie den VCS-Anbieter auf einstellen CodeCommit, gehen Sie wie folgt vor. (Optional) Nachdem Sie die CloudFormation Vorlage bereitgestellt haben, können Sie den Inhalt im neu erstellte n AFT-Bootstrap-Repository auffüllen oder überprüfen und testen, ob die Pipeline erfolgreich ausgeführt wurde. Wenn Sie den `Generate AFT Files` Parameter auf setzen`true`, fahren Sie mit dem nächsten Artikel fort (Validierung der Pipeline). Schritt 1: Füllen Sie das Repository 1. Öffnen Sie die AWS CodeCommit Konsole und wählen Sie das neu erstellte Repository aus. Wenn Sie den Standardn amen beibehalten haben, sollte der Repository-Name laute`aft-setup` . 2. Klonen Sie das Repositor y mithilfe von SSH, HTTPS oder HTTPS (GRC) auf Ihren lokalen Computer und öffnen Sie es in einem Editor.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Erstellen Sie einen Ordner mit dem Namen `terraform` und zwei leere Dateien darin: `backend.tf` und. `main.tf` 4. Öffnen Sie die `backend.tf` Datei und fügen Sie diesen Codeausschnitt hinzu: `terraform { backend "s3" { region = "<aft-main-region>" bucket = "<s3-bucket-name>" key = "aft-setup" } }` In der Datei: • `<aft-main-region>`Durch die AFT-Hauptregion ersetzen. Dies sollte mit der AWS Control Tower Hauptregion übereinstimmen. • `<s3-bucket-name>`Ersetzen Sie es durch den Namen des Terraform-Backend-Buckets. Sie finden dies in der `Terraform BackendBucketName`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ausgabe, die mit der zuvor bereitgestellten CloudFormation Vorlage generiert wurde. 5. Öffnen Sie die `main.tf` Datei und verwenden Sie eines der im AFT-Repository verfügbaren Beispiele, um AFT bereitzustellen. Sie können beispielsweise mit Ihrem bevorzugten Anbieter für Versionskontrollsysteme (VCS) (CodeCommit, GitHub, oder Bitbucket) arbeiten oder die AFT-VPC anpassen. Weitere AFT-Eingabeoptionen finden Sie in der README-Datei im AFT-Repository. Schritt 2: Bestätigen Sie Ihre Änderungen und übertragen Sie sie • Nachdem Sie den Ordner und die Dateien erstellt und gefüllt haben, bestätigen Sie Ihre Änderungen und laden Sie den Code in das Repository hoch. Die Pipeline wird automatisch gestartet, durchläuft die Phasen Source und Build und wartet dann vor der	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bereitstellungsphase auf eine Genehmigungsaktion.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die AFT-Bootstrap-Pipeline.	Schritt 1: Sehen Sie sich die Pipeline an • Öffnen Sie die CodePipeline Konsole und überprüfen Sie, ob die `aft-bootstrap-pipeline` Pipeline erfolgreich gestartet wurde. Es sollte einen Terraform -Plan ausführen oder auf eine manuelle Genehmigungsaktion warten. Schritt 2: Genehmigen Sie die Ergebnisse des Terraform-Plans • Sie können die Ergebnisse des Terraform-Plans überprüfen, indem Sie sich die Ausführungsprotokolle der Build-Phase ansehen und dann die Ausführung in der Genehmigungsphase genehmigen oder ablehnen. Wenn Sie zustimmen, beginnt die Pipeline mit der Bereitstellung von AFT-Ressourcen im bereitgestellten AFT-Verwaltungskonto. Schritt 3: Warten Sie auf die Bereitstellung	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Warten Sie, bis die Pipeline erfolgreich ausgeführt wurde. Dies sollte etwa 30 Minuten dauern. Alle Fehler, auf die Sie stoßen könnten, werden häufig durch API-Kontingente verursacht. In diesen Fällen können Sie die Pipeline erneut ausführen, um die Bereitstellung fortzusetzen. Schritt 4: Überprüfen Sie die erstellten Ressourcen • Greifen Sie auf das AFT-Verwaltungskonto zu und vergewissern Sie sich, dass die Ressourcen erstellt wurden.	

Fehlerbehebung

Problem	Lösung
Die in der CloudFormation Vorlage enthaltene benutzerdefinierte Lambda-Funktion schlägt während der Bereitstellung fehl.	Suchen Sie in den CloudWatch Amazon-Protokollen nach der Lambda-Funktion, um den Fehler zu identifizieren. Die Protokolle enthalten detaillierte Informationen und können helfen, das spezifische Problem zu lokalisieren. Vergewissern Sie sich, dass die Lambda-Funktion über die erforderlichen Berechtigungen verfügt und dass die Umgebungsvariablen korrekt festgelegt wurden.

Problem	Lösung
Sie stoßen auf Fehler bei der Erstellung oder Verwaltung von Ressourcen, die auf unzureich ende Berechtigungen zurückzuführen sind.	Überprüfen Sie die IAM-Rollen und -Richtlin ien, die mit der Lambda-Funktion verknüpft sind CodeBuild, und andere an der Bereitstellung beteiligte Dienste. Vergewissern Sie sich, dass sie über die erforderlichen Berechtigungen verfügen. Wenn es Probleme mit den Berechtig ungen gibt, passen Sie die IAM-Richtlinien an, um den erforderlichen Zugriff zu gewähren.
Sie verwenden eine veraltete Version der CloudFormation Vorlage mit neueren AWS-Services oder Terraform-Versionen.	Aktualisieren Sie die CloudFormation Vorlage regelmäßig, damit sie mit den neuesten Versionen AWS und Terraform-Versionen kompatibel ist. In den Versionshinweisen oder der Dokumentation finden Sie alle versionss pezifischen Änderungen oder Anforderungen.
Während der Bereitstellung erreichen Sie die AWS-Service Kontingente.	Bevor Sie die Pipeline bereitstellen, überprüfe n Sie die AWS-Service Kontingente für Ressourcen wie S3-Buckets, IAM-Rollen und Lambda-Funktionen. Die Anfrage wird bei Bedarf erhöht. Weitere Informationen finden Sie auf der AWS Website unter AWS-Service Kontingente.
Aufgrund falscher Eingabeparameter in der CloudFormation Vorlage treten Fehler auf.	Überprüfen Sie alle Eingabeparameter noch einmal auf Tippfehler oder falsche Werte. Vergewissern Sie sich, dass Ressourcen-Identif ikatoren wie Konto IDs - und Regionsnamen korrekt sind.

Zugehörige Ressourcen

Sehen Sie sich die folgenden Ressourcen an, um dieses Muster erfolgreich zu implementieren. Diese Ressourcen bieten zusätzliche Informationen und Anleitungen, die bei der Einrichtung und Verwaltung von AFT mit Hilfe AWS CloudFormation von unschätzbarem Wert sein können.

AWSDokumentation:

- AWS Control Tower Das Benutzerhandbuch bietet detaillierte Informationen zur Einrichtung und Verwaltung AWS Control Tower.
- AWS CloudFormation Die Dokumentation bietet Einblicke in CloudFormation Vorlagen, Stacks und Ressourcenmanagement.

IAM-Richtlinien und bewährte Verfahren:

- Bewährte Sicherheitsmethoden in IAM erläutern, wie Sie mithilfe von IAM-Rollen und -Richtlinien zur Sicherung von AWS Ressourcen beitragen können.

Terraform auf: AWS

- Die Terraform AWS Provider-Dokumentation enthält umfassende Informationen zur Verwendung von Terraform mit. AWS

AWS-Service Kontingente:

- AWS-Service Kontingente enthält Informationen darüber, wie Sie AWS-Service Kontingente einsehen und Erhöhungen beantragen können.

AWS Service Catalog-Produkte in mehreren AWS-Konten und AWS-Regionen verwalten

Erstellt von Ram Kandaswamy (AWS)

Übersicht

Der Amazon Web Services (AWS) Service Catalog vereinfacht und beschleunigt die Verwaltung und Verteilung von Infrastructure as Code (IaC) -Vorlagen für Unternehmen. Sie verwenden CloudFormation AWS-Vorlagen, um eine Sammlung von AWS-Ressourcen (Stacks) zu definieren, die für ein Produkt erforderlich sind. AWS CloudFormation StackSets erweitert diese Funktionalität, indem es Ihnen ermöglicht, Stacks für mehrere Konten und AWS-Regionen mit einem einzigen Vorgang zu erstellen, zu aktualisieren oder zu löschen.

AWS Service Catalog-Administratoren erstellen Produkte mithilfe von CloudFormation Vorlagen, die von Entwicklern verfasst wurden, und veröffentlichen sie. Diese Produkte werden dann einem Portfolio zugeordnet, und es gelten Einschränkungen für die Unternehmensführung. Um Ihre Produkte Benutzern in anderen AWS-Konten oder Organisationseinheiten (OUs) zur Verfügung zu stellen, teilen Sie in der Regel Ihr Portfolio mit ihnen. Dieses Muster beschreibt einen alternativen Ansatz für die Verwaltung von AWS Service Catalog-Produktangeboten, der auf AWS basiert CloudFormation StackSets. Anstatt Portfolios gemeinsam zu nutzen, verwenden Sie Stack-Set-Einschränkungen, um AWS-Regionen und Konten festzulegen, in denen Ihr Produkt bereitgestellt und verwendet werden kann. Mit diesem Ansatz können Sie Ihre AWS Service Catalog-Produkte in mehreren Konten und AWS-Regionen bereitstellen und sie von einem zentralen Standort aus verwalten, während Sie gleichzeitig Ihre Governance-Anforderungen erfüllen. OUs

Vorteile dieses Ansatzes:

- Das Produkt wird über das Hauptkonto bereitgestellt und verwaltet und nicht mit anderen Konten geteilt.
- Dieser Ansatz bietet eine konsolidierte Ansicht aller bereitgestellten Produkte (Stacks), die auf einem bestimmten Produkt basieren.
- Die Konfiguration mit dem AWS Service Management Connector ist einfacher, da sie nur auf ein Konto abzielt.
- Es ist einfacher, Produkte aus dem AWS Service Catalog abzufragen und zu verwenden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- CloudFormation AWS-Vorlagen für IaC und Versionierung
- Einrichtung mehrerer Konten und AWS Service Catalog für die Bereitstellung und Verwaltung von AWS-Ressourcen

Einschränkungen

- Bei diesem Ansatz wird AWS verwendet CloudFormation StackSets, und es StackSets gelten die folgenden Einschränkungen:
  - StackSets unterstützt die Bereitstellung von CloudFormation Vorlagen über Makros nicht. Wenn Sie ein Makro zur Vorverarbeitung der Vorlage verwenden, können Sie keine StackSets basierte Bereitstellung verwenden.
  - StackSets bietet die Möglichkeit, einen Stack vom Stack-Set zu trennen, sodass Sie einen bestimmten Stack als Ziel auswählen können, um ein Problem zu beheben. Ein getrennter Stapel kann jedoch nicht erneut mit dem Stack-Set verknüpft werden.
- AWS Service Catalog generiert automatisch StackSet Namen. Die Anpassung wird derzeit nicht unterstützt.

Architektur

Zielarchitektur

1. Der Benutzer erstellt eine CloudFormation AWS-Vorlage zur Bereitstellung von AWS-Ressourcen im JSON- oder YAML-Format.
2. Die CloudFormation Vorlage erstellt ein Produkt im AWS Service Catalog, das einem Portfolio hinzugefügt wird.
3. Der Benutzer erstellt ein bereitgestelltes Produkt, das CloudFormation Stapel in den Zielkonten erstellt.
4. Jeder Stapel stellt die in den Vorlagen angegebenen Ressourcen bereit. CloudFormation

Tools

AWS-Services

- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Mit AWS Service Catalog können Sie Kataloge von IT-Services, die für AWS zugelassen sind, zentral verwalten. Endbenutzer können schnell nur die jeweils benötigten genehmigten IT-Services bereitstellen, wobei die Einschränkungen Ihrer Organisation berücksichtigt werden.

Epen

Stellen Sie Produkte kontenübergreifend bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Portfolio.	Ein Portfolio ist ein Container, der ein oder mehrere Produkte enthält, die nach bestimmte n Kriterien gruppiert sind. Die Verwendung eines Portfolio s für Ihre Produkte hilft Ihnen dabei, allgemeine Einschrän kungen für Ihr gesamtes Produktsortiment anzuwende n. Um ein Portfolio zu erstellen, folgen Sie den Anweisungen in der AWS-Servicekatalog-Dokumentation. Wenn Sie die	AWS Service Catalog, IAM

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	AWS-CLI verwenden, finden Sie hier einen Beispielbefehl: `aws servicecatalog create-portfolio --provider-name my-provider --display-name my-portfolio` Weitere Informationen finden Sie in der AWS-CLI-Dokumentation.	
Erstellen Sie eine CloudFormation Vorlage.	Erstellen Sie eine CloudFormation Vorlage, die die Ressourcen beschreibt. Die Eigenschaftswerte von Ressourcen sollten gegebenenfalls parametrisiert werden.	AWS CloudFormation, JSON/YAML

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Produkt mit Versionsinformationen.	Die CloudFormation Vorlage wird zu einem Produkt, wenn Sie sie im AWS Service Catalog veröffentlichen. Geben Sie Werte für die optionalen Versionsdetailparameter an, z. B. den Versionstitel und die Beschreibung. Dies ist hilfreich, wenn Sie später nach dem Produkt suchen möchten. Um ein Produkt zu erstellen, folgen Sie den Anweisungen in der AWS-Servicekatalog-Dokumentation. Wenn Sie die AWS-CLI verwenden, lautet ein Beispielbefehl: `aws servicecatalog create-product --cli-input-json file://create-product-input.json` wo `create-product-input.json` ist die Datei, die die Parameter für das Produkt übergibt. Ein Beispiel für diese Datei finden Sie im Abschnitt Zusätzliche Informationen. Weitere Informationen finden Sie in der AWS-CLI-Dokumentation.	AWS Service Catalog

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wenden Sie Einschränkungen an.	Wenden Sie Stack-Set-Einschränkungen auf das Portfolio an, um Produktbereitstellungsoptionen wie mehrere AWS-Konten, Regionen und Berechtigungen zu konfigurieren. Anweisungen finden Sie in der Dokumentation zum AWS Service Catalog.	AWS Service Catalog
Fügen Sie -Berechtigungen hinzu.	Stellen Sie Benutzern Berechtigungen zur Verfügung, damit sie die Produkte im Portfolio auf den Markt bringen können. Anweisungen für die Konsole finden Sie in der Dokumentation zum AWS Service Catalog. Wenn Sie die AWS-CLI verwenden, finden Sie hier einen Beispielbefehl: `aws servicecatalog associate-principal-with-portfolio \ --portfolio-id port-2s6abcdefwdh4 \ --principal-arn arn:aws:iam::444455556666:role/Admin \ --principal-type IAM` Weitere Informationen finden Sie in der AWS-CLI-Dokumentation.	AWS Service Catalog, IAM

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie das Produkt bereit.	Ein bereitgestelltes Produkt ist eine mit Ressourcen ausgestattete Instance eines Produkts. Durch die Bereitstellung eines Produkts auf der Grundlage einer CloudFormation Vorlage werden ein CloudFormation Stack und die zugrunde liegenden Ressourcen gestartet. Stellen Sie das Produkt bereit, indem Sie die entsprechenden AWS-Regionen und -Konten auf der Grundlage von Stack-Set-Einschränkungen ansprechen. In der AWS-CLI ist hier ein Beispielbefehl: `aws servicecatalog provision-product \ --product-id prod-abcdfz3syn2rg \ --provisioning-artifact-id pa-abc347pcsccfm \ --provisioned-product-name "mytestppname3"` Weitere Informationen finden Sie in der AWS-CLI-Dokumentation.	AWS Service Catalog

Zugehörige Ressourcen

Referenzen

- Überblick über den AWS Service Catalog
- Verwenden von AWS CloudFormation StackSets

Tutorials und Videos

- AWS re:Invent 2019: Alles automatisieren: Optionen und bewährte Methoden (Video)

Zusätzliche Informationen

Wenn Sie den `create-product` Befehl verwenden, verweist der `cli-input-json` Parameter auf eine Datei, die Informationen wie den Produkteigentümer, die Support-E-Mail-Adresse und CloudFormation Vorlagendetails enthält. Hier ist ein Beispiel für eine solche Datei:

```
{
   "Owner": "Test admin",
      "SupportDescription": "Testing",
         "Name": "SNS",
            "SupportEmail": "example@example.com",
            "ProductType": "CLOUD_FORMATION_TEMPLATE",
               "AcceptLanguage": "en",
                  "ProvisioningArtifactParameters": {
                     "Description": "SNS product",
                        "DisableTemplateValidation": true,
                           "Info": {
                              "LoadTemplateFromURL": "<url>"
                     },
                           "Name": "version 1"
}
```

Migrieren Sie ein AWS-Mitgliedskonto von AWS Organizations zu AWS Control Tower

Erstellt von Rodolfo Jr. Cerrada (AWS)

Übersicht

Dieses Muster beschreibt, wie ein Amazon Web Services (AWS) -Konto von AWS Organizations, wo es sich um ein Mitgliedskonto handelt, das von einem Verwaltungskonto verwaltet wird, zu AWS Control Tower migriert wird. Wenn Sie das Konto bei AWS Control Tower registrieren, können Sie präventive und detektive Schutzmaßnahmen und Funktionen nutzen, die Ihre Kontoverwaltung optimieren. Möglicherweise möchten Sie auch Ihr Mitgliedskonto migrieren, wenn Ihr Verwaltungskonto bei AWS Organizations kompromittiert wurde und Sie Mitgliedskonten in eine neue Organisation verschieben möchten, die von AWS Control Tower verwaltet wird.

AWS Control Tower bietet ein Framework, das die Funktionen mehrerer anderer AWS-Services, einschließlich AWS Organizations, kombiniert und integriert und für konsistente Compliance und Governance in Ihrer Umgebung mit mehreren Konten sorgt. Mit AWS Control Tower können Sie eine Reihe von vorgeschriebenen Regeln und Definitionen befolgen, die die Funktionen von AWS Organizations erweitern. Sie können beispielsweise mithilfe von Guardrails sicherstellen, dass Sicherheitsprotokolle und die erforderlichen kontoübergreifenden Zugriffsberechtigungen erstellt und nicht verändert werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Einrichtung von AWS Control Tower in Ihrer Zielorganisation in AWS Organizations (Anweisungen finden Sie unter Einrichtung in der AWS Control Tower Tower-Dokumentation)
- Administratoranmeldedaten für AWS Control Tower (Mitglied der AWSControlTowerAdminsGruppe)
- Administratoranmeldedaten für das AWS-Quellkonto

Einschränkungen

- Das Quellverwaltungskonto in AWS Organizations muss sich vom Zielverwaltungskonto in AWS Control Tower unterscheiden.

Produktversionen

- AWS Control Tower Version 2.3 (Februar 2020) oder höher (siehe Versionshinweise)

Architektur

Das folgende Diagramm veranschaulicht den Migrationsprozess und die Referenzarchitektur. Dieses Muster migriert das AWS-Konto von der Quellorganisation zu einer Zielorganisation, die von AWS Control Tower verwaltet wird.

Der Registrierungsprozess besteht aus den folgenden Schritten:

1. Das Konto verlässt die Quellorganisation in AWS Organizations.
2. Das Konto wird zu einem eigenständigen Konto. Das bedeutet, dass es keiner Organisation gehört, sodass Verwaltung und Abrechnung unabhängig von den Kontoadministratoren verwaltet werden.
3. Die Zielorganisation sendet eine Einladung für das Konto, der Organisation beizutreten.
4. Das eigenständige Konto akzeptiert die Einladung und wird Mitglied der Zielorganisation.
5. Das Konto ist bei AWS Control Tower registriert und in eine registrierte Organisationseinheit (OU) verschoben. (Wir empfehlen, dass Sie das AWS Control Tower Tower-Dashboard überprüfen, um die Registrierung zu bestätigen.) Zu diesem Zeitpunkt werden alle Guardrails wirksam, die in der registrierten Organisationseinheit aktiviert sind.

Tools

AWS-Services

- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer einzigen Einheit (einer Organisation) konsolidieren können, die Sie erstellen und zentral verwalten.
- AWS Control Tower integriert die Funktionen anderer Services, darunter AWS Organizations, AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) und AWS Service Catalog, um Sie bei der Durchsetzung und Verwaltung von Governance-Regeln für Sicherheit, Betrieb und Compliance in all Ihren Organisationen und Konten in der AWS-Cloud zu unterstützen.

Epen

Entfernen Sie das Mitgliedskonto aus der Quellorganisation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass das Mitgliedskonto als eigenstän diges Konto ausgeführt werden kann.	Vergewissern Sie sich, dass das Mitgliedskonto, das die Quellorganisation verlässt, über die Informationen verfügt, die erforderlich sind, damit es als eigenständiges Konto betrieben werden kann. Wenn das Mitgliedskonto beispiels weise keine Rechnungs informationen enthält, kann es nicht als eigenständiges Konto betrieben werden, da AWS die Zahlungsinformationen verwendet, um alle abrechnun gsfähigen AWS-Aktivitäten abzubuchen, die stattfinden, während das Konto keiner Organisation zugeordnet ist. Wenn Sie das Mitgliedskonto mithilfe der AWS Organizat ions Organizations-Konsole, der API oder der AWS-Befeh lszeilenschnittstelle (CLI) erstellt haben, werden die für eigenständige Konten erforderlichen Informationen in der Regel nicht automatis ch erfasst. Um diese Informati onen hinzuzufügen, melden Sie sich bei dem Konto an und	Kontoadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	geben Sie einen Supportplan, Kontaktinformationen und eine Zahlungsmethode an. Weitere Informationen dazu, was Sie wissen müssen, bevor Sie ein Konto aus einer Organisation entfernen, finden Sie unter Bevor Sie ein Konto aus einer Organisation entfernen in der Dokumentation zu AWS Organizations.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie das Mitglieds konto aus seiner Quellorga nisation.	Folgen Sie den Anweisung en in der Dokumentation zu AWS Organizations, um ein Mitgliedskonto aus einer Organisation zu entfernen. Sie können sich beim Verwaltun gskonto der Organisation anmelden und das Mitglieds konto entfernen, oder Sie können sich mit dem Mitglieds konto anmelden und die Organisation verlassen. Wenn Sie nicht über Administr atoranmeldeinformationen verfügen, um das Konto zu entfernen oder zu verlassen , bitten Sie den Administr ator Ihrer Organisation um Unterstützung. Wenn für das Mitgliedskonto ein Supportplan, Kontaktin formationen oder Zahlungsi nformationen fehlen, werden Sie aufgefordert, diese Informationen anzugeben und zu überprüfen. Wenn Sie die Organisation verlassen, werden Sie auf die Seite Erste Schritte der AWS Organizations Organizations-Konsole weitergeleitet, auf der Sie Einladungen für Ihr	Administrator des Verwaltun gskontos oder Kontoadmi nistrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Konto zum Beitritt zu anderen Organisationen einsehen können. **Important** Zu diesem Zeitpunkt ist Ihr Konto ein eigenständiges Konto. Wenn Sie Workloads ausführen , die nicht durch das kostenlose AWS-Kontingent abgedeckt sind, werden Ihnen die Zahlungs- und Rechnungsinformati onen in Rechnung gestellt, die Sie für das Konto angegeben haben.	
Stellen Sie sicher, dass das Mitgliedskonto nicht mehr Teil der Quellorganisation ist.	In der Konsole von AWS Organizations sollte die Schaltfläche Organisat ion verlassen nicht mehr angezeigt werden. Stattdess en sollten Sie eventuell ausstehende Einladungen von anderen Organisationen sehen.	Kontoadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die IAM-Rollen, die Zugriff auf Ihr Konto gewähren, aus der Organisation, die Sie verlassen haben.	Wenn Sie das Konto aus der Quellorganisation entfernen, werden die von AWS Organizations oder von Administratoren erstellten AWS Identity and Access Management (IAM) -Rollen nicht automatisch gelöscht. Um den Zugriff über das Verwaltungskonto der Quellorganisation zu beenden, müssen Sie die IAM-Rollen manuell löschen. Weitere Informationen finden Sie in der IAM-Dokumentation unter Löschen von Rollen oder Instanzprofilen. Wenn ein Mitgliedskonto eine Organisation verlässt, werden alle dem Konto zugewiesenen Stichwörter gelöscht. Eigenständige Konten unterstützen keine Stichwörter.	Kontoadministrator

Laden Sie das Konto ein, der neuen Organisation mit AWS Control Tower beizutreten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie sich bei AWS Control Tower an.	Melden Sie sich als Administrator bei der AWS Control Tower Tower-Konsole an.	AWS Control Tower Tower-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Derzeit gibt es keine direkte Möglichkeit, ein AWS-Konto von einer Quellorganisation zu einer Organisation in einer Organisationseinheit zu verschieben, die von AWS Control Tower verwaltet wird. Sie können AWS Control Tower Governance jedoch auf ein bestehendes AWS-Konto ausweiten, wenn Sie es in einer Organisationseinhe it registrieren, die bereits von AWS Control Tower verwaltet wird. Aus diesem Grund müssen Sie sich für diesen Schritt bei AWS Control Tower anmelden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das Mitgliedskonto ein.	1. Melden Sie sich bei der AWS Organizations Organizations-Konsole an und navigieren Sie zur Seite AWS-Konten. 2. Wählen Sie auf der Seite AWS-Konto hinzufügen die Option Bestehendes AWS-Konto einladen aus. 3. Vervollständigen Sie die Kontoinformationen , einschließlich der 12-stelligen Kontonummer (ohne Bindestriche) und der optionalen Beschreibung und der Tags, und wählen Sie dann Einladung senden aus. ⚠ Important Vergewissern Sie sich, dass die Kontoüber tragung keine Auswirkungen auf Anwendungen oder Netzwerkverbindung en hat. Diese Aktion sendet eine Einladungs-E-Mail mit einem Link zum Mitgliedskonto. Wenn der Kontoadministrator	AWS Control Tower Tower-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dem Link folgt und die Einladung annimmt, wird das Mitgliedskonto auf der AWS-Kontoseite angezeigt. Weitere Informationen finden Sie unter Einladen eines AWS-Kontos zum Beitritt zu Ihrer Organisation in der Dokumentation zu AWS Organizations.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie Anwendungen und Konnektivität.	Wenn das Mitgliedskonto in der neuen Organisation registriert wurde, wird es in der Organisationseinheit als Stammkonto angezeigt . Es wird auch in der AWS Control Tower Tower-Kon sole angezeigt und als nicht in Konten registriert gekennzei chnet, da es noch nicht in der registrierten AWS Control Tower Tower-Organisation seinheit registriert wurde. Überprüfen Sie Folgendes: • Prüfen Sie im AWS Control Tower Tower-Dashboard, ob Verstöße gegen die Leitplanken vorliegen. • Überprüfen Sie die Netzwerkkonnektivität (VPN oder AWS Direct Connect), um sicherzustellen, dass sie durch die Übertragung nicht beeinträchtigt wurde. • (Anwendungsbesitzer) Testen Sie die Anwendung en, die diesem Konto zugeordnet sind, um sicherzustellen, dass sie erwartungsgemäß ausgeführt werden und dass die Abhängigkeiten durch	AWS Control Tower Tower-Administrator, Administr ator des Mitgliedskontos, Anwendungsbesitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Kontoübertragung nicht beeinträchtigt wurden.	

Bereiten Sie das Konto für die Registrierung vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfe die Leitplanken und behebt etwaige Verstöße.	Überprüfen Sie die in der Ziel-OU definierten Leitplanken, insbesondere die präventiven Leitplanken, und korrigieren Sie etwaige Verstöße. Eine Reihe von obligatorischen, präventiven Schutzmaßnahmen sind standardmäßig aktiviert, wenn Sie Ihre AWS Control Tower Tower-Landezone einrichten. Diese können nicht deaktiviert werden. Sie müssen diese obligatorischen Schutzmaßnahmen überprüfen und das Mitgliedskonto korrigieren (manuell oder mithilfe eines Skripts), bevor Sie das Konto registrieren. **Note** Präventive Schutzmaßnahmen sorgen dafür, dass registrierte AWS Control Tower Tower-Konten konform	AWS Control Tower Tower-Administrator, Administrator des Mitgliedskontos

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bleiben und Richtlini enverstöße verhindert werden. Jeder Verstoß gegen die präventiven Richtlinien kann sich auf die Registrierung auswirken. Detective Guardrail-Verstöße werden nach erfolgrei cher Registrierung im AWS Control Tower Tower-Dashboard angezeigt, sofern sie erkannt werden. Sie haben keinen Einfluss auf den Registrie rungsprozess. Weitere Informationen finden Sie unter Guardrails in AWS Control Tower in der AWS-Dokum entation.	
Prüfen Sie, ob Verbindun gsprobleme vorliegen, nachdem Sie Verstöße gegen die Leitplanken behoben haben.	In einigen Fällen müssen Sie möglicherweise bestimmte Ports schließen oder Dienste deaktivieren, um Verstöße gegen die Leitplanken zu beheben. Stellen Sie sicher, dass Anwendungen, die diese Ports und Dienste verwenden , repariert wurden, bevor Sie das Konto registrieren.	Besitzer der Anwendung

Registrieren Sie das Konto bei AWS Control Tower

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie sich bei der AWS Control Tower Tower-Konsole an.	Verwenden Sie Anmeldeinformationen mit Administratorberechtigungen für AWS Control Tower. Verwenden Sie nicht die Root-Benutzeranmeldeinformationen (Verwaltungskonto), um ein AWS Organizations Organizations-Konto zu registrieren. Daraufhin wird eine Fehlermeldung angezeigt.	AWS Control Tower Tower-Administrator
Registrieren Sie das Konto.	1. Wählen Sie auf der Seite Account Factory in AWS Control Tower die Option Konto registrieren aus. 2. Geben Sie die Details ein, einschließlich der E-Mail-Adresse, die mit dem Konto verknüpft ist, das Sie registrieren möchten, des Anzeigenamens, der in AWS Control Tower angezeigt wird, der E-Mail-Adresse des IAM Identity Center, des Vor- und Nachnamens des Kontoinhabers und der Organisationseinheit, in der Sie das Konto registrieren möchten. Die IAM Identity Center-E-Mail-Adresse ist Ihre bevorzugte	AWS Control Tower Tower-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Benutzer-E-Mail-Adresse. Sie können dieselbe E-Mail-Adresse wie die Konto-E-Mail verwenden. 3. Wählen Sie Enroll account (Konto anmelden). Weitere Informationen finden Sie unter Registrierung eines bestehenden Kontos in der AWS Control Tower Tower-Dokumentation.	

Überprüfen Sie das Konto nach der Registrierung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verifizieren Sie das Konto.	Wählen Sie in AWS Control Tower Accounts aus. Das Konto, das Sie gerade registriert haben, hat den Anfangsstatus Registrierung. Wenn die Registrierung abgeschlossen ist, ändert sich der Status in Registriert.	AWS Control Tower Tower-Administrator, Administrator des Mitgliedskontos
Suchen Sie nach Verstößen gegen die Leitplanken.	Die in der Organisationseinheit definierten Leitplanken gelten automatisch für das registrierte Mitgliedskonto. Überwachen Sie das AWS Control Tower Tower-Dashboard auf Verstöße und beheben Sie diese entsprech	AWS Control Tower Tower-Administrator, Administrator des Mitgliedskontos

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	end. Weitere Informationen finden Sie unter Guardrails in AWS Control Tower in der AWS-Dokumentation.	

Fehlerbehebung

Problem	Lösung
Sie erhalten die Fehlermeldung: Ein unbekannter Fehler ist aufgetreten. Versuchen Sie es später erneut, oder wenden Sie sich an den AWS-Support.	Dieser Fehler tritt auf, wenn Sie Root-Benutzeranmeldedaten (Verwaltungskonto) in AWS Control Tower verwenden, um ein neues Konto zu registrieren. AWS Service Catalog kann das Account Factory Portfolio oder das Produkt nicht dem Root-Benutzer zuordnen, was zu der Fehlermeldung führt. Um diesen Fehler zu beheben, verwenden Sie zur Registrierung des neuen Kontos Benutzeranmeldedaten (Administrator) mit vollem Zugriff, die kein Root-Konto sind. Weitere Informationen darüber, wie Sie einem Administratorbenutzer Administratorzugriff zuweisen, finden Sie unter Erste Schritte in der Dokumentation zu AWS IAM Identity Center (Nachfolger von AWS Single Sign-On).
Auf der Seite AWS Control Tower Activities wird die Aktion Get Catastrophic Drift angezeigt .	Diese Aktion spiegelt eine Drift-Prüfung des Service wider und weist nicht auf Probleme mit dem AWS Control Tower Tower-Setup hin. Es ist keine Aktion erforderlich.

Zugehörige Ressourcen

Dokumentation

- Terminologie und Konzepte von AWS Organizations (Dokumentation zu AWS Organizations)
- Was ist AWS Control Tower? (AWS Control Tower Tower-Dokumentation)
- Ein Mitgliedskonto aus Ihrer Organisation entfernen (Dokumentation zu AWS Organizations)
- Erstellen eines Administratorkontos in AWS Control Tower (AWS Control Tower Tower-Dokumentation)

Tutorials und Videos

- AWS Control Tower Workshop (Workshop zum Selbststudium)
- Was ist AWS Control Tower? (Video)
- Bereitstellen von Benutzern in AWS Control Tower (Video)
- AWS Control Tower für bestehende Organisationen aktivieren (Video)

Überwachen Sie SAP RHEL Pacemaker-Cluster mithilfe von AWS-Services

Erstellt von Harsh Thoria (AWS), Randy Germann (AWS) und RAVEENDRA Voore (AWS)

Übersicht

Dieses Muster beschreibt die Schritte zur Überwachung und Konfiguration von Warnmeldungen für einen Red Hat Enterprise Linux (RHEL) Pacemaker-Cluster für SAP-Anwendungen und SAP HANA-Datenbankdienste mithilfe von Amazon CloudWatch und Amazon Simple Notification Service (Amazon SNS).

Die Konfiguration ermöglicht es Ihnen, SAP SCS- oder ASCS-, Enqueue Replication Server- (ERS) - und SAP HANA-Clusterressourcen mithilfe von CloudWatch Protokollströmen, metrischen Filtern und Alarmen zu überwachen, wenn sie sich im Status „gestoppt“ befinden. Amazon SNS sendet eine E-Mail an das Infrastruktur- oder SAP-Basis-Team über den Status des gestoppten Clusters.

Sie können die AWS Ressourcen für dieses Muster mithilfe von AWS CloudFormation Skripten oder den AWS Servicekonsolen erstellen. Bei diesem Muster wird davon ausgegangen, dass Sie die Konsolen verwenden. Es enthält keine CloudFormation Skripts CloudWatch und deckt auch keine Infrastrukturbereitstellung für Amazon SNS ab. Pacemaker-Befehle werden verwendet, um die Konfiguration der Cluster-Warnmeldungen festzulegen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS Konto.
- Amazon SNS wurde für den Versand von E-Mail- oder Handybenachrichtigungen eingerichtet.
- Ein RHEL Pacemaker-Cluster aus SAP ASCS/ERS for ABAP or SCS/ERS für Java und SAP HANA Database. Detaillierte Informationen finden Sie hier:
  - Einrichtung eines SAP HANA-Clusters
  - Einrichtung des SAP Netweaver ABAP/Java-Clusters

Einschränkungen

- Diese Lösung funktioniert derzeit für auf RHEL Version 7.3 und spätere Pacemaker-basierte Cluster. Sie wurde nicht auf SUSE-Betriebssystemen getestet.

Produktversionen

- RHEL 7.3 und höher

Architektur

Zieltechnologie-Stack

- RHEL Pacemaker Alert, ereignisgesteuerter Agent
- Amazon Elastic Compute Cloud (Amazon EC2)
- CloudWatch Alarm
- CloudWatch Protokollgruppe und metrischer Filter
- Amazon SNS

Zielarchitektur

Das folgende Diagramm veranschaulicht die Komponenten und Workflows für diese Lösung.

Automatisierung und Skalierung

- Sie können die Erstellung von AWS Ressourcen mithilfe von CloudFormation Skripten automatisieren. Sie können auch zusätzliche Metrikfilter verwenden, um mehrere Cluster zu skalieren und abzudecken.

Tools

AWS-Services

- Amazon CloudWatch hilft Ihnen dabei, die Kennzahlen Ihrer AWS Ressourcen und der Anwendungen, auf denen Sie laufen, AWS in Echtzeit zu überwachen.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.

Tools

- CloudWatch agent (unified) ist ein Tool, das Metriken, Protokolle und Traces auf Systemebene von EC2 Instances sammelt und benutzerdefinierte Metriken aus Ihren Anwendungen abruft.
- Der Pacemaker-Alert-Agent (für RHEL 7.3 und höher) ist ein Tool, das bei einer Änderung eine Aktion auslöst, z. B. wenn eine Ressource in einem Pacemaker-Cluster gestoppt oder neu gestartet wird.

Bewährte Methoden

- Bewährte Methoden für die Verwendung von SAP-Workloads auf AWS finden Sie im SAP Lens for the AWS Well-Architected Framework.
- Berücksichtigen Sie die Kosten, die mit der Einrichtung der CloudWatch Überwachung für SAP HANA-Cluster verbunden sind. Weitere Informationen finden Sie in der CloudWatch - Dokumentation.
- Erwägen Sie die Verwendung eines Pagers oder eines Ticketing-Mechanismus für Amazon SNS SNS-Benachrichtigungen.
- Suchen Sie immer nach RHEL-Hochverfügbarkeitsversionen (HA) des RPM-Pakets für PCs, Pacemaker und den Fencing-Agenten. AWS

Epen

Einrichten von Amazon SNS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein SNS-Thema.	1. Melden Sie sich bei https://console.aws.amazon.com/sns/v3/home an AWS Management Console und öffnen Sie die Amazon SNS SNS-Konsole. 2. Wählen Sie auf dem Amazon-SNS-Dashboard unter Common actions die Option Create Topic.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie im Dialogfeld Neues Thema erstellen unter Typ die Option Standard aus. 4. Geben Sie unter Themenname einen Namen für das Thema ein (z. B.`my-topic`). 5. Wählen Sie Thema erstellen aus. Dadurch wird ein SNS-Thema mit einer Ressourcenrichtlinie erstellt, mit der Sie Benachrichtigungen veröffentlichen können. 6. Kopieren Sie den Themen-ARN (z. B.`arn:aws:sns:us-east-1:111122223333:my-topic`). Sie werden diesen ARN in einem späteren Schritt verwenden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Zugriffsr ichtlinie für das SNS-Thema.	1. Wählen Sie in der Amazon SNS SNS-Konsole im Navigationsbereich Themen und dann das von Ihnen erstellte Thema aus. 2. Wählen Sie Bearbeiten und gehen Sie zum Abschnitt Zugriffsrichtlinie. 3. Stellen Sie sicher, dass die Zugriffsrichtlinie einen der Dienstprinzipale enthält CloudWatch , die zu diesem Thema veröffentlichen dürfen. Zum Beispiel: `{ "Sid": "Allow AWS CloudWatch to Publish to this SNS topic", "Effect": "Allow", "Principal": { "Service": [ "cloudwatch.amazonaws.com" ] }, "Action": "SNS:Publish", "Resource": "arn:aws:sns:us-east-1:111122223333:my-topic" }`	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie Änderungen speichern aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Abonnieren Sie das SNS-Thema.	1. Wählen Sie in der Amazon SNS SNS-Konsole im Navigationsbereich Abonnements, Abonnement erstellen aus. 2. Fügen Sie für Topic ARN den ARN ein, den Sie in der ersten Aufgabe erstellt haben. 3. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus. 4. Geben Sie für Endpoint eine E-Mail-Adresse für die Person oder das Team ein, die für den SAP Pacemaker -Cluster verantwortlich ist und Benachrichtigungen erhalten soll. Dies kann beispielsweise die E-Mail-Adresse für die Verteiler liste des SAP-Basis- oder Infrastrukturteams sein. 5. Wählen Sie Create subscription (Abonnement erstellen) aus. 6. Öffnen Sie in Ihrer E-Mail-Anwendung die Nachricht unter AWS Benachric htigungen und bestätigen Sie Ihr Abonnement.	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ihr Webbrowser zeigt eine Bestätigungsantwort vom Amazon SNS an.	

Bestätigen Sie die Einrichtung des Clusters

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie den Clusterstatus.	Verwenden Sie den Befehl pcs status, um zu überprüfen, ob die Ressourcen online sind.	SAP-Basisadministrator

Pacemaker-Warnmeldungen konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie den Pacemaker-Alert-Agenten auf der primären Cluster-Instanz.	Melden Sie sich bei der EC2 Instanz im primären Cluster an und führen Sie die folgenden Befehle aus:
	`install --mode=0755 /usr/share/pacemaker/alerts/alert_file.sh.sample`
	`touch /var/lib/pacemaker/alert_file.sh`
	`touch /var/log/pcmk_alert_file.log`
	`chown hacluster:haclient /var/log/pcmk_alert_file.log`
	`chmod 600 /var/log/pcmk_alert_file.log`
		SAP-Basisadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`pcs alert create id=alert_file description="Log events to a file." path=/var/lib/pacemaker/alert_file.sh` `pcs alert recipient add alert_file id=my-alert_logfile value=/var/log/pcmk_alert_file.log`	

Konfigurieren Sie den Pacemaker-Alert-Agenten auf der sekundären Clusterinstanz.	Melden Sie sich bei der sekundären EC2 Clusterinstanz im sekundären Cluster an und führen Sie die folgenden Befehle aus:
	`install --mode=0755 /usr/share/pacemaker/alerts/alert_file.sh.sample /var/lib/pacemaker/alert_file.sh`
	`touch /var/log/pcmk_alert_file.log`
	`chown hacluster:haclient /var/log/pcmk_alert_file.log`
	`chmod 600 /var/log/pcmk_alert_file.log`
		SAP-Basisadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Vergewissern Sie sich, dass die RHEL-Alert-Ressource erstellt wurde.	Verwenden Sie den folgenden Befehl, um zu bestätigen, dass die Warnungsressource erstellt wurde:
	`pcs alert`
	Die Ausgabe des Befehls wird wie folgt aussehen:
	`[root@xxxxxxx ~]# pcs alert`
	`Alerts:`
	` Alert: alert_file (path=/var/lib/pacemaker/alert_file.sh)`
	`  Description: Log events to a file.`
	`  Recipients:`
	`   Recipient: my-alert_logfile (value=/var/log/pcmk_alert_file.log)`
		SAP-Basisadministrator

Konfigurieren Sie den CloudWatch Agenten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie den CloudWatch Agenten.	Es gibt mehrere Möglichkeiten, den CloudWatch Agenten auf einer EC2 Instanz zu installieren. Um die Befehlszeile zu verwenden: 1. Laden Sie das CloudWatch Agentenpaket herunter:	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`wget https://s3.<region>.amazonaws.com/amazoncloudwatch-agent-region/redhat/amd64/latest/amazon-cloudwatch-agent.rpm`
	
	wo `<region>` ist der AWS-Region Ort, an dem sich die EC2 Instanz befindet (zum Beispiel`us-west-2`).
	2. Optional) Überprüfen Sie die Paketsignatur. Anweisungen finden Sie in der CloudWatch Dokumentation unter Überprüfen der Signatur des CloudWatch Agentenpakets.
	3. Installieren Sie das Paket auf der ersten Instanz:
	
	`sudo rpm -U ./amazon-cloudwatch-agent.rpm`
	
	4. Wiederholen Sie den Vorgang für die sekundäre Instanz.
	
	Weitere Informationen finden Sie in der CloudWatch - Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie der EC2 Instance eine IAM-Rolle hinzu.	Damit der CloudWatch Agent Daten von den Instances senden kann, müssen Sie jeder Instance die CloudWatchAgentServerRoleIAM-Rolle zuordnen. Oder Sie können Ihrer bestehenden IAM-Rolle eine Richtlinie für den CloudWatch Agenten hinzufügen. Weitere Informationen finden Sie in der CloudWatch -Dokumentation.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie den CloudWatch Agenten so, dass er die Protokolldatei des Pacemaker Alert Agents auf der primären Clusterinstanz überwacht.	1. Konfigurieren Sie die primäre Clusterinstanz, indem Sie den folgenden Befehl ausführen: `sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard` 2. Wählen Sie 1 für Linux und wählen Sie dann die Optionen für Ihre Überwachungsstrategie aus. 3. Bei der Frage „Möchten Sie irgendwelche Protokoll dateien überwache n?“ wählen Sie Ja und geben Sie den Pfad der Pacemaker-Protokolldatei aus dem Befehl pcs alert an. In unserem Fall ist `var/log/pcmk_alert_file.log` es das. 4. Geben Sie den Namen der Protokollgruppe und des Protokollstreams an. Wenn Sie keinen Log-Strea m angeben, wird die AWS Instanz-ID als Standard verwendet.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Wiederholen Sie die Schritte 1—4 für die sekundäre Clusterinstanz.	
Starten Sie den CloudWatch Agenten auf den primären und sekundären Cluster-Instances.	Um den Agenten zu starten, führen Sie den folgenden Befehl auf den EC2 Instances im primären und sekundären Cluster aus: `sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json`	AWS-Administrator

CloudWatch Ressourcen einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten CloudWatch Sie Protokollgruppen ein.	1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/ 2. Wählen Sie im Navigationsbereich Protokollgruppen, Protokollgruppe erstellen aus. 3. Geben Sie einen Namen für die Protokollgruppe ein und wählen Sie dann Protokollgruppe erstellen aus.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Der CloudWatch Agent überträgt die Pacemaker-Warndatei als CloudWatch Log-Stream an die Log-Gruppe.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie CloudWatch metrische Filter ein.	Metrische Filter helfen Ihnen bei der Suche nach einem Muster, z. B. `stop <cluster-resource-name>` in den CloudWatch Log-Streams. Wenn dieses Muster identifiziert wird, aktualisiert der Metrikfilter eine benutzerdefinierte Metrik. 1. Wählen Sie auf der CloudWatch Konsole im Navigationsbereich die Option Protokollgruppen aus. 2. Wählen Sie den Namen der Protokollgruppe, die Sie in der vorherigen Aufgabe erstellt haben. 3. Wählen Sie Aktionen, Metrikfilter erstellen aus. 4. Geben Sie unter Filtermuster das Filtermuster ein, das verwendet werden soll, z. B. `stop ABC_scs` um dem Stopp-Ereignis für eine SAP SCS-Clusterressource mit dem Namen `ABC_scs` zu entsprechen. Weitere Informationen finden Sie in der CloudWatch Dokumentation unter Syntax des Filtermusters.	AWS-Administrator, SAP-Basisadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. (Optional) Um das Filtermuster zu testen, geben Sie unter Test Pattern (Muster testen) ein oder mehrere Protokollereignisse ein, die zum Testen des Musters verwendet werden sollen. Jedes Protokollereignis muss in einer separaten Zeile angegeben werden, da Zeilenumbrüche verwendet werden, um Ereignisse im Feld Ereignismeldungen protokollieren voneinander zu trennen. 6. Wählen Sie Next (Weiter) aus und geben Sie einen Namen für den Filter ein. 7. Geben Sie unter Metrikdetails für Metrik-Namespace einen Namen für den CloudWatch Namespace ein, in dem die Metrik veröffentlicht werden soll (z. B.`sapcluster_monitoring`). Wenn dieser Namespace noch nicht existiert, wählen Sie Neu erstellen aus. 8. Geben Sie unter Metriknamen einen Namen für die neue Metrik ein (z. `sapcluster_<sid>` B. wo `<sid>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ist der SAP-Systemidentifikationsname). 9. Geben Sie für Metrikwert den Wert 1 ein. Alternativ können Sie ein Token wie eingeben`$size`. Dadurch wird die Metrik für jedes Protokollereignis, das ein `size`-Feld enthält, um den Wert der Zahl in der `size` erhöht. 10. Geben Sie als Standardwert 0 ein. 11. Wählen Sie Metrikfilter erstellen aus. Wenn der Metrikfilter das Muster in Schritt 4 identifiziert, aktualisiert er den Wert der CloudWatch benutzerdefinierten Metrik `sapcluster_abc` auf 1. Der CloudWatch Alarm `SAP-Cluster-QA1-ABC` überwacht die Metrik `sapcluster_abc` und sendet eine SNS-Benachrichtigung, wenn sich der Wert der Metrik auf 1 ändert. Dies weist darauf hin, dass die Clusterressource gestoppt	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wurde und Maßnahmen ergriffen werden müssen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie einen CloudWatch Metrikalarm für die SAP ASCS/SCS- und ERS-Metrik ein.	So erstellen Sie einen Alarm, der auf einer einzelnen Metrik basiert: 1. Wählen Sie auf der CloudWatch Konsole im Navigationsbereich Alarme, Alle Alarme aus. 2. Wählen Sie Create alarm (Alarm erstellen) aus. 3. Wählen Sie Select Metric (Metrik auswählen) aus. 4. Suchen Sie nach der benutzerdefinierten Metrik `sapcluster_monitoring` , die in der vorherigen Aufgabe erstellt wurde. 5. Wählen Sie den Metriknamen für SAP SCS (z. B. `sapcluster_<abc>`), der ebenfalls in der vorherigen Aufgabe erstellt wurde. 6. Stellen Sie auf der Registerkarte Graphische Metriken Folgendes ein: • Wählen Sie für Statistic (Statistik) Maximum aus. • Wählen Sie als Zeitraum die Option 1 Minute aus. • Wählen Sie als Schwellenwerttyp die Option	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Statisch und legen Sie den Schwellenwert für **`sapcluster_<sid>`** auf einen Wert fest, der größer oder gleich 1 ist. 7. Wählen Sie Weiter aus. 8. Wählen Sie unter Benachrichtigung das SNS-Thema aus, das Sie im ersten Epic erstellt haben. 9. Geben Sie unter Name und Beschreibung den Namen des Alarms und eine kurze Beschreibung ein und wählen Sie dann Weiter. 10. Wählen Sie Alarm erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Richten Sie einen CloudWatch Metrikalarm für die SAP HANA-Metrik ein.	Wiederholen Sie die Schritte zur Einrichtung eines CloudWatch metrischen Alarms aus der vorherigen Aufgabe mit den folgenden Änderungen: • Wählen Sie für Schritt 5 den Metriknamen für SAP HANA aus (z. B.`sapcluster_db_<abc>`). • Legen Sie für Schritt 6 den Schwellenwert für `sapcluster_<sid>` auf einen Wert fest, der größer als 0 ist.	AWS-Administrator

Zugehörige Ressourcen

- Auslösen von Skripten für Cluster-Ereignisse (RHEL-Dokumentation)
- Erstellen Sie die CloudWatch Agent-Konfigurationsdatei mit dem Assistenten (Dokumentation) CloudWatch
- Installation und Ausführung des CloudWatch Agenten auf Ihren Servern (CloudWatch Dokumentation)
- Erstellen Sie einen CloudWatch Alarm auf der Grundlage eines statischen Schwellenwerts (CloudWatch Dokumentation)
- Manuelle Bereitstellung von SAP HANA on AWS mit Hochverfügbarkeitsclustern (SAP-Dokumentation auf der AWS Website)
- NetWeaver SAP-Leitfäden (SAP-Dokumentation auf der AWS Website)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Überwachen Sie die Anwendungsaktivität mithilfe von CloudWatch Logs Insights

Erstellt von Ram Kandaswamy (AWS)

Übersicht

Dieses Muster bietet eine Lösung für die automatische Erkennung und Warnung bei Anwendungsausnahmen mithilfe von Amazon CloudWatch Logs Insights. Durch die Implementierung automatisierter Protokollanalysen und Warnmeldungen können Sie Anwendungsprobleme in Ihrer Produktionsumgebung schnell erkennen und darauf reagieren.

Protokolle spielen eine entscheidende Rolle bei der Überwachung des Systemverhaltens, der Identifizierung von Problemen und der Sicherstellung einer optimalen Leistung. Während eines Migrationsprozesses sind Protokolldateien von unschätzbarem Wert, wenn es darum geht, die Funktionsfähigkeit des Systems in der neuen Umgebung zu überprüfen, Kompatibilitätsprobleme zu erkennen und unerwartetes Verhalten zu identifizieren. Probleme können betriebs- oder sicherheitsbedingt sein. Bei sicherheitsrelevanten Problemen ist es wichtig, die frühzeitige Erkennung von unbefugten Zugriffsversuchen oder verdächtigen Aktivitäten zu ermöglichen, um die Sicherheit und die Einhaltung gesetzlicher Vorschriften zu gewährleisten. Diese Fähigkeit ist besonders wichtig, wenn es um sensible Daten oder kritische Systeme geht.

Dieses Muster ist besonders nützlich für Teams, die eine hohe Anwendungsverfügbarkeit aufrechterhalten und schnell auf Produktionsprobleme reagieren müssen. Es ist für verschiedene Branchen und Anwendungsfälle relevant. In der Telekommunikation ermöglicht es beispielsweise die schnelle Identifizierung von Fehlkonfigurationen oder Ausfällen im Netzwerk und die Erkennung suboptimaler Routing-Pfade, um potenzielle Engpässe zu lokalisieren. Im Bereich Internet der Dinge (IoT) können Greengrass-Komponenten Protokolle veröffentlichen CloudWatch, sodass mit dieser Technik relevante Protokolldetails extrahiert und in einem umfassenden Dashboard dargestellt werden können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Produktionsanwendung, die aktiv bereitgestellt wird AWS-Konto
- Grundlegendes Verständnis des Protokollierungsformats und der Ausnahmemuster der Produktionsanwendung
- Anwendungsprotokolle, die für das Streaming zu Amazon CloudWatch Logs konfiguriert sind

Einschränkungen

- Einige AWS-Services sind nicht in allen verfügbar AWS-Regionen. Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie unter AWS Dienste nach Regionen. Informationen zu bestimmten Endpunkten finden Sie unter Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Architektur

Das folgende Diagramm zeigt, wie CloudWatch Logs Insights Ressourcenprotokolle auswertet und eine entsprechende Datenvisualisierung an ein Dashboard sendet. CloudWatch

Das Diagramm zeigt den folgenden Workflow:

1. Die Ressourcen veröffentlichen Protokolle in CloudWatch Logs. Zu den Ressourcen können AWS Ressourcen wie Amazon Elastic Compute Cloud (Amazon EC2) -Instances oder Amazon Simple Storage Service (Amazon S3) -Buckets gehören. Ein anderes Beispiel sind lokale Systeme, auf denen ein CloudWatch Agent installiert ist und auf denen Protokolle veröffentlicht werden können. CloudWatch
2. CloudWatch Logs Insights filtert nach der entsprechenden Musterzeichenfolge. Beispiele für Suchmusterzeichenfolgen sind „Fehler“, „Ausnahme“ oder ein bestimmter regulärer Ausdruck.
3. In der Regel fügen das Produktionsunterstützungsteam oder die Entwickler die Mustervisualisierung dem CloudWatch Dashboard hinzu.

Automatisierung und Skalierung

Entwickler können die Lösung dieses Musters automatisieren, indem sie das AWS Cloud Development Kit (AWS CDK),, oder verwenden AWS CloudFormation, AWS SDKs um mehrere Zeichenkettenmuster zu verarbeiten. Teams können diese Automatisierung in ihre kontinuierlichen Integrations- und Bereitstellungsprozesse (CI/CD) DevOps integrieren.

Tools

AWS-Services

- Amazon CloudWatch Logs hilft Ihnen dabei, die Protokolle all Ihrer Systeme und Anwendungen zu zentralisieren, AWS-Services sodass Sie sie überwachen und sicher archivieren können.

- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Key Management Service (AWS KMS) hilft Ihnen dabei, kryptografische Schlüssel zu erstellen und zu kontrollieren, um Ihre Daten zu schützen.

Bewährte Methoden

- Definieren und konfigurieren Sie Protokollgruppen, um relevante Protokolldaten zu analysieren.
- Verwenden Sie Feld-Explorer, um die Struktur und die Felder zu verstehen, die in Ihren Protokolldaten verfügbar sind.
- Schreiben Sie effiziente Abfragen mithilfe der CloudWatch Logs Insights-Abfragesyntax.
- Passen Sie Beispielabfragen für eine schnellere Analyse an Ihre spezifischen Anforderungen an.
- Überwachen Sie Abfragen, um potenzielle Leistungsprobleme oder Engpässe zu identifizieren.
- Legen Sie Abfragegrenzwerte fest, um übermäßige Kosten oder einen übermäßigen Ressourcenverbrauch zu vermeiden.
- Speichern Sie Abfragen für die future Verwendung, um Zeit zu sparen und eine konsistente Analyse sicherzustellen.
- Wenden Sie die entsprechenden IAM-Richtlinien an, um den Zugriff auf CloudWatch Logs Insights und Protokollgruppen zu kontrollieren. Folgen Sie dem Prinzip der geringsten Rechte und gewähren Sie die für die Ausführung einer Aufgabe erforderlichen Mindestberechtigungen. Weitere Informationen finden Sie in der IAM-Dokumentation unter Gewährung der geringsten Rechte und bewährte Methoden zur Sicherheit.
- Aktivieren Sie die Protokolldatenverschlüsselung AWS KMS für sensible Protokolldaten.

Epen

Erstellen Sie eine Protokollgruppe und konfigurieren Sie die Protokolle zur Anzeige im Dashboard.

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie IAM-Berec htigungen.	Gehen Sie wie folgt vor, um IAM-Berechtigungen zu konfigurieren:	AWS-Administrator DevOps, AWS, AWS-Systemadminist rator, Cloud-Administrato

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Identifizieren Sie die IAM-Rollen, die von Ihrer Anwendung zum Schreiben von Protokollen und von Benutzern oder Diensten verwendet werden, die Dashboards, Abfragen und Alarme erstellen. 2. Fügen Sie für die Anwendungsrolle die folgenden API-Aktionen und Ressourcen zu einer Richtlinie hinzu: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "logs:CreateLogGroup", "logs:CreateLogStream", "logs:PutLogEvents" ], "Resource": [ "arn:aws:logs:*:*:*" ]`	r, Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre> }
	        ]
	    }</pre>
	3. Um CloudWatch Ressourcen zu verwalten, fügen Sie einer Richtlinie Folgendes hinzu:
	<pre>{
	    "Version": "2012-10-17",
	    "Statement": [
	        {
	            "Effect": "Allow",
	            "Action": [
	"cloudwatch:PutDashboard",
	"cloudwatch:GetDashboard",
	"logs:StartQuery",
	"logs:StopQuery",
	"logs:GetQueryResults",
	"cloudwatch:PutMetricAlarm"
	            ],
	            "Resource": "*"
	        }
	    ]
	}</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Informationen zum Erstellen von IAM-Richtlinien oder zum Hinzufügen von Berechtigungen zu vorhandenen Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien und Bearbeiten von IAM-Richtlinien im IAM-Benutzerhandbuch. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für Amazon CloudWatch Logs und Referenz zu CloudWatch Logs-Berechtigungen im Amazon CloudWatch Logs-Benutzerhandbuch.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie eine -Protokollgruppe.	Verwenden Sie eine der folgenden Optionen, um eine Protokollgruppe zu erstellen:
	• Erstellen oder öffnen Sie eine CloudFormation Vorlagendatei (YAML- oder JSON-Format) mit der `.json` Erweiterung `.yaml` oder. (Der folgende Code verwendet das YAML-Format.) Fügen Sie dem Abschnitt Ressourcen Ihrer Vorlage die folgende Ressourcendefinition hinzu:
	`MyLogGroup:`
	`  Type: AWS::Logs::LogGroup`
	`  Properties:`
	`  LogGroupName: my-log-group`
	Weitere Informationen finden Sie unter Schnellstart: Verwenden Sie für AWS CloudFormation die ersten Schritte mit CloudWatch Logs im Amazon CloudWatch Logs-Benutzerhandbuch.
	• Verwenden Sie die CloudWatch Konsole, wie unter Erstellen einer Protokollgruppe
		AWS-Administrator DevOps, AWS, AWS-Systemadministrator, Cloud-Administrator, Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in CloudWatch Logs im Amazon CloudWatch Logs-Benutzerhandbuch beschrieben. • Verwenden Sie den CreateLogGroupVorgang in der CloudWatch Logs-API.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie eine CloudWatch Logs Insights-Abfrage.	So erstellen und speichern Sie eine CloudWatch Logs Insights-Abfrage: 1. Öffnen Sie die CloudWatch Konsole. 2. Navigieren Sie zu Logs Insights. 3. Erstellen Sie Ihre Abfrage mit einer der folgenden Methoden: • Beginnen Sie mit einer Beispielabfrage aus dem Abschnitt Abfragen. • Schreiben Sie eine benutzerdefinierte Abfrage. • Ändern Sie die folgende Beispielabfrage: `fields @timestamp, @message | filter @message like /(?i)exception/|stats count() by bin(30s)` Diese Abfrage überprüft die Protokolldatei, extrahiert den Zeitstempel und den Nachrichteninhalt, filtert nach dem Wort „Ausnahme“ (ohne Berücksichtigung von Groß- und	AWS-Administrator DevOps, AWS, AWS-Systemadministrator, Cloud-Administrator, Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Kleinschreibung) und zählt Ereignisse in 30-Sekunden-Intervallen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Visualisierung in einem CloudWatch Dashboard.	Gehen Sie wie folgt vor, um ein CloudWatch Dashboard zum Erstellen einer Visualisierung zu verwenden: 1. Öffnen Sie die CloudWatch Konsole und erstellen Sie ein CloudWatch Dashboard (falls Sie noch keines haben) oder öffnen Sie ein vorhandenes Dashboard. 2. Fügen Sie Ihre Visualisierung zur Ausnahmeüberwachung hinzu. Balken-, Linien- und Kreisdiagramme sind je nach Ihren Geschäftsanforderungen verfügbar. Weitere Informationen finden Sie unter Verwenden von Widgets auf CloudWatch Dashboards im Amazon CloudWatch Logs-Benutzerhandbuch. Für Datenvisualisierungen in Echtzeit können Sie ein Widget an Ihre Anforderungen anpassen. Weitere Informationen zu Dashboard-Optionen und -Funktionen finden Sie unter Verwenden von CloudWatch Amazon-Dashboards und Erstellen flexibler CloudWatc	AWS-Administrator DevOps, AWS, AWS-Systemadministrator, Cloud-Administrator, Cloud-Architekt, DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	h Dashboards mit Dashboard -Variablen im Amazon CloudWatch Logs-Benu tzerhandbuch.	

Fehlerbehebung

Problem	Lösung
Die Abfrageergebnisse können nicht angezeigt werden oder die Abfrage scheint defekt zu sein	Beginnen Sie mit einer funktionierenden Abfrage, die anhand einer Beispielabfrage geändert wurde. Nehmen Sie kleine inkrement elle Änderungen an Teilen der Abfrage vor (z. B. an einem Filter oder Feld) und nutzen Sie die Funktion zum Generieren von CloudWatch Protokollabfragen.
Protokollgruppen, die keine Protokolldatenströ me erstellen	Stellen Sie in der IAM-Richtlinie sicher, dass die Ressource für die CreateLogStreamund die CreateLogGroupOperationen mit einem Platzhalterzeichen versehen ist. (`*`) Ohne diese Platzhalterberechtigung ist der `create` Vorgang nicht erfolgreich.

Zugehörige Ressourcen

- Analysieren von Protokolldaten mit CloudWatch Logs Insights
- Amazon CloudWatch FAQs
- Erstellung flexibler CloudWatch Dashboards mit Dashboard-Variablen
- Erste Schritte mit Logs Insights QL: Query tutorials
- Verwenden Sie natürliche Sprache, um CloudWatch Logs Insights-Abfragen zu generieren und zu aktualisieren
- Verwendung PutDashboard mit einem AWS SDK oder CLI

- Arbeiten mit Protokollgruppen und Protokollströmen

Überwachen Sie die Nutzung eines gemeinsam genutzten Amazon Machine Image über mehrere AWS-Konten

Erstellt von Naveen Suthar (AWS) und Sandeep Gawande (AWS)

Übersicht

Amazon Machine Images (AMIs) werden verwendet, um Amazon Elastic Compute Cloud (Amazon EC2) -Instances in Ihrer Amazon Web Services (AWS) -Umgebung zu erstellen. Sie können ein separates, zentrales AWS-Konto erstellen AMIs , das in diesem Muster als Creator-Konto bezeichnet wird. Sie können das AMI dann für mehrere Benutzer gemeinsam nutzen AWS-Konten , die sich in demselben Muster befinden AWS-Region, die in diesem Muster als Verbraucherkonten bezeichnet werden. Die Verwaltung AMIs von einem einzigen Konto aus bietet Skalierbarkeit und vereinfacht die Verwaltung. In den Verbraucherkonten können Sie auf das gemeinsam genutzte AMI in Amazon EC2 Auto Scaling Scaling-Startvorlagen und Amazon Elastic Kubernetes Service (Amazon EKS) - Knotengruppen verweisen.

Wenn ein gemeinsam genutztes AMI veraltet, deregistriert oder nicht gemeinsam genutzt ist, können die auf AWS-Services das AMI in den Verbraucherkonten verweisenden AMIs dieses AMI nicht verwenden, um neue Instances zu starten. Jedes Auto Scaling-Ereignis oder jeder Relaunch derselben Instance schlägt fehl. Dies kann zu Problemen in der Produktionsumgebung führen, z. B. zu Anwendungsausfällen oder Leistungseinbußen. Wenn AMI-Sharing- und Nutzungsereignisse mehrfach auftreten AWS-Konten, kann es schwierig sein, diese Aktivität zu überwachen.

Dieses Muster hilft Ihnen dabei, die gemeinsame AMI-Nutzung und den Status von Konten in derselben Region zu überwachen. Es verwendet serverlose AWS-Services Systeme wie Amazon EventBridge, Amazon DynamoDB und Amazon Simple Email Service (Amazon SES). AWS Lambda Sie stellen die Infrastruktur als Code (IaC) mithilfe von Terraform bereit. HashiCorp Diese Lösung gibt Warnmeldungen aus, wenn ein Dienst in einem Verbraucherkonto auf ein abgemeldetes oder nicht gemeinsam genutztes AMI verweist.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zwei oder mehr aktive Konten AWS-Konten: ein Erstellerkonto und ein oder mehrere Verbraucherkonten
- Eines oder mehrere AMIs , die vom Erstellerkonto mit einem Verbraucherkonto geteilt werden
- Terraform CLI, installiert (Terraform-Dokumentation)

- Terraform AWS Provider, konfiguriert (Terraform-Dokumentation)
- (Optional, aber empfohlen) Terraform-Backend, konfiguriert (Terraform-Dokumentation)
- Git, installiert

Einschränkungen

- Dieses Muster überwacht anhand der Konto-ID, AMIs welche für bestimmte Konten freigegeben wurden. Dieses Muster überwacht nicht AMIs , welche Daten mithilfe der Organisations-ID für eine Organisation freigegeben wurden.
- AMIs kann nur mit Konten geteilt werden, die sich innerhalb derselben Gruppe befinden AWS-Region. Dieses Muster überwacht AMIs innerhalb einer einzigen Zielregion. Um die Nutzung von AMIs in mehreren Regionen zu überwachen, setzen Sie diese Lösung in jeder Region ein.
- Bei diesem Muster werden keine Daten überwacht AMIs , die vor der Bereitstellung dieser Lösung geteilt wurden. Wenn Sie das bereits geteilte AMI überwachen möchten AMIs, können Sie die Freigabe des AMI aufheben und es dann erneut mit den Benutzerkonten teilen.

Produktversionen

- Terraform Version 1.2.0 oder höher
- Terraform AWS Provider Version 4.20 oder höher

Architektur

Zieltechnologie-Stack

Die folgenden Ressourcen werden als IaC über Terraform bereitgestellt:

- Amazon-DynamoDB-Tabellen
- EventBridge Amazon-Regeln
- AWS Identity and Access Management (IAM) -Rolle
- AWS Lambda Funktionen
- Amazon SES

Zielarchitektur

Das Diagramm zeigt den folgenden Workflow:

1. Ein AMI im Erstellerkonto wird mit einem Verbraucherkonto im selben Konto geteilt AWS-Region.
2. Wenn das AMI gemeinsam genutzt wird, erfasst eine EventBridge Regel im Erstellerkonto das `ModifyImageAttribute` Ereignis und initiiert eine Lambda-Funktion im Erstellerkonto.
3. Die Lambda-Funktion speichert Daten, die sich auf das AMI beziehen, in einer DynamoDB-Tabelle im Creator-Konto.
4. Wenn ein AWS-Service Kundenkonto das gemeinsame AMI verwendet, um eine EC2 Amazon-Instance zu starten, oder wenn das gemeinsam genutzte AMI mit einer Startvorlage verknüpft ist, erfasst eine EventBridge Regel im Verbraucherkonto die Nutzung des gemeinsamen AMI.
5. Die EventBridge Regel initiiert eine Lambda-Funktion im Verbraucherkonto. Die Lambda-Funktion bewirkt Folgendes:
   a. Die Lambda-Funktion aktualisiert die AMI-bezogenen Daten in einer DynamoDB-Tabelle im Verbraucherkonto.
   b. Die Lambda-Funktion nimmt eine IAM-Rolle im Creator-Konto an und aktualisiert die Lambda-Tabelle im Creator-Konto. In der `Mapping` Tabelle wird ein Element erstellt, das die Instance-ID oder die Startvorlagen-ID der jeweiligen AMI-ID zuordnet.
6. Das AMI, das zentral im Creator-Konto verwaltet wird, ist veraltet, deregistriert oder nicht gemeinsam genutzt.
7. Die EventBridge Regel im Creator-Konto erfasst das `ModifyImageAttribute` `DeregisterImage` OR-Ereignis mit der `remove` Aktion und initiiert die Lambda-Funktion.
8. Die Lambda-Funktion überprüft die DynamoDB-Tabelle, um festzustellen, ob das AMI in einem der Verbraucherkonten verwendet wird. Wenn in der `Mapping` Tabelle keine Instance IDs oder Startvorlage mit dem AMI IDs verknüpft ist, ist der Vorgang abgeschlossen.
9. Wenn dem AMI in der `Mapping` Tabelle eine Instance IDs oder Startvorlage IDs zugeordnet ist, verwendet die Lambda-Funktion Amazon SES, um eine E-Mail-Benachrichtigung an die konfigurierten Abonnenten zu senden.

Tools

AWS-Services

- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.

- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS Lambda Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen. AWS-Konten
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, sie zu verwenden.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Email Service (Amazon SES) unterstützt Sie beim Senden und Empfangen von E-Mails mithilfe Ihrer eigenen E-Mail-Adressen und Domains.

Andere Tools

- HashiCorp Terraform ist ein Infrastructure-as-Code-Tool (IaC), mit dem Sie mithilfe von Code Cloud-Infrastruktur und -Ressourcen bereitstellen und verwalten können.
- Python ist eine Allzweck-Computerprogrammiersprache.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub cross-account-ami-monitoring-terraform-samples verfügbar.

Bewährte Methoden

- Folgen Sie den Best Practices für die Arbeit mit Funktionen. AWS Lambda
- Folgen Sie den Best Practices für das Bauen AMIs.
- Halten Sie sich bei der Erstellung der IAM-Rolle an das Prinzip der geringsten Rechte und gewähren Sie nur die für die Ausführung einer Aufgabe erforderlichen Mindestberechtigungen. Weitere Informationen finden Sie in der IAM-Dokumentation unter Gewährung der geringsten Rechte und bewährte Methoden zur Sicherheit.
- Richten Sie die Überwachung und Warnmeldungen für die AWS Lambda Funktionen ein. Weitere Informationen finden Sie unter Überwachung und Problembehandlung von Lambda-Funktionen.

Epen

Passen Sie die Terraform-Konfigurationsdateien an

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die AWS CLI benannten Profile.	Erstellen Sie für das Ersteller konto und jedes Verbrauch erkonto ein AWS Command Line Interface (AWS CLI) benanntes Profil. Anweisung en dazu finden Sie AWS CLI im Ressourcencenter für die ersten AWS Schritte unter Einrichten von.	DevOps Ingenieur
Klonen Sie das Repository	Geben Sie den folgenden Befehl ein. Dadurch wird das Repository cross-account-ami-monitoring-terraform-samples mithilfe von SSH geklont. GitHub `git clone git@github.com:aws-samples/cross-account-ami-monitoring-terraform-samples.git`	DevOps Ingenieur
Aktualisieren Sie die Datei provider.tf.	1. Geben Sie den folgenden Befehl ein, um zu dem `terraform` Ordner im geklonten Repository zu navigieren. `cd cross-account-ami-monitoring/terraform`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Öffnen Sie die `provider.tf` Datei. 3. Aktualisieren Sie die Terraform AWS Provider-Konfigurationen für das Creator-Konto und das Consumer-Konto wie folgt: • Geben Sie für `alias` einen Namen für die Anbieterkonfiguration ein. • Geben Sie für das Ziel ein`region`, auf AWS-Region dem Sie diese Lösung bereitstellen möchten. • Geben Sie für `profile` das AWS CLI angegebene Profil für den Zugriff auf das Konto ein. 4. Wenn Sie mehr als ein Verbraucherkonto konfigurieren, erstellen Sie ein Profil für jedes weitere Verbraucherkonto. 5. Speichern und schließen Sie die Datei `provider.tf` . Weitere Informationen zur Konfiguration der Anbieter finden Sie unter Konfigurationen mehrerer Anbieter in der Terraform-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Datei terraform.tfvars.	1. Öffnen Sie die `terraform.tfvars` Datei. 2. Konfigurieren Sie im `account_email_mapping` Parameter die Benachrichtigungen für das Erstellerkonto und das Verbraucherkonto wie folgt: • Geben Sie für `account` die Konto-ID ein. • Geben Sie für `email` die E-Mail-Adresse ein, an die Sie Benachrichtigungen senden möchten. Sie können für jedes Konto nur eine E-Mail-Adresse eingeben. 3. Wenn Sie mehr als ein Verbraucherkonto konfigurieren, geben Sie für jedes weitere Verbraucherkonto ein Konto und eine E-Mail-Adresse ein. 4. Speichern und schließen Sie die Datei `terraform.tfvars` .	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Datei main.tf.	Führen Sie diese Schritte nur aus, wenn Sie diese Lösung für mehr als ein Kundenkonto bereitstellen. Wenn Sie diese Lösung nur für ein Verbraucherkonto bereitstellen, ist keine Änderung dieser Datei erforderlich. 1. Öffnen Sie die `main.tf` Datei. 2. Erstellen Sie für jedes weitere Verbraucherkonto ein neues Modul, das auf dem `consumer_account_A` Modul in der Vorlage basiert. Für jedes Verbraucherkonto sollte der Wert für dem Alias entsprechen`provider`, den Sie in der `provider.tf` Datei eingegeben haben. 3. Speichern und schließen Sie die Datei `main.tf`.	DevOps Ingenieur

Stellen Sie die Lösung mithilfe von Terraform bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Lösung bereit.	Geben Sie in der Terraform-CLI die folgenden Befehle ein, um die AWS Ressourcen in	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	den Creator- und Consumer-Konten bereitzustellen:
	1. Geben Sie den folgenden Befehl ein, um Terraform zu initialisieren.
	`terraform init`
	2. Geben Sie den folgenden Befehl ein, um die Terraform-Konfigurationen zu validieren.
	`terraform validate`
	3. Geben Sie den folgenden Befehl ein, um einen Terraform-Ausführungsplan zu erstellen.
	`terraform plan`
	4. Überprüfen Sie die Konfigurationsänderungen im Terraform-Plan und bestätigen Sie, dass Sie diese Änderungen implementieren möchten.
	5. Geben Sie den folgenden Befehl ein, um die Ressourcen bereitzustellen.
	`terraform apply`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Identität der E-Mail-Adresse.	Bei der Bereitstellung des Terraform-Plans hat Terraform für jedes Verbraucherkonto in Amazon SES eine E-Mail-Adressidentität erstellt. Bevor Benachrichtigungen an diese E-Mail-Adresse gesendet werden können, müssen Sie die E-Mail-Adresse überprüfen. Anweisungen finden Sie in der Amazon SES SES-Dokumentation unter Verifizieren der Identität einer E-Mail-Adresse.	Allgemeines AWS

Validieren Sie den Ressourceneinsatz

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie die Bereitstellung im Creator-Konto.	1. Loggen Sie sich in das Creator-Konto ein. 2. Bestätigen Sie in der Navigationsleiste, dass Sie das Ziel sehen AWS-Region. Wenn Sie sich in einer anderen Region befinden, wählen Sie den Namen der aktuell angezeigten Region und dann die Zielregion aus. 3. Öffnen Sie die DynamoDB-Konsole.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Wählen Sie im Navigationsbereich Tables (Tabellen) aus. 5. Überprüfen Sie in der Tabellenliste, ob die `AmiShare` Tabelle vorhanden ist. 6. Öffnen Sie die Lambda-Konsole. 7. Wählen Sie im Navigationsbereich Funktionen aus. 8. Überprüfen Sie in der Liste der Funktionen, ob die `ami-share` Funktion vorhanden ist. 9. Öffnen Sie die IAM-Konsole. 10. Wählen Sie im Navigationsbereich Roles aus. 11. Überprüfen Sie in der Rollenliste, ob die `external-ddb-role` Rolle vorhanden ist. 12. Öffnen Sie die EventBridge-Konsole. 13. Wählen Sie im Navigationsbereich Regeln aus. 14. Überprüfen Sie in der Liste der Regeln, ob die `modify_image_attribute_event` Regel vorhanden ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	15. Öffnen Sie die Amazon SES SES-Konsole. 16. Wählen Sie im Navigationsbereich Verifizierte Identitäten aus. 17. Vergewissern Sie sich in der Identitätsliste, dass für jedes Kundenkonto eine E-Mail-Adressidentität registriert und verifiziert wurde.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Bereitstellung im Kundenkonto.	1. Melden Sie sich beim Verbraucherkonto an. 2. Bestätigen Sie in der Navigationsleiste, dass Sie das Ziel sehen AWS-Region. Wenn Sie sich in einer anderen Region befinden, wählen Sie den Namen der aktuell angezeigten Region und dann die Zielregion aus. 3. Öffnen Sie die DynamoDB-Konsole. 4. Wählen Sie im Navigationsbereich Tables (Tabellen) aus. 5. Überprüfen Sie in der Tabellenliste, ob die `Mapping` Tabelle vorhanden ist. 6. Öffnen Sie die Lambda-Konsole. 7. Wählen Sie im Navigationsbereich Funktionen aus. 8. Überprüfen Sie in der Liste der Funktionen, ob die `ami-deregister-function` Funktionen `ami-usage-function` und vorhanden sind. 9. Öffnen Sie die EventBridge-Konsole.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	10. Wählen Sie im Navigationsbereich Regeln aus. 11. Vergewissern Sie sich, dass die Regeln `ami_usage_events` und in der Liste der `ami_deregister_events` Regeln vorhanden sind.	

Überwachung validieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein AMI im Creator-Konto.	1. Erstellen Sie im Creator-Konto ein privates AMI. Anweisungen finden Sie unter Erstellen eines AMI aus einer EC2 Amazon-Instance. 2. Teilen Sie das neue AMI mit einem der Verbrauch erkonten. Anweisungen finden Sie unter Ein AMI mit bestimmten Personen teilen AWS-Konten.	DevOps Ingenieur
Verwenden Sie das AMI im Verbraucherkonto.	Verwenden Sie im Verbrauch erkonto das gemeinsam genutzte AMI, um eine EC2 Amazon-Instance oder eine Startvorlage zu erstellen . Anweisungen finden Sie unter Wie starte ich eine EC2 Amazon-Instance von einem	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	benutzerdefinierten AMI aus (AWS re:POST Knowledge Center) oder Erstellen Sie eine Startvorlage für eine Auto Scaling Scaling-Gruppe (Amazon EC2 Auto Scaling Scaling-Dokumentation).	
Überprüfen Sie die Überwachung und Alarmierung.	1. Loggen Sie sich in das Creator-Konto ein. 2. Öffnen Sie die EC2 Amazon-Konsole. 3. Wählen Sie im Navigationsbereich AMIs aus. 4. Wählen Sie das AMI in der Liste aus und klicken Sie dann auf Aktionen, AMI-Berechtigungen bearbeiten. 5. Wählen Sie im Abschnitt Gemeinsam genutzte Konten das Verbrauchserkonto aus und klicken Sie dann auf Ausgewählte entfernen. 6. Wählen Sie Änderungen speichern aus. 7. Stellen Sie sicher, dass die Ziel-E-Mail-Adresse, die Sie für das Verbrauchserkonto definiert haben, eine Benachrichtigung erhält, dass die gemeinsame Nutzung für das AMI storniert wurde.	DevOps Ingenieur

(Optional) Beenden Sie die gemeinsame Überwachung AMIs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie die Ressourcen.	1. Geben Sie den folgenden Befehl ein, um die nach diesem Muster bereitgestellten Ressourcen zu entfernen und die gemeinsame Überwachung zu beenden AMIs. `terraform destroy` 2. Bestätigen Sie den `destroy` Befehl mit der Eingabe `yes`.	DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Ich habe keine E-Mail-Benachrichtigung erhalten.	Es kann mehrere Gründe geben, warum die Amazon SES SES-E-Mail nicht gesendet wurde. Überprüfen Sie, ob Folgendes der Fall ist: 1. Verwenden Sie im Abschnitt Epics das Epic Validate Resource Deployment, um zu überprüfen, ob die Infrastruktur insgesamt ordnungsgemäß bereitgestellt wurde. AWS-Konten 2. Überprüfen Sie die Lambda-Funktionser eignisse in Amazon CloudWatch Logs. Anweisungen finden Sie in der Lambda-Dokumentation unter Verwenden der CloudWatch Konsole. Vergewissern Sie sich,

Problem	Lösung
	dass in identitäts- oder ressourcenbasierte n Richtlinien keine Probleme mit Berechtig ungen vorliegen, wie z. B. eine ausdrückliche Ablehnung. Weitere Informationen finden Sie in der IAM-Dokumentation unter Bewertung slogik für Richtlinien. 3. Vergewissern Sie sich in Amazon SES, dass der Status der E-Mail-Adressident ität Verifiziert lautet. Weitere Informationen finden Sie unter Überprüfen der Identität einer E-Mail-Adresse.

Zugehörige Ressourcen

AWS Dokumentation

- Lambda-Funktionen mit Python erstellen (Lambda-Dokumentation)
- Ein AMI erstellen (EC2 Amazon-Dokumentation)
- Teilen Sie ein AMI mit bestimmten Personen AWS-Konten (EC2 Amazon-Dokumentation)
- Ihr AMI abmelden (EC2 Amazon-Dokumentation)

Terraform-Dokumentation

- Installieren Sie Terraform
- Terraform-Backend-Konfiguration
- Terraform AWS-Anbieter
- Terraform-Binärdatei herunterladen

Benachrichtigungen für programmatische Kontoschließungen in AWS Organizations einrichten

Erstellt von Richard Milner-Watts (AWS), Debojit Bhadra (AWS) und Manav Yadav (AWS)

Übersicht

Die CloseAccount API für AWS Organizations ermöglicht es Ihnen, Mitgliedskonten innerhalb einer Organisation programmgesteuert zu schließen, ohne sich mit Root-Anmeldeinformationen bei dem Konto anmelden zu müssen. Die RemoveAccountFromOrganization API ruft ein Konto aus einer Organisation in AWS Organizations ab, sodass es zu einem eigenständigen Konto wird.

Diese erhöhen APIs potenziell die Anzahl der Betreiber, die ein AWS-Konto schließen oder entfernen können. Alle Benutzer, die über AWS Identity and Access Management (IAM) im Verwaltungskonto von AWS Organizations Zugriff auf die Organisation haben, können diese aufrufen APIs, sodass der Zugriff nicht auf den Inhaber der Root-E-Mail-Adresse des Kontos mit einem zugehörigen Multi-Faktor-Authentifizierungsgerät (MFA) beschränkt ist.

Dieses Muster implementiert Warnmeldungen, wenn die `CloseAccount` und aufgerufen `RemoveAccountFromOrganization` APIs werden, sodass Sie diese Aktivitäten überwachen können. Für Benachrichtigungen wird ein Amazon Simple Notification Service (Amazon SNS) -Thema verwendet. Sie können Slack-Benachrichtigungen auch über einen Webhook einrichten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Organisation in AWS Organizations
- Zugriff auf das Organisationsverwaltungskonto unter dem Stammkonto der Organisation, um die erforderlichen Ressourcen zu erstellen

Einschränkungen

- Wie in der API-Referenz für AWS Organizations beschrieben, ermöglicht die `CloseAccount` API nur die Schließung von 10 Prozent der aktiven Mitgliedskonten innerhalb eines fortlaufenden Zeitraums von 30 Tagen.

- Wenn ein AWS-Konto geschlossen wird, ändert sich sein Status in GESPERRT. 90 Tage nach diesem Statuswechsel kann AWS Support das Konto erneut eröffnen. Nach 90 Tagen wird das Konto dauerhaft gelöscht.
- Benutzer, die Zugriff auf das Verwaltungskonto von AWS Organizations haben und APIs möglicherweise auch berechtigt sind, diese Benachrichtigungen zu deaktivieren. Wenn das Hauptproblem böswilliges Verhalten und nicht das versehentliche Löschen ist, sollten Sie erwägen, die durch dieses Muster erstellten Ressourcen mit einer IAM-Rechtegrenze zu schützen.
- Die API-Aufrufe beziehen `RemoveAccountFromOrganization` sich auf die Region USA Ost (Nord-Virginia) `CloseAccount` und werden dort verarbeitet (`us-east-1`). Daher müssen Sie diese Lösung einsetzen, `us-east-1` um die Ereignisse beobachten zu können.

Architektur

Zieltechnologie-Stack

- AWS Organizations
- AWS CloudTrail
- Amazon EventBridge
- AWS Lambda
- Amazon SNS

Zielarchitektur

Das folgende Diagramm zeigt die Lösungsarchitektur für dieses Muster.

1. AWS Organizations verarbeitet eine `CloseAccount` `RemoveAccountFromOrganization` Oder-Anfrage.
2. Amazon EventBridge ist in AWS integriert CloudTrail , um diese Ereignisse an den Standard-Event-Bus zu übertragen.
3. Eine benutzerdefinierte EventBridge Amazon-Regel entspricht den Anfragen von AWS Organizations und ruft eine AWS-Lambda-Funktion auf.
4. Die Lambda-Funktion übermittelt eine Nachricht zu einem SNS-Thema, die Benutzer abonnieren können, um E-Mail-Benachrichtigungen oder die weitere Verarbeitung zu erhalten.

5. Wenn Slack-Benachrichtigungen aktiviert sind, übermittelt die Lambda-Funktion eine Nachricht an einen Slack-Webhook.

Tools

AWS-Services

- AWS CloudFormation bietet die Möglichkeit, eine Sammlung verwandter AWS- und Drittanbieter-Ressourcen zu modellieren, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus zu verwalten, indem Infrastruktur als Code behandelt wird.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen verbinden können. EventBridge empfängt ein Ereignis, ein Indikator für eine Änderung der Umgebung, und wendet eine Regel an, um das Ereignis an ein Ziel weiterzuleiten. Regeln ordnen Ereignisse Zielen entweder auf der Grundlage der Struktur des Ereignisses, eines so genannten Ereignismusters, oder anhand eines Zeitplans zu.
- AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch, von wenigen Anfragen pro Tag bis hin zu Tausenden pro Sekunde. Sie zahlen nur für die tatsächlich konsumierte Zeit. Es werden keine Gebühren berechnet, solange Ihr Code nicht ausgeführt wird.
- AWS Organizations hilft Ihnen dabei, Ihre Umgebung zentral zu verwalten und zu steuern, während Sie Ihre AWS-Ressourcen erweitern und skalieren. Mit AWS Organizations können Sie programmgesteuert neue AWS-Konten erstellen und Ressourcen zuweisen, Konten gruppieren, um Ihre Workflows zu organisieren, Richtlinien auf Konten oder Gruppen zur Verwaltung anwenden und die Abrechnung vereinfachen, indem Sie eine einzige Zahlungsmethode für alle Ihre Konten verwenden.
- AWS CloudTrail überwacht und zeichnet Kontoaktivitäten in Ihrer gesamten AWS-Infrastruktur auf und gibt Ihnen die Kontrolle über Speicher-, Analyse- und Behebungsmaßnahmen.
- Amazon Simple Notification Service (Amazon SNS) ist ein vollständig verwalteter Messaging-Dienst für die Kommunikation sowohl application-to-application (A2A) als auch application-to-person (A2P).

Andere Tools

- Die Bibliothek AWS Lambda Powertools for Python besteht aus einer Reihe von Dienstprogrammen, die Funktionen zur Ablaufverfolgung, Protokollierung, Metriken und Ereignisbehandlung für Lambda-Funktionen bereitstellen.

Code

Der Code für dieses Muster befindet sich im GitHub AWS Account Closer Notifier-Repository.

Die Lösung umfasst eine CloudFormation Vorlage, die die Architektur für dieses Muster bereitstellt. Es verwendet die AWS Lambda Powertools for Python-Bibliothek, um Protokollierung und Tracing bereitzustellen.

Epen

Stellen Sie die Architektur bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die CloudFormation Vorlage für den Lösungsstapel.	Die CloudFormation Vorlage für dieses Muster befindet sich im Hauptzweig des GitHub Repositorys. Es stellt die IAM-Rollen, EventBridge Regeln, Lambda-Funktionen und das SNS-Thema bereit. Um die Vorlage zu starten: 1. Klonen Sie das GitHub Repository, um eine Kopie des Lösungscodes zu erhalten. 2. Öffnen Sie die AWS-Management konsole für das Verwaltungskonto von AWS Organizations. 3. Wählen Sie die Region USA Ost (Nord-Virginia) (`us-`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`east-1`) aus und öffnen Sie dann die CloudFormation Konsole. 4. Erstellen Sie den Stack, indem Sie die `account-closure-notifier.yml` Vorlage verwenden und die folgenden Werte angeben: • Stackname: `aws-account-closure-notifier-stack` • `ResourcePrefix` Parameter: `aws-account-closure-notifier` • `SlackNotification` Parameter: Wenn Slack-Benachrichtigungen erforderlich sind, ändere diese Einstellung in `true`. • `SlackWebhookEndpoint` Parameter: Wenn Slack-Benachrichtigungen erforderlich sind, gib die Webhook-URL an. Weitere Informationen zum Starten eines CloudFormation Stacks finden Sie in der AWS-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die Lösung erfolgreich gestartet wurde.	1. Warten Sie, bis der CloudFormation Stack den Status CREATE_COMPLETE erreicht hat. 2. Öffnen Sie die EventBridge Konsole in. `us-east-1` 3. Stellen Sie sicher, dass eine neue Regel mit dem Namen erstellt wurde`aws-account-closure-notifier-event-rule` .	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Abonnieren Sie das SNS-Thema.	(Optional) Wenn Sie das SNS-Thema abonnieren möchten: 1. Öffnen Sie die Amazon SNS SNS-Konsole in `us-east-1` und suchen Sie das Thema mit dem Namen `aws-account-closure-notifier-sns-topic` . 2. Wählen Sie den Namen des Themas und dann Abonnement erstellen. 3. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus. 4. Geben Sie für Endpoint die E-Mail-Adresse an, an die die Benachrichtigung gesendet werden soll, und wählen Sie dann Abonnement erstellen aus. 5. Suchen Sie in Ihrem E-Mail-Posteingang nach einer Nachricht von AWS Notifications. Verwenden Sie den Link in dieser E-Mail, um das Abonnement zu bestätigen. Weitere Informationen zum Einrichten von SNS-Benac hrichtigungen finden Sie in der	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Amazon SNS SNS-Dokumentation.	

Überprüfen Sie die Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sendet ein Testereignis an den Standard-Event-Bus.	Das GitHub Repository stellt ein Beispielereignis bereit, das Sie zu Testzwecken an den EventBridge Standard-Event-Bus senden können. Die EventBridge Regel reagiert auch auf Ereignisse, die die benutzerdefinierte Ereignisquelle verwenden `account.closure.notifier` . **Note** Sie können die CloudTrail Ereignisquelle nicht verwenden, um dieses Ereignis zu senden, da es nicht möglich ist, ein Ereignis als AWS-Service zu senden. Um ein Testereignis zu senden: 1. Öffnen Sie die EventBridge Konsole in `us-east-1` .	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie im Navigationsbereich unter Busse die Option Event-Busse und dann den Standard-Event-Bus aus. 3. Wählen Sie Ereignisse senden aus. 4. Geben Sie als Quelle des Ereignisses ein `account.closure.notifier` . 5. Geben Sie für Detailtyp `AWS API Call via CloudTrail` ein. 6. Kopieren Sie für Ereignisdetails den Inhalt von `tests/dummy-event.json` aus dem GitHub Repository und fügen Sie ihn in das Textfeld ein. 7. Wählen Sie Senden, um den Benachrichtigungs-Workflow zu starten.	
Stellen Sie sicher, dass die E-Mail-Benachrichtigung empfangen wurde.	Suchen Sie in dem Postfach, das das SNS-Thema abonniert hat, nach Benachrichtigungen. Sie sollten eine E-Mail mit Informationen zu dem Konto, das geschlossen wurde, und zum Principal, der den API-Aufruf durchgeführt hat, erhalten.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vergewissere dich, dass die Slack-Benachrichtigung empfangen wurde.	(Optional) Wenn du bei der Bereitstellung der CloudFormation Vorlage eine Webhook-URL für den `SlackWebhookEndpoint` Parameter angegeben hast, überprüfe den Slack-Kanal, der dem Webhook zugeordnet ist. Es sollte eine Meldung mit Details zu dem Konto, das geschlossen wurde, und zum Principal, der den API-Aufruf durchgeführt hat, angezeigt werden.	AWS-Administrator

Zugehörige Ressourcen

- CloseAccount Aktion (API-Referenz für AWS Organizations)
- RemoveAccountFromOrganization Aktion (API-Referenz für AWS Organizations)
- AWS Lambda Powertools für Python

EBS-Snapshot-Details für Ihr AWS-Konto oder Ihre Organisation anzeigen

Erstellt von Arun Chandapillai (AWS) und Parag Nagwekar (AWS)

Übersicht

Dieses Muster beschreibt, wie Sie automatisch einen On-Demand-Bericht über alle Amazon Elastic Block Store (Amazon EBS) -Snapshots in Ihrem Amazon Web Services (AWS) -Konto oder Ihrer Organisationseinheit (OU) in AWS Organizations generieren können.

Amazon EBS ist ein skalierbarer easy-to-use, leistungsstarker Blockspeicherservice, der für Amazon Elastic Compute Cloud (Amazon EC2) entwickelt wurde. Ein EBS-Volume bietet dauerhaften und persistenten Speicher, den Sie an Ihre EC2 Instances anhängen können. Sie können EBS-Volumes als Primärspeicher für Ihre Daten verwenden und eine point-in-time Sicherungskopie Ihrer EBS-Volumes erstellen, indem Sie einen Snapshot erstellen. Sie können die AWS-Managementkonsole oder die AWS-Befehlszeilenschnittstelle (AWS CLI) verwenden, um die Details bestimmter EBS-Snapshots anzuzeigen. Dieses Muster bietet eine programmatische Methode zum Abrufen von Informationen über alle EBS-Snapshots in Ihrem AWS-Konto oder Ihrer Organisationseinheit.

Sie können das in diesem Muster bereitgestellte Skript verwenden, um eine Datei mit kommagetrennten Werten (CSV) zu generieren, die die folgenden Informationen zu jedem Snapshot enthält: Konto-ID, Snapshot-ID, Volume-ID und -Größe, Datum, an dem der Snapshot aufgenommen wurde, Instance-ID und Beschreibung. Wenn Ihre EBS-Snapshots markiert sind, enthält der Bericht auch die Eigentümer- und Teamattribute.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS CLI Version 2 installiert und konfiguriert
- Rolle AWS Identity and Access Management (IAM) mit den entsprechenden Berechtigungen (Zugriffsberechtigungen für ein bestimmtes Konto oder für alle Konten in einer Organisationseinheit, wenn Sie planen, das Skript von AWS Organizations aus auszuführen)

Architektur

Das folgende Diagramm zeigt den Skript-Workflow, der einen On-Demand-Bericht über EBS-Snapshots generiert, die auf mehrere AWS-Konten in einer Organisationseinheit verteilt sind.

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Amazon Elastic Block Store (Amazon EBS) bietet Speichervolumes auf Blockebene zur Verwendung mit Instances. EC2
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten.

Code

Der Code für die in diesem Muster verwendete Beispielanwendung ist im aws-ebs-snapshots-awsorganizationsRepository verfügbar. GitHub Folgen Sie den Anweisungen im nächsten Abschnitt, um die Beispieldateien zu verwenden.

Epen

Laden Sie das Skript herunter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das Python-Skript herunter.	Laden Sie das Skript GetSnapshotDetailsAllAccountsOU.py aus dem GitHub Repository herunter.	Allgemeines AWS

EBS-Snapshot-Details für ein AWS-Konto abrufen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Führen Sie das Python-Skript aus.	Führen Sie den Befehl aus:
	`python3 getsnapshotinfo.py --file <output-file>.csv --region <region-name>`
	wobei `<output-file>` sich auf die CSV-Ausgabedatei bezieht, in der Sie Informationen zu den platzierten EBS-Snapshots abrufen möchten, und `<region-name>` ist die AWS-Region, in der die Snapshots gespeichert werden. Zum Beispiel:
	`python3 getsnapshotinfo.py --file snapshots.csv --region us-east-1`
		Allgemeines AWS

Rufen Sie EBS-Snapshot-Details für eine Organisation ab

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das Python-Skript aus.	Führen Sie den Befehl aus: `python3 getsnapshotinfo.py --file <output-file>.csv --role <IAM-role> --region <region-name>`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wobei `<output-file>` sich auf die CSV-Ausgabedatei bezieht, in der Sie Informationen zu den platzierten EBS-Snapshots abrufen möchten, `<IAM-role>` ist eine Rolle, die Berechtigungen für den Zugriff auf AWS Organizations bereitstellt, und `<region-name>` ist die AWS-Region, in der die Snapshots gespeichert werden. Zum Beispiel: `python3 getsnapshotinfo.py --file snapshots.csv --role <IAM role> --region us-west-2`	

Zugehörige Ressourcen

- Amazon EBS-Dokumentation
- Amazon EBS-Aktionen
- Amazon EBS API-Referenz
- Verbesserung der Leistung von Amazon EBS
- Amazon EBS-Ressourcen
- EBS-Snapshot-Preise

Zusätzliche Informationen

EBS-Snapshot-Typen

Amazon EBS bietet je nach Besitz und Zugriff drei Arten von Snapshots:

- Gehört Ihnen — Standardmäßig können nur Sie Volumes aus Snapshots erstellen, die Sie besitzen.
- Öffentliche Snapshots — Sie können Snapshots öffentlich mit allen anderen AWS-Konten teilen. Um einen öffentlichen Snapshot zu erstellen, ändern Sie die Berechtigungen für einen Snapshot, um ihn für die von Ihnen angegebenen AWS-Konten freizugeben. Benutzer, die Sie autorisieren, können dann die von Ihnen geteilten Snapshots verwenden, indem sie ihre eigenen EBS-Volumes erstellen. Ihr ursprünglicher Snapshot bleibt davon unberührt. Sie können Ihre unverschlüsselten Snapshots auch allen AWS-Benutzern öffentlich zugänglich machen. Aus Sicherheitsgründen können Sie Ihre verschlüsselten Snapshots jedoch nicht öffentlich zugänglich machen. Öffentliche Schnappschüsse stellen ein erhebliches Sicherheitsrisiko dar, da persönliche und sensible Daten offengelegt werden können. Wir empfehlen dringend, Ihre EBS-Snapshots nicht mit allen AWS-Konten zu teilen. Weitere Informationen zum Teilen von Snapshots finden Sie in der AWS-Dokumentation.
- Private Snapshots — Sie können Snapshots privat mit einzelnen AWS-Konten teilen, die Sie angeben. Um den Snapshot privat mit bestimmten AWS-Konten zu teilen, folgen Sie den Anweisungen in der AWS-Dokumentation und wählen Sie Privat für die Berechtigungseinstellung. Benutzer, die Sie autorisiert haben, können die von Ihnen freigegebenen Snapshots zur Erstellung ihrer eigenen EBS-Volumes verwenden, während Ihr Original-Snapshot davon unberührt bleibt.

Übersichten und Verfahren

Die folgende Tabelle enthält Links zu weiteren Informationen über EBS-Snapshots, einschließlich Informationen dazu, wie Sie die EBS-Volumenkosten senken können, indem Sie unbenutzte Snapshots suchen und löschen und selten aufgerufene Snapshots archivieren, auf die selten zugegriffen wird und die nicht häufig oder schnell abgerufen werden müssen.

Für Informationen über	See
Schnappschüsse, ihre Funktionen und Einschränkungen	Amazon EBS-Snapshots erstellen
Wie erstelle ich einen Snapshot	Konsole: Erstellen Sie einen Snapshot AWS-CLI: Befehl create-snapshot Zum Beispiel:

```
aws ec2 create-snapshot --volume-id
 vol-1234567890abcdef0 --description
 " volume snapshot"
```

Löschen von Snapshots (allgemeine Informationen)	Löschen Sie einen Amazon EBS-Snapshot
Wie lösche ich einen Snapshot	Konsole: Löscht einen Snapshot AWS-CLI: Befehl delete-snapshot Zum Beispiel:

```
aws ec2 delete-snapshot --snapshot-id
 snap-1234567890abcdef0
```

Archivieren von Snapshots (allgemeine Informationen)	Amazon EBS-Snapshots archivieren Amazon EBS-Snapshot-Archiv (Blogbeitrag)
Wie archiviere ich einen Snapshot	Konsole: Archivieren Sie einen Snapshot AWS CLI: modify-snapshot-tier Befehl
Wie rufe ich einen archivierten Snapshot ab	Konsole: Stellen Sie einen archivierten Snapshot wieder her AWS CLI: restore-snapshot-tier Befehl
Preise für Snapshots	Amazon EBS-Preise

HÄUFIG GESTELLTE FRAGEN

Was ist der Mindestarchivierungszeitraum?

Der minimale Archivzeitraum beträgt 90 Tage.

Wie lange würde es dauern, einen archivierten Snapshot wiederherzustellen?

Je nach Größe des Snapshots kann es bis zu 72 Stunden dauern, bis ein archivierter Snapshot von der Archivstufe auf die Standardstufe wiederhergestellt wird.

Sind archivierte Snapshots vollständige Snapshots?

Archivierte Snapshots sind immer vollständige Snapshots.

Welche Snapshots kann ein Benutzer archivieren?

Sie können nur Snapshots archivieren, deren Eigentümer Sie in Ihrem Konto sind.

Können Sie einen Snapshot des Root-Geräte-Volumes eines registrierten Amazon Machine Image (AMI) archivieren?

Nein, Sie können keinen Snapshot des Root-Geräte-Volumes eines registrierten AMI archivieren.

Was sind Sicherheitsaspekte bei der gemeinsamen Nutzung eines Snapshots?

Wenn Sie einen Snapshot teilen, gewähren Sie anderen Zugriff auf alle Daten im Snapshot. Teilen Sie Snapshots nur mit Personen, denen Sie Ihre Daten anvertrauen.

Wie teilen Sie einen Snapshot mit einer anderen AWS-Region?

Snapshots sind auf die Region beschränkt, in der sie erstellt wurden. Um einen Snapshot in einer anderen Region freizugeben, kopieren Sie den Snapshot in die Region und geben dann die Kopie frei.

Können Sie verschlüsselte Snapshots teilen?

Sie können keine Snapshots teilen, die mit dem standardmäßigen verwalteten AWS-Schlüssel verschlüsselt sind. Sie können nur Snapshots teilen, die mit einem vom Kunden verwalteten Schlüssel verschlüsselt sind. Wenn Sie einen verschlüsselten Snapshot teilen, müssen Sie auch den vom Kunden verwalteten Schlüssel teilen, der zum Verschlüsseln des Snapshots verwendet wurde.

Was ist mit unverschlüsselten Snapshots?

Sie können unverschlüsselte Snapshots öffentlich teilen.

Mehr Muster

- Automatisieren Sie die Kontoerstellung mit dem Landing Zone Accelerator auf AWS
- Automatisieren Sie den AWS Infrastrukturbetrieb mithilfe von Amazon Bedrock
- Automatisieren Sie die AWS-Ressourcenbewertung
- Automatische Inventarisierung von AWS Ressourcen für mehrere Konten und Regionen
- Automatisieren Sie das AWS Service Catalog-Portfolio und die Produktbereitstellung mithilfe von AWS CDK
- Automatisieren Sie das dynamische Pipeline-Management für die Bereitstellung von Hotfix-Lösungen in Gitflow-Umgebungen mithilfe von und AWS Service CatalogAWS CodePipeline
- Automatisieren Sie die Erfassung und Visualisierung von benutzerdefinierten Amazon MWAA-Metriken auf Amazon Managed Grafana mithilfe von Terraform
- Automatisieren Sie Sicherheitsscans für kontoübergreifende Workloads mit Amazon Inspector und AWS Security Hub
- Automatisches Hinzufügen einer von AWS verwalteten Richtlinie für Systems Manager zu EC2 Instanzprofilen mithilfe von Cloud Custodian und AWS CDK
- Automatisches Verschlüsseln vorhandener und neuer Amazon EBS-Volumes
- Zentralisieren Sie die Überwachung mithilfe von Amazon CloudWatch Observability Access Manager
- EC2 Instances beim Start auf obligatorische Tags überprüfen
- Bereinigen Sie die Ressourcen von AWS Account Factory for Terraform (AFT) nach dem Verlust von Statusdateien sicher
- Konfigurieren Sie die Protokollierung und Überwachung von Sicherheitsereignissen in Ihrer AWS IoT Umgebung
- Erstellen Sie eine Amazon ECS-Aufgabendefinition und mounten Sie mithilfe von Amazon EFS ein Dateisystem auf EC2 Instances
- Erstellen Sie AWS Config benutzerdefinierte Regeln mithilfe von AWS CloudFormation Guard Richtlinien
- Passen Sie Standardrollennamen mithilfe von AWS CDK Aspekten und Escape-Schraffuren an
- Löschen Sie ungenutzte Amazon EBS-Volumes mit AWS Config und AWS Systems Manager
- Implementieren und verwalten Sie AWS Control Tower Kontrollen mithilfe von AWS CDK und CloudFormation
- Stellen Sie AWS Control Tower Kontrollen mithilfe von Terraform bereit und verwalten Sie sie

- Stellen Sie mithilfe von AWS CodePipeline, AWS und AWS Code in mehreren CodeCommit AWS-Regionen bereit CodeBuild
- Aktivieren Sie Amazon GuardDuty unter bestimmten Bedingungen mithilfe von Vorlagen AWS CloudFormation
- Exportieren Sie einen Bericht über AWS IAM Identity Center-Identitäten und deren Zuweisungen mithilfe von PowerShell
- Generieren Sie mithilfe von Troposphere eine CloudFormation AWS-Vorlage, die von AWS Config verwaltete Regeln enthält
- Geben Sie SageMaker Notebook-Instances temporären Zugriff auf ein CodeCommit Repository in einem anderen AWS-Konto
- Integrieren Sie den Stonebranch Universal Controller in die AWS-Mainframe-Modernisierung
- Starten Sie mithilfe von Step Functions und einer Lambda-Proxyfunktion ein CodeBuild Projekt für alle AWS-Konten
- Migrieren Sie Windows-SSL-Zertifikate mithilfe von ACM zu einem Application Load Balancer
- IAM-Root-Benutzeraktivitäten überwachen
- Optimieren Sie serverlose Bereitstellungen mit mehreren Konten mithilfe der AWS CDK Workflows und Aktionen GitHub
- Führen Sie benutzerdefinierte Aktionen aus CodeCommit AWS-Ereignissen durch
- Beibehaltung von routingfähigem IP-Speicherplatz in VPC-Designs mit mehreren Konten für Subnetze ohne Arbeitslast
- Stellen Sie IAM-Rollen mit den geringsten Rechten bereit, indem Sie eine Rollenautomatenlösung bereitstellen
- Registrieren Sie mehrere AWS-Konten mit einer einzigen E-Mail-Adresse mithilfe von Amazon SES
- Entfernen Sie EC2 Amazon-Einträge AWS Managed Microsoft AD mithilfe AWS-Konten von AWS Lambda Automatisierung
- Entfernen Sie EC2 Amazon-Einträge in derselben AWS-Konto Form AWS Managed Microsoft AD mithilfe von AWS Lambda Automatisierung
- Datenbankanmeldedaten rotieren, ohne Container neu zu starten
- Führen Sie ereignisgesteuerte und geplante Workloads in großem Umfang mit AWS Fargate aus
- Senden Sie Benachrichtigungen für eine Amazon RDS for SQL Server Server-Datenbank-Instance mithilfe eines lokalen SMTP-Servers und Datenbank-E-Mail
- Richten Sie ein Grafana-Monitoring-Dashboard für AWS ein ParallelCluster

- Richten Sie mithilfe von Terraform eine zentrale Protokollierung auf Unternehmensebene ein
- Automatisches Taggen Transit Gateway Gateway-Anhängen mithilfe von AWS Organizations
- Verwenden Sie BMC Discovery-Abfragen, um Migrationsdaten für die Migrationsplanung zu extrahieren
- Überprüfen Sie betriebliche Best Practices für PCI DSS 4.0 mithilfe von AWS Config
- Visualisieren Sie IAM-Anmeldedaten für alle AWS-Konten mithilfe von Amazon QuickSight

Nachrichtenübermittlung und Kommunikation

Themen

- Automatisieren Sie die RabbitMQ-Konfiguration in Amazon MQ
- Verbessern Sie die Anrufqualität auf den Agentenarbeitsplätzen in Amazon Connect Connect-Kontaktzentren
- Mehr Muster

Automatisieren Sie die RabbitMQ-Konfiguration in Amazon MQ

Erstellt von Yogesh Bhatia (AWS) und Afroz Khan (AWS)

Übersicht

Amazon MQ ist ein verwalteter Message Broker-Service, der Kompatibilität mit vielen gängigen Message Brokern bietet. Die Verwendung von Amazon MQ mit RabbitMQ bietet einen robusten RabbitMQ-Cluster, der in der Amazon Web Services (AWS) -Cloud mit mehreren Brokern und Konfigurationsoptionen verwaltet wird. Amazon MQ bietet eine hochverfügbare, sichere und skalierbare Infrastruktur und kann problemlos eine große Anzahl von Nachrichten pro Sekunde verarbeiten. Mehrere Anwendungen können die Infrastruktur mit unterschiedlichen virtuellen Hosts, Warteschlangen und Exchanges nutzen. Die Verwaltung dieser Konfigurationsoptionen oder die manuelle Erstellung der Infrastruktur kann jedoch Zeit und Mühe erfordern. Dieses Muster beschreibt eine Möglichkeit, Konfigurationen für RabbitMQ in einem Schritt über eine einzige Datei zu verwalten. Sie können den mit diesem Muster bereitgestellten Code in jedes Continuous Integration (CI) -Tool wie Jenkins oder Bamboo einbetten.

Du kannst dieses Muster verwenden, um jeden RabbitMQ-Cluster zu konfigurieren. Alles, was es benötigt, ist Konnektivität zum Cluster. Obwohl es viele andere Möglichkeiten gibt, RabbitMQ-Konfigurationen zu verwalten, erstellt diese Lösung ganze Anwendungskonfigurationen in einem Schritt, sodass Sie Warteschlangen und andere Details einfach verwalten können.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Die AWS-Befehlszeilenschnittstelle (AWS CLI) wurde so installiert und konfiguriert, dass sie auf Ihr AWS-Konto verweist (Anweisungen finden Sie in der AWS-CLI-Dokumentation)
- Ansible ist installiert, sodass Sie Playbooks ausführen können, um die Konfiguration zu erstellen
- rabbitmqadmin ist installiert (Anweisungen finden Sie in der RabbitMQ-Dokumentation)
- Ein RabbitMQ-Cluster in Amazon MQ, erstellt mit gesunden Amazon-Metriken CloudWatch

Zusätzliche Anforderungen

- Stellen Sie sicher, dass Sie die Konfigurationen für virtuelle Hosts und Benutzer separat und nicht als Teil von JSON erstellen.

- Stellen Sie sicher, dass das Konfigurations-JSON Teil des Repositorys ist und versionsgesteuert ist.
- Die Version der rabbitmqadmin-CLI muss mit der Version des RabbitMQ-Servers identisch sein, daher ist es am besten, die CLI von der RabbitMQ-Konsole herunterzuladen.
- Stellen Sie im Rahmen der Pipeline sicher, dass die JSON-Syntax vor jedem Lauf validiert wird.

Produktversionen

- AWS-CLI Version 2.0
- Ansible Version 2.9.13
- rabbitmqadmin Version 3.9.13 (muss mit der RabbitMQ-Serverversion identisch sein)

Architektur

Quelltechnologie-Stack

- Ein RabbitMQ-Cluster, der auf einer vorhandenen lokalen virtuellen Maschine (VM) oder einem Kubernetes-Cluster (vor Ort oder in der Cloud) ausgeführt wird

Zieltechnologie-Stack

- Automatisierte RabbitMQ-Konfigurationen auf Amazon MQ für RabbitMQ

Zielarchitektur

Es gibt viele Möglichkeiten, RabbitMQ zu konfigurieren. Dieses Muster verwendet die Importkonfigurationsfunktion, bei der eine einzelne JSON-Datei alle Konfigurationen enthält. Diese Datei wendet alle Einstellungen an und kann von einem Versionskontrollsystem wie Bitbucket oder Git verwaltet werden. Dieses Muster verwendet Ansible, um die Konfiguration über die rabbitmqadmin-CLI zu implementieren.

Tools

Tools

- rabbitmqadmin ist ein Befehlszeilentool für die HTTP-basierte RabbitMQ-API. Es wird zur Verwaltung und Überwachung von RabbitMQ-Knoten und -Clustern verwendet.
- Ansible ist ein Open-Source-Tool zur Automatisierung von Anwendungen und IT-Infrastruktur.
- Mit AWS CLI können Sie mithilfe von Befehlen in einer Befehlszeilen-Shell mit AWS-Services interagieren.

AWS-Services

- Amazon MQ ist ein verwalteter Message Broker-Service, der es einfach macht, Message Broker in der Cloud einzurichten und zu betreiben.
- AWS CloudFormation hilft Ihnen dabei, Ihre AWS-Infrastruktur einzurichten und die Cloud-Bereitstellung mit Infrastruktur als Code zu beschleunigen.

Code

Die in diesem Muster verwendete JSON-Konfigurationsdatei und ein Beispiel für ein Ansible-Playbook sind im Anhang enthalten.

Epen

Erstellen Sie Ihre AWS-Infrastruktur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen RabbitMQ-Cluster auf AWS.	Wenn Sie noch keinen RabbitMQ-Cluster haben, können Sie AWS verwenden , um den Stack CloudForm ation auf AWS zu erstellen . Oder Sie können das Cloudformation-Modul in Ansible verwenden, um den Stack zu erstellen. Bei letzterem Ansatz können Sie Ansible für beide Aufgaben verwenden: zum Erstellen der RabbitMQ-Infrastruktur und	AWS CloudFormation, Ansible

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zum Verwalten von Konfigura tionen.	

Erstellen Sie die Konfiguration von Amazon MQ für RabbitMQ

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Eigenscha ftendatei.	Laden Sie die JSON-Konf igurationsdatei (`rabbitmqc onfig.json`) im Anhang herunter oder exportieren Sie sie aus der RabbitMQ-Konsole. Ändern Sie sie, um Warteschlangen, Austausch e und Bindungen zu konfiguri eren. Diese Konfigura tionsdatei zeigt Folgendes: - Erzeugt zwei Warteschl angen: `sample-queue1` und `sample-queue2` - Erzeugt zwei Börsen: `sample-exchange1` und `sample-exchange2` - Implementiert die Bindung zwischen den Warteschlangen und den Börsen Diese Konfigurationen werden gemäß den Anforderungen von rabbitmqadmin unter dem virtuellen Root-Host (/) ausgeführt.	JSON

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie die Details der Amazon MQ for RabbitMQ-Infrastruktur ab.	Rufen Sie die folgenden Details für die RabbitMQ-Infrastruktur auf AWS ab: • Broker-Name • RabbitMQ-Host • RabbitMQ-Benutzername (der Administratorbenutzer, der bei der Clustererstellung erstellt wurde) • RabbitMQ-Passwort Sie können die AWS-Manag ementkonsole oder die AWS-CLI verwenden, um diese Informationen abzurufen. Diese Details ermöglichen es dem Ansible-Playbook, eine Verbindung zu Ihrem AWS-Konto herzustellen und den RabbitMQ-Cluster zum Ausführen von Befehlen zu verwenden. ⚠ Important Der Computer, auf dem das Ansible-P laybook ausgeführ t wird, muss auf Ihr AWS-Konto zugreifen können, und die AWS-CLI muss bereits konfiguriert sein,	AWS-CLI, Amazon MQ

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wie im Abschnitt Voraussetzungen beschrieben.	

Erstellen Sie die Datei hosts_var.	Erstellen Sie die `hosts_var` Datei für Ansible und stellen Sie sicher, dass alle Variablen in der Datei definiert sind. Erwägen Sie, Ansible Vault zum Speichern des Passworts zu verwenden. Sie können die `hosts_var` Datei wie folgt konfigurieren (ersetzen Sie die Sternchen durch Ihre Informationen):
	`RABBITMQ_HOST: "**********.mq.us-east-2.amazonaws.com"`
	`RABBITMQ_VHOST: "/"`
	`RABBITMQ_USERNAME: "admin"`
	`RABBITMQ_PASSWORD: "*******"`
		Ansible

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Ansible-P laybook.	Ein Beispiel-Playbook finden Sie `ansible-rabbit-config.yaml` im Anhang. Laden Sie diese Datei herunter und speichern Sie sie. Das Ansible-Playbook importiert und verwaltet alle RabbitMQ-Konfigura tionen, wie Warteschlangen, Exchanges und Bindungen, die Anwendungen benötigen. Folgen Sie den bewährten Methoden für Ansible-P laybooks, z. B. zum Sichern von Passwörtern. Verwenden Sie Ansible Vault für die Passwortverschlüsselung und rufen Sie das RabbitMQ-Passwort aus der verschlüs selten Datei ab.	Ansible

Bereitstellen der Konfiguration

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das Playbook aus.	Führen Sie das Ansible-Playbook aus, das Sie im vorherigen Epos erstellt haben. `ansible-playbook ansible-rabbit-con fig.yaml`	RabbitMQ, Amazon MQ, Ansible

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie können die neuen Konfigurationen auf der RabbitMQ-Konsole überprüfen.	

Zugehörige Ressourcen

- Migration von RabbitMQ zu Amazon MQ (AWS-Blogbeitrag)
- Management-Befehlszeilentool (RabbitMQ-Dokumentation)
- Einen CloudFormation AWS-Stack erstellen oder löschen (Ansible-Dokumentation)
- Migration nachrichtengesteuerter Anwendungen zu Amazon MQ für RabbitMQ (AWS-Blogbeitrag)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Verbessern Sie die Anrufqualität auf den Agentenarbeitsplätzen in Amazon Connect Connect-Kontaktzentren

Erstellt von Ernest Ozdoba (AWS)

Übersicht

Probleme mit der Anrufqualität gehören zu den am schwierigsten zu behebenden Problemen in Kontaktzentren. Um Probleme mit der Sprachqualität und komplexe Verfahren zur Fehlerbehebung zu vermeiden, müssen Sie die Arbeitsumgebung und die Workstation-Einstellungen Ihrer Agenten optimieren. Dieses Muster beschreibt Techniken zur Optimierung der Sprachqualität für Agentenarbeitsplätze in Amazon Connect Connect-Kontaktzentren. Es enthält Empfehlungen in den folgenden Bereichen:

- Anpassungen der Arbeitsumgebung. Die Umgebung der Agenten hat keinen Einfluss darauf, wie Sprache über das Netzwerk übertragen wird, sie hat jedoch Auswirkungen auf die Anrufqualität.
- Einstellungen der Agenten-Workstation. Hardware- und Netzwerkkonfigurationen für Contact-Center-Workstations haben erhebliche Auswirkungen auf die Anrufqualität.
- Browser-Einstellungen. Agenten verwenden einen Webbrowser, um auf die Amazon Connect Contact Control Panel (CCP) -Website zuzugreifen und mit Kunden zu kommunizieren, sodass die Browsereinstellungen die Anrufqualität beeinflussen können.

Die folgenden Komponenten können sich ebenfalls auf die Anrufqualität auswirken, sie fallen jedoch nicht in den Zuständigkeitsbereich der Workstation und werden in diesem Muster nicht behandelt:

- Der Datenverkehr fließt über AWS Direct Connect, ein Full-Tunnel-VPN oder ein Split-Tunnel-VPN in die Amazon Web Services (AWS) -Cloud
- Netzwerkbedingungen bei der Arbeit in oder außerhalb der Unternehmenszentrale
- Konnektivität über ein öffentliches Telefonnetz (PSTN)
- Das Gerät und der Telefonanbieter des Kunden
- Einrichtung der virtuellen Desktop-Infrastruktur (VDI)

Weitere Informationen zu diesen Bereichen finden Sie in der Amazon Connect Connect-Dokumentation unter Häufig auftretende Probleme mit dem Contact Control Panel (CCP) und Verwenden des Endpoint Test Utility.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Headsets und Workstations müssen die im Amazon Connect Connect-Administratorhandbuch angegebenen Anforderungen erfüllen.

Einschränkungen

- Die Optimierungstechniken in diesem Muster beziehen sich auf die Sprachqualität von Softphones. Sie gelten nicht, wenn Sie Amazon Connect CCP im Tischtelefonmodus konfigurieren. Sie können jedoch den Tischtelefonmodus verwenden, wenn Ihr Softphone-Setup keine akzeptable Sprachqualität für den Anruf bietet.

Produktversionen

- Informationen zu unterstützten Browsern und Versionen finden Sie im Amazon Connect Connect-Administratorhandbuch.

Architektur

Dieses Muster ist architekturunabhängig, da es auf die Workstation-Einstellungen der Agenten abzielt. Wie das folgende Diagramm zeigt, wird der Sprachpfad vom Agenten zum Kunden durch das Headset, den Browser, das Betriebssystem, die Workstation-Hardware und das Netzwerk des Agenten beeinflusst.

In Amazon Connect Connect-Kontaktzentren wird die Audiokonnektivität des Benutzers mit WebRTC hergestellt. Die Sprache wird mit dem interaktiven Audiocodec Opus codiert und bei der Übertragung mit dem Secure Real-Time Transport Protocol (SRTP) verschlüsselt. Andere Netzwerkarchitekturen sind möglich, darunter VPN-, private WAN/LAN- und ISP-Netzwerke.

Tools

- Amazon Connect Endpoint Test Utility — Dieses Tool überprüft die Netzwerkkonnektivität und die Browsereinstellungen.
- Browserkonfigurationseditoren für WebRTC-Einstellungen:
  - Für Firefox: about:config

  - Für Chrome: chrome: //flags
- CCP Log Parser — Dieses Tool hilft Ihnen bei der Analyse von CCP-Protokollen zur Fehlerbehebung.

Epen

Passen Sie die Arbeitsumgebung an

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Reduzieren Sie Hintergrundgeräusche.	Vermeiden Sie laute Umgebungen. Wenn dies nicht möglich ist, optimieren Sie die Umgebung mit diesen Tipps zur Schalldämmung: • Absorbieren Sie Geräusche, indem Sie schallableitende Oberflächen wie Gardinen, Teppiche und Polstermöbel verwenden. • Blockieren Sie Lärm, indem Sie Barrieren zwischen den Schreibtischen platzieren. • Erwägen Sie eine aktive Geräuschunterdrückungslösung (ANC), z. B. einen Generator für weißes Rauschen, um die Konzentration zu fördern und die Privatsphäre zu schützen, oder verwenden Sie Headsets mit Geräuschminimierung. • Vermeiden Sie Echos bei Ihren Anrufen. Große, leere	Agent, Manager

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Räume können Echoeffekte erzeugen oder Geräusche verstärken. Das Abdecken von Oberflächen, auf denen Geräusche reflektiert werden können, trägt dazu bei, Echos zu reduzieren.	

Optimieren Sie die Workstation-Einstellungen für Agenten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie das richtige Headset.	• Wenn die Umgebung laut ist, wählen Sie ein Stereo-Headset. Wenn der Ton in beide Ohren geleitet wird, können sich die Agenten besser konzentrieren und den Kunden besser hören. Außerdem wird das allgemeine Geräusch reduziert, da es weniger wahrscheinlich ist, dass Agenten ihre Stimme erheben. • Vermeiden Sie die Verwendung von Lautsprechern oder integriertem Computeraudio. Verwenden Sie für optimale Qualität ein kabelgebundenes Headset, das speziell für die Nutzung im Contact Center vorgesehen ist. Drahtlose	Agent, Manager

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Headsets sind praktisch , können jedoch aufgrund von Funkstörungen und Transcodierung zu zusätzlic her Audioverzögerung und verminderter Audioqualität führen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie das Headset wie vorgesehen.	• Aktivieren Sie die aktiven Geräuschunterdrückungs- und Sprachverbesserungsfunktionen Ihres Headsets, sofern sie verfügbar sind. Suchen Sie nach Einstellungen wie ANC oder ANR. Anweisungen zur Aktivierung dieser Einstellungen finden Sie in der Bedienungsanleitung Ihres Headsets. • Stellen Sie Ihr Mikrofon so ein, dass Sie direkt in das Mikrofon sprechen können. Die beste Position für Ihr Mikrofon befindet sich direkt unter Ihrem Kinn. Eine korrekte Platzierung kann einen Unterschied von 10 Dezibel (dB) im Schallpegel bewirken. Bei den meisten Headsets können Sie den Mikrofonarm (Mikrofonarm) drehen oder beugen. Daher ist es wichtig, ihn beim Sprechen an der richtigen Stelle zu halten. • Einige Headsets sind mit mehreren Mikrofonen und fortschrittlichen Funktionen wie Voice Beamforming ausgestattet, mit deren Hilfe Sprache ohne Boom aufgenommen werden kann.	Kundendienstmitarbeiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Um sicherzustellen, dass Sie das Hauptmikrofon wie vom Hersteller vorgesehen verwenden, lesen Sie in der Bedienungsanleitung Ihres Geräts nach.	
Überprüfen Sie die Workstation-Ressourcen.	Stellen Sie sicher, dass die Computer Ihrer Agenten leistungsfähig sind. Wenn sie Anwendungen von Drittanbietern verwenden, die Ressourcen verbrauchen, erfüllen ihre Computer möglicherweise nicht die Hardware-Mindestanforderungen für die Ausführung von CCP. Wenn Agenten Probleme mit der Anrufqualität haben, stellen Sie sicher, dass sie über genügend Rechenleistung (CPU), Festplattenspeicher, Netzwerkbandbreite und Arbeitsspeicher für CCP verfügen. Agenten sollten alle nicht benötigten Anwendungen und Tabs schließen, um die Leistung und die Anrufqualität von CCP zu verbessern.	Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Soundeinstellungen des Betriebssystems.	Die Standardeinstellungen für Mikrofonpegel und Boost funktionieren normalerweise einwandfrei. Wenn Sie feststellen, dass die ausgehende Stimme leise ist oder das Mikrofon zu viel aufnimmt, kann es hilfreich sein, diese Einstellungen anzupassen. Die Mikrofoneinstellungen finden Sie in der System-Soundkonfiguration Ihres Computers (Sound, Eingabe unter macOS, Mikrofone igenschaften in Windows). Sie können über Systemtools oder Anwendungen von Drittanbietern auf erweiterte Einstellungen zugreifen, die sich auf die Sprachqualität auswirken können. Hier sind einige der Einstellungen, die Sie überprüfen können: • Samplerate — Dieser Wert bestimmt, wie oft der Ton pro Sekunde abgetastet wird. Die Standardeinstellung ist normalerweise 44 oder 48 Kilohertz (kHz). Der optimale Wert für Amazon Connect ist 48 kHz. Sie können Ihre Browsereinstellungen verwenden, um den Standardwert zu	Agent, Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	überschreiben. Weitere Informationen finden Sie im Abschnitt zur Fehlerbehebung im Amazon Connect Connect-Administratorhandbuch. • Verstärkung — Dieser Wert bestimmt, wie stark das Mikrofon den Ton verstärkt. Wenn Sie die Verstärkung erhöhen, nimmt Ihr Mikrofon möglicherweise mehr Hintergrundgeräusche auf. • Bittiefe — Dieser Wert für die digitale Auflösung beschreibt, wie viele Stufen der Schallamplitude erkannt werden. Je höher die Bittiefe, desto flüssiger klingt die Stimme. Viele herkömmliche Telefonnetzwerke verwenden jedoch den PCM-Standard (Pulscode modulation), der nur eine 8-Bit-Auflösung unterstützt. • Offener Schwellenwert — Dies ist die minimale Schallamplitude, die ein Mikrofon aufnimmt. Wenn Sie Probleme mit der Sprachqualität haben, versuchen Sie, diese Werte	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	auf ihre Standardeinstellungen zurückzusetzen, bevor Sie weitere Untersuchungen durchführen. Weitere Informationen zu diesen und anderen einstellbaren Einstellungen finden Sie im Handbuch Ihres Geräts.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie ein verkabeltes Netzwerk.	In der Regel weist kabelgebundenes Ethernet eine geringere Latenz auf, sodass es einfacher ist, die für die Sprachdatenübertragung erforderliche konsistente Übertragungsqualität bereitzustellen. Wir empfehlen mindestens 100 KB Bandbreite pro Anruf. • Wenn Mitarbeiter von zu Hause aus arbeiten, empfehlen wir eine kabelgebundene Verbindung über WLAN. Es sollte nicht länger als 150 Millisekunden dauern, bis Sie den Kunden hören. Sie können über das Amazon Connect Endpoint Test Utility auf den Latenztest von Amazon Connect zugreifen. Dieses Tool misst jedoch die Verzögerung vom Browser zu Amazon Connect Connect-Regionen, nicht zu Kunden. Die Empfehlung für eine einseitige Verzögerung von 150 Millisekunden verhindert, dass der Agent und der Kunde miteinander sprechen. Der Wert wird von Ende zu Ende gemessen,	Netzwerkadministrator, Agent

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und jedes Element führt zu einer Verzögerung, einschlie ßlich des Teils des Anrufs zwischen der Amazon Connect Connect-Region und dem Kunden. • Wenn Mitarbeiter vom Büro aus arbeiten, ist Unternehm ens-WLAN akzeptabel, solange die Parameter im empfohlenen Bereich liegen und der RTP-Verkehr (Real-Time Transport Protocol) Priorität hat.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Hardwaretreiber.	Wenn Sie ein USB-Headset oder ein anderes Headset mit eigener Firmware verwenden , empfehlen wir, es mit der neuesten Version auf dem neuesten Stand zu halten. Einfache Headsets, die einen AUX-Anschluss verwenden , verwenden das integrierte Audiogerät des Computers . Stellen Sie daher sicher, dass der Hardwaretreiber des Betriebssystems auf dem neuesten Stand ist. In seltenen Fällen kann ein Audiotreiber-Update zu Audioproblemen führen, sodass Sie es möglicherweise rückgängig machen müssen. Weitere Informationen zum Ändern der Firmware- und Treiberversionen finden Sie im Handbuch Ihres Geräts.	Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vermeiden Sie USB-Hubs und -Dongles.	Vermeiden Sie beim Anschließen Ihres Headsets zusätzliche Geräte wie Dongles, Port-Konverter, Hubs und Verlängerungskabel. Diese Geräte können die Anrufqualität beeinträchtigen. Connect Sie Ihr Gerät stattdessen direkt an den Anschluss Ihres Computers an.	Kundendienstmitarbeiter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die CCP-Protokolle.	Der CCP Log Parser bietet eine einfache Möglichkeit, Anwendungsprotokolle zu überprüfen. 1. Laden Sie die CCP-Protokolle nach einem Anruf herunter. 2. Öffnen Sie den CCP Log Parser. 3. Ziehen Sie die Protokolldatei per Drag-and-Drop, um das Protokoll zur Analyse hochzuladen. 4. Wenn das Protokoll analysiert wurde, wird standardmäßig die Registerkarte Snapshots & Logs ausgewählt. Wählen Sie den Tab Metriken daneben aus, um die Erkenntnisse zu überprüfen. 5. Überprüfen Sie im Abschnitt WebRTC Metrics — audio_input Folgendes: • Das Audiopegeldiagramm, um zu sehen, ob Ihr empfangener Audiopegel über 0 liegt. Dies zeigt an, dass Audio von Ihrem Anrufer empfangen wurde. • Das Paketdiagramm für alle verlorenen Pakete.	Agent (fortgeschrittene Fähigkeiten)

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wenn dieses Diagramm deutliche Zunahmen zeigt, wenden Sie sich an Ihr IT-Supportteam. 6. Überprüfen Sie im Abschnitt WebRTC Metrics — audio_output Folgendes: • Das Audiopegeldiagramm , um zu bestätigen, dass Audio von Ihrem Gerät gesendet wurde. • Das Diagramm „Pakete“. Wenn Sie einen Anstieg des Paketverlusts feststellen, melden Sie dies Ihrem IT-Suppor tteam. • Das Jitter-Puffer- und RTT-Diagramm. Werte für die Roundtrip Time (RTT) über 300 wirken sich auf das Anruferlebnis aus. Melden Sie diese Ihrem IT-Supportteam.	

Optimieren Sie die Browsereinstellungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Standard-WebRTC-Einstellungen wieder her.	WebRTC muss aktiviert sein, um Softphone-Anrufe mit CCP tätigen zu können. Wir empfehlen, die Standarde	Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	instellungen für WebRTC-be zogene Funktionen beizubeha lten. • In Chrome können Sie Flaggen setzen, indem Sie zur URL chrome: // flags navigieren. Geben Sie WebRTC in das Suchfeld ein, um nach Einstellu ngen zu suchen, die CCP beeinträchtigen können, und setzen Sie diese auf Standard. • Geben Sie in Firefox about:config in die Adresslei ste ein und geben Sie dann WebRTC in das Suchfeld auf der Konfigurationsseite ein. Nicht standardmäßige Einstellungen werden fett gedruckt und können auf Standard geändert werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Deaktivieren Sie Browserer weiterungen bei der Fehlerbeh ebung.	Einige Browsererweiterung en können die Anrufqualität beeinträchtigen oder sogar verhindern, dass Anrufe ordnungsgemäß verbunden werden. Verwenden Sie das Inkognito-Fenster oder den privaten Modus in Ihrem Browser und deaktivieren Sie alle Erweiterungen. Wenn das Problem dadurch behoben wird, überprüfen Sie Ihre Browsererweiterungen und suchen Sie nach verdächtigen Add-Ons, oder deaktivieren Sie sie einzeln.	Agent, Administrator
Überprüfen Sie die Samplerat e des Browsers.	Vergewissern Sie sich, dass Ihr Mikrofoneingang auf die optimale Abtastrate von 48 kHz eingestellt ist. Anweisung en finden Sie im Amazon Connect Connect-Administra torhandbuch.	Agent, Administrator

Zugehörige Ressourcen

Wenn Sie die Schritte in diesem Muster befolgt haben, aber immer noch Probleme mit der Anrufqualität haben, finden Sie in den folgenden Ressourcen Tipps zur Fehlerbehebung.

- Informieren Sie sich über häufig auftretende Probleme mit dem Contact Control Panel (CCP).
- Überprüfen Sie die Verbindung mit dem Endpoint Test Utility.
- Folgen Sie bei allen anderen Problemen der Anleitung zur Fehlerbehebung.

Wenn Ihre Fehlerbehebung und Anpassungen das Problem mit der Anrufqualität nicht lösen, liegt die Ursache möglicherweise außerhalb Ihrer Workstation. Wenden Sie sich für weitere Problembehebungen an Ihr IT-Supportteam.

Mehr Muster

- Zerlegen Sie Monolithen mithilfe von CQRS und Event Sourcing in Microservices
- Stellen Sie eine ChatOps Lösung zur Verwaltung von SAST-Scanergebnissen bereit, indem Sie Amazon Q Developer in Chat-Anwendungen verwenden, benutzerdefinierte Aktionen und AWS CloudFormation
- Integrieren Sie Amazon API Gateway mit Amazon SQS, um asynchrones REST zu handhaben APIs
- Registrieren Sie mehrere AWS-Konten mit einer einzigen E-Mail-Adresse mithilfe von Amazon SES
- Mithilfe von AWS Fargate können Sie nachrichtengesteuerte Workloads in großem Umfang ausführen
- Optimieren Sie die Entwicklung und Bereitstellung von Amazon Lex Lex-Bot mithilfe eines automatisierten Workflows

Sicherheit, Identität und Compliance

Themen

- Zugriff über eine ASP.NET Core-App mithilfe AWS-Services von Amazon Cognito Cognito-Identitätspools
- Authentifizieren Sie Microsoft SQL Server auf Amazon EC2 mithilfe von AWS Directory Service
- Automatisieren Sie die Reaktion auf Vorfälle und die Forensik
- Automatisieren Sie die Behebung von AWS Security Hub Standardergebnissen
- Automatisieren Sie Sicherheitsscans für kontoübergreifende Workloads mit Amazon Inspector und AWS Security Hub
- Automatische Prüfung von AWS Sicherheitsgruppen, die den Zugriff von öffentlichen IP-Adressen aus ermöglichen
- Automatisches Reaktivieren CloudTrail von AWS mithilfe einer benutzerdefinierten Behebungsregel in AWS Config
- Automatically remediate unencrypted Amazon RDS DB instances and clusters
- Automatische und skalierbare Rotation von IAM-Benutzerzugriffsschlüsseln mit AWS Organizations und AWS Secrets Manager
- Automatische Validierung und Bereitstellung von IAM-Richtlinien und -Rollen in einem AWS-Konto mithilfe CodePipeline von IAM Access Analyzer und AWS-Makros CloudFormation
- Bidirektionale Integration AWS Security Hub mit Jira-Software
- Erstellen Sie mit EC2 Image Builder und Terraform eine Pipeline für gehärtete Container-Images
- Zentralisieren Sie die Verwaltung von IAM-Zugriffsschlüsseln in AWS Organizations mithilfe von Terraform
- Suchen Sie in einer CloudFront Amazon-Distribution nach Zugriffsprotokollierung, HTTPS- und TLS-Version
- Suchen Sie in den Eingangsregeln für Sicherheitsgruppen nach Einzelhost-Netzwerkeinträgen für und IPv4 IPv6
- Wählen Sie einen Amazon Cognito Cognito-Authentifizierungsablauf für Unternehmensanwendungen
- Erstellen Sie AWS Config benutzerdefinierte Regeln mithilfe von AWS CloudFormation Guard Richtlinien

- Erstellen Sie einen konsolidierten Bericht mit den Sicherheitsergebnissen von Prowler aus mehreren AWS-Konten
- Löschen Sie ungenutzte Amazon EBS-Volumes mit AWS Config und AWS Systems Manager
- Implementieren und verwalten Sie AWS Control Tower Kontrollen mithilfe von AWS CDK und CloudFormation
- Stellen Sie AWS Control Tower Kontrollen mithilfe von Terraform bereit und verwalten Sie sie
- Stellen Sie eine Pipeline bereit, die Sicherheitsprobleme in mehreren Codeergebnissen gleichzeitig erkennt
- Stellen Sie detektivattributebasierte Zugriffskontrollen für öffentliche Subnetze bereit, indem Sie AWS Config
- Implementieren Sie präventive attributebasierte Zugriffskontrollen für öffentliche Subnetze
- Stellen Sie die Security Automations for AWS WAF Solution mithilfe von Terraform bereit
- Erkennen Sie Amazon RDS- und Aurora-Datenbank-Instances mit ablaufenden CA-Zertifikaten
- Dynamisches Generieren einer IAM-Richtlinie mit IAM Access Analyzer mithilfe von Step Functions
- Aktivieren Sie Amazon GuardDuty unter bestimmten Bedingungen mithilfe von Vorlagen AWS CloudFormation
- Aktivieren Sie die transparente Datenverschlüsselung in Amazon RDS for SQL Server
- Stellen Sie sicher, dass AWS-Load Balancer sichere Listener-Protokolle (HTTPS, SSL/TLS) verwenden
- Stellen Sie sicher, dass die Verschlüsselung für Amazon EMR-Daten im Ruhezustand beim Start aktiviert ist
- Stellen Sie sicher, dass ein IAM-Profil mit einer EC2 Instance verknüpft ist
- Stellen Sie sicher, dass ein Amazon Redshift Redshift-Cluster bei der Erstellung verschlüsselt ist
- Exportieren Sie einen Bericht über AWS IAM Identity Center-Identitäten und deren Zuweisungen mithilfe von PowerShell
- Überwachen und korrigieren Sie das geplante Löschen von AWS-KMS-Schlüsseln
- Identifizieren Sie öffentliche Amazon S3 S3-Buckets mithilfe AWS Organizations von Security Hub
- Erfassung und Analyse von AWS-Sicherheitsprotokollen in Microsoft Sentinel
- AWS Organizations Richtlinien mithilfe AWS CodePipeline von Amazon Bedrock als Code verwalten
- Verwalten Sie AWS IAM Identity Center Berechtigungssätze als Code, indem Sie AWS CodePipeline

- Anmeldeinformationen mit AWS Secrets Manager verwalten
- ElastiCache Cluster für Sicherheitsgruppen überwachen
- Überwachen Sie Amazon EMR-Cluster beim Start auf Verschlüsselung während der Übertragung
- ElastiCache Amazon-Cluster auf Verschlüsselung im Ruhezustand überwachen
- Überwachen Sie EC2 Instanzschlüsselpaare mit AWS Config
- IAM-Root-Benutzeraktivitäten überwachen
- Eine Benachrichtigung senden, wenn ein IAM-Benutzer erstellt wird
- Verhindern Sie den Internetzugang auf Kontoebene mithilfe einer Dienststeuerungsrichtlinie
- Beschränken Sie den Zugriff basierend auf IP-Adresse oder Geolokalisierung mithilfe von AWS WAF
- Scannen Sie Git-Repositorys mithilfe von Git-Secrets auf vertrauliche Informationen und Sicherheitsprobleme
- Benachrichtigungen von der AWS-Netzwerk-Firewall an einen Slack-Channel senden
- Vereinfachen Sie die Verwaltung privater Zertifikate mithilfe von AWS Private CA und AWS RAM
- Deaktivieren Sie die Sicherheitsstandardkontrollen für alle Security Hub Hub-Mitgliedskonten in einer Umgebung mit mehreren Konten
- Aktualisieren Sie die AWS-CLI-Anmeldeinformationen aus dem AWS IAM Identity Center mithilfe von PowerShell
- Verwenden Sie AWS Config, um die Sicherheitskonfigurationen von Amazon Redshift zu überwachen
- Verwenden Sie die Network Firewall, um die DNS-Domänennamen aus der Servernamenanzeige für ausgehenden Datenverkehr zu erfassen
- Verwenden Sie Terraform, um Amazon automatisch GuardDuty für eine Organisation zu aktivieren
- Überprüfen Sie betriebliche Best Practices für PCI DSS 4.0 mithilfe von AWS Config
- Stellen Sie sicher, dass für neue Amazon Redshift Redshift-Cluster SSL-Endpunkte erforderlich sind
- Stellen Sie sicher, dass neue Amazon Redshift Redshift-Cluster in einer VPC gestartet werden
- Mehr Muster

Zugriff über eine ASP.NET Core-App mithilfe AWS-Services von Amazon Cognito Cognito-Identitätspools

Erstellt von Bibhuti Sahu (AWS) und Marcelo Barbosa (AWS)

Übersicht

In diesem Muster wird beschrieben, wie Sie Amazon Cognito Cognito-Benutzerpools und Identitätspools konfigurieren und dann einer ASP.NET Core-App den Zugriff auf AWS Ressourcen nach erfolgreicher Authentifizierung ermöglichen können.

Amazon Cognito bietet Authentifizierung, Autorisierung und Benutzerverwaltung für Ihre Web- und mobilen Apps. Die beiden Hauptkomponenten von Amazon Cognito sind Benutzerpools und Identitätspools.

Ein Benutzerpool ist ein Benutzerverzeichnis in Amazon Cognito. Mit einem Benutzerpool können sich Ihre Benutzer über Amazon Cognito bei Ihrer Web- oder mobilen Anwendung anmelden. Ihre Benutzer können sich auch über soziale Identitätsanbieter wie Google, Facebook, Amazon oder Apple sowie über SAML-Identitätsanbieter anmelden.

Amazon-Cognito-Identitätspools (Verbundidentitäten) bieten Ihnen die Möglichkeit, eindeutige Identitäten für die Benutzer zu erstellen und diese mit Identitätsanbietern zu verbinden. Mit einem Identitätspool können Sie temporäre AWS Anmeldeinformationen mit eingeschränkten Rechten abrufen, um auf andere zuzugreifen. AWS-Services Bevor Sie mit der Nutzung Ihres neuen Amazon Cognito Cognito-Identitätspools beginnen können, müssen Sie eine oder mehrere Rollen AWS Identity and Access Management (IAM) zuweisen, um die Zugriffsebene zu bestimmen, die Ihre Anwendungsbenutzer auf Ihre AWS Ressourcen haben sollen. Identitäten-Pools definieren zwei Arten von Identitäten: authentifizierte und nicht authentifizierte. Jedem Identitätstyp kann eine eigene Rolle in IAM zugewiesen werden. Authentifizierte Identitäten gehören Benutzern, die von einem öffentlichen Anmeldeanbieter (Amazon Cognito Cognito-Benutzerpools, Facebook, Google, SAML oder einem beliebigen OpenID Connect-Anbieter) oder einem Entwickler-Anbieter (Ihr eigener Backend-Authentifizierungsprozess) authentifiziert wurden, wohingegen nicht authentifizierte Identitäten in der Regel Gastbenutzern gehören. Wenn Amazon Cognito eine Benutzeranfrage erhält, bestimmt der Service, ob die Anfrage authentifiziert oder nicht authentifiziert ist, bestimmt, welche Rolle diesem Authentifizierungstyp zugeordnet ist, und verwendet dann die dieser Rolle zugeordnete Richtlinie, um auf die Anfrage zu antworten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Und AWS-Konto mit Amazon Cognito- und IAM-Berechtigungen
- Zugriff auf die AWS Ressourcen, die Sie verwenden möchten
- ASP.NET Core 2.0.0 oder höher

Architektur

Technologie-Stack

- Amazon Cognito
- ASP.NET-Kern

Zielarchitektur

Tools

Tools, und SDKs AWS-Services

- Visual Studio oder Visual Studio Code
- Amazon. AspNetCore.Identity.Cognito (1.0.4) — Paket NuGet
- AWSSDK.S3 (3.3.110.32) — Paket NuGet
- Amazon Cognito

Code

Die angehängte ZIP-Datei enthält Beispieldateien, die Folgendes veranschaulichen:

- Wie rufe ich ein Zugriffstoken für den angemeldeten Benutzer ab
- Wie tausche ich ein Zugriffstoken gegen AWS Anmeldeinformationen aus
- So greifen Sie mit AWS Anmeldeinformationen auf den Amazon Simple Storage Service (Amazon S3) -Service zu

IAM-Rolle für authentifizierte Identitäten

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "mobileanalytics:PutEvents",
        "cognito-sync:*",
        "cognito-identity:*",
        "s3:ListAllMyBuckets*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Epen

Erstellen Sie einen Amazon Cognito Cognito-Benutzerpool

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Benutzerpool.	1. Melden Sie sich bei der Amazon Cognito Cognito-Konsole an AWS Management Console und öffnen Sie sie. 2. Wählen Sie Manage User Pools (Benutzerpools verwalten). 3. Wählen Sie in der rechten oberen Ecke der Seite Create a User Pool (Benutzerpool erstellen) aus.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Geben Sie einen Namen für Ihren Benutzerpool ein, wählen Sie Standardwerte überprüfen und anschließ end Pool erstellen aus. 5. Notieren Sie die Pool-ID.	
Fügen Sie einen App-Client hinzu.	Sie können eine App erstellen, um die integrierten Webseiten für die Registrierung und Anmeldung Ihrer Benutzer zu verwenden. 1. Wählen Sie in der Navigatio nsleiste auf der linken Seite der Benutzerpool-Seite unter Allgemeine Einstellu ngen die Option App-Clien ts und dann App-Client hinzufügen aus. 2. Geben Sie Ihrer App einen Namen und wählen Sie dann App-Client erstellen. 3. Notieren Sie sich die App-Client-ID und den geheimen Client-Schlüssel (wählen Sie „Details anzeigen“, um den geheimen Client-Sc hlüssel zu sehen).	Developer

Amazon-Cognito-Identitätspool erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen -Identitä tenpool.	1. Wählen Sie in der Amazon Cognito Cognito-Konsole Manage Identity Pools und dann Create new identity pool aus. 2. Geben Sie einen Namen für den Identitätspool ein. 3. Wenn Sie nicht authentif izierte Identitäten aktivieren möchten, wählen Sie diese Option im Abschnitt Nicht authentifizierte Identitäten aus. 4. Konfigurieren Sie im Abschnitt Authentifizierungs anbieter den Amazon Cognito Cognito-Identitäts pool, indem Sie die Benutzerpool-ID und die App-Client-ID festlegen und dann Create Pool wählen.	Developer
Weisen Sie IAM-Rollen für den Identitätspool zu.	Sie können die IAM-Rollen für authentifizierte und nicht authentifizierte Benutzer bearbeiten oder die Standarde instellungen beibehalten und dann Zulassen wählen. Für dieses Muster bearbeiten wir die authentifizierte IAM-Rolle und gewähren Zugriff für. `s3:ListAllMyBuckets`	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Beispielcode finden Sie weiter oben im Abschnitt Tools für die IAM-Rolle.	
Kopieren Sie die Identität spool-ID.	Wenn Sie im vorherigen Schritt Zulassen ausgewähl t haben, wird die Seite Erste Schritte mit Amazon Cognito angezeigt. Auf dieser Seite können Sie entweder die Identitätspool-ID aus dem Abschnitt AWS-Anmel deinformationen abrufen kopieren oder oben rechts Identitätspool bearbeiten auswählen und die Identität spool-ID aus dem angezeigten Bildschirm kopieren.	Developer

Konfigurieren Sie Ihre Beispiel-App

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie die ASP.NET Core-Beispiel-Web-App.	1. Klonen Sie die Beispiel-.NET-Core-Web-App von https://github.com/aws/aws-aspnet-cognito-identity-provider.git. 2. Navigieren Sie zum `samples` Ordner und öffnen Sie die Lösung. In diesem Projekt konfiguri eren Sie die `appsettin gs.json` Datei und fügen	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	eine neue Seite hinzu, auf der nach erfolgreicher Anmeldung alle S3-Buckets gerendert werden.	
Fügen Sie Abhängigkeiten hinzu.	Fügen Sie Ihrer ASP.NET Core-Anwendung eine NuGet Abhängigkeit für `Amazon.AspNetCore.Identity.Cognito` hinzu.	Developer
Fügen Sie die Konfigurationsschlüssel und Werte zu `appsettings.json` hinzu.	Fügen Sie den Code aus der angehängten `appsettings.json` Datei in Ihre `appsettings.json` Datei ein und ersetzen Sie dann die Platzhalter durch die Werte aus den vorherigen Schritten.	Developer
Erstellen Sie einen neuen Benutzer und melden Sie sich an.	Erstellen Sie einen neuen Benutzer im Amazon Cognito Cognito-Benutzerpool und stellen Sie sicher, dass der Benutzer unter Benutzer und Gruppen im Benutzerpool vorhanden ist.	Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine neue Razor-Seite namens. `MyS3Buckets`	Fügen Sie Ihrer Beispiel-App eine neue ASP.NET Core Razor-Seite hinzu und ersetzen Sie den Inhalt für `MyS3Bucket.cshtml` und `MyS3Bucket.cshtml.cs` aus dem angehängten Beispiel. Fügen Sie die neue MyS3Bucket-Seite unter Navigation auf der Seite hinzu. `_Layout.cshtml`	Developer

Fehlerbehebung

Problem	Lösung
Nachdem Sie die Beispielanwendung aus dem GitHub Repository geöffnet haben, erhalten Sie eine Fehlermeldung, wenn Sie versuchen, das NuGet Paket zum Samples-Projekt hinzuzufügen.	Stellen Sie sicher, dass Sie in dem `src` Ordner den Verweis auf das `Amazon.AspNetCore.Identity.Cognito` Projekt aus der `Samples.sln` Datei entfernen. Sie können das NuGet Paket dann problemlos zum Samples-Projekt hinzufügen.

Zugehörige Ressourcen

- Amazon Cognito
- Amazon-Cognito-Benutzerpools
- Amazon Cognito Cognito-Identitätspools
- Beispiele für Zugriffsrichtlinien
- GitHub - AWS ASP.NET Cognito Identitätsanbieter

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Authentifizieren Sie Microsoft SQL Server auf Amazon EC2 mithilfe von AWS Directory Service

Erstellt von Jagadish Kantubugata (AWS) und Oludahun Bade Ajidahun (AWS)

Übersicht

Dieses Muster beschreibt, wie Sie ein AWS Directory Service erstellen und es zur Authentifizierung von Microsoft SQL Server auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance verwenden.

AWS Directory Service bietet mehrere Möglichkeiten, Amazon Cloud Directory und Microsoft Active Directory (AD) mit anderen AWS-Services zu verwenden. Verzeichnisse speichern Informationen über Benutzer, Gruppen und Geräte, und Administratoren verwenden sie, um den Zugriff auf Informationen und Ressourcen zu verwalten. AWS Directory Service bietet mehrere Verzeichnisoptionen für Benutzer, die ihre vorhandenen Microsoft AD- oder LDAP-fähigen Anwendungen (Lightweight Directory Access Protocol) in der Cloud verwenden möchten. Dieselben Optionen bietet es Entwicklern, die ein Verzeichnis zum Verwalten von Benutzern, Gruppen, Geräten und Zugriff benötigen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine virtuelle private Cloud (VPC) mit mindestens zwei privaten Subnetzen und zwei öffentlichen Subnetzen
- Eine AWS Identity and Access Management (IAM) -Rolle, um den Server der Domain hinzuzufügen

Architektur

Quelltechnologie-Stack

- Die Quelle kann ein lokales Active Directory sein

Zieltechnologie-Stack

- AWS Directory Service für Microsoft Active Directory (AWS Managed Microsoft AD)

Zielarchitektur

Tools

- SQL Server Management Studio (SSMS) ist ein Tool für die Verwaltung von Microsoft SQL Server, einschließlich des Zugriffs auf, der Konfiguration und der Verwaltung von SQL Server-Komponenten.

Epen

Richten Sie ein Verzeichnis ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie AWS Managed Microsoft AD als Verzeichnistyp aus.	Wählen Sie in der AWS Directory Service Service-Konsole Verzeichnisse, Verzeichnis einrichten, AWS Managed Microsoft AD, Weiter aus.	DevOps
Wählen Sie Edition aus.	Wählen Sie aus den verfügbaren Editionen für AWS Managed Microsoft AD die Standard Edition aus.	DevOps
Geben Sie den DNS-Namen des Verzeichnisses an.	Verwenden Sie einen vollqualifizierten Domänennamen. Dieser Name wird nur innerhalb Ihrer VPC aufgelöst. Er muss nicht öffentlich auflösbar sein.	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie das Administrator-Passwort fest.	Legen Sie das Passwort für den standardmäßigen Administratorbenutzer mit dem Namen Admin fest.	DevOps
Wählen Sie die VPC und die Subnetze aus.	Wählen Sie die VPC aus, die Ihr Verzeichnis und die Subnetze für die Domänenco ntroller enthalten soll. Wenn Sie keine VPC mit mindesten s zwei Subnetzen haben, müssen Sie eines erstellen.	DevOps
Überprüfen Sie das Verzeichn is und starten Sie es.	Prüfen Sie die Editionen- und Preisinformationen für das Verzeichnis und wählen Sie dann Verzeichnis erstellen.	DevOps

Starten Sie eine EC2 Instanz für SQL Server in der Domäne

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie ein AMI für SQL Server aus.	Die Schritte in diesem Epos verbinden eine EC2 Windows-Instance nahtlos mit Ihrem AWS Managed Microsoft AD-Verzeichnis. Wählen Sie in der EC2 Amazon-Konsole Launch instance und dann das entsprechende Amazon Machine Image (AMI) für SQL Server aus.	DevOps, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren von Instance-Details.	Konfigurieren Sie die Windows-Instanz so, dass sie Ihre Anforderungen für SQL Server erfüllt.	DevOps, DBA
Wählen Sie den Namen des key pair aus.	Wählen Sie ein key pair aus und starten Sie dann die Instance.	DevOps, DBA
Fügen Sie ein Netzwerk hinzu.	Sie können die VPC auswählen, in der Ihr Verzeichnis erstellt wurde.	DevOps, DBA
Wählen Sie unter IAM role (IAM-Rolle) eine Rolle aus.	Wählen Sie unter Erweitert e Einstellungen ein IAM-Profil aus, dem die von AWS `AmazonSSMManagedIn stanceCore` verwaltet en Richtlinien `AmazonSSM DirectoryServiceAc cess` zugeordnet sind.	DevOps, DBA
Fügen Sie ein Subnetz hinzu.	Wählen Sie eines der öffentlic hen Subnetze in Ihrer VPC aus. Das von Ihnen gewählte Subnetz muss den gesamten externen Datenverkehr an ein Internet-Gateway weiterleiten. Ist dies nicht der Fall, können Sie keine Remote-Verbindung zur Instance einrichten.	DevOps, DBA
Wählen Sie Ihre Domain aus.	Wählen Sie die Domäne, die Sie erstellt haben, aus der Liste des Domänenbeitritts aus.	DevOps, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die Instanz.	Wählen Sie Launch Instance (Instance starten) aus.	DBA

Authentifizieren Sie SQL Server mithilfe des Directory Service

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Melden Sie sich als Windows-Administrator an.	Melden Sie sich mit den Windows-Administratoranmeldedaten bei der EC2 Windows-Instanz an.	DBA
Melden Sie sich bei SQL Server an.	Starten Sie SQL Server Management Studio (SSMS) und melden Sie sich mithilfe der Windows-Authentifizierungsmethode bei SQL Server an.	DBA
Erstellen Sie ein Login für den Verzeichnisbenutzer.	Wählen Sie in SSMS Security und anschließend New Login aus.	DBA
Suchen Sie nach einem Anmeldenamen.	Wählen Sie die Suchschaltfläche neben dem Anmeldetextfeld.	DBA
Wählen Sie einen Standort aus.	Wählen Sie im Dialogfeld „Benutzer oder Gruppe auswählen“ die Option Standorte aus.	DBA
Geben Sie die Anmeldeinformationen für das Netzwerk ein.	Geben Sie die vollqualifizierten Netzwerkanmeldedaten ein, die Sie bei der	DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Erstellung des Verzeichn isdienstes verwendet haben; zum Beispiel:`test.com\admin` .	
Wählen Sie das Verzeichnis aus.	Wählen Sie den AWS-Verze ichnisnamen und dann OK.	DBA
Wählen Sie einen Objektnam en aus.	Wählen Sie den Benutzer aus, für den Sie das Login erstellen möchten. Wählen Sie den Speicherort aus, wählen Sie das gesamte Verzeichn is aus, suchen Sie nach dem Benutzer und fügen Sie den Anmeldenamen hinzu.	DBA
Melden Sie sich bei der SQL Server-Instanz an.	Melden Sie sich mit Ihren Domänenanmeldedaten bei der EC2 Windows-Instanz für SQL Server an.	DBA
Melden Sie sich als Domänenbenutzer bei SQL Server an.	Starten Sie SSMS und stellen Sie mithilfe der Windows-A uthentifizierungsmethode eine Verbindung zur Datenbank-Engine her.	DBA

Zugehörige Ressourcen

- Dokumentation zu AWS Directory Service (AWS-Website)
- Erstellen Sie Ihr AWS Managed Microsoft AD-Verzeichnis (AWS Directory Service Service-Dokumentation)
- Nahtloses Beitreten zu einer EC2 Windows-Instanz (AWS Directory Service Service-Dokumentation)

- Microsoft SQL Server auf AWS (AWS-Website)
- SSMS-Dokumentation (Microsoft-Website)
- Erstellen Sie ein Login in SQL Server (SQL Server-Dokumentation)

Automatisieren Sie die Reaktion auf Vorfälle und die Forensik

Erstellt von Lucas Kauffman (AWS) und Tomek Jakubowski (AWS)

Übersicht

Dieses Muster stellt eine Reihe von Prozessen bereit, die Funktionen verwenden, um Folgendes bereitzustellen: AWS Lambda

- Eine Möglichkeit, den Incident-Response-Prozess mit minimalem Wissen einzuleiten
- Automatisierte, wiederholbare Prozesse, die auf den Leitfaden zur Reaktion auf Sicherheitsvorfälle abgestimmt sind AWS
- Trennung der Konten, um die Automatisierungsschritte durchzuführen, Artefakte zu speichern und forensische Umgebungen zu erstellen

Das Framework für automatisierte Reaktion auf Vorfälle und Forensik folgt einem standardmäßigen digitalen forensischen Prozess, der aus den folgenden Phasen besteht:

1. Eindämmung
2. Akquisition
3. Prüfung
4. Analyse

Sie können Untersuchungen an statischen Daten (z. B. erworbenem Speicher oder Festplattenabbildern) und an dynamischen Daten durchführen, die zwar live sind, sich jedoch auf getrennten Systemen befinden.

Weitere Informationen finden Sie im Abschnitt Zusätzliche Informationen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Zwei AWS-Konten:
  - Sicherheitskonto, bei dem es sich um ein vorhandenes Konto handeln kann, das jedoch vorzugsweise ein neues ist

  - Forensik-Konto, vorzugsweise neu
- AWS Organizations eingerichtet
- In den Mitgliedskonten der Organizations:
  - Die Amazon Elastic Compute Cloud (Amazon EC2) -Rolle muss Abruf- und Listenzugriff auf Amazon Simple Storage Service (Amazon S3) haben und für zugänglich sein AWS Systems Manager. Wir empfehlen die Verwendung der `AmazonSSMManagedInstanceCore` AWS verwalteten Rolle. Beachten Sie, dass diese Rolle automatisch der EC2 Amazon-Instance zugewiesen wird, wenn die Reaktion auf einen Vorfall eingeleitet wird. Nach Abschluss der Antwort entfernt AWS Identity and Access Management (IAM) alle Rechte an der Instance.
  - Virtual Private Cloud (VPC) -Endpunkte im AWS Mitgliedskonto und in der Incident Response and Analysis. VPCs Diese Endpunkte sind: S3-Gateway, EC2 Messages, SSM und SSM-Nachrichten.
- AWS Command Line Interface (AWS CLI) auf den EC2 Amazon-Instances installiert. Wenn die EC2 Amazon-Instances nicht AWS CLI installiert sind, ist Internetzugang erforderlich, damit der Festplatten-Snapshot und die Speichererfassung funktionieren. In diesem Fall greifen die Skripts auf das Internet zu, um die AWS CLI Installationsdateien herunterzuladen und sie auf den Instances zu installieren.

Einschränkungen

- Dieser Rahmen zielt nicht darauf ab, Artefakte zu erzeugen, die als elektronische Beweismittel betrachtet werden können, die vor Gericht eingereicht werden können.
- Derzeit unterstützt dieses Muster nur Linux-basierte Instances, die auf der x86-Architektur ausgeführt werden.

Architektur

Zielarchitektur

Neben dem Mitgliedskonto besteht die Zielumgebung aus zwei Hauptkonten: einem Sicherheitskonto und einem Forensikkonto. Zwei Konten werden aus den folgenden Gründen verwendet:

- Um sie von allen anderen Kundenkonten zu trennen, um den Explosionsradius im Falle einer fehlgeschlagenen forensischen Analyse zu verringern
- Um die Isolierung und den Schutz der Integrität der zu analysierenden Artefakte sicherzustellen

- Um die Untersuchung vertraulich zu behandeln
- Um Situationen zu vermeiden, in denen die Bedrohungsakteure möglicherweise alle Ressourcen genutzt haben, die Ihnen unmittelbar zur Verfügung standen, AWS-Konto indem sie Servicekontingente überschritten haben und Sie so daran gehindert haben, eine EC2 Amazon-Instance zur Durchführung von Untersuchungen zu instanziieren.

Mit separaten Konten für Sicherheit und Forensik können außerdem separate Rollen eingerichtet werden — ein Responder für die Beschaffung von Beweisen und ein Ermittler für deren Analyse. Jede Rolle hätte Zugriff auf ihr eigenes Konto.

Das folgende Diagramm zeigt nur die Interaktion zwischen den Konten. Einzelheiten zu den einzelnen Konten werden in den nachfolgenden Diagrammen dargestellt, und ein vollständiges Diagramm ist beigefügt.

Das folgende Diagramm zeigt das Mitgliedskonto.

1. Ein Ereignis wird an das Thema Slack Amazon Simple Notification Service (Amazon SNS) gesendet.

Das folgende Diagramm zeigt das Sicherheitskonto.

2. Das Amazon SNS SNS-Thema im Sicherheitskonto löst forensische Ereignisse aus.

Das folgende Diagramm zeigt das Forensics-Konto.

Das Sicherheitskonto ist der Ort, an dem die beiden wichtigsten AWS Step Functions Workflows für die Erfassung von Arbeitsspeicher- und Festplatten-Images erstellt werden. Nachdem die Workflows ausgeführt wurden, greifen sie auf das Mitgliedskonto zu, bei dem die EC2 Amazon-Instances an einem Vorfall beteiligt sind, und sie initiieren eine Reihe von Lambda-Funktionen, die ein Speicherabbild oder ein Festplattenabbild erfassen. Diese Artefakte werden dann im Forensics-Konto gespeichert.

Das Forensics-Konto speichert die Artefakte, die durch den Step Functions Functions-Workflow gesammelt wurden, im Amazon S3 S3-Bucket für Analyseartefakte. Das Forensics-Konto wird auch

über eine Amazon EC2 Image Builder Builder-Pipeline verfügen, die ein Amazon Machine Image (AMI) einer Forensics-Instance erstellt. Derzeit basiert das Image auf SANS SIFT Workstation.

Der Build-Prozess verwendet die Maintenance-VPC, die über eine Verbindung zum Internet verfügt. Das Bild kann später verwendet werden, um die EC2 Amazon-Instance zur Analyse der gesammelten Artefakte in der Analysis VPC hochzufahren.

Die Analyse-VPC hat keine Internetverbindung. Standardmäßig erstellt das Muster drei private Analyse-Subnetze. Sie können bis zu 200 Subnetze erstellen, was dem Kontingent für die Anzahl der Subnetze in einer VPC entspricht. Den VPC-Endpunkten müssen diese Subnetze jedoch hinzugefügt werden, um die Ausführung von Befehlen in ihnen AWS Systems Manager Session Manager zu automatisieren.

Aus Sicht der Best Practices empfehlen wir, Folgendes zu verwenden und zu tun: AWS CloudTrail AWS Config

- Verfolgen Sie die in Ihrem Forensics-Konto vorgenommenen Änderungen
- Überwachen Sie den Zugriff und die Integrität der gespeicherten und analysierten Artefakte

Workflow

Das folgende Diagramm zeigt die wichtigsten Schritte eines Workflows, der den Prozess und die Entscheidungsstruktur vom Zeitpunkt der Kompromittierung einer Instanz bis zu ihrer Analyse und Eindämmung umfasst.

1. Wurde dem `SecurityIncidentStatus` Tag der Wert Analyze zugewiesen? Falls ja, gehen Sie wie folgt vor:
   a. Hängen Sie die richtigen IAM-Profile für AWS Systems Manager und Amazon S3 an.
   b. Sende eine Amazon SNS-Nachricht an die Amazon SNS SNS-Warteschlange in Slack.
   c. Senden Sie eine Amazon SNS SNS-Nachricht an die `SecurityIncident` Warteschlange.
   d. Rufen Sie die Zustandsmaschine für die Speicher- und Festplattenerfassung auf.
2. Wurden Arbeitsspeicher und Festplatte erworben? Falls nein, liegt ein Fehler vor.
3. Taggen Sie die EC2 Amazon-Instance mit dem `Contain` Tag.
4. Fügen Sie die IAM-Rolle und die Sicherheitsgruppe hinzu, um die Instance vollständig zu isolieren.

Automatisierung und Skalierung

Ziel dieses Musters ist es, eine skalierbare Lösung für die Reaktion auf Vorfälle und Forensik für mehrere Konten innerhalb einer einzigen AWS Organizations Organisation bereitzustellen.

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend AWS-Konten zu verwalten.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie AWS-Services über Befehle in Ihrer Befehlszeilen-Shell interagieren können.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Key Management Service (AWS KMS) hilft Ihnen dabei, kryptografische Schlüssel zum Schutz Ihrer Daten zu erstellen und zu kontrollieren.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Security Hubbietet einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS. Es hilft Ihnen auch dabei, Ihre AWS Umgebung anhand der Sicherheitsstandards und bewährten Verfahren der Branche zu überprüfen.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.
- AWS Step Functionsist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Funktionen und andere Funktionen kombinieren können, um geschäftskritische Anwendungen AWS-Services zu erstellen.
- AWS Systems Managerhilft Ihnen bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der ausgeführt werden. AWS Cloud Es vereinfacht das Anwendungs- und

Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme und hilft Ihnen, Ihre AWS Ressourcen sicher und in großem Umfang zu verwalten.

Code

Den Code und spezifische Anleitungen zur Implementierung und Nutzung finden Sie im Repository GitHub Automated Incident Response and Forensics Framework.

Epen

Stellen Sie die Vorlagen CloudFormation bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie CloudFormation Vorlagen bereit.	Die CloudFormation Vorlagen sind mit 1 bis 7 gekennzeichnet, wobei das erste Wort des Skriptnamens angibt, in welchem Konto die Vorlage bereitgestellt werden muss. Beachten Sie, dass die Reihenfolge, in der die CloudFormation Vorlagen gestartet werden, wichtig ist. • `1-forensic-AnalysisVPCnS3Buckets.yaml` : Wird im Forensik-Konto bereitgestellt. Es erstellt die Amazon S3 S3-Buckets und die Analysis VPC und wird aktiviert. CloudTrail • `2-forensic-MaintenanceVPCnEC2ImageBuilderPipeline.yaml` : Stellt die Wartungs-VPC und die Image Builder-P	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ipeline auf Basis von SANS SIFT bereit. • `3-security_IR-Disk_Mem_automation.yaml` : Stellt die Funktionen im Sicherheitskonto bereit, die die Festplatten- und Speichererfassung ermöglichen. • `4-security_LiME_Volatility_Factory.yaml` : Initiiert eine Build-Funktion, um mit der Erstellung der Speichermodule auf der Grundlage des angegebenen AMI IDs zu beginnen. Beachten Sie, dass AMI von Land zu Land unterschiedlich IDs sind AWS-Regionen. Wann immer Sie neue Speichermodule benötigen, können Sie dieses Skript mit dem neuen AMI IDs erneut ausführen. Erwägen Sie, dies in Ihre Golden Image AMI Builder-Pipelines zu integrieren (falls in Ihrer Umgebung verwendet). • `5-member-IR-automation.yaml` : Erzeugt die Automatisierungsfunktion für Mitglieder, die den Incident-Response-Prozess einleitet. Es ermöglicht	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die gemeinsame Nutzung von Amazon Elastic Block Store (Amazon EBS) - Volumen zwischen Konten, die automatische Veröffentlichung in Slack-Channels während des Incident-Response-Prozesses, die Initiierung des forensischen Prozesses und die Isolierung der Instances nach Abschluss des Vorgangs. • `6-forensic-artifact-s3-policies.yaml` : Nachdem alle Skripts bereitgestellt wurden, korrigiert dieses Skript die Berechtigungen, die für alle kontoübergreifenden Interaktionen erforderlich sind. • `7-security-IR-vpc.yaml` : Konfiguriert eine VPC, die für die Verarbeitung von Incident-Response-Volumen verwendet wird. Um das Incident Response Framework für eine bestimmte EC2 Amazon-Instance zu initiieren, erstellen Sie ein Tag mit dem Schlüssel `SecurityIncidentStatus` und	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	dem Wert`Analyze`. Dadurch wird die Lambda-Funktion des Mitglieds gestartet, die automatisch die Isolierung und den Speicher sowie die Festplattenerfassung startet.	
Betreiben Sie das Framework.	Die Lambda-Funktion taggt das Asset auch am Ende (oder bei einem Ausfall) neu mit. `Contain` Dadurch wird das Containment initiiert, bei dem die Instance vollständ ig isoliert wird. Es gibt keine Sicherheitsgruppe ohne INBOUND/OUTBOUND und eine IAM-Rolle, die jeglichen Zugriff verbietet. Folgen Sie GitHub den Schritten im Repository.	AWS-Administrator

Implementieren Sie benutzerdefinierte Security Hub Hub-Aktionen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die benutzerd efinierten Security Hub Hub-Aktionen mithilfe einer CloudFormation Vorlage bereit.	Um eine benutzerdefinierte Aktion zu erstellen, sodass Sie die Dropdownliste von Security Hub verwenden können, stellen Sie die `Modules/SecurityHu b Custom Actions/S ecurityHubCustomAc tions.yaml` CloudForm	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ation Vorlage bereit. Ändern Sie dann die `IRAutomation` Rolle in den einzelnen Mitgliedskonten, sodass die Lambda-Funktion, die die Aktion ausführt, die `IRAutomation` Rolle übernehmen kann. Weitere Informationen finden Sie im GitHub Repository.	

Zugehörige Ressourcen

- AWS Leitfaden zur Reaktion auf Sicherheitsvorfälle

Zusätzliche Informationen

Mithilfe dieser Umgebung kann ein Security Operations Center (SOC) -Team seinen Prozess zur Reaktion auf Sicherheitsvorfälle wie folgt verbessern:

- Die Fähigkeit, forensische Untersuchungen in einer getrennten Umgebung durchzuführen, um eine versehentliche Beeinträchtigung der Produktionsressourcen zu vermeiden
- Wir verfügen über einen standardisierten, wiederholbaren und automatisierten Prozess zur Eindämmung und Analyse.
- Jeder Kontoinhaber oder Administrator hat die Möglichkeit, den Prozess zur Reaktion auf Vorfälle mit minimalem Wissen über die Verwendung von Tags einzuleiten
- Eine standardisierte, saubere Umgebung für die Durchführung von Vorfallanalysen und Forensik ohne den Lärm einer größeren Umgebung
- Die Fähigkeit, mehrere Analyseumgebungen parallel zu erstellen
- Konzentrierung der SOC-Ressourcen auf die Reaktion auf Vorfälle statt auf die Wartung und Dokumentation einer Cloud-Forensik-Umgebung
- Abkehr von einem manuellen Prozess hin zu einem automatisierten Prozess, um Skalierbarkeit zu erreichen

- Verwendung von CloudFormation Vorlagen aus Gründen der Konsistenz und zur Vermeidung wiederholbarer Aufgaben

Darüber hinaus vermeiden Sie die Verwendung einer persistenten Infrastruktur und zahlen für Ressourcen, wenn Sie sie benötigen.

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Automatisieren Sie die Behebung von AWS Security Hub Standardergebnissen

Erstellt von Chandini Penmetsa (AWS) und Aromal Raj Jayarajan (AWS)

Übersicht

Mit AWS Security Hub können Sie Prüfungen für bewährte Standardpraktiken wie die folgenden aktivieren:

- AWS Bewährte grundlegende Sicherheitsmethoden
- Maßstab für AWS GUS-Stiftungen
- Payment Card Industry Data Security Standard (PCI DSS)

Jeder dieser Standards hat vordefinierte Kontrollen. Security Hub prüft, ob eine bestimmte Kontrolle vorliegt, AWS-Konto und meldet die Ergebnisse.

AWS Security Hub sendet EventBridge standardmäßig alle Ergebnisse an Amazon. Dieses Muster bietet eine Sicherheitskontrolle, die eine EventBridge Regel zur Identifizierung der Standardergebnisse von Best Practices im Bereich der AWS grundlegenden Sicherheit einsetzt. Die Regel identifiziert die folgenden Ergebnisse für automatische Skalierung, virtuelle private Clouds (VPCs), Amazon Elastic Block Store (Amazon EBS) und Amazon Relational Database Service (Amazon RDS) aus dem Standard AWS Foundational Security Best Practices:

- [AutoScaling.1] Auto Scaling Scaling-Gruppen, die einem Load Balancer zugeordnet sind, sollten Load Balancer-Zustandsprüfungen verwenden
- [EC2.2] Die VPC-Standardsicherheitsgruppe sollte keinen eingehenden und ausgehenden Datenverkehr zulassen
- [EC2.6] Die VPC-Flow-Protokollierung sollte in allen aktiviert sein VPCs
- [EC2.7] Die EBS-Standardverschlüsselung sollte aktiviert sein
- [RDS.1] RDS-Snapshots sollten privat sein.
- [RDS.6] Die erweiterte Überwachung sollte für RDS-DB-Instances und -Cluster konfiguriert werden
- [RDS.7] Bei RDS-Clustern sollte der Löschschutz aktiviert sein

Die EventBridge Regel leitet diese Ergebnisse an eine AWS Lambda Funktion weiter, die das Ergebnis behebt. Die Lambda-Funktion sendet dann eine Benachrichtigung mit Informationen zur Problembehebung an ein Amazon Simple Notification Service (Amazon SNS) -Thema.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Eine E-Mail-Adresse, an die Sie die Behebungsbenachrichtigung erhalten möchten
- Security Hub und dort AWS Config aktiviert AWS-Region , wo Sie das Steuerelement einsetzen möchten
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket in derselben Region wie die Steuerung zum Hochladen des AWS Lambda Codes

Einschränkungen

- Diese Sicherheitskontrolle behebt automatisch neue Ergebnisse, die nach der Implementierung der Sicherheitskontrolle gemeldet wurden. Um bestehende Ergebnisse zu korrigieren, wählen Sie die Ergebnisse manuell in der Security Hub Hub-Konsole aus. Wählen Sie dann unter Aktionen die AFSBPRemedybenutzerdefinierte Aktion aus, die im Rahmen der Bereitstellung von AWS CloudFormation erstellt wurde.
- Diese Sicherheitskontrolle ist regional und muss in der Region eingesetzt werden AWS-Regionen , die Sie überwachen möchten.
- Für die Lösung EC2 5.6 wird zur Aktivierung von VPC Flow Logs eine Amazon CloudWatch Logs-Protokollgruppe im Format erstellt. `/VpcFlowLogs/vpc_id` Wenn eine Protokollgruppe mit demselben Namen existiert, wird die bestehende Protokollgruppe verwendet.
- Für die Lösung EC2 1.7, um die Amazon EBS-Standardverschlüsselung zu aktivieren, wird der Standardschlüssel AWS Key Management Service (AWS KMS) verwendet. Diese Änderung verhindert die Verwendung bestimmter Instances, die keine Verschlüsselung unterstützen.

Architektur

Zieltechnologie-Stack

- Lambda-Funktion

- Amazon SNS-Thema
- EventBridge Regel
- AWS Identity and Access Management (IAM) -Rollen für die Lambda-Funktion, VPC Flow Logs und Amazon RDS Enhanced Monitoring

Zielarchitektur

Automatisierung und Skalierung

Wenn Sie diese Vorlage verwenden AWS Organizations, können Sie AWS CloudFormation StackSetssie verwenden, um sie in mehreren Konten bereitzustellen, die Sie überwachen möchten.

Tools

- AWS CloudFormationist ein Dienst, der Ihnen hilft, AWS Ressourcen zu modellieren und einzurichten, indem er Infrastruktur als Code verwendet.
- Amazon EventBridge liefert einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen und SaaS-Anwendungen (Software as a Service) und AWS-Services leitet diese Daten an Ziele wie Lambda-Funktionen weiter.
- AWS Lambdaunterstützt die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern.
- Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice, den Sie für eine Vielzahl von Speicherlösungen verwenden können, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Bewährte Methoden

- Neun AWS Security Hub bewährte Methoden
- AWS Grundlegender Standard für bewährte Sicherheitsverfahren

Epen

Stellen Sie die Sicherheitskontrolle bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den Amazon S3 S3-Bucket.	Wählen oder erstellen Sie auf der Amazon S3 S3-Konsole einen Amazon S3 S3-Bucket mit einem eindeutigen Namen, der keine führenden Schrägstriche enthält. Ein Amazon S3 S3-Bucket-Name ist weltweit einzigartig, und der Namespace wird von allen AWS-Konten gemeinsam genutzt. Ihr Amazon S3 S3-Bucket muss sich in derselben Region befinden wie die Security Hub Hub-Ergebnisse, die ausgewertet werden.	Cloud-Architekt
Laden Sie den Lambda-Code in den Amazon S3 S3-Bucket hoch.	Laden Sie die Lambda-Code-ZIP-Datei, die im Abschnitt „Anlagen“ bereitgestellt wird, in den definierten Amazon S3 S3-Bucket hoch.	Cloud-Architekt
Stellen Sie die AWS CloudFormation Vorlage bereit.	Stellen Sie die AWS CloudFormation Vorlage bereit, die als Anlage zu diesem Muster bereitgestellt wird. Geben Sie im nächsten Epos die Werte für die Parameter an.	Cloud-Architekt

Vervollständigen Sie die Parameter in der AWS CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den Namen des Amazon S3 S3-Buckets an.	Geben Sie den Namen des Amazon S3 S3-Buckets ein, den Sie im ersten Epic erstellt haben.	Cloud-Architekt
Geben Sie das Amazon S3 S3-Präfix an.	Geben Sie den Speicherort der Lambda-Code-ZIP-Datei in Ihrem Amazon S3 S3-Bucket an, ohne vorangestellte Schrägstriche (z. B.). `<directory>/<file-name>.zip`	Cloud-Architekt
Geben Sie den ARN des Amazon SNS SNS-Themas an.	Wenn Sie ein vorhandenes Amazon SNS SNS-Thema für Behebungsbenachrichtigungen verwenden möchten, geben Sie den Amazon-Ressourcennamen (ARN) des Amazon SNS-Themas an. Wenn Sie ein neues Amazon SNS SNS-Thema verwenden möchten, behalten Sie den Wert bei `None` (den Standardwert).	Cloud-Architekt
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine E-Mail-Adresse an, an die Sie die Behebungsbenachrichtigungen erhalten möchten (nur erforderlich, wenn Sie das Amazon SNS SNS-Thema	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	erstellen AWS CloudForm ation möchten).	
Definieren Sie die Protokoll ierungsebene.	Definieren Sie die Protokoll ierungsebene und die Häufigkeit für Ihre Lambda-Funktion. `Info`bezeichnet detaillierte Informationsmeldun gen über den Fortschritt der Anwendung. `Error`bezeichne t Fehlerereignisse, die es der Anwendung dennoch ermöglichen könnten, weiter zu laufen. `Warning`bezeichnet potenziell schädliche Situation en.	Cloud-Architekt
Geben Sie den ARN der IAM-Rolle für VPC Flow Logs an.	Geben Sie den ARN der IAM-Rolle an, die für VPC-Flow-Logs verwendet werden soll. Wenn Sie eingeben`None`, AWS CloudFormation wird eine IAM-Rolle erstellt und verwendet.	Cloud-Architekt
Geben Sie den ARN der IAM-Rolle für Amazon RDS Enhanced Monitoring an.	Geben Sie den ARN der IAM-Rolle an, die für Amazon RDS Enhanced Monitorin g verwendet werden soll. Wenn Sie eingeben`None`, AWS CloudFormation wird eine IAM-Rolle erstellt und verwendet.	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Amazon SNS SNS-Abonnement.	Wenn die Vorlage erfolgreich bereitgestellt wurde und ein neues Amazon SNS SNS-Thema erstellt wurde, wird eine Abonnementnachricht an die von Ihnen angegebene E-Mail-Adresse gesendet. Um Benachrichtigungen über Problembehebungen zu erhalten, müssen Sie diese Abonnement-E-Mail-Nachricht bestätigen.	Cloud-Architekt

Zugehörige Ressourcen

- Einen Stack auf der AWS CloudFormation Konsole erstellen
- AWS Lambda website
- AWS Security Hub Dokumentation

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Automatisieren Sie Sicherheitsscans für kontoübergreifende Workloads mit Amazon Inspector und AWS Security Hub

Erstellt von Ramya Pulipaka (AWS) und Mikesh Khanal (AWS)

Übersicht

Dieses Muster beschreibt, wie in kontoübergreifenden Workloads in der Amazon Web Services (AWS) Cloud automatisch nach Sicherheitslücken gesucht wird.

Das Muster hilft bei der Erstellung eines Zeitplans für hostbasierte Scans von Amazon Elastic Compute Cloud (Amazon EC2) -Instances, die nach Tags gruppiert sind, oder für netzwerkbasierte Amazon Inspector-Scans. Ein AWS CloudFormation Stack stellt alle erforderlichen AWS Ressourcen und Dienste für Sie bereit. AWS-Konten

Die Ergebnisse von Amazon Inspector werden in Ihre Konten, AWS-Regionen virtuellen privaten Clouds (VPCs) und EC2 Amazon-Instances exportiert und bieten Einblicke in Sicherheitslücken. AWS Security Hub Sie können diese Ergebnisse per E-Mail erhalten oder ein Amazon Simple Notification Service (Amazon SNS) -Thema erstellen, das einen HTTP-Endpunkt verwendet, um die Ergebnisse an Ticketing-Tools, SIEM-Software (Security Information and Event Management) oder andere Sicherheitslösungen von Drittanbietern zu senden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Aktiv AWS-Konten , das kontenübergreifende Workloads hostet, einschließlich eines zentralen Audit-Kontos.
- Eine bestehende E-Mail-Adresse für den Empfang von E-Mail-Benachrichtigungen von Amazon SNS.
- Ein vorhandener HTTP-Endpunkt, der von Ticketing-Tools, SIEM-Software oder anderen Sicherheitslösungen von Drittanbietern verwendet wird.
- Security Hub, aktiviert und konfiguriert. Sie können dieses Muster auch ohne Security Hub verwenden, wir empfehlen jedoch die Verwendung von Security Hub aufgrund der damit generierten Erkenntnisse. Weitere Informationen finden Sie unter Security Hub einrichten in der Security Hub Hub-Dokumentation.

- Auf jeder EC2 Instance, die Sie scannen möchten, muss ein Amazon Inspector-Agent installiert sein. Sie können den Amazon Inspector-Agent mithilfe von AWS Systems Manager Run Command auf mehreren EC2 Instances installieren.

Fähigkeiten

- Erfahrung in der Nutzung `self-managed` und `service-managed` Berechtigungen für Stacksets in CloudFormation. Wenn Sie `self-managed` Berechtigungen verwenden möchten, um Stack-Instances für bestimmte Konten in bestimmten Regionen bereitzustellen, müssen Sie die erforderlichen Rollen AWS Identity and Access Management (IAM) erstellen. Wenn Sie `service-managed` Berechtigungen verwenden möchten, um Stack-Instances für Konten bereitzustellen, die AWS Organizations in bestimmten Regionen verwaltet werden, müssen Sie die erforderlichen IAM-Rollen nicht erstellen. Weitere Informationen finden Sie in der CloudFormation Dokumentation unter Erstellen eines Stack-Sets.

Einschränkungen

- Wenn in einem Konto keine Tags auf EC2 Amazon-Instances angewendet werden, scannt Amazon Inspector alle Instances in diesem Konto.
- Die CloudFormation Stack-Sets und die `onboard-audit-account.yaml` Datei (angehängt) müssen in derselben Region bereitgestellt werden.
- Der Ansatz dieses Musters kann unter die Veröffentlichungsquote von 30.000 Transaktionen pro Sekunde (TPS) für ein Amazon SNS SNS-Thema in der Region USA Ost (Nord-Virginia) () skaliert werden, obwohl die Grenzwerte je nach Region variieren. `us-east-1` Um effektiver zu skalieren und Datenverlust zu vermeiden, empfehlen wir, Amazon Simple Queue Service (Amazon SQS) vor dem Amazon SNS SNS-Thema zu verwenden.

Architektur

Das folgende Diagramm veranschaulicht den Arbeitsablauf für das automatische Scannen von EC2 Amazon-Instances.

Der Workflow besteht aus folgenden Schritten:

1. Eine EventBridge Amazon-Regel verwendet einen Cron-Ausdruck, um sich nach einem bestimmten Zeitplan selbst zu initiieren, und initiiert Amazon Inspector.

2. Amazon Inspector scannt die markierten EC2 Amazon-Instances im Konto.
3. Amazon Inspector sendet die Ergebnisse an Security Hub, der Erkenntnisse für Arbeitsabläufe, Priorisierung und Problembehebung generiert.
4. Amazon Inspector sendet den Status der Bewertung auch an ein Amazon SNS SNS-Thema im Prüfkonto. Eine AWS Lambda Funktion wird aufgerufen, wenn ein `findings reported` Ereignis zum Amazon SNS SNS-Thema veröffentlicht wird.
5. Die Lambda-Funktion ruft die Ergebnisse ab, formatiert sie und sendet sie an ein anderes Amazon SNS SNS-Thema im Prüfkonto.
6. Die Ergebnisse werden an die E-Mail-Adressen gesendet, die das Amazon SNS SNS-Thema abonniert haben. Die vollständigen Details und Empfehlungen werden im JSON-Format an den abonnierten HTTP-Endpunkt gesendet.

Tools

- AWS CloudFormationhilft Ihnen dabei, Ihre AWS Ressourcen zu modellieren und einzurichten, sodass Sie weniger Zeit mit der Verwaltung dieser Ressourcen verbringen und sich mehr auf Ihre Anwendungen konzentrieren können.
- AWS CloudFormation StackSetserweitert die Funktionalität von Stacks, indem es Ihnen ermöglicht, Stacks für mehrere Konten und Regionen mit einem einzigen Vorgang zu erstellen, zu aktualisieren oder zu löschen.
- AWS Control Towererstellt eine Abstraktions- oder Orchestrierungsebene, die die Funktionen mehrerer anderer Ebenen kombiniert und integriert, darunter. AWS-Services AWS Organizations
- Amazon EventBridge ist ein serverloser Event-Bus-Service, der es einfach macht, Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen zu verbinden.
- AWS Lambdaist ein Rechendienst, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen.
- AWS Security Hubbietet Ihnen einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS und hilft Ihnen dabei, Ihre Umgebung anhand der Sicherheitsstandards und Best Practices der Branche zu überprüfen.
- Amazon Simple Notification Service (Amazon SNS) ist ein verwalteter Service, der die Nachrichtenzustellung von Verlagen an Abonnenten ermöglicht.

Epen

Stellen Sie die Vorlage CloudFormation bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation Vorlage im Auditkonto bereit.	Laden Sie die `onboard-audit-account.yaml` Datei (angehängt) herunter und speichern Sie sie in einem lokalen Pfad auf Ihrem Computer. Melden Sie sich AWS Management Console bei Ihrem Audit-Konto an, öffnen Sie die CloudFormation Konsole und wählen Sie dann Create Stack aus. Wählen Sie im Abschnitt Voraussetzungen die Option Vorlage vorbereiten aus und wählen Sie dann Vorlage ist bereit aus. Wählen Sie im Abschnitt „Vorlage angeben“ die Option „Vorlagenquelle“ und wählen Sie dann „Vorlage ist bereit“. Laden Sie die `onboard-audit-account.yaml` Datei hoch und konfigurieren Sie dann die verbleibenden Optionen entsprechend Ihren Anforderungen.	Entwickler, Sicherheitsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Stellen Sie sicher, dass Sie die folgenden Eingabepa rameter konfigurieren: • `DestinationEmailAd dress` — Geben Sie eine E-Mail-Adresse ein, um die Ergebnisse zu erhalten. • `HTTPEndpoint` — Stellen Sie einen HTTP-Endpunkt für Ihre Ticketing- oder SIEM-Tools bereit. **Note** Sie können die CloudFormation Vorlage auch mithilfe von AWS Command Line Interface ()AWS CLI bereitstellen. Weitere Informationen dazu finden Sie in der CloudFormation Dokumentation unter Einen Stack erstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Amazon SNS SNS-Abonnement.	Öffnen Sie Ihren E-Mail-Posteingang und wählen Sie in der E-Mail, die Sie von Amazon SNS erhalten, die Option Abonnement bestätigen aus. Dadurch wird ein Webbrowser-Fenster geöffnet und die Abonnementbestätigung angezeigt.	Entwickler, Sicherheitsingenieur

Erstellen Sie CloudFormation Stack-Sets, um den Amazon Inspector-Scanplan zu automatisieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie Stack-Sets im Audit-Konto.	Laden Sie die `vulnerability-management-program.yaml` Datei (angehängt) in einen lokalen Pfad auf Ihrem Computer herunter. Wählen Sie auf der CloudFormation Konsole „Stacksets anzeigen“ und anschließend „Erstellen“. StackSet Wählen Sie „Vorlage ist bereit“, wählen Sie „Eine Vorlagendatei hochladen “ und laden Sie dann die **`vulnerability-management-program.yaml`** Datei hoch. Wenn Sie `self-managed` Berechtigungen	Entwickler, Sicherheitsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	verwenden möchten, folgen Sie den Anweisungen unter Erstellen eines Stack-Sets mit selbstverwalteten Berechtigungen in der CloudFormation Dokumentation. Dadurch werden Stack-Sets in einzelnen Konten erstellt. Wenn Sie `service-managed` Berechtigungen verwenden möchten, folgen Sie den Anweisungen unter Erstellen eines Stack-Sets mit vom Service verwalteten Berechtigungen in der CloudFormation Dokumentation. Dadurch werden Stacksets in Ihrer gesamten Organisation oder in bestimmten Organisationseinheiten (OUs) erstellt. Stellen Sie sicher, dass die folgenden Eingabeparameter für Ihre Stack-Sets konfiguriert sind: • `AssessmentSchedule` — Der Zeitplan für die EventBridge Verwendung von Cron-Ausdrücken. • `Duration`— Die Dauer des Amazon Inspector	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Inspector-Bewertungslaufs in Sekunden. • `CentralSNSTopicArn` — Der Amazon-Ressourcenname (ARN) für das zentrale Amazon SNS-Thema. • `Tagkey` — Der Tag-Schlüssel, der der Ressourcengruppe zugeordnet ist. • `Tagvalue` — Der Tag-Wert, der der Ressourcengruppe zugeordnet ist. Wenn Sie EC2 Amazon-Instances im Audit-Konto scannen möchten, müssen Sie die `vulnerability-management-program.yaml` Datei als CloudFormation Stapel im Auditkonto ausführen.	
Validieren Sie die Lösung.	Vergewissern Sie sich, dass Sie die Ergebnisse per E-Mail oder HTTP-Endpunkt gemäß dem Zeitplan erhalten, den Sie für Amazon Inspector festgelegt haben.	Entwickler, Sicherheitsingenieur

Zugehörige Ressourcen

- Skalieren Sie Ihre Tests auf Sicherheitslücken mit Amazon Inspector (AWS Blogbeitrag)

- Automatische Behebung von Sicherheitslücken bei Amazon Inspector (AWS Blogbeitrag)
- So vereinfachen Sie die Einrichtung der Sicherheitsbeurteilung mithilfe von Amazon EC2 AWS Systems Manager, und Amazon Inspector (AWS Blogbeitrag)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Automatische Prüfung von AWS Sicherheitsgruppen, die den Zugriff von öffentlichen IP-Adressen aus ermöglichen

Erstellt von Eugene Shifer (AWS) und Stephen DiCato (AWS)

Übersicht

Als bewährte Sicherheitsmethode ist es von entscheidender Bedeutung, den Einsatz von AWS Ressourcen nur für das absolut Notwendige zu minimieren. Beispielsweise müssen Webserver, die der allgemeinen Öffentlichkeit dienen, eingehenden Zugriff aus dem Internet ermöglichen, aber der Zugriff auf andere Workloads sollte auf bestimmte Netzwerke beschränkt werden, um unnötiges Risiko zu vermeiden. Sicherheitsgruppen in Amazon Virtual Private Cloud (Amazon VPC) sind eine effektive Kontrolle, mit der Sie den Ressourcenzugriff einschränken können. Die Bewertung von Sicherheitsgruppen kann jedoch eine umständliche Aufgabe sein, insbesondere in Architekturen mit mehreren Konten.AWS Config Mithilfe von Regeln und AWS Security Hub Kontrollen können Sie Sicherheitsgruppen identifizieren, die den Zugriff vom öffentlichen Internet (0.0.0.0/0) auf bestimmte Netzwerkkommunikationsprotokolle wie Secure Shell (SSH), HTTP, HTTPS und Windows Remote Desktop Protocol (RDP) ermöglichen. Diese Regeln und Kontrollen gelten jedoch nicht, wenn Dienste auf nicht standardmäßigen Ports ausgeführt werden oder wenn der Zugriff auf bestimmte öffentliche IP-Adressen beschränkt ist. Dies kann beispielsweise der Fall sein, wenn ein Webdienst dem TCP-Port 8443 anstelle des Standard-TCP-Ports 443 zugeordnet ist. Dies kann auch der Fall sein, wenn Entwickler von ihren Heimnetzwerken aus Zugriff auf den Server haben, z. B. zu Testzwecken.

Um dieses Problem zu lösen, können Sie die in diesem Muster bereitgestellte Infrastructure-as-Code-Lösung (IaC) verwenden, um Sicherheitsgruppen zu identifizieren, die den Zugriff von beliebigen nicht privaten (nicht RFC 1918-konformen) IP-Adressen auf beliebige Workloads in Ihrem Unternehmen oder Ihrer Organisation ermöglichen. AWS-Konto AWS Die AWS CloudFormationVorlage stellt eine benutzerdefinierte AWS Config Regel, eine AWS LambdaFunktion und die erforderlichen Berechtigungen bereit. Sie können es als Stack in einem einzelnen Konto oder als Stack-Set für die gesamte Organisation bereitstellen, das über verwaltet wird AWS Organizations.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Erfahrung mit GitHub

- Wenn Sie die Bereitstellung in einem einzigen System durchführen AWS-Konto:
  - Berechtigungen zum Erstellen von CloudFormation Stacks
  - AWS Config im Zielkonto eingerichtet
  - (Optional) Security Hub, der im Zielkonto eingerichtet ist
- Wenn Sie die Implementierung in einer AWS Organisation durchführen:
  - Berechtigungen zum Erstellen von CloudFormation Stack-Sets
  - Security Hub mit AWS Organizations Integration eingerichtet
  - AWS Config in den Konten einrichten, in denen Sie diese Lösung einsetzen
  - Benennen Sie einen AWS-Konto zum delegierten Administrator für AWS Config und Security Hub

Einschränkungen

- Wenn Sie die Installation für ein einzelnes Konto durchführen, für das Security Hub nicht aktiviert ist, können Sie es verwenden, AWS Config um die Ergebnisse auszuwerten.
- Wenn Sie die Bereitstellung in einer Organisation durchführen, die keinen delegierten Administrator für AWS Config und Security Hub hat, müssen Sie sich bei den einzelnen Mitgliedskonten anmelden, um die Ergebnisse einzusehen.
- Wenn Sie die Konten in Ihrer Organisation verwalten und verwalten, stellen Sie die IaC AWS Control Tower nach diesem Muster bereit, indem Sie Customizations for AWS Control Tower (cFcT) verwenden. Die Verwendung der CloudFormation Konsole würde dazu führen, dass die Konfiguration von den AWS Control Tower Leitplanken abweicht und Sie die Organisationseinheiten () oder verwalteten Konten erneut registrieren müssten. OUs
- Einige AWS-Services sind nicht in allen verfügbar. AWS-Regionen Informationen zur Verfügbarkeit in den einzelnen Regionen finden Sie AWS-Services unter Nach Regionen. Informationen zu bestimmten Endpunkten finden Sie auf der Seite Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Architektur

Bereitstellung für eine Einzelperson AWS-Konto

Das folgende Architekturdiagramm zeigt den Einsatz der AWS Ressourcen innerhalb einer einzigen AWS-Konto. Sie stellen die Ressourcen mithilfe einer CloudFormation Vorlage direkt über die

CloudFormation Konsole bereit. Wenn Security Hub aktiviert ist, können Sie die Ergebnisse entweder in Security Hub AWS Config oder in Security Hub anzeigen. Wenn Security Hub nicht aktiviert ist, können Sie die Ergebnisse nur in anzeigen AWS Config.

Das Diagramm zeigt den folgenden Workflow:

1. Sie erstellen einen CloudFormation Stack. Dadurch werden eine Lambda-Funktion und eine AWS Config Regel bereitgestellt. Sowohl die Regel als auch die Funktion sind mit den AWS Identity and Access Management (IAM-) Berechtigungen eingerichtet, die für die Veröffentlichung von Ressourcenbewertungen und Protokollen erforderlich sind. AWS Config
2. Die AWS Config Regel arbeitet im Modus Detective Evaluation und ruft die Lambda-Funktion alle 24 Stunden auf.
3. Die Lambda-Funktion bewertet die Sicherheitsgruppen und sendet Updates an. AWS Config
4. Security Hub erhält alle AWS Config Ergebnisse.
5. Sie können die Ergebnisse im Security Hub oder in einsehen AWS Config, je nachdem, welche Dienste Sie im Konto eingerichtet haben.

Bereitstellung in einer AWS Organisation

Das folgende Diagramm zeigt die Implementierung des Musters für mehrere Konten, die über AWS Organizations und verwaltet werden AWS Control Tower. Sie stellen die CloudFormation Vorlage über CfCT bereit. Die Bewertungsergebnisse werden in Security Hub im delegierten Administratorkonto zentralisiert. Der AWS CodePipeline Workflow-Abschnitt des Diagramms zeigt die Hintergrundschritte, die während der cFCT-Bereitstellung ausgeführt werden.

Das Diagramm zeigt den folgenden Workflow:

1. Im Verwaltungskonto laden Sie eine komprimierte (ZIP-) Datei der IaC-Vorlage in einen Amazon Simple Storage Service (Amazon S3) -Bucket hoch, der von CfCT bereitgestellt wird.
2. Die CfCT-Pipeline entpackt die Datei, führt cfn-nag (GitHub) -Prüfungen durch und stellt die Vorlage als Stack-Set bereit. CloudFormation
3. Abhängig von der Konfiguration, die Sie in der CFCT-Manifestdatei angeben, CloudFormation StackSets werden Stacks in einzelnen Konten oder in bestimmten Konten bereitgestellt. OUs Dadurch werden eine Lambda-Funktion und eine AWS Config Regel in den Zielkonten

bereitgestellt. Sowohl die Regel als auch die Funktion sind mit den IAM-Berechtigungen eingerichtet, die für die Veröffentlichung von Ressourcenbewertungen in AWS Config und Protokollen erforderlich sind.

4. Die AWS Config Regel arbeitet im Modus Detective Evaluation und ruft die Lambda-Funktion alle 24 Stunden auf.
5. Die Lambda-Funktion bewertet die Sicherheitsgruppen und sendet Updates an. AWS Config
6. AWS Config leitet alle Ergebnisse an Security Hub weiter.
7. Die Security Hub Hub-Ergebnisse werden im delegierten Administratorkonto zusammengefasst.
8. Sie können die aggregierten Ergebnisse in Security Hub im delegierten Administratorkonto einsehen.

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten AWS-Konten Lebenszyklus über und zu verwalten. AWS-Regionen
- AWS Configbietet einen detaillierten Überblick über die Ressourcen in Ihrem System AWS-Konto und darüber, wie sie konfiguriert sind. Es hilft Ihnen zu erkennen, wie Ressourcen miteinander zusammenhängen und wie sich ihre Konfigurationen im Laufe der Zeit geändert haben. Eine AWS Config Regel definiert Ihre idealen Konfigurationseinstellungen für eine Ressource und AWS Config kann bewerten, ob Ihre AWS Ressourcen die Bedingungen der Regel erfüllen.
- AWS Control Towerhilft Ihnen dabei, eine Umgebung mit AWS mehreren Konten einzurichten und zu verwalten und dabei die vorgeschriebenen Best Practices zu befolgen. Customizations for AWS Control Tower (cFCT) hilft dir dabei, deine AWS Control Tower landing zone individuell anzupassen und dich an bewährte Methoden zu AWS halten. Anpassungen für diese Lösung werden mithilfe von CloudFormation Vorlagen und Richtlinien zur AWS Organizations Servicesteuerung () implementiert. SCPs
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Sie führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Organizationsist ein Kontoverwaltungsservice, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie erstellen und zentral verwalten.

- AWS Security Hubbietet einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS. Es hilft Ihnen auch dabei, Ihre AWS Umgebung anhand von Industriestandards und Best Practices im Bereich Sicherheit zu überprüfen.

Andere Tools

- Python ist eine Allzweck-Computerprogrammiersprache.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub Detect vulnerable security groups verfügbar.

Bewährte Methoden

Wir empfehlen Ihnen, sich an die bewährten Methoden in den folgenden Ressourcen zu halten:

- Bewährte Methoden für Organisationseinheiten mit AWS Organizations (AWS Cloud Operations & Migrations Blog)
- Leitfaden für die Einrichtung einer ersten Grundlage mithilfe von AWS Control Tower on AWS (AWS Solutions Library)
- Anleitung zum Erstellen und Ändern von AWS Control Tower Ressourcen (AWS Control Tower Dokumentation)
- Überlegungen zur CfCT-Bereitstellung (AWS Control Tower Dokumentation)
- Wenden Sie Berechtigungen mit den geringsten Rechten an (IAM-Dokumentation)

Epen

Überprüfe die Vorlage CloudFormation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestimmen Sie Ihre Bereitste llungsstrategie.	Prüfen Sie die Lösung und den Code, um die Bereitste llungsstrategie für Ihre AWS Umgebung festzulegen. Stellen Sie fest, ob Sie die	Inhaber der App, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bereitstellung für ein einzelnes Konto oder für eine AWS Organisation durchführen.	
Klonen Sie das Repository	Geben Sie den folgenden Befehl ein, um das Repository Detect Vulnerable Security Groups zu klonen: `git clone https://github.com/aws-samples/detect-public-security-groups.git`	App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Python-Version.	1. Navigieren Sie in das Verzeichnis der obersten Ebene im geklonten Repository: `cd detect-public-security-groups` 2. Öffnen Sie Security-Group-Public-Assessment.yaml. 3. Vergewissern Sie sich in der `SgPublicAccessCheckLambdaFunction` Ressource, dass die Python-Version mit Ihrem Ziel kompatibel ist AWS-Regionen. Standardmäßig verwendet diese Funktion Python 3.12. Weitere Informationen finden Sie unter AWS Lambda Fügt Unterstützung für Python 3.12 hinzu. Aktualisieren Sie gegebenenfalls die Python-Version. 4. Speichern und schließen Sie Security-Group-Public-Assessment.yaml.	AWS-Administrator, App-Entwickler

Stellen Sie die CloudFormation Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation Vorlage bereit.	Stellen Sie die CloudFormation Vorlage in Ihrer AWS Umgebung bereit. Führen Sie eine der folgenden Aktionen aus: • Wenn Sie die Bereitstellung in einer einzelnen Datei durchführen AWS-Konto, folgen Sie den Anweisungen unter Erstellen eines Stacks. • Wenn Sie die Bereitstellung in einer Organisation durchführen, die nicht von verwaltet wird AWS Control Tower, folgen Sie den Anweisungen unter Erstellen eines Stack-Sets. • Wenn Sie die Bereitstellung in einer Organisation durchführen, die von verwaltet wird AWS Control Tower, lesen Sie die Anweisungen im Abschnitt Eigene Anpassungen erstellen.	App-Entwickler, AWS-Administrator, Allgemeines AWS
Überprüfen Sie die Bereitstellung.	Stellen Sie in der CloudFormation Konsole sicher, dass der Stack oder das Stack-Set erfolgreich bereitgestellt wurde.	AWS-Administrator, App-Besitzer

Überprüfen Sie die Ergebnisse

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich die Ergebnisse AWS Config der Regel an.	Gehen Sie in Security Hub wie folgt vor, um eine Liste der einzelnen Ergebnisse anzuzeigen: 1. Öffnen Sie die Security Hub Hub-Konsole. 2. Wählen Sie im Navigatio nsbereich Findings aus. 3. Fügen Sie im Feld Filter hinzufügen die folgenden Filter hinzu: • Der Konformitätsstatus ist `FAILED` • Titel ist `SgPublicA ccessCheck` 4. Wählen Sie Anwenden aus. Gehen Sie in Security Hub wie folgt vor, um eine Liste der Gesamtergebnisse anzuzeige n, gruppiert nach AWS-Konto: 1. Öffnen Sie die Security Hub Hub-Konsole. 2. Wählen Sie im Navigatio nsbereich Insights aus. 3. Wählen Sie Create Insight (Insight erstellen) aus.	AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. So wählen Sie das Gruppierungsattribut für den Insight aus: a. Wählen Sie das Suchfeld, um die Filteroptionen anzuzeige n. b. Wählen Sie Group by (Gruppieren nach). c. Wählen Sie AwsAccoun tId. d. Wählen Sie Anwenden aus. 5. Fügen Sie im Feld Filter hinzufügen die folgenden Filter hinzu: • Der Titel lautet `SgPublicAccessChec k` • Der Compliance-Status ist `FAILED` 6. Wählen Sie Create Insight (Insight erstellen) aus. 7. Geben Sie einen Insight-N amen ein und wählen Sie dann Create Insight aus. Um eine Liste der Ergebniss e einzusehen, folgen Sie den Anweisungen unter Konformitätsinformationen und Bewertungsergebnisse	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	anzeigen in der AWS Config Dokumentation. AWS Config	

Fehlerbehebung

Problem	Lösung
Das Erstellen oder Löschen des CloudForm ation Stack-Sets schlägt fehl.	Wenn es bereitgestellt AWS Control Tower wird, setzt es die erforderlichen Schutzmaß nahmen durch und übernimmt die Kontrolle über AWS Config Aggregatoren und Regeln. Dazu gehört auch die Verhinderung direkter Änderungen durch. CloudFormation Um diese CloudFormation Vorlage, einschließlich aller zugehörigen Ressourcen, ordnungsgemäß bereitzustellen oder zu entfernen, müssen Sie CfCT verwenden.
CfCT kann die Vorlage nicht löschen. CloudFormation	Wenn die CloudFormation Vorlage auch nach den erforderlichen Änderungen an der Manifestdatei und dem Entfernen der Vorlagendateien weiterhin besteht, stellen Sie sicher, dass die Manifestdatei den `enable_st ack_set_deletion` Parameter enthält und dass der Wert auf gesetzt ist. `false` Weitere Informationen finden Sie in der CfCt-Doku mentation unter Löschen eines Stack-Sets.

Zugehörige Ressourcen

- AWS Config Benutzerdefinierte Regeln (AWS Config Dokumentation)

Automatisches Reaktivieren CloudTrail von AWS mithilfe einer benutzerdefinierten Behebungsregel in AWS Config

Erstellt von Manigandan Shri (AWS)

Übersicht

Der Überblick über die Aktivitäten in Ihrem Amazon Web Services (AWS) -Konto ist eine wichtige bewährte Methode für Sicherheit und Betrieb. AWS CloudTrail unterstützt Sie bei der Verwaltung, Einhaltung von Vorschriften sowie bei der Betriebs- und Risikoprüfung Ihres Kontos.

Um sicherzustellen, dass dies in Ihrem Konto aktiviert CloudTrail bleibt, stellt AWS Config die `cloudtrail-enabled` verwaltete Regel bereit. Wenn sie deaktiviert CloudTrail ist, aktiviert die `cloudtrail-enabled` Regel sie mithilfe der automatischen Problembehebung automatisch wieder.

Sie müssen jedoch sicherstellen, dass Sie die bewährten Sicherheitsmethoden befolgen, CloudTrail wenn Sie die automatische Problembehebung verwenden. Zu diesen bewährten Methoden gehören die Aktivierung CloudTrail in allen AWS-Regionen, das Protokollieren von Lese- und Schreib-Workloads, das Aktivieren von Erkenntnissen und das Verschlüsseln von Protokolldateien mit serverseitiger Verschlüsselung mithilfe von verwalteten Schlüsseln (SSE-KMS) von AWS Key Management Service (AWS KMS).

Dieses Muster hilft Ihnen dabei, diese bewährten Sicherheitsmethoden zu befolgen, indem es eine benutzerdefinierte Abhilfemaßnahme bereitstellt, die in Ihrem Konto automatisch wieder aktiviert wird. CloudTrail

> **Important**
>
> Wir empfehlen die Verwendung von Richtlinien zur Dienstkontrolle (SCPs), um jegliche Manipulation zu verhindern. CloudTrail Weitere Informationen dazu finden Sie im AWS-Sicherheitsblog im CloudTrail Abschnitt Verhinderung von Manipulationen mit AWS Organizations, um Sicherheit in großem Umfang zu vereinfachen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto

- Berechtigungen zum Erstellen eines AWS Systems Manager Automation Automation-Runbooks
- Ein vorhandener Trail für Ihr Konto

Einschränkungen

Dieses Muster unterstützt die folgenden Aktionen nicht:

- Einen Amazon Simple Storage Service (Amazon S3) -Präfixschlüssel für den Speicherort einrichten
- In einem Amazon Simple Notification Service (Amazon SNS) -Thema veröffentlichen
- Konfiguration von Amazon CloudWatch Logs zur Überwachung Ihrer CloudTrail Logs

Architektur

Technologie-Stack

- AWS Config
- CloudTrail
- Systems Manager
- Systems Manager Automation

Tools

- AWS Config bietet eine detaillierte Ansicht der Konfiguration der AWS-Ressourcen in Ihrem Konto.
- AWS CloudTrail unterstützt Sie dabei, die Unternehmensführung, die Einhaltung von Vorschriften sowie die Betriebs- und Risikoprüfung Ihres Kontos zu ermöglichen.
- AWS Key Management Service (AWS KMS) ist ein Verschlüsselungs- und Schlüsselverwaltungsservice.
- Mit AWS Systems Manager können Sie Ihre Infrastruktur auf AWS anzeigen und steuern.
- AWS Systems Manager Automation vereinfacht allgemeine Wartungs- und Bereitstellungsaufgaben von Amazon Elastic Compute Cloud (Amazon EC2) -Instances und anderen AWS-Ressourcen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code

Die cloudtrail-remediation-action.yml-Datei (angehängt) hilft Ihnen, ein Systems Manager Automation-Runbook zu erstellen, das Sie CloudTrail mithilfe bewährter Sicherheitsmethoden einrichten und erneut aktivieren können.

Epen

Konfiguration CloudTrail

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die Amazon S3 S3-Konsole und erstellen Sie dann einen S3-Bucket zum Speichern der CloudTrail Protokolle. Weitere Informationen finden Sie unter Erstellen eines S3-Buckets in der Amazon S3 S3-Dokumentation.	Systemadministrator
Fügen Sie eine Bucket-Richtlinie hinzu, um CloudTrail die Übermittlung von Protokolldateien an den S3-Bucket zu ermöglichen.	CloudTrail muss über die erforderlichen Berechtigungen verfügen, um Protokolldateien an Ihren S3-Bucket zu liefern. Wählen Sie in der Amazon S3 S3-Konsole den S3-Bucket aus, den Sie zuvor erstellt haben, und wählen Sie dann Permissions aus. Erstellen Sie eine S3-Bucket-Richtlinie, indem Sie die Amazon S3 S3-Bucket-Richtlinie für CloudTrail aus der CloudTrail Dokumentation verwenden.	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Schritte zum Hinzufügen einer Richtlinie zu einem S3-Bucket finden Sie unter Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3 S3-Konsole in der Amazon S3 S3-Dokumentation. **Important** Wenn Sie bei der Erstellung Ihres Trails ein Präfix angegeben haben CloudTrail, stellen Sie sicher, dass Sie es in die S3-Bucket-Richtlinie aufnehmen. Das Präfix ist eine optionale Ergänzung zum S3-Objektschlüssel, die eine ordnerähnliche Organisation in Ihrem S3-Bucket erstellt. Weitere Informationen dazu finden Sie in der Dokumentation unter Creating a trail. CloudTrail	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen eines KMS-Schlüssels.	Erstellen Sie einen AWS-KMS-Schlüssel CloudTrail zum Verschlüsseln von Objekten, bevor Sie sie dem S3-Bucket hinzufügen. Hilfe zu dieser Geschichte finden Sie in der Dokumentation unter Verschlüsseln von CloudTrail Protokolldateien mit verwalteten AWS-KMS-Schlüsseln (SSE-KMS). CloudTrail	Systemadministrator
Fügen Sie dem KMS-Schlüssel eine Schlüsselrichtlinie hinzu.	Fügen Sie eine KMS-Schlüsselrichtlinie hinzu, um die Verwendung des KMS-Schlüssels CloudTrail zu ermöglichen. Hilfe zu dieser Geschichte finden Sie in der Dokumentation unter Verschlüsseln von CloudTrail Protokolldateien mit von AWS KMS verwalteten Schlüsseln (SSE-KMS). CloudTrail **Important** CloudTrail benötigt keine Berechtigungen. `Decrypt`	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
AssumeRole Runbook für Systems Manager erstellen	Erstellen Sie ein `AssumeRole` für Systems Manager Automation, um das Runbook auszuführen. Anweisungen und weitere Informationen dazu finden Sie unter Automatisierung einrichten in der Systems Manager Manager-Dokumentation.	Systemadministrator

Das Systems Manager Automation-Runbook erstellen und testen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das Systems Manager Automation-Runbook.	Verwenden Sie die `cloudtrail-remediation-action.yml` Datei (angehängt), um das Systems Manager Automation-Runbook zu erstellen. Weitere Informationen dazu finden Sie unter Systems Manager Manager-Dokumente erstellen in der Systems Manager Manager-Dokumentation.	Systemadministrator
Testen Sie das Runbook.	Testen Sie auf der Systems Manager-Konsole das Systems Manager Automation-Runbook, das Sie zuvor erstellt haben. Weitere Informationen dazu finden Sie in der Systems Manager Manager-Dokumentation unter	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ausführen einer einfachen Automatisierung.	

Richten Sie die automatische Behebungsregel in AWS Config ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die CloudTrail -aktivierte Regel hinzu.	Wählen Sie in der AWS Config-Konsole Regeln und dann Regel hinzufügen aus. Klicken Sie auf der Seite Add Rule (Regel hinzufügen) auf Add Custom Rule (Benutzer definierte Regel hinzufüge n). Geben Sie auf der Seite „Regel konfigurieren“ einen Namen und eine Beschreib ung ein und fügen Sie die `cloudtrail-enabled` Regel hinzu. Weitere Informationen finden Sie unter Verwaltung Ihrer AWS Config-Regeln in der AWS Config-Do kumentation.	Systemadministrator
Fügen Sie die automatische Behebungsaktion hinzu.	Wählen Sie in der Dropdown-Liste Aktionen die Option Behebung verwalten aus. Wählen Sie Automatische Korrektur und dann das Systems Manager Manager-Runbook aus, das Sie zuvor erstellt haben.	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Die folgenden Eingabepa rameter sind erforderlich für: CloudTrail • `CloudTrailName` • `CloudTrailS3Bucket Name` • `CloudTrailKmsKeyId` • `AssumeRole` (optional) Die folgenden Eingabepa rameter sind standardmäßig auf true gesetzt: • `IsMultiRegionTrail` • `IsOrganizationTrail` • `IncludeGlobalServi ceEvents` • `EnableLogFileValid ation` Behalten Sie die Standardw erte für die Parameter Rate Limits und Resource ID bei. Wählen Sie Speichern. Weitere Informationen finden Sie unter Behebung nicht konformer AWS-Ressourcen mit AWS Config-Regeln in der AWS Config-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die automatische Behebungsregel.	Um die automatische Behebungsregel zu testen, öffnen Sie die CloudTrail Konsole, wählen Sie Trails und dann den Trail aus. Wählen Sie Protokollierung beenden, um die Protokoll ierung für den Trail zu deaktivieren. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Protokoll ierung beenden. CloudTrail beendet die Protokollierung der Aktivitäten für diesen Trail. Folgen Sie den Anweisung en unter Evaluieren Ihrer Ressourcen in der AWS Config-Dokumentation, um sicherzustellen, dass diese automatisch wieder aktiviert CloudTrail wurden.	Systemadministrator

Zugehörige Ressourcen

Konfiguration CloudTrail

- Erstellen Sie einen S3-Bucket
- Amazon S3 S3-Bucket-Richtlinie für CloudTrail
- Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3 S3-Konsole
- Creating a trail
- Automatisierung einrichten
- Verschlüsselung von CloudTrail Protokolldateien mit verwalteten AWS KMS KMS-Schlüsseln (SSE-KMS)

Das Systems Manager Automation-Runbook erstellen und testen

- Systems Manager Manager-Dokumente erstellen
- Ausführen einer einfachen Automatisierung

Richten Sie die automatische Behebungsregel in AWS Config ein

- Verwaltung Ihrer AWS Config-Regeln
- Behebung nicht konformer AWS-Ressourcen mit AWS Config-Regeln

Weitere Ressourcen

- AWS CloudTrail — Bewährte Sicherheitsmethoden
- Erste Schritte mit AWS Systems Manager
- Erste Schritte mit AWS Config
- Erste Schritte mit AWS CloudTrail

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Automatically remediate unencrypted Amazon RDS DB instances and clusters

Erstellt von Ajay Rawat (AWS) und Josh Joy (AWS)

Übersicht

Dieses Muster beschreibt, wie unverschlüsselte Amazon Relational Database Service (Amazon RDS) -DB-Instances und -Cluster auf Amazon Web Services (AWS) mithilfe von AWS Systems Manager Runbooks und AWS Key Management Service () AWS Config-Schlüsseln automatisch behoben werden.AWS KMS

Verschlüsselte RDS-DB-Instances bieten eine zusätzliche Datenschutzebene, indem sie Ihre Daten vor unbefugtem Zugriff auf den zugrunde liegenden Speicher schützen. Sie können die Amazon RDS-Verschlüsselung verwenden, um den Datenschutz Ihrer in der bereitgestellten Anwendungen zu erhöhen und die AWS Cloud Compliance-Anforderungen für die Verschlüsselung im Ruhezustand zu erfüllen. Sie können die Verschlüsselung für eine RDS-DB-Instance aktivieren, wenn Sie sie erstellen, aber nicht, nachdem sie erstellt wurde. Sie können jedoch einer unverschlüsselten RDS-DB-Instance Verschlüsselung hinzufügen, indem Sie einen Snapshot Ihrer DB-Instance und anschließend eine verschlüsselte Kopie dieses Snapshots erstellen. Anschließend können Sie eine DB-Instance aus dem verschlüsselten Snapshot wiederherstellen, um eine verschlüsselte Kopie Ihrer ursprünglichen DB-Instance zu erhalten.

Dieses Muster wird verwendet AWS-Config-Regeln , um RDS-DB-Instances und -Cluster auszuwerten. Es wendet die Problembehebung an, indem AWS Systems Manager Runbooks verwendet werden, die die Aktionen definieren, die für nicht konforme Amazon RDS-Ressourcen ausgeführt werden sollen, sowie AWS KMS Schlüssel zum Verschlüsseln der DB-Snapshots. Anschließend werden Richtlinien zur Servicesteuerung (SCPs) durchgesetzt, um die Erstellung neuer DB-Instances und Cluster ohne Verschlüsselung zu verhindern.

Den Code für dieses Muster finden Sie unter GitHub.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Dateien aus dem GitHub Quellcode-Repository für dieses Muster wurden auf Ihren Computer heruntergeladen

- Eine unverschlüsselte RDS-DB-Instance oder -Cluster
- Ein vorhandener AWS KMS Schlüssel zum Verschlüsseln von RDS-DB-Instances und -Clustern
- Zugriff zur Aktualisierung der KMS-Schlüsselressourcenrichtlinie
- AWS Config aktiviert in Ihrem AWS-Konto (siehe Erste Schritte mit AWS Config in der AWS Dokumentation)

Einschränkungen

- Sie können die Verschlüsselung für eine RDS-DB-Instance nur aktivieren, wenn Sie sie erstellen, nicht nachdem sie erstellt wurde.
- Es ist nicht möglich, ein verschlüsseltes Lesereplikat einer unverschlüsselten DB-Instance oder ein unverschlüsseltes Lesereplikat einer verschlüsselten DB-Instance zu erstellen.
- Sie können ein unverschlüsseltes Backup oder einen solchen Snapshot nicht als verschlüsselte DB-Instance wiederherstellen.
- Amazon RDS-Verschlüsselung ist für die meisten DB-Instance-Klassen verfügbar. Eine Liste der Ausnahmen finden Sie unter Verschlüsseln von Amazon RDS-Ressourcen in der Amazon RDS-Dokumentation.
- Um einen verschlüsselten Snapshot von einem Snapshot in einen anderen AWS-Region zu kopieren, müssen Sie den KMS-Schlüssel im Ziel AWS-Region angeben. Das liegt daran, dass KMS-Schlüssel spezifisch für AWS-Region das sind, in dem sie erstellt wurden.
- Der Quell-Snapshot bleibt den gesamten Kopiervorgang über verschlüsselt. Amazon RDS verwendet Umschlagverschlüsselung, um Daten während des Kopiervorgangs zu schützen. Weitere Informationen finden Sie in der AWS KMS Dokumentation unter Umschlagverschlüsselung.
- Eine verschlüsselte DB-Instance kann nicht entschlüsselt werden. Sie können jedoch Daten aus einer verschlüsselten DB-Instance exportieren und die Daten in eine unverschlüsselte DB-Instance importieren.
- Sie sollten einen KMS-Schlüssel nur löschen, wenn Sie sicher sind, dass Sie ihn nicht mehr benötigen. Wenn Sie sich nicht sicher sind, sollten Sie den KMS-Schlüssel deaktivieren, anstatt ihn zu löschen. Sie können einen deaktivierten KMS-Schlüssel erneut aktivieren, wenn Sie ihn später erneut verwenden müssen, aber Sie können einen gelöschten KMS-Schlüssel nicht wiederherstellen.

- Wenn Sie sich nicht dafür entscheiden, automatische Backups beizubehalten, werden Ihre automatisierten Backups, die sich in derselben AWS-Region DB-Instance befinden, gelöscht. Sie können nicht wiederhergestellt werden, nachdem Sie die DB-Instance gelöscht haben.
- Ihre automatisierten Backups werden für den Aufbewahrungszeitraum aufbewahrt, der auf der DB-Instance zum Zeitpunkt des Löschens festgelegt ist. Dieser festgelegte Aufbewahrungszeitraum tritt unabhängig davon ein, ob Sie einen endgültigen DB-Snapshot erstellen möchten oder nicht.
- Wenn die automatische Wiederherstellung aktiviert ist, verschlüsselt diese Lösung alle Datenbanken, die denselben KMS-Schlüssel haben.

Architektur

Das folgende Diagramm veranschaulicht die Architektur für die AWS CloudFormation Implementierung. Beachten Sie, dass Sie dieses Muster auch mithilfe von implementieren können AWS Cloud Development Kit (AWS CDK).

Tools

Tools

- AWS CloudFormationhilft Ihnen bei der automatischen Einrichtung Ihrer AWS Ressourcen. Es ermöglicht Ihnen, eine Vorlagendatei zu verwenden, um eine Sammlung von Ressourcen zu einer einzigen Einheit (einem Stapel) zu erstellen und zu löschen.
- AWS Cloud Development Kit (AWS CDK)ist ein Softwareentwicklungs-Framework, mit dem Sie Ihre Cloud-Infrastruktur im Code definieren und mithilfe vertrauter Programmiersprachen bereitstellen können.

AWS-Services und -Funktionen

- AWS Configverfolgt die Konfiguration Ihrer AWS Ressourcen und deren Beziehungen zu Ihren anderen Ressourcen. Es kann diese AWS Ressourcen auch auf ihre Einhaltung überprüfen. Dieser Dienst verwendet Regeln, die konfiguriert werden können, um AWS Ressourcen anhand der gewünschten Konfigurationen zu bewerten. Sie können einen Satz AWS Config verwalteter Regeln für allgemeine Konformitätsszenarien verwenden, oder Sie können Ihre eigenen Regeln für benutzerdefinierte Szenarien erstellen. Wenn festgestellt wird, dass eine AWS Ressource nicht konform ist, können Sie in einem AWS Systems Manager Runbook eine Abhilfemaßnahme

angeben und optional eine Warnung über ein Amazon Simple Notification Service (Amazon SNS) -Thema senden. Mit anderen Worten, Sie können Abhilfemaßnahmen mit Ressourcen verknüpfen AWS-Config-Regeln und festlegen, dass diese automatisch ausgeführt werden, um diese zu beheben, ohne dass Sie manuell eingreifen müssen. Wenn eine Ressource nach der automatischen Korrektur immer noch nicht konform ist, können Sie die Regel so einrichten, dass die automatische Korrektur erneut versucht wird.

- Amazon Relational Database Service (Amazon RDS) erleichtert die Einrichtung, den Betrieb und die Skalierung einer relationalen Datenbank in der Cloud. Der grundlegende Baustein von Amazon RDS ist die DB-Instance, eine isolierte Datenbankumgebung in der AWS Cloud. Amazon RDS bietet eine Auswahl an Instance-Typen, die für verschiedene Anwendungsfälle relationaler Datenbanken optimiert sind. Instance-Typen bestehen aus verschiedenen Kombinationen von CPU-, Arbeitsspeicher-, Speicher- und Netzwerkkapazität und bieten Ihnen die Flexibilität, den geeigneten Ressourcenmix für Ihre Datenbank auszuwählen. Jeder Instance-Typ umfasst mehrere Instance-Größen, sodass Sie Ihre Datenbank an die Anforderungen Ihres Ziel-Workloads anpassen können.
- AWS Key Management Service (AWS KMS) ist ein verwalteter Dienst, mit dem Sie auf einfache Weise festlegen und kontrollieren können AWS KMS keys, welche Ihre Daten verschlüsseln. Ein KMS-Schlüssel ist eine logische Darstellung eines Stammschlüssels. Der KMS-Schlüssel enthält Metadaten wie die Schlüssel-ID, das Erstellungsdatum, die Beschreibung und den Schlüsselstatus.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- Richtlinien zur Dienstkontrolle (SCPs) bieten eine zentrale Kontrolle über die maximal verfügbaren Berechtigungen für alle Konten in Ihrer Organisation. SCPs helfen Ihnen dabei, sicherzustellen, dass Ihre Konten die Richtlinien für die Zugriffskontrolle Ihrer Organisation einhalten. SCPs wirken sich nicht auf Benutzer oder Rollen im Verwaltungskonto aus. Sie wirken sich nur auf die Mitgliedskonten Ihrer Organisation aus. Es wird dringend empfohlen, dass Sie keine SCPs Verbindung zum Stammverzeichnis Ihrer Organisation herstellen, ohne die Auswirkungen der Richtlinie auf Konten gründlich zu testen. Erstellen Sie stattdessen eine Organisationseinheit (OU), in die Sie Ihre Konten einzeln oder zumindest in geringer Anzahl verschieben können, um sicherzustellen, dass Sie Benutzer nicht versehentlich von wichtigen Diensten ausschließen.

Code

Der Quellcode und die Vorlagen für dieses Muster sind in einem Repository verfügbar. GitHub
Das Muster bietet zwei Implementierungsoptionen: Sie können eine AWS CloudFormation Vorlage

bereitstellen, um die Behebungsrolle zu erstellen, die RDS-DB-Instances und -Cluster verschlüsselt, oder Sie verwenden das. AWS CDK Das Repository hat separate Ordner für diese beiden Optionen.

Der Abschnitt Epics enthält step-by-step Anweisungen zur Bereitstellung der CloudFormation Vorlage. Wenn Sie die verwenden möchten AWS CDK, folgen Sie den Anweisungen in der `README.md` Datei im GitHub Repository.

Bewährte Methoden

- Aktivieren Sie die Datenverschlüsselung sowohl im Ruhezustand als auch bei der Übertragung.
- AWS Config In allen Konten aktivieren und AWS-Regionen.
- Zeichnen Sie Konfigurationsänderungen für alle Ressourcentypen auf.
- Wechseln Sie regelmäßig die IAM-Anmeldeinformationen.
- Nutzen Sie das Tagging für AWS Config, um Ressourcen einfacher zu verwalten, zu suchen und zu filtern.

Epen

Erstellen Sie die IAM-Wartungsrolle und das Systems Manager Manager-Runbook

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die CloudFormation Vorlage herunter.	Laden Sie die `unencrypted-to-encrypted-rds.template.json` Datei aus dem GitHub Repository herunter.	DevOps Ingenieur
Erstellen Sie den CloudFormation Stapel.	1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudFormation Konsole. 2. Starten Sie die `unencrypted-to-encrypted-rds.template.json` Vorlage, um einen neuen Stack zu erstellen.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen zum Bereitstellen von Vorlagen finden Sie in der AWS CloudFormation Dokumentation.	
Überprüfen Sie CloudFormation die Parameter und Werte.	1. Überprüfen Sie die Stack-Details und aktualisieren Sie die Werte auf der Grundlage Ihrer Umgebungsanforderungen. 2. Wählen Sie Stack erstellen aus, um die Vorlage bereitzustellen.	DevOps Ingenieur
Überprüfen Sie die Ressourcen.	Wenn der Stack erstellt wurde, ändert sich sein Status in CREATE_COMPLETE. Überprüfen Sie die erstellten Ressourcen (IAM-Rolle, Systems Manager Manager-Runbook) in der CloudFormation Konsole.	DevOps Ingenieur

Aktualisieren Sie die AWS KMS wichtigsten Richtlinien

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie Ihre KMS-Schlüsselrichtlinie.	1. Stellen Sie sicher, dass der Schlüssel-Alias `alias/RDSEncryptionAtRestKMSAlias` existiert. 2. Die wichtige Richtlinienerklärung sollte die Rolle	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der IAM-Problembehebung enthalten. (Überprüfen Sie die Ressourcen, die mit der CloudFormation Vorlage erstellt wurden, die Sie im vorherigen Epic bereitgestellt haben.) 3. Aktualisieren Sie in der folgenden wichtigen Richtlinie die fett gedruckten Bereiche so, dass sie Ihrem Konto und der IAM-Rolle entsprechen, die erstellt wurde. `{ "Sid": "Allow access through RDS for all principals in the account that are authorized to use RDS", "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam:: <your-AWS-account-ID>”:role/<your-IAM-remediation-role>" }, "Action": ["kms:Encrypt", "kms:Decrypt", "kms:ReEncrypt*", "kms:GenerateDataKey*",`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	"kms:Crea
	teGrant",
	"kms:List
	Grants",
	"kms:Desc
	ribeKey"
	],
	"Resource": "*",
	"Condition": {
	"StringEquals":
	{
	"kms:ViaS
	ervice": "rds.us-e
	ast-1.amazonaws.com",
	"kms:Call
	erAccount": "<your-AW
	S-account-ID>"
	}
	}
	}	

Finden und korrigieren Sie nicht richtlinienkonforme Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ressourcen anzeigen, die nicht den Vorschriften entsprechen.	1. Um eine Liste der nicht konformen Ressourcen anzuzeigen, öffnen Sie die AWS Config Konsole. 2. Wählen Sie im Navigationsbereich Regeln und dann die `rds-storage-encrypted` Regel aus. Bei den in der AWS Config Konsole aufgelisteten nicht konformen Ressourcen	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	handelt es sich um Instanzen , nicht um Cluster. Die automatische Problembehebung verschlüsselt Instanzen und Cluster und erstellt entweder eine neu verschlüsselte Instanz oder einen neu erstellten Cluster. Achten Sie jedoch darauf, nicht mehrere Instanzen gleichzeitig zu standardisieren, die zu demselben Cluster gehören. Bevor Sie RDS-DB-Instances oder Volumes standardisieren, stellen Sie sicher, dass die RDS-DB-Instance nicht verwendet wird. Stellen Sie sicher, dass während der Erstellung des Snapshots keine Schreibvorgänge ausgeführt werden, um sicherzustellen, dass der Snapshot die Originaldaten enthält. Erwägen Sie, ein Wartungsfenster vorzuschreiben, in dem die Problembehebung ausgeführt wird.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Korrigieren Sie Ressourcen, die nicht den Vorschriften entsprechen.	1. Wenn Sie bereit sind und das Wartungsfenster aktiv ist, wählen Sie die Ressource aus, die Sie korrigieren möchten, und klicken Sie dann auf Korrigieren. In der Spalte Aktionsstatus sollte jetzt die Meldung Ausführung der Aktion in der Warteschlange angezeigt werden. 2. Zeigen Sie den Fortschritt und den Status der Problembehebung in Systems Manager an. Öffnen Sie die Systems Manager-Konsole. Wählen Sie im Navigationsbereich Automatisierung und dann die Ausführungs-ID der entsprechenden Automatisierung aus, um weitere Details anzuzeigen.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie sicher, dass die RDS-DB-Instance verfügbar ist.	Nach Abschluss der Automatisierung wird die neu verschlüsselte RDS-DB-Instance verfügbar. Die verschlüsselte RDS-DB-Instance wird das Präfix `encrypted` gefolgt vom ursprünglichen Namen haben. Wenn beispielsweise der Name der unverschlüsselten RDS-DB-Instance lauten würde`database-1` , wäre `encrypted-database-1` dies auch der Name der neu verschlüsselten RDS-DB-Instance.	DevOps Ingenieur
Beenden Sie die unverschlüsselte Instanz.	Nachdem die Wiederherstellung abgeschlossen ist und die neu verschlüsselte Ressource validiert wurde, können Sie die unverschlüsselte Instanz beenden. Stellen Sie sicher, dass die neu verschlüsselte Ressource mit der unverschlüsselten Ressource übereinstimmt, bevor Sie Ressourcen beenden.	DevOps Ingenieur

Durchsetzen SCPs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Durchsetzen SCPs.	Erzwingen SCPs Sie es, um zu verhindern, dass DB-Instances und -Cluster in future ohne Verschlüsselung erstellt werden. Verwenden Sie zu diesem Zweck die `rds_encrypted.json` Datei, die im GitHub Repository bereitgestellt wird, und folgen Sie den Anweisungen in der AWS Dokumentation.	Sicherheitsingenieur

Zugehörige Ressourcen

Referenzen

- Einrichtung AWS Config
- AWS Config benutzerdefinierte Regeln
- AWS KMS Konzepte
- AWS Systems Manager Dokumente
- Service-Kontrollrichtlinien

Tools

- AWS CloudFormation
- AWS Cloud Development Kit (AWS CDK)

Anleitungen und Muster

- Automatische Reaktivierung AWS CloudTrail mithilfe einer benutzerdefinierten Behebungsregel in AWS Config

Zusätzliche Informationen

Wie funktioniert das? AWS Config

Bei der Verwendung werden zunächst die unterstützten AWS Ressourcen erkannt AWS Config, die in Ihrem Konto vorhanden sind, und für jede Ressource wird ein Konfigurationselement generiert. AWS Config generiert außerdem Konfigurationselemente, wenn sich die Konfiguration einer Ressource ändert, und verwaltet historische Aufzeichnungen der Konfigurationselemente Ihrer Ressourcen ab dem Zeitpunkt, an dem Sie den Konfigurationsrekorder starten. AWS Config Erstellt standardmäßig Konfigurationselemente für jede unterstützte Ressource in der AWS-Region. Wenn Sie nicht Konfigurationselemente für alle unterstützten Ressourcen erstellen möchten AWS Config , können Sie die Ressourcentypen angeben, die nachverfolgt werden sollen.

Wie sind AWS Config und AWS-Config-Regeln hängen damit zusammen AWS Security Hub?

AWS Security Hub ist ein Sicherheits- und Compliance-Service, der Sicherheits- und Compliance-Management als Service anbietet. Er verwendet AWS Config und AWS-Config-Regeln als primären Mechanismus zur Bewertung der Konfiguration von AWS Ressourcen. AWS-Config-Regeln kann auch verwendet werden, um die Ressourcenkonfiguration direkt auszuwerten. Andere AWS-Services, solche AWS Control Tower und AWS Firewall Manager, auch verwenden AWS-Config-Regeln.

Automatische und skalierbare Rotation von IAM-Benutzerzugriffsschlüsseln mit AWS Organizations und AWS Secrets Manager

Erstellt von Tracy Hickey (AWS), Gaurav Verma (AWS), Laura Seletos (AWS), Michael Davie (AWS) und Arvind Patel (AWS)

Übersicht

> **Important**
>
> Als bewährte Methode empfiehlt AWS, dass Sie AWS Identity and Access Managemen t (IAM) -Rollen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen wie Zugriffsschlüsseln verwenden. Der in diesem Muster dokumentierte Ansatz ist nur für ältere Implementierungen vorgesehen, für die langlebige AWS-API-Anmeldeinformatione n erforderlich sind. Für diese Implementierungen empfehlen wir dennoch, Optionen für die Verwendung kurzfristiger Anmeldeinformationen in Betracht zu ziehen, z. B. die Verwendung von Amazon Elastic Compute Cloud (Amazon EC2) -Instanzprofilen oder IAM Roles Anywhere. Der Ansatz in diesem Artikel ist nur für Fälle vorgesehen, in denen Sie nicht sofort auf die Verwendung kurzfristiger Anmeldeinformationen umsteigen können und Sie verlangen, dass langfristige Anmeldeinformationen nach einem bestimmten Zeitplan rotiert werden. Bei diesem Ansatz sind Sie dafür verantwortlich, Ihren alten Anwendung scode oder Ihre Konfiguration regelmäßig zu aktualisieren, um die rotierten API-Anmel deinformationen zu verwenden.

Zugriffsschlüssel sind langfristige Anmeldeinformationen für einen IAM-Benutzer. Durch die regelmäßige Rotation Ihrer IAM-Anmeldeinformationen können Sie verhindern, dass ein kompromittierter Satz von IAM-Zugriffsschlüsseln auf Komponenten in Ihrem AWS-Konto zugreift. Die Rotation der IAM-Anmeldeinformationen ist auch ein wichtiger Bestandteil der bewährten Sicherheitsverfahren in IAM.

Dieses Muster hilft Ihnen dabei, IAM-Zugriffsschlüssel mithilfe von CloudFormation AWS-Vorlagen, die im GitHub IAM-Schlüsselrotationsrepository bereitgestellt werden, automatisch zu rotieren.

Das Muster unterstützt die Bereitstellung in einem einzelnen Konto oder in mehreren Konten. Wenn Sie AWS Organizations verwenden, identifiziert diese Lösung alle AWS-Konten IDs innerhalb Ihrer Organisation und skaliert dynamisch, wenn Konten entfernt oder neue Konten erstellt werden. Die zentralisierte AWS Lambda Lambda-Funktion verwendet eine angenommene IAM-Rolle, um die Rotationsfunktionen lokal für mehrere von Ihnen ausgewählte Konten auszuführen.

- Neue IAM-Zugriffsschlüssel werden generiert, wenn die vorhandenen Zugriffsschlüssel 90 Tage alt sind.
- Die neuen Zugriffsschlüssel werden als Geheimnis in AWS Secrets Manager gespeichert. Eine ressourcenbasierte Richtlinie ermöglicht es nur dem angegebenen IAM-Prinzipal, auf das Geheimnis zuzugreifen und es abzurufen. Wenn Sie Schlüssel im Verwaltungskonto speichern möchten, werden die Schlüssel für alle Konten im Verwaltungskonto gespeichert.
- Die E-Mail-Adresse, die dem Besitzer des AWS-Kontos zugewiesen wurde, auf dem die neuen Zugriffsschlüssel erstellt wurden, erhält eine Benachrichtigung.
- Die vorherigen Zugangsschlüssel werden deaktiviert, wenn sie 100 Tage alt sind, und dann gelöscht, wenn sie 110 Tage alt sind.
- Eine zentrale E-Mail-Benachrichtigung wird an den AWS-Kontoinhaber gesendet.

Lambda-Funktionen und Amazon führen diese Aktionen CloudWatch automatisch aus. Sie können dann das neue Zugriffsschlüsselpaar abrufen und es in Ihrem Code oder Ihren Anwendungen ersetzen. Die Rotations-, Lösch- und Deaktivierungszeiträume können angepasst werden.

Voraussetzungen und Einschränkungen

- Mindestens ein aktives AWS-Konto.
- AWS Organizations, konfiguriert und eingerichtet (siehe Tutorial).
- Berechtigungen zur Abfrage von AWS Organizations von Ihrem Verwaltungskonto aus. Weitere Informationen finden Sie unter AWS Organizations und serviceverknüpften Rollen in der Dokumentation zu AWS Organizations.
- Ein IAM-Principal, der berechtigt ist, die CloudFormation AWS-Vorlage und die zugehörigen Ressourcen zu starten. Weitere Informationen finden Sie in der CloudFormation AWS-Dokumentation unter Gewähren selbstverwalteter Berechtigungen.
- Ein vorhandener Amazon Simple Storage Service (Amazon S3) -Bucket zur Bereitstellung der Ressourcen.

- Amazon Simple Email Service (Amazon SES) wurde aus der Sandbox entfernt. Weitere Informationen finden Sie unter Verlassen der Amazon SES SES-Sandbox in der Amazon SES SES-Dokumentation.
- Wenn Sie Lambda in einer Virtual Private Cloud (VPC) ausführen möchten, sollten die folgenden Ressourcen erstellt werden, bevor Sie die CloudFormation Hauptvorlage ausführen:
  - Eine VPC.
  - ein Subnetz.
  - Endpunkte für Amazon SES, AWS Systems Manager, AWS Security Token Service (AWS STS), Amazon S3 und AWS Secrets Manager. (Sie können die Endpunktvorlage ausführen, die im GitHub IAM-Repository für die Schlüsselrotation bereitgestellt wird, um diese Endpoints zu erstellen.)
- Der SMTP-Benutzer (Simple Mail Transfer Protocol) und das Passwort, die in den AWS Systems Manager Manager-Parametern (SSM-Parameter) gespeichert sind. Die Parameter müssen mit den wichtigsten CloudFormation Vorlagenparametern übereinstimmen.

Architektur

Technologie-Stack

- Amazon CloudWatch
- Amazon EventBridge
- IAM
- AWS Lambda
- AWS Organizations
- Amazon S3

Architektur

Die folgenden Diagramme zeigen die Komponenten und Workflows für dieses Muster. Die Lösung unterstützt zwei Szenarien für das Speichern der Anmeldeinformationen: in einem Mitgliedskonto und im Verwaltungskonto.

Option 1: Speichern Sie die Anmeldeinformationen in einem Mitgliedskonto

Option 2: Speichern Sie die Anmeldeinformationen im Verwaltungskonto

Die Diagramme zeigen den folgenden Arbeitsablauf:

1. Ein EventBridge Ereignis initiiert alle 24 Stunden eine `account_inventory` Lambda-Funktion.
2. Diese Lambda-Funktion fragt AWS Organizations nach einer Liste aller AWS-Konten IDs, Kontonamen und Konto-E-Mails ab.
3. Die `account_inventory` Lambda-Funktion initiiert eine `access_key_auto_rotation` Lambda-Funktion für jede AWS-Konto-ID und übergibt die Metadaten zur weiteren Verarbeitung an sie.
4. Die `access_key_auto_rotation` Lambda-Funktion verwendet eine angenommene IAM-Rolle, um auf die AWS-Konto-ID zuzugreifen. Das Lambda-Skript führt eine Prüfung aller Benutzer und ihrer IAM-Zugriffsschlüssel im Konto durch.
5. Wenn das Alter des IAM-Zugriffsschlüssels den Best-Practice-Schwellenwert nicht überschritten hat, ergreift die Lambda-Funktion keine weiteren Maßnahmen.
6. Wenn das Alter des IAM-Zugriffsschlüssels den Best-Practice-Schwellenwert überschritten hat, bestimmt die `access_key_auto_rotation` Lambda-Funktion, welche Rotationsaktion ausgeführt werden soll.
7. Wenn eine Aktion erforderlich ist, erstellt und aktualisiert die `access_key_auto_rotation` Lambda-Funktion ein Geheimnis in AWS Secrets Manager, wenn ein neuer Schlüssel generiert wird. Außerdem wird eine ressourcenbasierte Richtlinie erstellt, die es nur dem angegebenen IAM-Prinzipal ermöglicht, auf das Geheimnis zuzugreifen und es abzurufen. Bei Option 1 werden die Anmeldeinformationen im Secrets Manager im jeweiligen Konto gespeichert. Bei Option 2 (wenn das `StoreSecretsInCentralAccount` Flag auf True gesetzt ist) werden die Anmeldeinformationen im Secrets Manager im Verwaltungskonto gespeichert.
8. Eine `notifier` Lambda-Funktion wird initiiert, um den Kontoinhaber über die Rotationsaktivität zu informieren. Diese Funktion empfängt die AWS-Konto-ID, den Kontonamen, die Konto-E-Mail und die durchgeführten Rotationsaktionen.
9. Die `notifier` Lambda-Funktion fragt den S3-Bereitstellungs-Bucket nach einer E-Mail-Vorlage ab und aktualisiert ihn dynamisch mit den entsprechenden Aktivitätsmetadaten. Die E-Mail wird dann an die E-Mail-Adresse des Kontoinhabers gesendet.

Hinweise:

- Diese Lösung unterstützt Ausfallsicherheit in mehreren Availability Zones. Es unterstützt jedoch keine Resilienz in mehreren AWS-Regionen. Für Support in mehreren Regionen können Sie

die Lösung in der zweiten Region bereitstellen und die EventBridge Schlüsselrotationsregel deaktiviert lassen. Sie können die Regel dann aktivieren, wenn Sie die Lösung in der zweiten Region ausführen möchten.

- Sie können diese Lösung im Überwachungsmodus ausführen. Im Überwachungsmodus werden die IAM-Zugriffsschlüssel nicht geändert, es wird jedoch eine E-Mail gesendet, um die Benutzer zu benachrichtigen. Um die Lösung im Auditmodus auszuführen, setzen Sie das `DryRunFlag` Flag auf True, wenn Sie die Vorlage für die Schlüsselrotation oder in der Umgebungsvariablen für die `access_key_auto_rotation` Lambda-Funktion ausführen.

Automatisierung und Skalierung

Die CloudFormation Vorlagen zur Automatisierung dieser Lösung befinden sich im GitHub IAM-Repository für die Schlüsselrotation und sind im Abschnitt Code aufgeführt. In AWS Organizations können CloudFormation StackSetsSie die `ASA-iam-key-auto-rotation-iam-assumed-roles.yaml` CloudFormation Vorlage für mehrere Konten bereitstellen, anstatt die Lösung einzeln für jedes Mitgliedskonto bereitzustellen.

Tools

AWS-Services

- Amazon CloudWatch hilft Ihnen dabei, die Metriken Ihrer AWS-Ressourcen und der Anwendungen, die Sie auf AWS ausführen, in Echtzeit zu überwachen.
- Mit AWS Identity and Access Management (IAM) können Sie den Zugriff auf Ihre AWS-Ressourcen sicher verwalten, indem Sie kontrollieren, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten.
- AWS Secrets Manager hilft Ihnen dabei, hartcodierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Geheimnis programmgesteuert abzurufen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

- Amazon Simple Email Service (Amazon SES) unterstützt Sie beim Senden und Empfangen von E-Mails mithilfe Ihrer eigenen E-Mail-Adressen und Domains.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.
- Amazon VPC-Endpunkte bieten eine Schnittstelle für die Verbindung zu Services, die von AWS betrieben werden PrivateLink, einschließlich vieler AWS-Services. Für jedes Subnetz, das Sie von Ihrer VPC aus angeben, wird eine Endpunkt-Netzwerkschnittstelle im Subnetz erstellt und eine private IP-Adresse aus dem Subnetzadressbereich zugewiesen.

Code

Die erforderlichen CloudFormation AWS-Vorlagen, Python-Skripte und die Runbook-Dokumentation sind im GitHub IAM-Repository für die Schlüsselrotation verfügbar. Die Vorlagen werden wie folgt bereitgestellt.

Vorlage	Bereitstellen in	Hinweise
`ASA-iam-key-auto-rotation-and-notifier-solution.yaml`	Bereitstellungskonto	Dies ist die Hauptvorlage für die Lösung.
`ASA-iam-key-auto-rotation-iam-assumed-roles.yaml`	Einzelne oder mehrere Mitgliedskonten, bei denen Sie die Anmeldeinformationen wechseln möchten	Sie können CloudFormation Stacksets verwenden, um diese Vorlage in mehreren Konten bereitzustellen.
`ASA-iam-key-auto-rotation-list-accounts-role.yaml`	Zentral-/Verwaltungskonto	Verwenden Sie diese Vorlage, um ein Inventar der Konten in AWS Organizations zu führen.

`ASA-iam-key-auto-rotation-vpc-endpoints.yaml`	Bereitstellungskonto	Verwenden Sie diese Vorlage nur dann, um die Erstellung von Endpoints zu automatisieren, wenn Sie die Lambda-Funktionen in einer VPC ausführen möchten (setzen Sie den `RunLambdaInVPC` Parameter in der Hauptvorlage auf True).

Epen

Richten Sie die Lösung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie Ihren S3-Bucket für die Bereitstellung aus.	Melden Sie sich bei der AWS-Managementkonsole für Ihr Konto an, öffnen Sie die Amazon S3 S3-Konsole und wählen Sie dann den S3-Bucket für Ihre Bereitstellung aus. Wenn Sie die Lösung für mehrere Konten in AWS Organizations implementieren möchten, melden Sie sich mit dem Verwaltungskonto Ihrer Organisation an.	Cloud-Architekt
Klonen Sie das Repository	Klonen Sie das GitHub IAM-Repository für die Schlüsselrotation auf Ihren lokalen Desktop.	Cloud-Architekt
Laden Sie die Dateien in den S3-Bucket hoch.	Laden Sie die geklonten Dateien in Ihren S3-Bucket	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	hoch. Verwenden Sie die folgende Standardordnerstruktur, um alle geklonten Dateien und Verzeichnisse zu kopieren und einzufügen: `asa/asa-iam-rotation` **Note** Sie können diese Ordnerstruktur in den CloudFormation Vorlagen anpassen.	
Ändern Sie die E-Mail-Vorlage.	Ändern Sie die `iam-auto-key-rotation-enforcement.html` E-Mail-Vorlage (im `template` Ordner) gemäß Ihren Anforderungen. Ersetzen Sie das `[Department Name Here]` Ende der Vorlage durch den Namen Ihrer Abteilung.	Cloud-Architekt

Stellen Sie die Lösung bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die CloudFormation Vorlage für die Schlüsselrotation.	1. Starten Sie die `ASA-iam-key-auto-rotation-and-notifier-solution.yaml` Vorlage im Bereitstellungskonto. Weitere Informationen	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	finden Sie in der CloudFormation Dokumentation unter Auswahl einer Stack-Vorlage. 2. Geben Sie Werte für Parameter an, darunter: • CloudFormation S3-Bucket-Name (`S3BucketName`) — Der Name des S3-Bereitstellungs-Buckets, der Ihren Lambda-Code enthält. • CloudFormation S3-Bucket-Präfix (`S3BucketPrefix`) — Das Präfix des S3-Buckets. • Angenommener IAM-Rollenname (`IAMRoleName`) — Der Rollenname, den die `key-rotation` Lambda-Funktion für die Rotation der Schlüssel annimmt. • Name der IAM-Ausführungsrolle (`ExecutionRoleName`) — Der Name der IAM-Ausführungsrolle, die von der `key-rotation` Lambda-Funktion verwendet wird.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Name der Inventara usführungsrolle (`Inventory Execution RoleName`) — Der Name der IAM-Ausfü hrungsrolle, die von der `account_inventory` Lambda-Funktion verwendet wird. • Dry Run Flag (Audit-Modus) (`DryRunFla g`) — Auf True setzen, um den Auditmodus zu aktivieren (Standard). Auf False setzen, um den Erzwingungsmodus zu aktivieren. • Konto zum Auflisten von Organisationskonten (`OrgListAccount`) — Die Konto-ID des Zentral-/Verwaltun gskontos, das zum Auflisten der Konten in der Organisation verwendet wird. • Rollenname der Konten auflisten (`OrgListRo le`) — Der Rollennam e, der zur Auflistung der Konten in der Organisat ion verwendet wird.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Kennzeichnung zum Speichern von Geheimnissen für das zentrale Konto (`StoreSecretsInCentralAccount`) — Auf True setzen, um Geheimnisse im zentralen Konto zu speichern. Auf False setzen, um Geheimnisse im jeweiligen Konto zu speichern. • Regionen für die Replikation der Anmeldeinformationen (`CredentialReplicationRegions`) — Die AWS-Regionen, in denen Sie die Anmeldeinformationen replizieren möchten (Secrets Manager), getrennt durch Kommas; zum Beispiel. `us-east-2,us-west-1,us-west-2` Überspringen Sie die Region, in der Sie den Stack erstellen. • Lambda in VPC ausführen (`RunLambdaInVpc`) — Auf True setzen, um Lambda-Funktionen in einer	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	angegebenen VPC auszuführen. Sie müssen VPC-Endpoints erstellt haben und ein NAT-Gateway an das Subnetz anhängen, das die Lambda-Funktion enthält. Weitere Informationen finden Sie im re:POST-Artikel, der diese Option behandelt. • VPC-ID für Lambda-Funktionen (**`VpcId`**), VPC CIDR für Sicherheitsgruppenregel (**`VpcCidr`**) und Subnetz-ID für Lambda-Funktionen (**`SubnetId`**) — Geben Sie Informationen über die VPC, CIDR und das Subnetz an, wenn Sie auf True setzen. **`RunLambdaInVpc`** • Admin-E-Mail-Adresse (**`AdminEmailAddress`**) — Eine gültige E-Mail-Adresse, an die Benachrichtigungen gesendet werden sollen. • AWS-Organisations-ID (`AWSOrgID`) — Die eindeutige ID Ihrer Organisation. Diese ID beginnt mit `o-` und	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	gefolgt von 10-32 Kleinbuchstaben oder Ziffern. • Dateiname der E-Mail-Vorlage [Auditmodus] (`EmailTemplateAudit`) und [Erzwingungsmodus] (`EmailTemplateEnforce`) — Der Dateiname der E-Mail-HTML-Vorlage, die vom `notifier` Modul für den Prüfmodus und den Erzwingungsmodus versendet werden soll. • SMTP-Benutzer-SSM-Parametername (`SMTPUserParamName`) und SMTP-Passwort SSM-Parametername (`SMTPPasswordParamName`) — Benutzer- und Kennworti nformationen für Simple Mail Transfer Protocol (SMTP).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die CloudFormation Vorlage für angenommene Rollen.	1. Starten Sie in der CloudFormation AWS-Konsole die `ASA-iam-key-auto-rotation-iam-assumed-roles.yaml` Vorlage für jedes Konto, für das Sie Schlüssel rotieren möchten. Wenn Sie mehr als ein Konto haben, können Sie die CloudFormation Hauptvorlage in Ihrem Verwaltungskonto als Stack bereitstellen und die `ASA-iam-key-auto-rotation-iam-assumed-roles.yaml` Vorlage mit CloudFormation Stack-Sets für alle erforderlichen Konten bereitstellen. Weitere Informationen finden Sie CloudFormation StackSets in der CloudFormation Dokumentation unter Arbeiten mit AWS. 2. Geben Sie Werte für die folgenden Parameter an: • Angenommener IAM-Rollenname (`IAMRoleName`) — Name der IAM-Rolle, der von der `access_key_auto_rotation` Lambda-Funktion übernommen wird. Sie können den	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Standardwert beibehalten. • Name der IAM-Ausführungsrolle (`ExecutionRoleName`) — Die IAM-Rolle, die die Unterkontenrolle zur Ausführung der Lambda-Funktion übernimmt. • Primäre AWS-Konto-ID (`PrimaryAccountID`) — Die AWS-Konto-ID, unter der die Hauptvorlage bereitgestellt wird. • IAM-Ausnahmegruppe (`IAMExemptionGroup`) — Der Name der IAM-Gruppe, der verwendet wird, um IAM-Konten zu vereinfachen, die Sie von der automatischen Schlüsselrotation ausschließen möchten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die CloudFormation Vorlage für das Kontoinventar.	1. Starten Sie die `ASA-iam-key-auto-rotation-list-accounts-role.yaml` Vorlage im Verwaltungs-/Zentralkonto 2. Geben Sie Werte für die folgenden Parameter an: • Angenommener IAM-Rollenname (`IAMRoleName`) — Der Name der IAM-Rolle, den die `access_key_auto_rotation` Lambda-Funktion annehmen wird. • Name der IAM-Ausführungsrolle für Account Lambda (`AccountExecutionRoleName`) — Der Name der IAM-Rolle, die die `notifier` Lambda-Funktion annehmen wird. • Name der IAM-Ausführungsrolle für die Rotation Lambda (`RotationExecutionRoleName`) — Der Name der IAM-Rolle, die die `access_key_auto_rotation` Lambda-Funktion annehmen wird.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Primäre AWS-Konto-ID (`PrimaryAccountID`) — Die AWS-Konto-ID, unter der die Hauptvorl age bereitgestellt wird.	
Starten Sie die CloudForm ation Vorlage für VPC-Endpo ints.	Diese Aufgabe ist optional. 1. Starten Sie die `ASA-iam-key-auto-rotation-vpc-endpoints.yaml` Vorlage im Bereitste llungskonto. 2. Geben Sie Werte für die folgenden Parameter an: • VPC-ID (`pVpcId`), Subnetz-ID (`pSubnetId`) und CIDR-Bereich für VPC (**`pVPCCidr`**) — Stellt Informationen über die VPC, CIDR und das Subnetz bereit. • Setzen Sie den Parameter für jeden VPC-Endpunkt auf True. Wenn Sie bereits Endpoints haben, können Sie False wählen.	Cloud-Architekt

Zugehörige Ressourcen

- Bewährte Sicherheitsmethoden in IAM (IAM-Dokumentation)
- AWS Organizations und serviceverknüpfte Rollen (Dokumentation zu AWS Organizations)

- Auswahl einer Stack-Vorlage (CloudFormation Dokumentation)
- Arbeiten mit AWS CloudFormation StackSets (CloudFormation Dokumentation)

Automatische Validierung und Bereitstellung von IAM-Richtlinien und -Rollen in einem AWS-Konto mithilfe CodePipeline von IAM Access Analyzer und AWS-Makros CloudFormation

Erstellt von Helton Ribeiro (AWS) und Guilherme Simoes (AWS)

Übersicht

Hinweis: AWS CodeCommit ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen.

Dieses Muster beschreibt die Schritte und bietet Code zum Erstellen einer Bereitstellungspipeline, die es Ihren Entwicklungsteams ermöglicht, Richtlinien und Rollen für AWS Identity and Access Management (IAM) in Ihren Amazon Web Services (AWS) -Konten zu erstellen. Dieser Ansatz hilft Ihrem Unternehmen, den Aufwand für Ihre operativen Teams zu reduzieren und den Bereitstellungsprozess zu beschleunigen. Es hilft Ihren Entwicklern auch dabei, IAM-Rollen und -Richtlinien zu erstellen, die mit Ihren bestehenden Governance- und Sicherheitskontrollen kompatibel sind.

Der Ansatz dieses Musters verwendet AWS Identity and Access Management Access Analyzer, um die IAM-Richtlinien zu validieren, die Sie den IAM-Rollen zuordnen möchten, und verwendet AWS, CloudFormation um die IAM-Rollen bereitzustellen. Anstatt jedoch die CloudFormation AWS-Vorlagendatei direkt zu bearbeiten, erstellt Ihr Entwicklungsteam IAM-Richtlinien und -Rollen im JSON-Format. Ein CloudFormation AWS-Makro wandelt diese Richtliniendateien im JSON-Format vor Beginn der Bereitstellung in AWS CloudFormation IAM-Ressourcentypen um.

Die Bereitstellungspipeline (`RolesPipeline`) umfasst Quell-, Validierungs- und Bereitstellungsphasen. Während der Quellphase überträgt Ihr Entwicklungsteam die JSON-Dateien, die die Definition der IAM-Rollen und -Richtlinien enthalten, in ein CodeCommit AWS-Repository. AWS führt CodeBuild dann ein Skript aus, um diese Dateien zu validieren, und kopiert sie in einen Amazon Simple Storage Service (Amazon S3) -Bucket. Da Ihre Entwicklungsteams keinen direkten Zugriff auf die CloudFormation AWS-Vorlagendatei haben, die in einem separaten S3-Bucket gespeichert ist, müssen sie den Erstellungs- und Validierungsprozess der JSON-Datei befolgen.

Schließlich CodeDeploy verwendet AWS während der Bereitstellungsphase einen CloudFormation AWS-Stack, um die IAM-Richtlinien und -Rollen in einem Konto zu aktualisieren oder zu löschen.

> **Important**
>
> Der Workflow dieses Musters ist ein Machbarkeitsnachweis (POC), und wir empfehlen, ihn nur in einer Testumgebung zu verwenden. Wenn Sie den Ansatz dieses Musters in einer Produktionsumgebung verwenden möchten, finden Sie in der IAM-Dokumentation unter Bewährte Sicherheitsmethoden in IAM weitere Informationen und nehmen Sie die erforderlichen Änderungen an Ihren IAM-Rollen und AWS-Services vor.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein neuer oder vorhandener S3-Bucket für die Pipeline. `RolesPipeline` Stellen Sie sicher, dass die von Ihnen verwendeten Zugangsdaten berechtigt sind, Objekte in diesen Bucket hochzuladen.
- AWS-Befehlszeilenschnittstelle (AWS CLI), installiert und konfiguriert. Weitere Informationen dazu finden Sie unter Installation, Aktualisierung und Deinstallation der AWS-CLI in der AWS-CLI-Dokumentation.
- AWS Serverless Application Model (AWS SAM) CLI, installiert und konfiguriert. Weitere Informationen dazu finden Sie unter Installation der AWS SAM CLI in der AWS SAM-Dokumentation.
- Python 3, auf Ihrem lokalen Computer installiert. Weitere Informationen dazu finden Sie in der Python-Dokumentation.
- Ein Git-Client, installiert und konfiguriert.
- Das GitHub `IAM roles pipeline` Repository, auf Ihren lokalen Computer geklont.
- Bestehende IAM-Richtlinien und -Rollen im JSON-Format. Weitere Informationen dazu finden Sie in der ReadMeDatei im Github-Repository. `IAM roles pipeline`
- Ihr Entwicklerteam darf nicht berechtigt sein, die AWS- CodePipeline CodeBuild, und CodeDeploy Ressourcen dieser Lösung zu bearbeiten.

Einschränkungen

- Der Workflow dieses Musters ist ein Machbarkeitsnachweis (POC), und wir empfehlen, ihn nur in einer Testumgebung zu verwenden. Wenn Sie den Ansatz dieses Musters in einer

Produktionsumgebung verwenden möchten, finden Sie in der IAM-Dokumentation unter Bewährte Sicherheitsmethoden in IAM weitere Informationen und nehmen Sie die erforderlichen Änderungen an Ihren IAM-Rollen und AWS-Services vor.

Architektur

Das folgende Diagramm zeigt, wie Sie mithilfe CodePipeline von IAM Access Analyzer und CloudFormation AWS-Makros automatisch IAM-Rollen und -Richtlinien für ein Konto validieren und bereitstellen.

Das Diagramm zeigt den folgenden Workflow:

1. Ein Entwickler schreibt JSON-Dateien, die die Definitionen für die IAM-Richtlinien und -Rollen enthalten. Der Entwickler überträgt den Code in ein CodeCommit Repository und initiiert CodePipeline dann die Pipeline. `RolesPipeline`
2. CodeBuild validiert die JSON-Dateien mithilfe von IAM Access Analyzer. Wenn sicherheits- oder fehlerbezogene Ergebnisse vorliegen, wird der Bereitstellungsprozess gestoppt.
3. Wenn keine sicherheits- oder fehlerbezogenen Ergebnisse vorliegen, werden die JSON-Dateien an den S3-Bucket gesendet. `RolesBucket`
4. Ein als AWS-Lambda-Funktion implementiertes CloudFormation AWS-Makro liest dann die JSON-Dateien aus dem `RolesBucket` Bucket und wandelt sie in AWS CloudFormation IAM-Ressourcentypen um.
5. Ein vordefinierter CloudFormation AWS-Stack installiert, aktualisiert oder löscht die IAM-Richtlinien und -Rollen im Konto.

Automatisierung und Skalierung

CloudFormation AWS-Vorlagen, die dieses Muster automatisch bereitstellen, werden im Pipeline-Repository für GitHub IAM-Rollen bereitgestellt.

Tools

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- IAM Access Analyzer hilft Ihnen dabei, die Ressourcen in Ihrer Organisation und Konten, wie S3-Buckets oder IAM-Rollen, zu identifizieren, die mit einer externen Entität gemeinsam genutzt werden. Dies hilft Ihnen, unbeabsichtigten Zugriff auf Ihre Ressourcen und Daten zu identifizieren.
- Das AWS Serverless Application Model (AWS SAM) ist ein Open-Source-Framework, mit dem Sie serverlose Anwendungen in der AWS-Cloud erstellen können.

Code

Der Quellcode und die Vorlagen für dieses Muster sind im Pipeline-Repository für GitHub IAM-Rollen verfügbar.

Epen

Klonen Sie das Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Beispiel-Repository.	Klonen Sie das Pipeline-Repository für GitHub IAM-Rollen auf Ihren lokalen Computer.	App-Entwickler, General AWS

Stellen Sie die RolesPipeline Pipeline bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Pipeline bereit.	1. Navigieren Sie zu dem Verzeichnis, das das geklonte Repository enthält. 2. **Important** Führen Sie den `make deploy`	App-Entwickler, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`bucket=<bucket_name>` Befehl aus.: Sie müssen ihn `<bucket_name>` durch den Bucket-Namen für Ihren vorhandenen S3-Bucket ersetzen. 3. Führen Sie den `aws codepipeline get-pipeline –name RolesPipeline` Befehl aus, um zu überprüfen, ob Ihre Bereitstellung erfolgreich ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository der Pipeline.	1. Der `RolesPipeline` CloudFormation AWS-Stack erstellt das `roles-pipeline-repo` CodeCommit Repository. 2. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die CodeCommit AWS-Konsole und kopieren Sie dann die URL des CodeCommit Repositorys, um es auf Ihren lokalen Computer zu klonen. Weitere Informationen dazu finden Sie in der CodeCommit AWS-Dokumentation unter Connect zu einem CodeCommit AWS-Repository herstellen.	App-Entwickler, General AWS

Testen Sie die RolesPipeline Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die RolesPipeline Pipeline mit gültigen IAM-Richtlinien und -Rollen.	1. Erstellen Sie JSON-Dateien für Ihre IAM-Richtlinien und -Rollen. Sie können die Beispiele im `role-example` Verzeichnis aus dem GitHub `IAM roles pipeline` Repository verwenden.	App-Entwickler, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. **Important** Definieren Sie Ihre IAM-Richtlinien und -Rollen mit den erforderlichen Konfigurationen. : Stellen Sie sicher, dass Sie das in der `ReadMe` Datei aus dem GitHub `IAM roles pipeline` Repository beschriebene Format einhalten. 3. Schieben Sie die Änderungen in das `roles-pipeline-repo` CodeCommit Repository. 4. Überprüfen Sie die Implementierung der `RolesPipeline` Pipeline. 5. Stellen Sie sicher, dass die IAM-Richtlinien und -Rollen korrekt im Konto bereitgestellt sind. 6. Überprüfen Sie, ob den IAM-Richtlinien oder -Rollen eine Berechtigungsgrenze zugeordnet ist. Weitere Informationen dazu finden Sie in der IAM-Dokum	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	entation unter Berechtig ungsgrenzen für IAM-Entit äten.	
Testen Sie die RolesPipeline Pipeline mit ungültigen IAM-Richtlinien und -Rollen.	1. Ändern Sie das `roles-pipeline-repo` CodeCommit Repository und fügen Sie ungültige IAM-Rollen oder -Richtlin ien hinzu. Sie können beispielsweise eine Aktion verwenden, die nicht existiert, oder eine ungültige IAM-Richtlinienversion. 2. Überprüfen Sie die Pipeline-Implementierung. IAM Access Analyzer stoppt die Pipeline während der Überprüfungsphase, wenn ungültige IAM-Richt linien oder -Rollen erkannt werden.	App-Entwickler, General AWS

Bereinigen Ihrer Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereite dich auf die Säuberung vor.	Leeren Sie die S3-Bucket s und führen Sie dann den `destroy` Befehl aus.	App-Entwickler, General AWS
Löschen Sie den RolesStack Stack.	1. Die `RolesPipeline` Pipeline erstellt einen `RolesStack` CloudForm ation AWS-Stack, der die	App-Entwickler, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	IAM-Richtlinien und -Rollen bereitstellt. Sie müssen diesen Stack löschen, bevor Sie die `RolesPipeline` Pipeline löschen. 2. Melden Sie sich bei der AWS-Managementkonsole an, öffnen Sie die CloudFormation AWS-Konsole, wählen Sie dann den `RolesStack` Stack aus und klicken Sie auf Löschen.	
Löschen Sie den RolesPipeline Stack.	Um den `RolesPipeline` CloudFormation AWS-Stack zu löschen, folgen Sie den Anweisungen in der ReadMeDatei im `IAM roles pipeline` Github-Repository.	App-Entwickler, General AWS

Zugehörige Ressourcen

- IAM Access Analyzer — Richtlinienvalidierung (AWS-News-Blog)
- Verwenden von CloudFormation AWS-Makros zur benutzerdefinierten Verarbeitung von Vorlagen (CloudFormation AWS-Dokumentation)
- Lambda-Funktionen mit Python erstellen (AWS Lambda Lambda-Dokumentation)

Bidirektionale Integration AWS Security Hub mit Jira-Software

Erstellt von Joaquin Rinaudo (AWS)

Übersicht

Diese Lösung unterstützt eine bidirektionale Integration zwischen und Jira. AWS Security Hub Mit dieser Lösung können Sie automatisch und manuell Jira-Tickets anhand der Ergebnisse von Security Hub erstellen und aktualisieren. Sicherheitsteams können diese Integration verwenden, um Entwicklerteams über schwerwiegende Sicherheitslücken zu informieren, die Maßnahmen erfordern.

Die Lösung ermöglicht Ihnen:

- Wählen Sie aus, welche Security Hub Hub-Kontrollen automatisch Tickets in Jira erstellen oder aktualisieren.
- Verwenden Sie in der Security Hub Hub-Konsole benutzerdefinierte Security Hub Hub-Aktionen, um Tickets in Jira manuell zu eskalieren.
- Weisen Sie Tickets in Jira automatisch auf der Grundlage der in definierten AWS-Konto Tags zu. AWS Organizations Wenn dieses Tag nicht definiert ist, wird ein Standardverantwortlicher verwendet.
- Unterdrücken Sie automatisch Security Hub Hub-Ergebnisse, die in Jira als falsch positiv oder als akzeptiertes Risiko gekennzeichnet sind.
- Schließt ein Jira-Ticket automatisch, wenn das zugehörige Ergebnis im Security Hub archiviert wird.
- Öffnen Sie Jira-Tickets erneut, wenn Security Hub Hub-Ergebnisse erneut auftreten.

Jira-Workflow

Die Lösung verwendet einen benutzerdefinierten Jira-Workflow, der es Entwicklern ermöglicht, Risiken zu verwalten und zu dokumentieren. Während das Problem den Workflow durchläuft, stellt die bidirektionale Integration sicher, dass der Status des Jira-Tickets und der Security Hub Hub-Ergebnisse in den Workflows in beiden Diensten synchronisiert werden. Dieser Workflow ist ein Derivat von SecDevOps Risk Workflow von Dinis Cruz, lizenziert unter der Apache License Version 2.0. Wir empfehlen, eine Jira-Workflow-Bedingung hinzuzufügen, sodass nur Mitglieder Ihres Sicherheitsteams den Ticketstatus ändern können.

Ein Beispiel für ein Jira-Ticket, das von dieser Lösung automatisch generiert wird, finden Sie im Abschnitt Zusätzliche Informationen dieses Musters.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Wenn Sie diese Lösung in einer Umgebung mit mehreren Konten AWS bereitstellen möchten:
  - Ihre Umgebung mit mehreren Konten ist aktiv und wird von verwaltet. AWS Organizations
  - Security Hub ist auf Ihrem aktiviert AWS-Konten.
  - AWS Organizations In haben Sie ein Security Hub-Administratorkonto eingerichtet.
  - Sie haben eine kontoübergreifende Rolle AWS Identity and Access Management (IAM), die über `AWSOrganizationsReadOnlyAccess` Berechtigungen für das AWS Organizations Verwaltungskonto verfügt.
  - (Optional) Sie haben Ihre AWS-Konten mit markiert. `SecurityContactID` Dieses Tag wird verwendet, um Jira-Tickets den definierten Sicherheitskontakten zuzuweisen.
- Wenn Sie diese Lösung in einer einzigen AWS-Konto Lösung bereitstellen möchten:
  - Sie haben eine aktive AWS-Konto.
  - Security Hub ist auf Ihrem aktiviert AWS-Konto.
- Eine Jira Data Center-Instanz

> **Important**
>
> Diese Lösung unterstützt die Verwendung von Jira Cloud. Jira Cloud unterstützt jedoch nicht den Import von XML-Workflows, sodass Sie den Workflow in Jira manuell neu erstellen müssen. Sie finden die Übergänge und den Status im Repository. GitHub

- Administratorrechte in Jira
- Eines der folgenden Jira-Token:
  - Für Jira Enterprise ein Personal Access Token (PAT). Weitere Informationen findest du unter Persönliche Zugriffstoken verwenden (Atlassian-Unterstützung).
  - Für Jira Cloud ein Jira-API-Token. Weitere Informationen findest du unter API-Token verwalten (Atlassian-Unterstützung).

Architektur

In diesem Abschnitt wird die Architektur der Lösung in verschiedenen Szenarien veranschaulicht, z. B. wenn der Entwickler und der Sicherheitsingenieur beschließen, das Risiko zu akzeptieren oder das Problem zu beheben.

Szenario 1: Der Entwickler behebt das Problem

1. Security Hub generiert ein Ergebnis gegen eine bestimmte Sicherheitskontrolle, wie sie beispielsweise im Standard AWS Foundational Security Best Practices enthalten sind.
2. Ein CloudWatch Amazon-Ereignis, das mit dem Befund und der `CreateJIRA` Aktion verknüpft ist, löst eine AWS Lambda Funktion aus.
3. Die Lambda-Funktion verwendet ihre Konfigurationsdatei und das `GeneratorId` Feld des Ergebnisses, um zu bewerten, ob sie das Ergebnis eskalieren sollte.
4. Die Lambda-Funktion bestimmt, dass das Ergebnis eskaliert werden soll, und ruft das `SecurityContactID` Konto-Tag aus dem Verwaltungskonto ab AWS Organizations . AWS Diese ID ist dem Entwickler zugeordnet und wird als Zuweisungs-ID für das Jira-Ticket verwendet.
5. Die Lambda-Funktion verwendet die in gespeicherten Anmeldeinformationen AWS Secrets Manager , um ein Ticket in Jira zu erstellen. Jira benachrichtigt den Entwickler.
6. Der Entwickler geht auf die zugrunde liegende Sicherheitslücke ein und ändert in Jira den Status des Tickets in. `TEST FIX`
7. Security Hub aktualisiert den Befund als `ARCHIVED` und ein neues Ereignis wird generiert. Dieses Ereignis veranlasst die Lambda-Funktion, das Jira-Ticket automatisch zu schließen.

Szenario 2: Der Entwickler beschließt, das Risiko zu akzeptieren

1. Security Hub generiert ein Ergebnis gegen eine bestimmte Sicherheitskontrolle, wie sie beispielsweise im Standard AWS Foundational Security Best Practices enthalten sind.
2. Ein mit dem Befund und der `CreateJIRA` Aktion verbundenes CloudWatch Ereignis initiiert eine Lambda-Funktion.
3. Die Lambda-Funktion verwendet ihre Konfigurationsdatei und das `GeneratorId` Feld des Ergebnisses, um zu bewerten, ob sie das Ergebnis eskalieren sollte.

4. Die Lambda-Funktion bestimmt, dass das Ergebnis eskaliert werden soll, und ruft das `SecurityContactID` Konto-Tag aus dem Verwaltungskonto ab AWS Organizations . AWS Diese ID ist dem Entwickler zugeordnet und wird als Zuweisungs-ID für das Jira-Ticket verwendet.
5. Die Lambda-Funktion verwendet die in Secrets Manager gespeicherten Anmeldeinformationen, um ein Ticket in Jira zu erstellen. Jira benachrichtigt den Entwickler.
6. Der Entwickler entscheidet, das Risiko zu akzeptieren, und ändert in Jira den Status des Tickets auf. `AWAITING RISK ACCEPTANCE`
7. Der Sicherheitsingenieur prüft die Anfrage und hält die geschäftliche Begründung für angemessen. Der Sicherheitsingenieur ändert den Status des Jira-Tickets in`ACCEPTED RISK`. Dadurch wird das Jira-Ticket geschlossen.
8. Ein CloudWatch tägliches Ereignis initiiert die Lambda-Aktualisierungsfunktion, die geschlossene Jira-Tickets identifiziert und die zugehörigen Security Hub Hub-Ergebnisse aktualisiert als. `SUPPRESSED`

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend AWS-Konten zu verwalten.
- Amazon CloudWatch Events unterstützt Sie bei der Überwachung von Systemereignissen für Ihre AWS Ressourcen, indem es Regeln verwendet, um Ereignisse zuzuordnen und sie an Funktionen oder Streams weiterzuleiten.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Organizationsist ein Kontoverwaltungsservice, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie erstellen und zentral verwalten.
- Mit AWS Secrets Manager können Sie fest codierte Anmeldeinformationen im Code (einschließlich Passwörter) durch einen API-Aufruf an Secrets Manager ersetzen und das Geheimnis programmgesteuert abrufen.

- AWS Security Hubbietet einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS. Es hilft Ihnen auch dabei, Ihre AWS Umgebung anhand von Industriestandards und Best Practices im Bereich Sicherheit zu überprüfen.

Code-Repository

Der Code für dieses Muster ist im Repository aws-securityhub-jira-software-integration verfügbar. GitHub Er enthält den Beispielcode und den Jira-Workflow für diese Lösung.

Epen

Jira konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Importieren Sie den Workflow.	Importieren Sie als Administrator in Jira die `issue-workflow.xml` Datei in Ihre Jira Data Center-Instanz. Wenn Sie Jira Cloud verwenden, müssen Sie den Workflow entsprechend den Dateien und erstellen . `assets/jira-cloud-transitions.png` `assets/jira-cloud-status.png` Dateien finden Sie im aws-securityhub-jira-software-integration-Repository unter. GitHub Anweisungen finden Sie unter Verwenden von XML zur Erstellung eines Workflows (Jira-Dokumentation).	Jira-Administrator
Aktivieren Sie den Workflow und weisen Sie ihn zu.	Workflows sind inaktiv, bis Sie sie einem Workflow-Schema	Jira-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zuweisen. Anschließend weisen Sie das Workflow-Schema einem Projekt zu. 1. Stellen Sie für Ihr Projekt sicher, dass Sie ein Problemtypschema für das Projekt identifiziert haben. Sie können einen neuen Problemtyp erstellen oder aus einem vorhandenen auswählen, z. Bug B. 2. Weisen Sie den importier ten Workflow einem Workflow-Schema zu. Folgen Sie den Anweisung en unter Aktivieren eines Workflows (Jira-Dok umentation). 3. Weisen Sie das Workflow-Schema einem Projekt zu. Folgen Sie den Anweisung en unter Ein Workflow-Schema einem Projekt zuordnen (Jira-Dok umentation).	

Richten Sie die Lösungsparameter ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Lösungsparameter.	1. Öffnen Sie im Ordner conf`params_pr od.shfile` .	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Geben Sie Werte für die folgenden Parameter an: • `ORG_ACCOUNT_ID` — Die Konto-ID für Ihr AWS Organizations Verwaltungskonto. Die Lösung liest Konto-Tags und weist Tickets den spezifischen Sicherheitskontakten zu, die in diesen AWS-Konto Tags definiert sind. • `ORG_ROLE`— Der Name der IAM-Rolle, die für den Zugriff auf das AWS Organizations Verwaltungskonto verwendet wird. Diese Rolle muss über `OrganizationsReadOnlyAccess` Berechtigungen verfügen. • `EXTERNAL_ID` — Ein optionaler Parameter, wenn Sie eine externe ID verwenden, um die in `ORG_ROLE` definierte IAM-Rolle anzunehmen. Weitere Informationen finden Sie unter So verwenden Sie eine externe ID (IAM-Dokumentation). • `JIRA_DEFAULT_ASSIGNEE` — Dies ist der standardmäßige	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Beauftragte von Jira für alle Sicherheitsprobleme. Dieser Standard-Beauftragte wird verwendet, falls das Konto nicht richtig markiert ist oder die Rolle nicht übernommen werden kann. • `JIRA_INSTANCE` — Die HTTPS-Adresse für Ihren Jira-Endpunkt im folgenden Format: `team-<team-id>.atlassian.net/` • `JIRA_PROJECT_KEY` — Der Name des Jira-Projektschlüssels, der zum Erstellen von Tickets verwendet wurde, z. B. `SEC` oder. `TEST` Dieses Projekt muss bereits in Jira existieren. • `ISSUE_TYPE` — Der Name des Problemtypschemas, das dem Projekt in Jira zugewiesen wurde, z. B. `Bug` oder. `Security Issue` • `REGIONS`— Liste der AWS-Region Codes, in denen Sie diese Lösung einsetzen möchten, z. B. `eu-west-1`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Speichern und schließen Sie die Lösungspa rameterdatei.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Ergebnisse, die Sie automatisieren möchten.	1. Öffnen Sie die Security Hub Hub-Konsole. 2. Wählen Sie im Security Hub-Navigationsbereich Findings aus. 3. Wählen Sie den Titel des Ergebnisses aus. 4. Wählen Sie die Fund-ID. Dadurch wird die vollständige JSON-Datei für den Befund angezeigt. 5. Kopieren Sie in der JSON-Datei die Zeichenfolge in das `GeneratorId` Feld. Dieser Wert ist im AWS Security Finding Format (ASFF) angegeben. `aws-foundational-security-best-practices/v/1.0.0/S3.1`Entspricht beispielsweise den Ergebnissen aus der Sicherheitskontrolle S3.1. Die Einstellung „Öffentlichen Zugriff sperren“ für S3 sollte aktiviert sein. 6. Wiederholen Sie diese Schritte, bis Sie alle `GeneratorID` Werte für alle Ergebnisse kopiert haben, die Sie automatisieren möchten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die Ergebnisse der Konfigurationsdatei hinzu.	1. Öffnen Sie die Datei in src/code. `config.js onconfig` 2. Fügen Sie die `Generator ID` Werte, die Sie in der vorherigen Geschicht e abgerufen haben, in den `default` Parameter ein, und trennen Sie die einzelnen IDs durch Kommas. 3. Speichern und schließen Sie die -Konfigurationsdatei. Das folgende Codebeisp iel zeigt die Automatis ierung der Ergebnisse `aws-foundational-s ecurity-best-pract ices/v/1.0.0/SNS.1` und`aws-foundational-security-best-pract ices/v/1.0.0/S3.1` . `{ "Controls" : { "eu-west-1": [ "arn:aws: securityhub:::rule set/cis-aws-founda tions-benchmark/v/ 1.2.0/rule/1.22" ], "default": [`	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>aws-foundational-security-best-practices/v/1.0.0/SNS.1,
	aws-foundational-security-best-practices/v/1.0.0/S3.1
	]
	}
	}</pre>
	Note
	Sie können wählen, ob Sie für jedes AWS-Region Ergebnis unterschiedliche Ergebnisse automatisieren möchten. Eine bewährte Methode zur Vermeidung doppelter Ergebnisse besteht darin, eine einzelne Region auszuwählen, um die Erstellung von Kontrollen im Zusammenhang mit IAM zu automatisieren.	

Stellen Sie die Integration bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Integration bereit.	Geben Sie in einem Befehlszeilenterminal den folgenden Befehl ein: `./deploy.sh prod`	AWS-Systemadministrator
Laden Sie die Jira-Anmeldeinformationen in Secrets Manager hoch.	1. Öffnen Sie die Secrets Manager-Konsole. 2. Wählen Sie unter Secrets (Geheimnisse) Store a new secret (Neues Geheimnis speichern) aus. 3. Als Secret-Typ wählen Sie Anderer Secret-Typ aus. 4. Wenn Sie Jira Enterprise verwenden, gehen Sie für Schlüssel/Wert-Paare wie folgt vor: • Geben Sie in der ersten Zeile `auth` in das Schlüsselfeld und dann `token_auth` in das Wertfeld ein. • Fügen Sie eine zweite Zeile hinzu, geben Sie sie `token` in das Schlüsselfeld ein und geben Sie dann Ihr persönliches Zugriffstoken in das Wertfeld ein.	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Wenn du Jira Cloud verwendest, gehe für Schlüssel/Wert-Paare wie folgt vor: • Geben Sie in der ersten Zeile `auth` in das Schlüsselfeld und dann `basic_auth` in das Wertfeld ein. • Fügen Sie eine zweite Zeile hinzu, geben Sie sie `token` in das Schlüssel feld ein und geben Sie dann Ihr API-Token in das Wertfeld ein. • Fügen Sie eine dritte Zeile hinzu, geben Sie sie `email` in das Schlüssel feld ein und geben Sie dann Ihre E-Mail-Adresse in das Wertfeld ein. 5. Wählen Sie Weiter aus. 6. Geben Sie das Feld Geheimer Name ein`Jira-Token` , und wählen Sie dann unten auf der Seite Weiter aus. 7. Behalten Sie auf der Seite Secret rotation (Geheimnis-Drehung) die Option Disable automatic rotation (Automatische Drehung deaktivieren) bei und	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wählen Sie dann unten auf der Seite Next (Weiter) aus. 8. Prüfen Sie auf der Seite Review (Überprüfen) die Geheimnis-Details und wählen Sie Store (Speichern).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die benutzerdefinierte Security Hub Hub-Aktion.	1. Verwenden Sie für jedes AWS-Region Objekt in AWS Command Line Interface (AWS CLI) den create-action-targetBefehl, um eine benutzerdefinierte Security Hub Hub-Aktion mit dem Namen zu erstellen `CreateJiraIssue` . `aws securityhub create-action-target --name "CreateJiraIssue" \ --description "Create ticket in JIRA" \ --id "CreateJiraIssue" --region $<aws-region>` 2. Öffnen Sie die Security Hub Hub-Konsole. 3. Wählen Sie im Security Hub-Navigationsbereich Findings aus. 4. Wählen Sie in der Ergebnisliste die Ergebnisse aus, die Sie eskalieren möchten. 5. Wählen `CreateJiraIssue` Sie im Menü Aktionen.	AWS-Systemadministrator

Zugehörige Ressourcen

- AWS Service Management-Konnektor für Jira Service Management
- AWS Standard für grundlegende Best Practices im Bereich Sicherheit

Zusätzliche Informationen

Beispiel für ein Jira-Ticket

Wenn ein bestimmter Security Hub Hub-Befund auftritt, erstellt diese Lösung automatisch ein Jira-Ticket. Das Ticket enthält die folgenden Informationen:

- Titel — Der Titel identifiziert das Sicherheitsproblem im folgenden Format:

```
AWS Security Issue :: <AWS account ID> :: <Security Hub finding title>
```

- Beschreibung — Der Beschreibungsabschnitt des Tickets beschreibt die Sicherheitskontrolle, die mit dem Ergebnis verknüpft ist, enthält einen Link zu dem Ergebnis in der Security Hub Hub-Konsole und bietet eine kurze Beschreibung, wie das Sicherheitsproblem im Jira-Workflow behandelt werden kann.

Im Folgenden finden Sie ein Beispiel für ein automatisch generiertes Jira-Ticket.

Titel	AWS Sicherheitsproblem:: 012345678912:: Lambda.1 Lambda-Funktionsrichtlinien sollten den öffentlichen Zugriff verbieten.
Beschreibung	Was ist das Problem? Wir haben eine Sicherheitslücke in der AWS-Konto 012345678912 festgestellt, für die Sie verantwortlich sind. Dieses Steuerelement prüft, ob die der Lambda-Ressource zugeordnete AWS Lambda Funktionsrichtlinie den öffentlichen Zugriff verbietet. Wenn die Lambda-Funktionsrichtlinie öffentlichen Zugriff zulässt, schlägt die Kontrolle fehl.

<Link to Security Hub finding>

Was muss ich mit dem Ticket machen?

- Greifen Sie auf das Konto zu und überprüfe n Sie die Konfiguration. Bestätigen Sie die Bearbeitung des Tickets, indem Sie es in den Bereich „Zur Behebung zugewiesen“ verschieben. Sobald das Problem behoben wurde, wurde es zur Testkorrektur übergegan gen, sodass die Sicherheit bestätigt, dass das Problem behoben ist.
- Wenn Sie der Meinung sind, dass das Risiko akzeptiert werden sollte, verschieben Sie es in „Warten auf Risikoakzeptanz“. Dies erfordert eine Überprüfung durch einen Sicherheitsingenieur.
- Wenn Sie der Meinung sind, dass es sich um ein falsch positives Ergebnis handelt, wechseln Sie zu „Als falsch positiv markieren “. Dies wird von einem Sicherheitsingenieur überprüft und entsprechend wieder geöffnet/ geschlossen.

Erstellen Sie mit EC2 Image Builder und Terraform eine Pipeline für gehärtete Container-Images

Erstellt von Mike Saintcross (AWS) und Andrew Ranes (AWS)

Übersicht

Dieses Muster erstellt eine EC2 Image Builder Builder-Pipeline, die ein gehärtetes Amazon Linux 2-Basis-Container-Image erzeugt. Terraform wird als IaC-Tool (Infrastructure as Code) zur Konfiguration und Bereitstellung der Infrastruktur verwendet, die zur Erstellung gehärteter Container-Images verwendet wird. Das Rezept hilft Ihnen bei der Bereitstellung eines Docker-basierten Amazon Linux 2-Container-Images, das gemäß Red Hat Enterprise Linux (RHEL) 7 STIG Version 3 Release 7 – Medium gehärtet wurde. (Siehe STIG-Build-Linux-Medium Version 2022.2.1 im Abschnitt Linux STIG-Komponenten der EC2 Image Builder Builder-Dokumentation.) Dies wird als goldenes Container-Image bezeichnet.

Der Build beinhaltet zwei EventBridge Amazon-Regeln. Eine Regel startet die Container-Image-Pipeline, wenn das Ergebnis von Amazon Inspector „Hoch“ oder „Kritisch“ lautet, sodass unsichere Images ersetzt werden. Für diese Regel müssen sowohl das erweiterte Scannen von Amazon Inspector als auch das erweiterte Scannen von Amazon Elastic Container Registry (Amazon ECR) aktiviert sein. Die andere Regel sendet nach einem erfolgreichen Image-Push an das Amazon ECR-Repository Benachrichtigungen an eine Amazon Simple Queue Service (Amazon SQS) - Warteschlange, um Ihnen bei der Verwendung der neuesten Container-Images zu helfen.

> **Note**
>
> Amazon Linux 2 nähert sich dem Ende des Supports. Weitere Informationen finden Sie unter Amazon Linux FAQs 2.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein AWS-Konto, in dem Sie die Infrastruktur bereitstellen können.
- Die AWS-Befehlszeilenschnittstelle (AWS CLI) wurde installiert, um Ihre AWS-Anmeldeinformationen für die lokale Bereitstellung festzulegen.

- Terraform wurde heruntergeladen und eingerichtet, indem Sie den Anweisungen in der Terraform-Dokumentation folgen.
- Git (wenn Sie von einem lokalen Computer aus bereitstellen).
- Eine Rolle innerhalb des AWS-Kontos, mit der Sie AWS-Ressourcen erstellen können.
- Alle in der Datei .tfvars definierten Variablen. Oder Sie können alle Variablen definieren, wenn Sie die Terraform-Konfiguration anwenden.

Einschränkungen

- Diese Lösung erstellt eine Amazon Virtual Private Cloud (Amazon VPC) -Infrastruktur, die ein NAT-Gateway und ein Internet-Gateway für Internetkonnektivität aus ihrem privaten Subnetz umfasst. Sie können keine VPC-Endpunkte verwenden, da der Bootstrap-Prozess von AWS Task Orchestrator and Executor (AWSTOE) AWS CLI Version 2 aus dem Internet installiert.

Produktversionen

- Amazon Linux 2
- AWS CLI Version 1.1 oder höher

Architektur

Zieltechnologie-Stack

Dieses Muster erzeugt 43 Ressourcen, darunter:

- Zwei Amazon Simple Storage Service (Amazon S3) -Buckets: einer für die Pipeline-Komponentendateien und einer für Serverzugriff und Amazon VPC-Flow-Logs
- Ein Amazon ECR-Repository
- Eine virtuelle private Cloud (VPC), die ein öffentliches Subnetz, ein privates Subnetz, Routing-Tabellen, ein NAT-Gateway und ein Internet-Gateway enthält
- Eine EC2 Image Builder Builder-Pipeline, ein Rezept und Komponenten
- Ein Container-Image
- Ein AWS Key Management Service (AWS KMS) -Schlüssel für die Bildverschlüsselung
- Eine SQS-Warteschlange

- Drei Rollen: eine für die Ausführung der EC2 Image Builder-Pipeline, ein Instanzprofil für EC2 Image Builder und eine für EventBridge Regeln
- Zwei EventBridge Regeln

Struktur des Terraform-Moduls

Den Quellcode finden Sie im GitHub Repository Terraform EC2 Image Builder Container Hardening Pipeline.

```
### components.tf
### config.tf
### dist-config.tf
### files
#   ###assumption-policy.json
### hardening-pipeline.tfvars
### image.tf
### infr-config.tf
### infra-network-config.tf
### kms-key.tf
### main.tf
### outputs.tf
### pipeline.tf
### recipes.tf
### roles.tf
### sec-groups.tf
### trigger-build.tf
### variables.tf
```

Einzelheiten zum Modul

- `components.tf`enthält eine Amazon S3 S3-Upload-Ressource, um den Inhalt des `/files` Verzeichnisses hochzuladen. Sie können hier auch modular benutzerdefinierte YAML-Komponentendateien hinzufügen.
- `/files`enthält die `.yml` Dateien, die die in verwendeten Komponenten definieren. `components.tf`
- `image.tf`enthält die Definitionen für das Basis-Image-Betriebssystem. Hier können Sie die Definitionen für eine andere Basis-Image-Pipeline ändern.
- `infr-config.tf`und `dist-config.tf` enthalten die Ressourcen für die AWS-Mindestinfrastruktur, die für die Einrichtung und Verteilung des Images erforderlich ist.

- `infra-network-config.tf`enthält die minimale VPC-Infrastruktur, in der das Container-Image bereitgestellt werden soll.
- `hardening-pipeline.tfvars`enthält die Terraform-Variablen, die zum Zeitpunkt der Anwendung verwendet werden sollen.
- `pipeline.tf`erstellt und verwaltet eine EC2 Image Builder Builder-Pipeline in Terraform.
- `recipes.tf`Hier können Sie verschiedene Mischungen von Komponenten angeben, um Container-Rezepte zu erstellen.
- `roles.tf`enthält die Definitionen der AWS Identity and Access Management (IAM) -Richtlinien für das Amazon Elastic Compute Cloud (Amazon EC2) -Instanzprofil und die Pipeline-Bereitstellungsrolle.
- `trigger-build.tf`enthält die EventBridge Regeln und SQS-Warteschlangenressourcen.

Zielarchitektur

Das Diagramm veranschaulicht den folgenden Arbeitsablauf:

1. EC2 Image Builder erstellt mithilfe des definierten Rezepts ein Container-Image, das Betriebssystemupdates installiert und RHEL Medium STIG auf das Amazon Linux 2-Basis-Image anwendet.
2. Das gehärtete Image wird in einer privaten Amazon ECR-Registry veröffentlicht, und eine EventBridge Regel sendet eine Nachricht an eine SQS-Warteschlange, wenn das Image erfolgreich veröffentlicht wurde.
3. Wenn Amazon Inspector für erweitertes Scannen konfiguriert ist, scannt er die Amazon ECR-Registrierung.
4. Wenn Amazon Inspector den Schweregrad Kritisch oder Hoch für das Image generiert, veranlasst eine EventBridge Regel, dass die EC2 Image Builder Builder-Pipeline erneut ausgeführt und ein neu gehärtetes Image veröffentlicht wird.

Automatisierung und Skalierung

- Dieses Muster beschreibt, wie Sie die Infrastruktur bereitstellen und die Pipeline auf Ihrem Computer aufbauen. Es ist jedoch für den Einsatz in großem Umfang vorgesehen. Anstatt die Terraform-Module lokal bereitzustellen, können Sie sie in einer Umgebung mit mehreren Konten verwenden, z. B. in einer AWS Control Tower mit Account Factory for Terraform-Umgebung.

In diesem Fall sollten Sie einen S3-Bucket mit Backend-Status verwenden, um Terraform-Statusdateien zu verwalten, anstatt den Konfigurationsstatus lokal zu verwalten.

- Für eine skalierte Nutzung stellen Sie die Lösung auf einem zentralen Konto bereit, z. B. einem Shared Services- oder Common Services-Konto, von einem Control Tower- oder Landingzone-Kontomodell aus und gewähren Sie Benutzerkonten die Erlaubnis, auf das Amazon ECR-Repository und den AWS KMS KMS-Schlüssel zuzugreifen. Weitere Informationen zur Einrichtung finden Sie im re:POST-Artikel Wie kann ich einem sekundären Konto erlauben, Bilder in meinem Amazon ECR-Image-Repository zu pushen oder abzurufen? Fügen Sie beispielsweise in einem Kontoautomaten oder Account Factory für Terraform Berechtigungen zu jeder Konto-Baseline oder Kontoanpassungs-Baseline hinzu, um Zugriff auf das Amazon ECR-Repository und den Verschlüsselungsschlüssel zu gewähren.
- Nachdem die Container-Image-Pipeline bereitgestellt wurde, können Sie sie mithilfe von EC2 Image Builder Builder-Funktionen wie Komponenten ändern, die Ihnen helfen, mehr Komponenten in den Docker-Build zu packen.
- Der AWS-KMS-Schlüssel, der zum Verschlüsseln des Container-Images verwendet wird, sollte von allen Konten gemeinsam genutzt werden, in denen das Image verwendet werden soll.
- Sie können Unterstützung für andere Images hinzufügen, indem Sie das gesamte Terraform-Modul duplizieren und die folgenden Attribute ändern: `recipes.tf`
  - Ändern Sie `parent_image = "amazonlinux:latest"` zu einem anderen Bildtyp.
  - Ändern Sie `repository_name` es so, dass es auf ein vorhandenes Amazon ECR-Repository verweist. Dadurch wird eine weitere Pipeline erstellt, die einen anderen übergeordneten Image-Typ für Ihr vorhandenes Amazon ECR-Repository bereitstellt.

Tools

Tools

- Terraform (IaC-Bereitstellung)
- Git (bei lokaler Bereitstellung)
- AWS CLI Version 1 oder Version 2 (bei lokaler Bereitstellung)

Kode

Der Code für dieses Muster befindet sich im GitHub Repository Terraform EC2 Image Builder Container Hardening Pipeline. Folgen Sie den Anweisungen im nächsten Abschnitt, um den Beispielcode zu verwenden.

Epen

Stellen Sie die Infrastruktur bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Richten Sie lokale Anmeldeinformationen ein.	Richten Sie Ihre temporären AWS-Anmeldeinformationen ein.
	1. Prüfen Sie, ob die AWS-CLI installiert ist:
	`$ aws --version aws-cli/1.16.249 Python/3.6.8...`
	• Die AWS-CLI-Version sollte 1.1 oder höher sein.
	• Wenn der Befehl nicht gefunden wird, installieren Sie die AWS-CLI.
	2. Führen Sie den `aws configure` Befehl aus und geben Sie die folgenden Werte an:
	`$ aws configure AWS Access Key ID [**********xxxx]: <Your AWS access key ID> AWS Secret Access Key [**********xxx`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	x]: <Your AWS secret access key> Default region name: [us-east-1]: <Your desired Region for deployment> Default output format [None]: <Your desired output format>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Klonen Sie das Repository	1. Klonen Sie das Repository, das mit diesem Muster bereitgestellt wurde. Sie können HTTPS oder Secure Shell (SSH) verwenden.
	
	HTTPS:
	
	`git clone https://github.com/aws-samples/terraform-ec2-image-builder-container-hardening-pipeline`
	
	SSH:
	
	`git clone git@github.com:aws-samples/terraform-ec2-image-builder-container-hardening-pipeline.git`
	
	2. Navigieren Sie zu Ihrem lokalen Verzeichnis, das diese Lösung enthält:
	
	`cd terraform-ec2-image-builder-container-hardening-pipeline`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Variablen aktualisieren.	Aktualisieren Sie die Variablen in der `hardening-pipeline.tfvars` Datei so, dass sie Ihrer Umgebung und Ihrer gewünschten Konfiguration entsprechen. Sie müssen Ihre eigenen angeben`account_id` . Sie sollten jedoch auch die restlichen Variablen so ändern, dass sie zu Ihrer gewünschten Bereitstellung passen. Alle Variablen sind erforderlich.
	
	`account_id = "<DEPLOYMENT-ACCOUNT-ID>"`
	`aws_region = "us-east-1"`
	`vpc_name = "example-hardening-pipeline-vpc"`
	`kms_key_alias = "image-builder-container-key"`
	`ec2_iam_role_name = "example-hardening-instance-role"`
	`hardening_pipeline_role_name = "example-hardening-pipeline-role"`
	`aws_s3_ami_resources_bucket = "example-hardening-ami-resources-bucket-0123"`
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`image_name = "example-hardening-al2-container-image"`
	`ecr_name = "example-hardening-container-repo"`
	`recipe_version = "1.0.0"`
	`ebs_root_vol_size = 10`
	
	Hier ist eine Beschreibung der einzelnen Variablen:
	• `account_id` – Die AWS-Kontonummer, in der Sie die Lösung bereitstellen möchten.
	• `aws_region` – Die AWS-Region, in der Sie die Lösung bereitstellen möchten.
	• `vpc_name`– Der Name für Ihre VPC-Infrastruktur.
	• `kms_key_alias` – Der AWS-KMS-Schlüsselname, der von der EC2 Image Builder Builder-Infrastruktkonfiguration verwendet werden soll.
	• `ec2_iam_role_name` – Der Name der Rolle, die als EC2 Instanzprofil verwendet wird.
	• `hardening_pipeline_role_name` – Der	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Name der Rolle, die für die Bereitstellung der Hardening -Pipeline verwendet wird. • `aws_s3_ami_resources_bucket` – Der Name für einen S3-Bucket, der alle Dateien hostet, die zum Erstellen der Pipeline und der Container-Images erforderlich sind. • `image_name` – Der Name des Container-Images. Dieser Wert muss zwischen 3 und 50 Zeichen lang sein und darf nur alphanumerische Zeichen und Bindestriche enthalten. • `ecr_name`– Der Name der Amazon ECR-Registrierung, in der die Container-Images gespeichert werden sollen. • `recipe_version` – Die Version des Image-Rezepts. Der Standardwert ist 1.0.0. • `ebs_root_vol_size` – Die Größe (in Gigabyte) des Amazon Elastic Block Store (Amazon EBS) -Root-Volumes. Der Standardwert ist 10 Gigabyte.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initialisieren Sie Terraform.	Nachdem Sie Ihre Variablen werte aktualisiert haben, können Sie das Terraform -Konfigurationsverzeichnis initialisieren. Durch die Initialisierung eines Konfigura tionsverzeichnisses wird der AWS-Anbieter herunterg eladen und installiert, der in der Konfiguration definiert ist. `terraform init` Sie sollten eine Meldung sehen, die besagt, dass Terraform erfolgreich initialis iert wurde und die Version des Anbieters identifiziert wird, die installiert wurde.	AWS DevOps
Stellen Sie die Infrastruktur bereit und erstellen Sie ein Container-Image.	Verwenden Sie den folgenden Befehl, um die Terraform-Module mithilfe der in Ihrer Datei definierten Variablen zu initialisieren, zu validieren und auf die Umgebung anzuwende n: `.tfvars` `terraform init && terraform validate && terraform apply -var-file *.tfvars -auto-app rove`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie den Container an.	Sie können eine neue Version eines Container-Rezepts erstellen, nachdem EC2 Image Builder die Pipeline und das erste Rezept bereitgestellt hat. Sie können jede der mehr als 31 in EC2 Image Builder verfügbaren Komponenten hinzufügen, um den Container -Build anzupassen. Weitere Informationen finden Sie im Abschnitt Komponenten unter Erstellen einer neuen Version eines Container-Rezepts in der EC2 Image Builder Builder-Dokumentation.	AWS-Administrator

Ressourcen validieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Bereitste llung der AWS-Infrastruktur.	Wenn Sie Ihren ersten `apply` Terraform-Befehl erfolgrei ch ausgeführt haben und lokal bereitstellen, sollten Sie diesen Ausschnitt im Terminal Ihres lokalen Computers sehen: `Apply complete! Resources: 43 added, 0 changed, 0 destroyed.`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie einzelne AWS-Infrastrukturressourcen.	Um die einzelnen Ressourcen zu validieren, die bereitgestellt wurden, können Sie bei einer lokalen Bereitstellung den folgenden Befehl ausführen: `terraform state list` Dieser Befehl gibt eine Liste von 43 Ressourcen zurück.	AWS DevOps

Ressourcen entfernen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entfernen Sie die Infrastruktur und das Container-Image.	Wenn Sie mit Ihrer Terraform -Konfiguration fertig sind, können Sie den folgenden Befehl ausführen, um Ressourcen zu entfernen: `terraform init && terraform validate && terraform destroy -var-file *.tfvars -auto-approve`	AWS DevOps

Fehlerbehebung

Problem	Lösung
Fehler bei der Überprüfung der Anbieteranmeldeinformationen	Wenn Sie den Terraform `apply` - oder `destroy` Befehl von Ihrem lokalen Computer

Problem	Lösung
	aus ausführen, tritt möglicherweise ein Fehler ähnlich dem folgenden auf: `Error: configuring Terraform AWS Provider: error validating provider credentials: error calling sts:GetCallerIdentity: operation error STS: GetCallerIdentity, https response error StatusCode: 403, RequestID: 123456a9-fbc1-40ed-b8d8-513d0133ba7f, api error InvalidClientTokenId: The security token included in the request is invalid.` Dieser Fehler wird durch den Ablauf des Sicherheitstokens für die in der Konfiguration Ihres lokalen Computers verwendeten Anmeldeinformationen verursacht. Informationen zur Behebung des Fehlers finden Sie unter Konfigurationseinstellungen einrichten und anzeigen in der AWS-CLI-Dokumentation.

Zugehörige Ressourcen

- Terraform EC2 Image Builder Container-Hardening-Pipeline (GitHub Repositorium)
- EC2 Image Builder Builder-Dokumentation
- AWS Control Tower Account Factory für Terraform (AWS-Blogbeitrag)
- S3-Bucket mit Backend-Status (Terraform-Dokumentation)
- Installation oder Aktualisierung der neuesten Version der AWS-CLI (AWS-CLI-Dokumentation)
- Laden Sie Terraform herunter

Zentralisieren Sie die Verwaltung von IAM-Zugriffsschlüsseln in AWS Organizations mithilfe von Terraform

Erstellt von Aarti Rajput (AWS), Chintamani Aphale (AWS), T.V.R.L.Phani Kumar Dadi (AWS), Pradip kumar Pandey (AWS), Mayuri Shinde (AWS) und Pratap Kumar Nanda (AWS)

Übersicht

AWS CodeCommit Hinweis: ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen

Die Durchsetzung von Sicherheitsregeln für Schlüssel und Passwörter ist eine wichtige Aufgabe für jedes Unternehmen. Eine wichtige Regel besteht darin, die Schlüssel von AWS Identity and Access Management (IAM) in regelmäßigen Abständen zu rotieren, um die Sicherheit zu gewährleisten. AWS-Zugriffsschlüssel werden in der Regel lokal erstellt und konfiguriert, wann immer Teams über die AWS-Befehlszeilenschnittstelle (AWS-CLI) oder über Anwendungen außerhalb von AWS auf AWS zugreifen möchten. Um eine hohe Sicherheit im gesamten Unternehmen aufrechtzuerhalten, müssen alte Sicherheitsschlüssel geändert oder gelöscht werden, nachdem die Anforderung erfüllt wurde, oder in regelmäßigen Abständen. Die Verwaltung von Schlüsselrotationen für mehrere Konten in einem Unternehmen ist zeitaufwändig und mühsam. Dieses Muster hilft Ihnen, den Rotationsprozess zu automatisieren, indem Sie Account Factory for Terraform (AFT) und AWS-Services verwenden.

Das Muster bietet die folgenden Vorteile:

- Verwaltet Ihren Zugriffsschlüssel IDs und Ihre geheimen Zugangsschlüssel für alle Konten in Ihrer Organisation von einem zentralen Ort aus.
- Die Umgebungsvariablen `AWS_ACCESS_KEY_ID` und die `AWS_SECRET_ACCESS_KEY` Umgebungsvariablen werden automatisch rotiert.
- Erzwingt eine Verlängerung, wenn Benutzeranmeldedaten kompromittiert werden.

Das Muster verwendet Terraform, um AWS Lambda Lambda-Funktionen, EventBridge Amazon-Regeln und IAM-Rollen bereitzustellen. Eine EventBridge Regel wird in regelmäßigen Abständen ausgeführt und ruft eine Lambda-Funktion auf, die alle Benutzerzugriffsschlüssel auflistet, je nachdem, wann sie erstellt wurden. Zusätzliche Lambda-Funktionen erstellen eine neue Zugriffsschlüssel-ID und einen neuen geheimen Zugriffsschlüssel, wenn der vorherige Schlüssel

älter ist als der von Ihnen definierte Rotationszeitraum (z. B. 45 Tage), und benachrichtigen einen Sicherheitsadministrator mithilfe von Amazon Simple Notification Service (Amazon SNS) und Amazon Simple Email Service (Amazon SES). Secrets werden in AWS Secrets Manager für diesen Benutzer erstellt, der alte geheime Zugriffsschlüssel wird in Secrets Manager gespeichert und die Berechtigungen für den Zugriff auf den alten Schlüssel werden konfiguriert. Um sicherzustellen, dass der alte Zugriffsschlüssel nicht mehr verwendet wird, wird er nach einer inaktiven Zeit deaktiviert (z. B. 60 Tage, was in unserem Beispiel 15 Tage nach der Rotation der Schlüssel wäre). Nach einer inaktiven Pufferzeit (z. B. 90 Tage oder 45 Tage nach der Rotation der Schlüssel in unserem Beispiel) werden die alten Zugriffsschlüssel aus AWS Secrets Manager gelöscht. Eine detaillierte Architektur und ein detaillierter Arbeitsablauf finden Sie im Abschnitt Architektur.

Voraussetzungen und Einschränkungen

- Eine landing zone für Ihr Unternehmen, die mithilfe von AWS Control Tower (Version 3.1 oder höher) erstellt wurde
- Account Factory for Terraform (AFT), konfiguriert mit drei Konten:
  - Das Organisationsverwaltungskonto verwaltet die gesamte Organisation von einem zentralen Standort aus.
  - Das AFT-Verwaltungskonto hostet die Terraform-Pipeline und stellt die Infrastruktur im Bereitstellungskonto bereit.
  - Das Bereitstellungskonto stellt diese Komplettlösung bereit und verwaltet die IAM-Schlüssel von einem zentralen Standort aus.
- Terraform Version 0.15.0 oder höher für die Bereitstellung der Infrastruktur im Bereitstellungskonto.
- Eine E-Mail-Adresse, die in Amazon Simple Email Service (Amazon SES) konfiguriert ist.
- (Empfohlen) Um die Sicherheit zu erhöhen, stellen Sie diese Lösung in einem privaten Subnetz (Bereitstellungskonto) innerhalb einer Virtual Private Cloud (VPC) bereit. Sie können die Details der VPC und des Subnetzes angeben, wenn Sie die Variablen anpassen (siehe Anpassen der Parameter für die Code-Pipeline im Abschnitt Epics).

Architektur

AFT-Repositorien

Dieses Muster verwendet Account Factory for Terraform (AFT), um alle erforderlichen AWS-Ressourcen und die Code-Pipeline für die Bereitstellung der Ressourcen in einem Bereitstellungskonto zu erstellen. Die Code-Pipeline läuft in zwei Repositorys:

- Die globale Anpassung enthält Terraform-Code, der auf allen bei AFT registrierten Konten ausgeführt wird.
- Kontoanpassungen enthalten Terraform-Code, der im Bereitstellungskonto ausgeführt wird.

Einzelheiten zur Ressource

CodePipeline AWS-Jobs erstellen die folgenden Ressourcen im Bereitstellungskonto:

- EventBridge AWS-Regel und konfigurierte Regel
- `account-inventory`-Lambda-Funktion
- `IAM-access-key-rotation`-Lambda-Funktion
- `Notification`-Lambda-Funktion
- Amazon Simple Storage Service (Amazon S3) -Bucket, der eine E-Mail-Vorlage enthält
- Erforderliche IAM-Richtlinie

Architektur

Das Diagramm veranschaulicht folgende Vorgänge:

1. Eine EventBridge Regel ruft die `account-inventory` Lambda-Funktion alle 24 Stunden auf.
2. Die `account-inventory` Lambda-Funktion fragt AWS Organizations nach einer Liste aller AWS-Konten IDs, Kontonamen und Konto-E-Mails ab.
3. Die `account-inventory` Lambda-Funktion initiiert eine `IAM-access-key-auto-rotation` Lambda-Funktion für jedes AWS-Konto und leitet die Metadaten zur weiteren Verarbeitung an dieses weiter.
4. Die `IAM-access-key-auto-rotation` Lambda-Funktion verwendet eine angenommene IAM-Rolle, um auf das AWS-Konto zuzugreifen. Das Lambda-Skript führt eine Prüfung aller Benutzer und ihrer IAM-Zugriffsschlüssel im Konto durch.
5. Der Schwellenwert für die IAM-Schlüsselrotation (Rotationsperiode) wird als Umgebungsvariable konfiguriert, wenn die `IAM-access-key-auto-rotation` Lambda-Funktion bereitgestellt wird. Wenn die Rotationsperiode geändert wird, wird die `IAM-access-key-auto-rotation` Lambda-Funktion mit einer aktualisierten Umgebungsvariablen erneut bereitgestellt. Sie können Parameter konfigurieren, um den Rotationsperiode, den inaktiven Zeitraum für alte Schlüssel

und den inaktiven Puffer festzulegen, nach dessen Ablauf alte Schlüssel gelöscht werden (siehe Anpassen der Parameter für die Code-Pipeline im Abschnitt Epics).

6. Die `IAM-access-key-auto-rotation` Lambda-Funktion validiert das Alter des Zugriffsschlüssels anhand seiner Konfiguration. Wenn das Alter des IAM-Zugriffsschlüssels den von Ihnen definierten Rotationszeitraum nicht überschritten hat, ergreift die Lambda-Funktion keine weiteren Maßnahmen.
7. Wenn das Alter des IAM-Zugriffsschlüssels den von Ihnen definierten Rotationszeitraum überschritten hat, erstellt die `IAM-access-key-auto-rotation` Lambda-Funktion einen neuen Schlüssel und rotiert den vorhandenen Schlüssel.
8. Die Lambda-Funktion speichert den alten Schlüssel in Secrets Manager und beschränkt die Berechtigungen auf den Benutzer, dessen Zugriffsschlüssel von den Sicherheitsstandards abgewichen sind. Die Lambda-Funktion erstellt außerdem eine ressourcenbasierte Richtlinie, die es nur dem angegebenen IAM-Prinzipal ermöglicht, auf das Geheimnis zuzugreifen und es abzurufen.
9. Die `IAM-access-key-rotation` Lambda-Funktion ruft die `Notification` Lambda-Funktion auf.
10. Die `Notification` Lambda-Funktion fragt den S3-Bucket nach einer E-Mail-Vorlage ab und generiert dynamisch E-Mail-Nachrichten mit den entsprechenden Aktivitätsmetadaten.
11. Die `Notification` Lambda-Funktion ruft Amazon SES zur weiteren Aktion auf.
12. Amazon SES sendet eine E-Mail mit den entsprechenden Informationen an die E-Mail-Adresse des Kontoinhabers.

Tools

AWS-Services

- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden. Für dieses Muster sind IAM-Rollen und -Berechtigungen erforderlich.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Secrets Manager hilft Ihnen dabei, hartcodierte Anmeldeinformationen in Ihrem Code, einschließlich Passwörter, durch einen API-Aufruf an Secrets Manager zu ersetzen, um das Geheimnis programmgesteuert abzurufen.

- Amazon Simple Email Service (Amazon SES) unterstützt Sie beim Senden und Empfangen von E-Mails mithilfe Ihrer eigenen E-Mail-Adressen und Domains.

Andere Tools

- Terraform ist ein IaC-Tool (Infrastructure as Code) HashiCorp , mit dem Sie Cloud- und lokale Ressourcen erstellen und verwalten können.

Code-Repository

Die Anweisungen und der Code für dieses Muster sind im Repository für die GitHub IAM-Zugriffsschlüsselrotation verfügbar. Sie können den Code im zentralen Bereitstellungskonto von AWS Control Tower bereitstellen, um die Schlüsselrotation von einem zentralen Standort aus zu verwalten.

Bewährte Methoden

- Informationen zu IAM finden Sie in der IAM-Dokumentation unter Bewährte Sicherheitsmethoden.
- Informationen zur Schlüsselrotation finden Sie in den Richtlinien für die Aktualisierung von Zugriffsschlüsseln in der IAM-Dokumentation.

Epen

Richten Sie Quelldateien ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	1. Klonen Sie das GitHub Repository für die Rotation des IAM-Zugriffsschlüssels: `$ git clone https://github.com/aws-samples/centralized-iam-key-management-aws-organizations-terraform.git`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	2. Vergewissern Sie sich, dass Ihre lokale Kopie des Repositorys drei Ordner enthält:
	`$ cd Iam-Access-keys-Rotation`
	`$ ls`
	`org-account-customization`
	`global-account-customization`
	`account-customization`	

Konfigurieren Sie Konten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie das Bootstrapping-Konto.	Im Rahmen des AFT-Bootstrapping-Vorgangs sollte `aft-bootstrap` auf Ihrem lokalen Computer ein Ordner aufgerufen werden. 1. Kopieren Sie alle Terraform-Dateien manuell aus Ihrem lokalen GitHub org-account-customizationOrdner in Ihren Ordner. `aft-bootstrap` 2. Führen Sie Terraform-Befehle aus, um die globale kontoübergreifende Rolle im AWS Control Tower	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Tower-Verwaltungskonto zu konfigurieren:
	`$ cd aft-bootstrap`
	`$ terraform init`
	`$ terraform apply –auto-approve`	

Konfigurieren Sie globale Anpassungen.	Als Teil der Einrichtung des AFT-Ordners sollten Sie `aft-global-customizations` auf Ihrem lokalen Computer einen Ordner namens haben.
	1. Kopieren Sie alle Terraform -Dateien manuell aus Ihrem lokalen GitHub global-account-customizationOrdner in Ihren `aft-global-customizations/terraform` Ordner.
	2. Senden Sie den Code an AWS CodeCommit:
	`$ git add *`
	`$ git commit -m "message"`
	`$ git push`
		DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Konfigurieren Sie Kontoanpassungen.	Im Rahmen der Einrichtung des AFT-Ordners haben Sie einen Ordner namens `aft-account-customizations` auf Ihrem lokalen Computer eingerichtet.
	1. Erstellen Sie einen Ordner mit Ihrer verkauften Kontonummer.
	2. Kopieren Sie manuell alle Terraform-Dateien aus Ihrem lokalen GitHub Kontoanpassungsordner in Ihren Ordner. `aft-account-customizations/<vended account>/terraform`
	3. Senden Sie den Code an AWS CodeCommit:
	`$ git add *`
	`$ git commit -m "message"`
	`$ git push`
		DevOps Ingenieur

Passen Sie die Parameter für die Code-Pipeline an

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie die Pipeline-Parameter für Nicht-Terraform-Codes für alle Konten an.	Erstellen Sie eine Datei mit dem Namen `input.auto.tfvars` im `aft-global-customizations/`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`terraform/` Ordner und geben Sie die erforderlichen Eingabedaten ein. Die Standardwerte finden Sie in der Datei im GitHub Repository.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie die Code-Pipeline-Parameter für das Bereitstellungskonto an.	Erstellen Sie eine Datei mit dem Namen `input.auto.tfvars` im `aft-account-customizations/<AccountName>/terraform/` Ordner und übertragen Sie den Code an AWS CodeCommit. Durch das Übertragen von Code an AWS CodeCommit wird die Code-Pipeline automatisch initiiert. Geben Sie Werte für Parameter an, die auf den Anforderungen Ihrer Organisation basieren, einschließlich der folgenden Werte (Standardwerte finden Sie in der Datei im Github-Repository): • `s3_bucket_name` — Ein eindeutiger Bucket-Name für die E-Mail-Vorlage. • `s3_bucket_prefix` — Ein Ordnername innerhalb des S3-Buckets. • `admin_email_address` — Die E-Mail-Adresse des Administrators, der die Benachrichtigung erhalten soll.	DevOps — Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `org_list_account` — Die Kontonummer des Verwaltungskontos. • `rotation_period` — Die Anzahl der Tage, nach denen ein Schlüssel von aktiv auf inaktiv umgestellt werden soll. • `inactive_period` — Die Anzahl der Tage, nach denen rotierte Schlüssel deaktiviert werden sollten. Dieser Wert muss größer sein als der Wert von`rotation_period` . • `inactive_buffer` — Die Übergangszeit zwischen der Rotation und der Deaktivierung eines Schlüssels. • `recovery_grace_period` — Die Nachfrist zwischen der Deaktivierung und dem Löschen eines Schlüssels. • `dry_run_flag` — Auf true setzen, wenn Sie zu Testzwecken eine Benachrichtigung an den Administrator senden möchten, ohne die Schlüssel zu wechseln. • `store_secrets_in_central_account` —	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Auf true setzen, wenn Sie das Geheimnis im Bereitstellungskonto speichern möchten. Wenn die Variable auf false gesetzt ist (Standard), wird das Geheimnis im Mitglieds konto gespeichert. • `credential_replica tion_region` — Die AWS-Region, in der Sie die Lambda-Funktion und die S3-Buckets für die E-Mail-Vorlage bereitstellen möchten. • `run_lambda_in_vpc` — Auf true setzen, um die Lambda-Funktion innerhalb der VPC auszuführen. • `vpc_id`— Die VPC-ID des Bereitstellungskontos, wenn Sie die Lambda-Fu nktion innerhalb der VPC ausführen möchten. • `vpc_cidr`— Der CIDR-Bereich für das Bereitste llungskonto. • `subnet_id` — Das Subnetz IDs für das Bereitstellungskonto. • `create_smtp_endpoi nt` — Auf true setzen,	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wenn Sie den E-Mail-En dpunkt aktivieren möchten.	

Überprüfen Sie die Schlüsselrotation

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Lösung.	1. Melden Sie sich in der AWS-Managementkonsole beim Bereitstellungskonto an. 2. Öffnen Sie die IAM-Konsole und überprüfen Sie, ob die Benutzeranmeldedaten (Zugriffsschlüssel IDs und geheime Schlüssel) wie angegeben ausgetauscht werden. 3. Nachdem ein IAM-Schlüssel rotiert wurde, bestätigen Sie Folgendes: • Der alte Wert wird in AWS Secrets Manager gespeichert. • Der geheime Name hat das Format `Account_<account ID>_User_<username>_AccessKey` . • Der Benutzer, den Sie im `admin_email_address` Parameter angegeben haben, erhält eine E-Mail-	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Benachrichtigung über die Schlüsselrotation.	

Erweitern Sie die Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie das Datum der E-Mail-Benachrichtigung an.	Wenn Sie an einem bestimmten Tag, bevor Sie den Zugriffsschlüssel deaktivieren, E-Mail-Benachrichtigungen senden möchten, können Sie die `IAM-access-key-auto-rotation` Lambda-Funktion mit diesen Änderungen aktualisieren: 1. Definieren Sie eine Variable namens `notify-period` . 2. Fügen Sie eine `if` Bedingung hinzu, `main.py` bevor Sie den Schlüssel deaktivieren: `If (keyage>rotation-period-notify-period){ send_to_notifier(context, aws_account_id, account_name, resource_owner, resource_actions[resource_owner], dryrun, config.emailTemplateAudit) }`	DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
Der `account-inventory` Lambda-Job schlägt `AccessDenied` beim Auflisten von Konten fehl.	Wenn dieses Problem auftritt, müssen Sie die Berechtigungen überprüfen: 1. Melden Sie sich bei dem neu verkaufte n Konto an, öffnen Sie die CloudWatc h Amazon-Konsole und sehen Sie sich dann die CloudWatch Protokollgruppe `/ aws/lambda/account-inventory- lambda` an. 2. Identifizieren Sie in den neuesten CloudWatc h Protokollen die Kontonummer, die das Problem mit der Zugriffsverweigerung verursacht hat. 3. Melden Sie sich beim AWS Control Tower Tower-Managementkonto an und bestätige n Sie, dass die Rolle erstellt `allow-list- account` wurde. 4. Wenn die Rolle nicht existiert, führen Sie den Terraform-Code erneut aus, indem Sie den Befehl verwenden. `terraform apply` 5. Wählen Sie die Registerkarte Vertrauen swürdiges Konto und überprüfen Sie, ob dasselbe Konto vertrauenswürdig ist.

Zugehörige Ressourcen

- Empfohlene Methoden für Terraform (Terraform-Dokumentation)
- Bewährte Sicherheitsmethoden in IAM (IAM-Dokumentation)
- Bewährte Methoden für die Schlüsselrotation (IAM-Dokumentation)

Suchen Sie in einer CloudFront Amazon-Distribution nach Zugriffsprotokollierung, HTTPS- und TLS-Version

Erstellt von SaiJeevan Devireddy (AWS) und Bijesh Bal (AWS)

Übersicht

Dieses Muster überprüft eine CloudFront Amazon-Distribution, um sicherzustellen, dass sie HTTPS verwendet, Transport Layer Security (TLS) Version 1.2 oder höher verwendet und die Zugriffsprotokollierung aktiviert ist. CloudFront ist ein von Amazon Web Services (AWS) bereitgestellter Service, der die Verteilung Ihrer statischen und dynamischen Webinhalte wie .html-, .css-, .js- und Bilddateien an Ihre Benutzer beschleunigt. CloudFront stellt Ihre Inhalte über ein weltweites Netzwerk von Rechenzentren bereit, die als Edge-Standorte bezeichnet werden. Wenn ein Benutzer Inhalte anfordert CloudFront, mit denen Sie sie bereitstellen, wird die Anfrage an den Edge-Standort weitergeleitet, der die niedrigste Latenz (Zeitverzögerung) bietet, sodass der Inhalt mit der bestmöglichen Leistung bereitgestellt wird.

Dieses Muster stellt eine AWS-Lambda-Funktion bereit, die ausgelöst wird, wenn Amazon CloudWatch Events den CloudFront API-Aufruf CreateDistribution, CreateDistributionWithTags, oder UpdateDistributionerkennt. Die benutzerdefinierte Logik in der Lambda-Funktion wertet alle CloudFront Verteilungen aus, die im AWS-Konto erstellt oder aktualisiert wurden. Es sendet mithilfe von Amazon Simple Notification Service (Amazon SNS) eine Benachrichtigung über Verstöße, wenn es die folgenden Verstöße feststellt:

- Globale Prüfungen:
  - Das benutzerdefinierte Zertifikat verwendet keine TLS-Version 1.2
  - Die Protokollierung ist für die Verteilung deaktiviert
- Herkunftsüberprüfungen:
  - Origin ist nicht mit TLS Version 1.2 konfiguriert
  - Die Kommunikation mit Origin ist über ein anderes Protokoll als HTTPS erlaubt
- Verhaltensprüfungen:
  - Kommunikation mit Standardverhalten ist auf einem anderen Protokoll als HTTPS zulässig
  - Kommunikation mit benutzerdefiniertem Verhalten ist in einem anderen Protokoll als HTTPS zulässig

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine E-Mail-Adresse, an die Sie die Benachrichtigungen über Verstöße erhalten möchten

Einschränkungen

- Diese Sicherheitskontrolle sucht nicht nach vorhandenen Cloudfront-Distributionen, es sei denn, die Distribution wurde aktualisiert.
- CloudFront gilt als globaler Service und ist nicht an eine bestimmte AWS-Region gebunden. Die CloudWatch Protokollierung von Amazon Logs und der AWS Cloudtrail API für globale Dienste erfolgt jedoch in der Region USA Ost (Nord-Virginia) (`us-east-1`). Daher CloudFront muss diese Sicherheitskontrolle für in `us-east-1` bereitgestellt und aufrechterhalten werden. Bei CloudFront dieser einzelnen Bereitstellung werden alle Distributionen auf überwacht. Stellen Sie die Sicherheitskontrolle nicht in anderen AWS-Regionen bereit. (Die Bereitstellung in anderen Regionen führt dazu, dass CloudWatch Ereignisse und die Lambda-Funktion nicht initiiert werden können und es werden keine SNS-Benachrichtigungen angezeigt.)
- Diese Lösung wurde umfangreichen Tests mit Distributionen von CloudFront Webinhalten unterzogen. Sie deckt keine RTMP-Streaming-Distributionen (Real-Time Messaging Protocol) ab.

Architektur

Zieltechnologie-Stack

- Lambda-Funktion
- SNS-Thema
- EventBridge Amazon-Regel

Zielarchitektur

Automatisierung und Skalierung

- Wenn Sie AWS Organizations verwenden, können Sie AWS Cloudformation verwenden, StackSets um die angehängte Vorlage für mehrere Konten bereitzustellen, die Sie überwachen möchten.

Tools

AWS-Services

- AWS CloudFormation — CloudFormation ist ein Service, der Sie bei der Modellierung und Einrichtung von AWS-Ressourcen unterstützt, indem Infrastruktur als Code verwendet wird.
- Amazon EventBridge — EventBridge stellt einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, SaaS-Anwendungen (Software as a Service) und AWS-Services bereit und leitet diese Daten an Ziele wie Lambda-Funktionen weiter.
- AWS Lambda — Lambda unterstützt die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice, der für eine Vielzahl von Speicherlösungen verwendet werden kann, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon SNS — Amazon SNS koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Code

Der beigefügte Code beinhaltet:

- Eine ZIP-Datei, die den Lambda-Code enthält (index.py)
- Eine CloudFormation Vorlage (.yml-Datei), die Sie ausführen, um den Lambda-Code bereitzustellen

Epen

Laden Sie die Sicherheitskontrolle hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den S3-Bucket für den Lambda-Code.	Erstellen Sie auf der Amazon S3 S3-Konsole einen S3-	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bucket mit einem eindeutigen Namen, der keine führenden Schrägstriche enthält. Ein S3-Bucket-Name ist weltweit eindeutig, und der Namespace wird von allen AWS-Konte n gemeinsam genutzt. Ihr S3-Bucket muss sich in der Region befinden, in der Sie den Lambda-Code bereitste llen möchten.	
Laden Sie den Lambda-Code in den S3-Bucket hoch.	Laden Sie den Lambda-Co de (Datei cloudfront_ssl_log _lambda.zip), der im Abschnitt Anlagen bereitgestellt wird, in den S3-Bucket hoch, den Sie im vorherigen Schritt erstellt haben.	Cloud-Architekt

Stellen Sie die CloudFormation Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudForm ation Vorlage bereit.	Stellen Sie auf der CloudForm ation AWS-Konsole, in derselben AWS-Region wie der S3-Bucket, die CloudForm ation Vorlage (cloudfront-ssl-logging.yml) bereit, die im Abschnitt Anlagen bereitges tellt wird.	Cloud-Architekt
Geben Sie den S3-Bucket-Namen an.	Geben Sie für den S3-Bucket -Parameter den Namen des	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	S3-Buckets an, den Sie im ersten Epic erstellt haben.	
Geben Sie den Amazon S3 S3-Schlüsselnamen für die Lambda-Datei an.	Geben Sie für den Parameter S3 Key den Amazon S3 S3-Speicherort der Lambda-Code-.zip-Datei in Ihrem S3-Bucket an. Fügen Sie keine führenden Schrägstriche ein (Sie können beispielsweise lambda.zip oder controls/lambda.zip eingeben).	Cloud-Architekt
Geben Sie eine E-Mail-Adresse für Benachrichtigungen an.	Geben Sie für den Parameter Benachrichtigungs-E-Mail eine E-Mail-Adresse an, an die Sie die Benachrichtigungen über Verstöße erhalten möchten.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie die Protokollierungsebene.	Definieren Sie für den Parameter Lambda Logging Level den Logging-Level für Ihre Lambda-Funktion. Wählen Sie einen der folgenden Werte aus: • INFO, um detaillierte Informationsmeldungen über den Fortschritt der Anwendung zu erhalten. • ERROR, um Informationen über Fehlerereignisse abzurufen, die dazu führen könnten, dass die Anwendung weiterhin ausgeführt werden kann. • WARNUNG, um Informationen über potenziell schädliche Situationen zu erhalten.	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die CloudFormation Vorlage erfolgreich bereitgestellt wurde, wird ein neues SNS-Thema erstellt und eine Abonnementnachricht an die von Ihnen angegebene E-Mail-Adresse gesendet. Sie müssen dieses E-Mail-	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Abonnement bestätigen, um Benachrichtigungen über Verstöße zu erhalten.	

Zugehörige Ressourcen

- CloudFormation AWS-Informationen
- Einen Stack auf der CloudFormation AWS-Konsole erstellen (CloudFormation Dokumentation)
- CloudFront Protokollierung (CloudFront Dokumentation)
- Informationen zu Amazon S3
- Informationen zu AWS Lambda

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Suchen Sie in den Eingangsregeln für Sicherheitsgruppen nach Einzelhost-Netzwerkeinträgen für und IPv4 IPv6

Erstellt von SaiJeevan Devireddy (AWS), Ganesh Kumar (AWS) und John Reynolds (AWS)

Übersicht

Dieses Muster bietet eine Sicherheitskontrolle, die Sie benachrichtigt, wenn Amazon Web Services (AWS) -Ressourcen nicht Ihren Spezifikationen entsprechen. Es bietet eine AWS-Lambda-Funktion, die nach Einzelhost-Netzwerkeinträgen sowohl in Internet Protocol Version 4 (IPv4) als auch in Quelladressfeldern für IPv6 Sicherheitsgruppen sucht. Die Lambda-Funktion wird initiiert, wenn Amazon CloudWatch Events den AuthorizeSecurityGroupIngressAPI-Aufruf von Amazon Elastic Compute Cloud (Amazon EC2) erkennt. Die benutzerdefinierte Logik in der Lambda-Funktion wertet die Subnetzmaske des CIDR-Blocks der Sicherheitsgruppeneingangsregel aus. Wenn festgestellt wird, dass die Subnetzmaske etwas anderes als /32 (IPv4) oder /128 (IPv6) ist, sendet die Lambda-Funktion mithilfe von Amazon Simple Notification Service (Amazon SNS) eine Benachrichtigung über einen Verstoß.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine E-Mail-Adresse, an die Sie die Benachrichtigungen über Verstöße erhalten möchten

Einschränkungen

- Diese Sicherheitsüberwachungslösung ist regional und muss in jeder AWS-Region bereitgestellt werden, die Sie überwachen möchten.

Architektur

Zieltechnologie-Stack

- Lambda-Funktion
- SNS-Thema

- EventBridge Amazon-Regel

Zielarchitektur

Automatisierung und Skalierung

- Wenn Sie AWS Organizations verwenden, können Sie AWS Cloudformation verwenden, StackSets um diese Vorlage für mehrere Konten bereitzustellen, die Sie überwachen möchten.

Tools

AWS-Services

- AWS CloudFormation ist ein Service, mit dem Sie AWS-Ressourcen modellieren und einrichten können, indem Sie Infrastruktur als Code verwenden.
- Amazon EventBridge stellt einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, SaaS-Anwendungen (Software as a Service) und AWS-Services bereit und leitet diese Daten an Ziele wie Lambda-Funktionen weiter.
- AWS Lambda unterstützt die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern.
- Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice, der für eine Vielzahl von Speicherlösungen verwendet werden kann, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon SNS koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Code

Der beigefügte Code beinhaltet:

- Eine ZIP-Datei, die den Lambda-Sicherheitskontrollcode () enthält `index.py`
- Eine CloudFormation Vorlage (`security-control.yml`Datei), die Sie ausführen, um den Lambda-Code bereitzustellen

Epen

Laden Sie die Sicherheitskontrolle hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den S3-Bucket für den Lambda-Code.	Erstellen Sie auf der Amazon S3 S3-Konsole einen S3-Bucket mit einem eindeutigen Namen, der keine führenden Schrägstriche enthält. Ein S3-Bucket-Name ist weltweit eindeutig, und der Namespace wird von allen AWS-Konten gemeinsam genutzt. Ihr S3-Bucket muss sich in der AWS-Region befinden, in der Sie die Sicherheitsgruppen-Eingangsprüfung bereitstellen möchten.	Cloud-Architekt
Laden Sie den Lambda-Code in den S3-Bucket hoch.	Laden Sie den Lambda-Code (`security-control-lambda.zip` Datei), der im Abschnitt Anlagen bereitgestellt wird, in den S3-Bucket hoch, den Sie im vorherigen Schritt erstellt haben.	Cloud-Architekt

Stellen Sie die CloudFormation Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Python-Version.	Laden Sie die CloudFormation Vorlage (`security-control.yml`) herunter, die im Abschnitt Anlagen bereitgestellt wird. Öffnen	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie die Datei und ändern Sie die Python-Version so, dass sie die neueste von Lambda unterstützte Version wiedergib t (derzeit Python 3.9). Sie können beispielsweise `python` im Code nach suchen und den Wert für `Runtime` von `python3.6` bis `python3.9` ändern. Die neuesten Informationen zur Unterstützung von Python-Runtime-Versionen finden Sie in der AWS Lambda Lambda-Dokumentation.	
Stellen Sie die CloudForm ation AWS-Vorlage bereit.	Stellen Sie auf der CloudForm ation AWS-Konsole, in derselben AWS-Regio n wie der S3-Bucket, die CloudFormation Vorlage bereit (`security-control.y ml`).	Cloud-Architekt
Geben Sie den S3-Bucket-Namen an.	Geben Sie für den S3-Bucket -Parameter den Namen des S3-Buckets an, den Sie im ersten Epic erstellt haben.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den Amazon S3 S3-Schlüsselnamen für die Lambda-Datei an.	Geben Sie für den Parameter S3 Key den Amazon S3 S3-Speicherort der Lambda-Code-.zip-Datei in Ihrem S3-Bucket an. Fügen Sie keine führenden Schrägstriche ein (Sie können beispielsweise oder eingeben `lambda.zip`). `controls/lambda.zip`	Cloud-Architekt
Geben Sie eine E-Mail-Adresse für Benachrichtigungen an.	Geben Sie für den Parameter Benachrichtigungs-E-Mail eine E-Mail-Adresse an, an die Sie die Benachrichtigungen über Verstöße erhalten möchten.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie die Protokollierungsebene.	Definieren Sie für den Parameter Lambda Logging Level den Logging-Level für Ihre Lambda-Funktion. Wählen Sie einen der folgenden Werte aus: • INFO, um detaillierte Informationsmeldungen über den Fortschritt der Anwendung zu erhalten. • ERROR, um Informationen über Fehlerereignisse abzurufen, die dazu führen könnten, dass die Anwendung weiterhin ausgeführt werden kann. • WARNUNG, um Informationen über potenziell schädliche Situationen zu erhalten.	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die CloudFormation Vorlage erfolgreich bereitgestellt wurde, wird ein neues SNS-Thema erstellt und eine Abonnementnachricht an die von Ihnen angegebene E-Mail-Adresse gesendet. Sie müssen dieses E-Mail-	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Abonnement bestätigen, um Benachrichtigungen über Verstöße zu erhalten.	

Zugehörige Ressourcen

- CloudFormation AWS-Informationen
- Einen Stack auf der CloudFormation AWS-Konsole erstellen (CloudFormation AWS-Dokumentation)
- Sicherheitsgruppen für Ihre VPC (Amazon VPC-Dokumentation)
- Informationen zu Amazon S3
- Informationen zu AWS Lambda

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Wählen Sie einen Amazon Cognito Cognito-Authentifizierungsablauf für Unternehmensanwendungen

Erstellt von Michael Daehnert (AWS) und Fabian Jahnke (AWS)

Übersicht

Amazon Cognito bietet Authentifizierung, Autorisierung und Benutzerverwaltung für Web- und Mobilanwendungen. Es bietet nützliche Funktionen für die Authentifizierung von föderierten Identitäten. Um es zum Laufen zu bringen, müssen technische Architekten entscheiden, wie sie diese Funktionen verwenden möchten.

Amazon Cognito unterstützt mehrere Abläufe für Authentifizierungsanfragen. Diese Abläufe definieren, wie Ihre Benutzer ihre Identität überprüfen können. Die Entscheidung, welcher Authentifizierungsablauf verwendet werden soll, hängt von den spezifischen Anforderungen Ihrer Anwendung ab und kann komplex werden. Dieses Muster hilft Ihnen bei der Entscheidung, welcher Authentifizierungsablauf für Ihre Unternehmensanwendung am besten geeignet ist. Es wird davon ausgegangen, dass Sie bereits über Grundkenntnisse in Amazon Cognito, OpenID Connect (OIDC) und Federation verfügen, und führt Sie durch Einzelheiten zu den verschiedenen föderierten Authentifizierungsabläufen.

Diese Lösung richtet sich an technische Entscheidungsträger. Sie hilft Ihnen dabei, die verschiedenen Authentifizierungsabläufe zu verstehen und sie Ihren Anwendungsanforderungen zuzuordnen. Technische Leiter sollten die erforderlichen Erkenntnisse sammeln, um die Amazon Cognito Cognito-Integrationen zu starten. Da sich Unternehmensorganisationen hauptsächlich auf den SAML-Verbund konzentrieren, enthält dieses Muster Beschreibungen für Amazon Cognito Cognito-Benutzerpools mit SAML-Föderation.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Rollen und Berechtigungen von AWS Identity and Access Management (IAM) mit vollem Zugriff auf Amazon Cognito
- (Optional) Zugriff auf Ihren Identitätsanbieter (IdP), z. B. Microsoft Entra ID, Active Directory Federation Service (AD FS) oder Okta
- Ein hohes Maß an Fachwissen für Ihre Anwendung

- Grundkenntnisse in Amazon Cognito, OpenID Connect (OIDC) und Federation

Einschränkungen

- Dieses Muster konzentriert sich auf Amazon Cognito Cognito-Benutzerpools und Identitätsanbieter. Informationen zu Amazon Cognito Cognito-Identitätspools finden Sie im Abschnitt Zusätzliche Informationen.

Architektur

Verwenden Sie die folgende Tabelle, um Ihnen bei der Auswahl eines Authentifizierungsablaufs zu helfen. Weitere Informationen zu den einzelnen Datenströmen finden Sie in diesem Abschnitt.

Benötigen Sie eine machine-to-machine Authentifizierung?	Ist Ihre App eine webbasierte Anwendung, bei der das Frontend auf dem Server gerendert wird?	Handelt es sich bei Ihrer App um eine einseitige Anwendung (SPA) oder um eine Frontend-Anwendung auf Mobilgeräten?	Benötigt Ihre Anwendung Aktualisierungstoken für die Funktion „Ich möchte angemeldet bleiben“?	Bietet das Frontend einen browserbasierten Umleitungsmechanismus?	Empfohlener Amazon Cognito Cognito-Flow
Ja	Nein	Nein	Nein	Nein	Ablauf der Kundenanmeldedaten
Nein	Ja	Nein	Ja	Ja	Ablauf des Autorisierungscodes
Nein	Nein	Ja	Ja	Ja	Ablauf des Autorisierungscodes mit Proof

					Key for Code Exchange (PKCE)
Nein	Nein	Nein	Nein	Nein	Passwortfluss für Ressource neigentümer*

* Der Passwortfluss für den Ressourcenbesitzer sollte nur verwendet werden, wenn dies unbedingt erforderlich ist. Weitere Informationen finden Sie im Abschnitt „Passwortfluss für Ressourcenbesitzer“ in diesem Muster.

Ablauf der Kundenanmeldedaten

Der Client Credentials Flow ist der kürzeste der Amazon Cognito Cognito-Flows. Er sollte verwendet werden, wenn Systeme oder Dienste ohne Benutzerinteraktion miteinander kommunizieren. Das anfragende System verwendet die Client-ID und das Client-Geheimnis, um ein Zugriffstoken abzurufen. Da beide Systeme ohne Benutzerinteraktion funktionieren, ist kein zusätzlicher Zustimmungsschritt erforderlich.

Das Diagramm veranschaulicht folgende Vorgänge:

1. Anwendung 1 sendet eine Authentifizierungsanfrage mit der Client-ID und dem geheimen Client-Schlüssel an den Amazon Cognito Cognito-Endpunkt und ruft ein Zugriffstoken ab.
2. Anwendung 1 verwendet dieses Zugriffstoken für jeden nachfolgenden Aufruf von Anwendung 2.
3. Anwendung 2 validiert das Zugriffstoken mit Amazon Cognito.

Dieser Ablauf sollte verwendet werden:

- Für die Kommunikation zwischen Anwendungen ohne Benutzerinteraktion

Dieser Ablauf sollte nicht verwendet werden:

- Für jede Kommunikation, bei der Benutzerinteraktionen möglich sind

Ablauf des Autorisierungscodes

Der Ablauf des Autorisierungscodes dient der klassischen webbasierten Authentifizierung. In diesem Ablauf kümmert sich das Backend um den gesamten Austausch und die Speicherung von Token. Der browserbasierte Client sieht die tatsächlichen Token nicht. Diese Lösung wird für Anwendungen verwendet, die in Frameworks wie.NET Core, Jakarta Faces oder Jakarta Server Pages (JSP) geschrieben wurden.

Der Autorisierungscodefluss ist ein Fluss, der auf Umleitungen basiert. Der Client muss in der Lage sein, mit dem Webbrowser oder einem ähnlichen Client zu interagieren. Der Client wird zu einem Authentifizierungsserver umgeleitet und authentifiziert sich bei diesem Server. Wenn sich der Client erfolgreich authentifiziert, wird er zurück zum Server umgeleitet.

Das Diagramm veranschaulicht folgende Vorgänge:

1. Der Client sendet eine Anfrage an den Webserver.
2. Der Webserver leitet den Client mithilfe eines HTTP 302-Statuscodes zu Amazon Cognito weiter. Der Client folgt automatisch dieser Weiterleitung zum konfigurierten IdP-Login.
3. Der IdP sucht nach einer bestehenden Browsersitzung auf der IdP-Seite. Wenn keine vorhanden ist, wird der Benutzer aufgefordert, sich zu authentifizieren, indem er seinen Benutzernamen und sein Passwort eingibt. Der IdP antwortet mit einem SAML-Token auf Amazon Cognito.
4. Amazon Cognito meldet Erfolg mit einem JSON-Webtoken (JWT), insbesondere einem Code-Token. Der Webservercalls /oauth2/token, der das Codetoken gegen ein Zugriffstoken eintauscht. Der Webserver sendet die Client-ID und das Client-Geheimnis zur Überprüfung an Amazon Cognito.
5. Das Zugriffstoken wird für jeden nachfolgenden Aufruf anderer Anwendungen verwendet.
6. Andere Anwendungen validieren das Zugriffstoken mit Amazon Cognito.

Dieser Ablauf sollte verwendet werden:

- Wenn der Benutzer in der Lage ist, mit dem Webbrowser oder Client zu interagieren. Der Anwendungscode wird auf dem Server ausgeführt und gerendert, um sicherzustellen, dass dem Browser keine Geheimnisse offengelegt werden.

Dieser Ablauf sollte nicht verwendet werden:

- Für einseitige Anwendungen (SPAs) oder mobile Apps, da sie auf dem Client gerendert werden und keine Client-Geheimnisse verwenden sollten.

Ablauf des Autorisierungscodes mit PKCE

Der Autorisierungscodefluss mit Proof Key for Code Exchange (PKCE) sollte für einseitige Anwendungen und mobile Anwendungen verwendet werden. Er ist der Nachfolger des impliziten Ablaufs und ist sicherer, da er PKCE verwendet. PKCE ist eine Erweiterung des OAuth 2.0-Autorisierungscodes, der öffentlichen Auftraggebern gewährt wird. PKCE schützt vor der Rücknahme abgefangener Autorisierungscodes.

Das Diagramm veranschaulicht folgende Vorgänge:

1. Die Anwendung erstellt einen Code-Verifier und eine Code-Challenge. Dies sind klar definierte, eindeutige Werte, die zur future Verwendung an Amazon Cognito gesendet werden.
2. Die Anwendung ruft den the /oauth2/authorization Endpunkt von Amazon Cognito auf. Es leitet den Benutzer automatisch zum konfigurierten IdP-Login weiter.
3. Der IdP sucht nach einer bestehenden Sitzung. Wenn keine vorhanden ist, wird der Benutzer aufgefordert, sich zu authentifizieren, indem er seinen Benutzernamen und sein Passwort eingibt. Der IdP antwortet mit einem SAML-Token auf Amazon Cognito.
4. Nachdem Amazon Cognito den Erfolg mit einem Code-Token zurückgibt, tauscht der Webserver calls /oauth2/token das Code-Token gegen ein Zugriffstoken aus.
5. Das Zugriffstoken wird für jeden nachfolgenden Aufruf anderer Anwendungen verwendet.
6. Die anderen Anwendungen validieren das Zugriffstoken mit Amazon Cognito.

Dieser Ablauf sollte verwendet werden:

- Für SPAs unsere mobilen Anwendungen

Dieser Flow sollte nicht verwendet werden:

- Wenn das Anwendungs-Backend die Authentifizierung abwickelt

Ablauf des Kennworts des Ressourcenbesitzers

Der Passwortfluss für den Ressourcenbesitzer ist für Anwendungen ohne Umleitungsfunktionen vorgesehen. Er wird erstellt, indem Sie ein Anmeldeformular in Ihrer eigenen Anwendung erstellen. Die Anmeldung wird auf Amazon Cognito über einen CLI- oder SDK-Aufruf überprüft, anstatt sich auf

Umleitungsflüsse zu verlassen. Ein Verbund ist in diesem Authentifizierungsablauf nicht möglich, da für den Verbund browserbasierte Weiterleitungen erforderlich sind.

Das Diagramm veranschaulicht folgende Vorgänge:

1. Der Benutzer gibt seine Anmeldeinformationen in ein von der Anwendung bereitgestelltes Anmeldeformular ein.
2. Die AWS-Befehlszeilenschnittstelle (AWS CLI) admin-initiated-authruft Amazon Cognito auf.

> **Note**
>
> Alternativ können Sie AWS SDKs anstelle der AWS-CLI verwenden.

3. Amazon Cognito gibt ein Zugriffstoken zurück.
4. Das Zugriffstoken wird für jeden nachfolgenden Aufruf anderer Anwendungen verwendet.
5. Die anderen Anwendungen validieren das Zugriffstoken mit Amazon Cognito.

Dieser Ablauf sollte verwendet werden:

- Bei der Migration vorhandener Clients, die direkte Authentifizierungslogik verwenden (z. B. Standardzugriffsauthentifizierung oder Digest-Zugriffsauthentifizierung), auf OAuth die Konvertierung der gespeicherten Anmeldeinformationen in ein Zugriffstoken

Dieser Ablauf sollte nicht verwendet werden:

- Wenn Sie föderierte Identitäten verwenden möchten
- Wenn Ihre Anwendung Weiterleitungen unterstützt

Tools

AWS-Services

- Amazon Cognito bietet Authentifizierung, Autorisierung und Benutzerverwaltung für Web- und mobile Apps.

Andere Tools

- Der JSON-Web-Token-Debugger (JWT) ist ein webbasiertes JWT-Validierungstool.

Epen

Beurteilen Sie Ihre Bewerbung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie die Authentifizierungsanforderungen.	Beurteilen Sie Ihre Anwendung anhand Ihrer spezifischen Authentifizierungsanforderungen.	App-Entwickler, App-Architekt
Passen Sie die Anforderungen an die Authentifizierungsabläufe an.	Verwenden Sie im Abschnitt Architektur die Entscheidungstabelle und die Erläuterungen der einzelnen Abläufe, um Ihren Amazon Cognito Cognito-Authentifizierungsablauf auszuwählen.	App-Entwickler, General AWS, App-Architekt

Den Amazon Cognito Cognito-Benutzerpool einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen Benutzerpool.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie dann die Amazon Cognito Cognito-Konsole. 2. Erstellen Sie einen neuen Cognito-Benutzerpool. Anweisungen finden Sie unter Amazon Cognito Cognito-Benutzerpools.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Aktualisieren Sie die Einstellungen und Attribute des Benutzerpools nach Bedarf. Legen Sie beispielsweise eine Kennwortrichtlinie für den Benutzerpool fest. Erstellen Sie noch keine App-Clients.	
(Optional) Konfigurieren Sie einen Identitätsanbieter.	1. Erstellen Sie einen SAML-Identitätsanbieter im Amazon Cognito Cognito-Benutzerpool. Anweisungen finden Sie unter Hinzufügen und Verwalten von SAML-Identitätsanbietern in einem Benutzerpool. 2. Konfigurieren Sie Ihren externen SAML-Identitätsanbieter so, dass er mit dem Verbund für Amazon Cognito Cognito-Benutzerpools funktioniert. Weitere Informationen finden Sie unter Konfiguration Ihres externen SAML-Identitätsanbieters. Wenn Sie AD FS verwenden, finden Sie weitere Informationen unter Aufbau eines AD FS-Verbunds für Ihre Web-App mithilfe von Amazon Cognito Cognito-Benutzerpools (AWS-Blogbeitrag).	Allgemeiner AWS, Verbundadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen App-Client.	1. Erstellen Sie einen App-Client für den Benutzerpool. Anweisungen finden Sie unter Einen App-Client erstellen. Beachten Sie Folgendes: • Ändern Sie die Einstellungen nach Bedarf, z. B. die Ablaufzeiten von Tokens. • Wenn für Ihren Authentifizierungsablauf kein Client-Geheimnis erforderlich ist, deaktivieren Sie das Kontrollkästchen Clientgeheimnis generieren. 2. Wählen Sie App-Client-Einstellungen, um die Integration in eine Benutzerpool-Anmeldung (Benutzername und Passwort) oder eine Verbundanmeldung über einen SAML-basierten IdP zu ändern. 3. Unterstützen Sie Ihren IdP, indem Sie nach Bedarf OAuth Flows oder Bereiche definieren URLs und definieren.	Allgemeines AWS

Integrieren Sie die Anwendung in Amazon Cognito

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Details zur Exchange Amazon Cognito Cognito-Integration.	Geben Sie je nach Ihrem Authentifizierungsablauf Amazon Cognito Cognito-Informationen an die Anwendung weiter, z. B. die Benutzerpool-ID und die App-Client-ID.	App-Entwickler, General AWS
Implementieren Sie die Amazon Cognito Cognito-Authentifizierung.	Dies hängt von Ihrem ausgewählten Authentifizierungsablauf, Ihrer Programmiersprache und den von Ihnen verwendeten Frameworks ab. Einige Links für den Einstieg finden Sie im Abschnitt Verwandte Ressourcen.	App-Developer

Zugehörige Ressourcen

AWS-Dokumentation

- Ablauf der Benutzerpool-Authentifizierung
- Überprüfen eines JSON-Web-Tokens
- Greifen Sie über eine ASP.NET Core-App mithilfe von Amazon Cognito Cognito-Identitätspools auf AWS-Services zu
- Frameworks und: SDKs
  - Amazon Amplify-Authentifizierung
  - Beispiele für Amazon Cognito Identity Provider (Dokumentation zum AWS SDK for Java 2.x)
  - Authentifizierung von Benutzern mit Amazon Cognito (AWS SDK for .NET .NET-Dokumentation)

AWS-Blogbeiträge

- Authorization @Edge mithilfe von Cookies: Schützen Sie Ihre CloudFront Amazon-Inhalte davor, von nicht authentifizierten Benutzern heruntergeladen zu werden
- Aufbau eines AD FS-Verbunds für Ihre Web-App mithilfe von Amazon Cognito Cognito-Benutzerpools

Implementierungspartner

- AWS-Partner für Authentifizierungslösungen

Zusätzliche Informationen

HÄUFIG GESTELLTE FRAGEN

Warum ist der implizite Flow veraltet?

Seit der Veröffentlichung des OAuth 2.1-Frameworks ist der Implicit Flow aus Sicherheitsgründen als veraltet markiert. Verwenden Sie als Alternative den Authorization Code Flow mit PKCE, der im Abschnitt Architektur beschrieben wird.

Was ist, wenn Amazon Cognito einige Funktionen, die ich benötige, nicht bietet?

AWS-Partner bieten verschiedene Integrationen für Authentifizierungs- und Autorisierungslösungen an. Weitere Informationen finden Sie unter AWS-Partner für Authentifizierungslösungen.

Was ist mit Amazon Cognito Cognito-Identitätspool-Flows?

Amazon Cognito Cognito-Benutzerpools und föderierte Identitäten dienen der Authentifizierung. Amazon Cognito Cognito-Identitätspools werden für die Autorisierung des Zugriffs auf AWS-Ressourcen verwendet, indem temporäre AWS-Anmeldeinformationen angefordert werden. Der Austausch von ID-Token und Zugriffstoken für Identitätspools wird in diesem Muster nicht behandelt. Weitere Informationen finden Sie unter Was ist der Unterschied zwischen Amazon Cognito-Benutzerpools und Identitätspools und Allgemeine Amazon Cognito-Szenarien.

Nächste Schritte

Dieses Muster bietet einen Überblick über die Amazon Cognito Cognito-Authentifizierungsabläufe. Als nächster Schritt muss die detaillierte Implementierung für die Programmiersprache der

Anwendung ausgewählt werden. Angebot SDKs und Frameworks in mehreren Sprachen, die Sie mit Amazon Cognito verwenden können. Hilfreiche Referenzen finden Sie im Abschnitt Verwandte Ressourcen.

Erstellen Sie AWS Config benutzerdefinierte Regeln mithilfe von AWS CloudFormation Guard Richtlinien

Erstellt von Andrew Lok (AWS), Kailash Havildar (AWS), Nicole Brown (AWS) und Tanya Howell (AWS)

Übersicht

AWS ConfigRegeln helfen Ihnen dabei, Ihre AWS Ressourcen und ihren Zielkonfigurationsstatus zu bewerten. Es gibt zwei Arten von AWS Config Regeln: verwaltete und benutzerdefinierte Regeln. Sie können benutzerdefinierte Regeln mit AWS Lambda Funktionen oder mit AWS CloudFormation Guard(GitHub), einer policy-as-code Sprache, erstellen.

Mit Guard erstellte Regeln bieten eine detailliertere Steuerung als verwaltete Regeln und sind in der Regel einfacher zu konfigurieren als vollständig benutzerdefinierte Lambda-Regeln. Dieser Ansatz bietet Ingenieuren und Architekten die Möglichkeit, Regeln zu erstellen, ohne Python, NodeJS oder Java kennen zu müssen, die für die Bereitstellung benutzerdefinierter Regeln über Lambda erforderlich sind.

Dieses Muster bietet praktikable Vorlagen, Codebeispiele und Bereitstellungsansätze, die Sie bei der Einführung benutzerdefinierter Regeln mit Guard unterstützen. Mithilfe dieses Musters kann ein Administrator benutzerdefinierte Compliance-Regeln mit Attributen für Konfigurationselemente erstellen. AWS Config Entwickler können beispielsweise Guard-Richtlinien für AWS Config Konfigurationselemente verwenden, um den Status bereitgestellter AWS und nicht vorhandener AWS Ressourcen kontinuierlich zu überwachen, Regelverstöße zu erkennen und automatisch Abhilfemaßnahmen einzuleiten.

Ziele

Nachdem Sie dieses Muster gelesen haben, sollten Sie in der Lage sein:

- Verstehen Sie, wie der Guard-Richtliniencode mit dem AWS Config Service interagiert.
- Stellen Sie Szenario 1 bereit. Dabei handelt es sich um eine AWS Config benutzerdefinierte Regel, die die Guard-Syntax verwendet, um die Konformität für verschlüsselte Volumes zu überprüfen. Diese Regel überprüft, ob das Laufwerk verwendet wird, und stellt sicher, dass der Laufwerkstyp gp3 ist.
- Stellen Sie Szenario 2 bereit, eine AWS Config benutzerdefinierte Regel, die die Guard-Syntax verwendet, um die GuardDuty Amazon-Konformität zu überprüfen. Diese Regel überprüft, ob bei

GuardDuty Rekordern Amazon Simple Storage Service (Amazon S3) Protection und Amazon Elastic Kubernetes Service (Amazon EKS) Protection aktiviert sind.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- AWS Config, eingerichtet in Ihrem AWS-Konto

Einschränkungen

- Benutzerdefinierte Guard-Regeln können nur Schlüssel-Wert-Paare in einem JSON-Datensatz für ein Zielkonfigurationselement abfragen

Architektur

Sie wenden die Guard-Syntax als benutzerdefinierte Richtlinie auf eine AWS Config Regel an. AWS Config erfasst die hierarchische JSON-Datei jeder der angegebenen Ressourcen. Das JSON des AWS Config Konfigurationselements enthält Schlüssel-Wert-Paare. Diese Attribute werden in der Guard-Syntax als Variablen verwendet, die ihrem entsprechenden Wert zugewiesen werden.

Im Folgenden wird die Guard-Syntax erklärt. Die Variablen aus dem Konfigurationselement JSON werden verwendet und ihnen wird ein % Zeichen vorangestellt.

```
# declare variable
let <variable name> = <'value'>

# create rule and assign condition and policy
    rule <rule name> when
        <CI json key> == <"CI json value"> {
            <top level CI json key>.<next level CI json key> == %<variable name>
        }
```

Szenario 1: Amazon EBS-Volumes

Szenario 1 stellt eine AWS Config benutzerdefinierte Regel bereit, die die Guard-Syntax verwendet, um die Konformität für verschlüsselte Volumes zu überprüfen. Diese Regel überprüft, ob das Laufwerk verwendet wird, und stellt sicher, dass der Laufwerkstyp gp3 ist.

Das Folgende ist ein Beispiel für ein AWS Config Konfigurationselement für Szenario 1. Dieses Konfigurationselement enthält drei Schlüssel-Wert-Paare, die als Variablen in der Guard-Richtlinie verwendet werden: `volumestatusvolumeencryptionstatus`, und. `volumetype` Außerdem wird der `resourceType` Schlüssel in der Guard-Richtlinie als Filter verwendet.


```
{
  "version": "1.3",
  "accountId": "111111111111",
  "configurationItemCaptureTime": "2023-01-15T19:04:45.402Z",
  "configurationItemStatus": "ResourceDiscovered",
  "configurationStateId": "4444444444444",
  "configurationItemMD5Hash": "",
  "arn": "arn:aws:ec2:us-west-2:111111111111:volume/vol-222222222222",
  "resourceType": "AWS::EC2::Volume",
  "resourceId": "vol-222222222222",
  "awsRegion": "us-west-2",
  "availabilityZone": "us-west-2b",
  "resourceCreationTime": "2023-01-15T19:03:22.247Z",
  "tags": {},
  "relatedEvents": [],
  "relationships": [
    {
      "resourceType": "AWS::EC2::Instance",
      "resourceId": "i-33333333333333333",
      "relationshipName": "Is attached to Instance"
    }
  ],
  "configuration": {
    "attachments": [
      {
        "attachTime": "2023-01-15T19:03:22.000Z",
        "device": "/dev/xvda",
        "instanceId": "i-33333333333333333",
        "state": "attached",
        "volumeId": "vol-222222222222",
        "deleteOnTermination": true,
        "associatedResource": null,
        "instanceOwningService": null
      }
    ],
    "availabilityZone": "us-west-2b",
    "createTime": "2023-01-15T19:03:22.247Z",
    "encrypted": false,
```

```
    "kmsKeyId": null,
    "outpostArn": null,
    "size": 8,
    "snapshotId": "snap-55555555555555555",
    "state": "in-use",
    "volumeId": "vol-222222222222",
    "iops": 100,
    "tags": [],
    "volumeType": "gp2",
    "fastRestored": null,
    "multiAttachEnabled": false,
    "throughput": null,
    "sseType": null
  },
  "supplementaryConfiguration": {}
}
```

Das Folgende ist ein Beispiel für die Verwendung der Guard-Syntax zur Definition der Variablen und Regeln in Szenario 1. Beachten Sie im folgenden Beispiel Folgendes:

- Die ersten drei Zeilen definieren die Variablen mithilfe des `let` Befehls. Ihnen wird ein Name und ein Wert zugewiesen, die von den Attributen des Konfigurationselements abgeleitet sind.
- Der `compliancecheck` Regelblock fügt eine Abhängigkeit vom Typ when hinzu, die nach einem übereinstimmenden `resourceType` Schlüssel-Wert-Paar sucht. `AWS::EC2::Volume` Wenn eine Übereinstimmung gefunden wird, durchsucht die Regel die restlichen JSON-Attribute und sucht unter den folgenden drei Bedingungen nach Übereinstimmungen: `stateencrypted`, und. `volumeType`

```
let volumestatus = 'available'
let volumetype = 'gp3'
let volumeencryptionstatus = true

    rule compliancecheck when
        resourceType == "AWS::EC2::Volume" {
            configuration.state == %volumestatus
            configuration.encrypted == %volumeencryptionstatus
            configuration.volumeType == %volumetype
        }
```

Die vollständige benutzerdefinierte Guard-Richtlinie, die diese benutzerdefinierte Regel implementiert, finden Sie unter awsconfig-guard-cft.yaml oder awsconfig-guard-tf-ec2vol.json im Code-Repository. GitHub HashiCorp Terraform-Code, der diese benutzerdefinierte Richtlinie in Guard bereitstellt, finden Sie unter .json im Code-Repository. awsconfig-guard-tf-example

Szenario 2: Einhaltung GuardDuty

Szenario 2 stellt eine AWS Config benutzerdefinierte Regel bereit, die die Guard-Syntax verwendet, um die GuardDuty Amazon-Konformität zu überprüfen. Diese Regel überprüft, ob bei GuardDuty Rekordern Amazon S3 S3-Schutz und Amazon EKS-Schutz aktiviert sind. Außerdem wird überprüft, ob die GuardDuty Ergebnisse alle 15 Minuten veröffentlicht werden. Dieses Szenario könnte überall AWS-Konten und AWS-Regionen in einer Organisation (in AWS Organizations) eingesetzt werden.

Das Folgende ist ein Beispiel für ein AWS Config Konfigurationselement für Szenario 2. Dieses Konfigurationselement enthält drei Schlüssel-Wert-Paare, die als Variablen in der Guard-Richtlinie verwendet werden: `FindingPublishingFrequency`S3Logs, und. `Kubernetes` Außerdem wird der `resourceType` Schlüssel in der Richtlinie als Filter verwendet.

```
{
  "version": "1.3",
  "accountId": "111111111111",
  "configurationItemCaptureTime": "2023-11-27T13:34:28.888Z",
  "configurationItemStatus": "OK",
  "configurationStateId": "7777777777777",
  "configurationItemMD5Hash": "",
  "arn": "arn:aws:guardduty:us-
west-2:111111111111:detector/66666666666666666666666666666666",
  "resourceType": "AWS::GuardDuty::Detector",
  "resourceId": "66666666666666666666666666666666",
  "resourceName": "66666666666666666666666666666666",
  "awsRegion": "us-west-2",
  "availabilityZone": "Regional",
  "resourceCreationTime": "2020-02-17T02:48:04.511Z",
  "tags": {},
  "relatedEvents": [],
  "relationships": [],
  "configuration": {
    "Enable": true,
    "FindingPublishingFrequency": "FIFTEEN_MINUTES",
    "DataSources": {
      "S3Logs": {
        "Enable": true
```

```
      },
      "Kubernetes": {
        "AuditLogs": {
          "Enable": true
        }
      }
    },

    "Id": "66666666666666666666666666666666",
    "Tags": []
  },
  "supplementaryConfiguration": {
    "CreatedAt": "2020-02-17T02:48:04.511Z"
  }
}
```

Im Folgenden finden Sie ein Beispiel für die Verwendung der Guard-Syntax zur Definition der Variablen und Regeln in Szenario 2. Beachten Sie im folgenden Beispiel Folgendes:

- Die ersten drei Zeilen definieren die Variablen mithilfe des `let` Befehls. Ihnen wird ein Name und ein Wert zugewiesen, die von den Attributen des Konfigurationselements abgeleitet sind.
- Der `compliancecheck` Regelblock fügt eine Abhängigkeit vom Typ when hinzu, die nach einem übereinstimmenden `resourceType` Schlüssel-Wert-Paar sucht. `AWS::GuardDuty::Detector` Wenn eine Übereinstimmung gefunden wird, durchsucht die Regel die restlichen JSON-Attribute und sucht unter den folgenden drei Bedingungen nach Übereinstimmungen: `S3Logs.Enable`Kubernetes.AuditLogs.Enable, und. `FindingPublishingFrequency`

```
let s3protection = true
let kubernetesprotection = true
let publishfrequency = 'FIFTEEN_MINUTES'

    rule compliancecheck when
        resourceType == "AWS::GuardDuty::Detector" {
            configuration.DataSources.S3Logs.Enable == %s3protection
            configuration.DataSources.Kubernetes.AuditLogs.Enable ==
 %kubernetesprotection
            configuration.FindingPublishingFrequency == %publishfrequency
        }
```

Die vollständige benutzerdefinierte Guard-Richtlinie, die diese benutzerdefinierte Regel implementiert, finden Sie unter awsconfig-guard-cft-gd.yaml im GitHub Code-Repository. HashiCorp Terraform-Code, der diese benutzerdefinierte Richtlinie in Guard bereitstellt, finden Sie unter awsconfig-guard-tf-gd.json im Code-Repository.

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend zu verwalten. AWS-Konten
- AWS Configbietet einen detaillierten Überblick über die Ressourcen in Ihrem System AWS-Konto und darüber, wie sie konfiguriert sind. Es hilft Ihnen zu erkennen, wie Ressourcen miteinander zusammenhängen und wie sich ihre Konfigurationen im Laufe der Zeit geändert haben.

Andere Tools

- HashiCorp Terraform ist ein Infrastructure-as-Code-Tool (IaC), mit dem Sie mithilfe von Code Cloud-Infrastruktur und -Ressourcen bereitstellen und verwalten können.

Code-Repository

Der Code für dieses Muster ist im AWS CloudFormation Guard Repository GitHub AWS Config with verfügbar. Dieses Code-Repository enthält Beispiele für beide in diesem Muster beschriebenen Szenarien.

Epen

AWS Config Benutzerdefinierte Regeln erstellen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Wählen Sie Schlüssel-Wert-Paare für die Regel aus.	Gehen Sie wie folgt vor, wenn Sie eine benutzerdefinierte Guard-Richtlinie definieren. Wenn Sie eine der Beispielr ichtlinien für Szenario 1 oder 2	AWS-Administrator, Sicherhei tsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	verwenden, überspringen Sie diese Schritte. 1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole. 2. Wählen Sie in der linken Navigationsleiste Ressourcen aus. 3. Wählen Sie im Ressource ninventar den Ressource ntyp aus, für den Sie eine AWS Config benutzerd efinierte Regel erstellen möchten. 4. Wählen Sie die Option Details anzeigen aus. 5. Wählen Sie Konfigura tionselement anzeigen (JSON). Dieser Abschnitt wird erweitert und zeigt das Konfigurationselement im JSON-Format an. 6. Identifizieren Sie die Schlüssel-Wert-Paare, für die Sie eine AWS Config benutzerdefinierte Regel erstellen möchten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die benutzerdefinierte Regel.	Folgen Sie den Anweisungen unter Benutzerdefinierte Richtlinienregeln erstellen, um eine AWS Config benutzerdefinierte Regel zu erstellen, indem Sie die zuvor identifizierten Schlüssel-Wert-Paare verwenden oder eine der bereitgestellten Guard-Beispielrichtlinien verwenden.	AWS-Administrator, Sicherheitsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die benutzerd efinierte Regel.	Führen Sie einen der folgenden Schritte aus, um die benutzerdefinierte Guard-Reg el zu validieren: • Geben Sie den folgenden Befehl in das Feld AWS Command Line Interface (AWS CLI) ein. `cfn-guard validate -r guard-s3.guard -d s3bucket-prod-pass.json` • Folgen Sie den Anweisung en im Detektivmodus unter Evaluieren Ihrer Ressourcen mit AWS Config Regeln, um die Regel in zu implementieren AWS Config. Vergewissern Sie sich, dass die Guard-Syn tax den entsprechenden Ressourcen im Zielkonto oder in der Zieldatei korrekt entspricht.	AWS-Administrator, Sicherhei tsingenieur

Fehlerbehebung

Problem	Lösung
Testen Sie die Guard-Richtlinie außerhalb von AWS Config	Unit-Tests können auf Ihrem lokalen Gerät oder in einer integrierten Entwicklungsumgebung (IDE), z. B. einer AWS Cloud9 IDE, durchgefü

Problem	Lösung

	hrt werden. Gehen Sie wie folgt vor, um Komponententests durchzuführen:
	1. Installieren Sie die AWS CloudFormation Guard CLI und ihre Abhängigkeiten.
	2. Speichern Sie ein CI-Beispiel im JSON-Form at als JSON-Datei auf Ihrer Workstation.
	3. Speichern Sie die GuardDuty Richtlinie als .guard-Datei auf Ihrer Workstation.
	4. Geben Sie in der Guard-CLI den folgenden Befehl ein, um die JSON-Beispieldatei mithilfe der Guard-Richtlinie zu validieren.
	`cfn-guard validate \`
	`-r guard-s3.guard \`
	`-d s3bucket-prod-pass.json`

Debuggen Sie eine AWS Config benutzerd efinierte Regel	Ändern Sie den `EnableDebugLogDeli very` Wert in Ihrer Guard-Richtlinie in `true`. Der Standardwert ist `false`. Die Protokoll nachrichten werden in Amazon gespeichert CloudWatch.

Zugehörige Ressourcen

AWS Dokumentation

- Erstellen AWS Config benutzerdefinierter Richtlinienregeln (AWS Config Dokumentation)
- AWS CloudFormation Guard Regeln schreiben (Guard-Dokumentation)

AWS Blogbeiträge und Workshops

- Wir stellen vor AWS CloudFormation Guard 2.0 (AWS Blogbeitrag)

Sonstige Ressourcen

- AWS CloudFormation Guard (GitHub)
- AWS CloudFormation Guard CLI-Dokumentation (GitHub)

Erstellen Sie einen konsolidierten Bericht mit den Sicherheitsergebnissen von Prowler aus mehreren AWS-Konten

Erstellt von Mike Virgilio (AWS), Andrea Di Fabio (AWS) und Jay Durga (AWS)

Übersicht

Prowler (GitHub) ist ein Open-Source-Befehlszeilentool, mit dem Sie Ihre Amazon Web Services (AWS) -Konten bewerten, prüfen und überwachen können, um sicherzustellen, dass sie die bewährten Sicherheitsmethoden einhalten. Bei diesem Muster setzen Sie Prowler in einem zentralen System AWS-Konto in Ihrer Organisation ein, das von verwaltet wird AWS Organizations, und verwenden dann Prowler, um eine Sicherheitsbewertung aller Konten in der Organisation durchzuführen.

Es gibt zwar viele Methoden, um Prowler für eine Bewertung einzusetzen und zu nutzen, aber diese Lösung wurde für eine schnelle Implementierung, eine vollständige Analyse aller Konten in der Organisation oder definierter Zielkonten und eine leicht zugängliche Berichterstattung über die Sicherheitsergebnisse konzipiert. Bei dieser Lösung werden die Ergebnisse konsolidiert, sobald Prowler die Sicherheitsbeurteilung aller Konten im Unternehmen abgeschlossen hat. Außerdem werden alle erwarteten Fehlermeldungen herausgefiltert, z. B. Fehler im Zusammenhang mit Einschränkungen, die Prowler daran hindern, Amazon Simple Storage Service (Amazon S3) -Buckets in Konten zu scannen, die über bereitgestellt wurden. AWS Control Tower Die gefilterten, konsolidierten Ergebnisse werden in einer Microsoft Excel-Vorlage gemeldet, die in diesem Muster enthalten ist. Sie können diesen Bericht verwenden, um potenzielle Verbesserungen der Sicherheitskontrollen in Ihrem Unternehmen zu ermitteln.

Bei der Entwicklung dieser Lösung wurde Folgendes berücksichtigt:

- Die AWS CloudFormation Vorlagen reduzieren den Aufwand, der für die Bereitstellung der AWS Ressourcen in diesem Muster erforderlich ist.
- Sie können die Parameter in den CloudFormation Vorlagen und im Skript prowler_scan.sh zum Zeitpunkt der Bereitstellung anpassen, um die Vorlagen an Ihre Umgebung anzupassen.
- Die Geschwindigkeit der Bewertung und Berichterstattung durch Prowler wird durch die parallel Verarbeitung aggregierter Ergebnisse AWS-Konten, konsolidierte Berichte mit empfohlenen Abhilfemaßnahmen und automatisch generierte Visualisierungen optimiert.

- Der Benutzer muss den Scanfortschritt nicht überwachen. Wenn die Bewertung abgeschlossen ist, wird der Benutzer über ein Amazon Simple Notification Service (Amazon SNS) -Thema benachrichtigt, sodass er den Bericht abrufen kann.
- Die Berichtsvorlage hilft Ihnen dabei, nur die relevanten Ergebnisse für Ihr gesamtes Unternehmen zu lesen und zu bewerten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine AWS-Konto zum Hosten von Sicherheitsdiensten und -tools, die als Mitgliedskonto einer Organisation in verwaltet AWS Organizations werden. In diesem Muster wird dieses Konto als Sicherheitskonto bezeichnet.
- Im Sicherheitskonto müssen Sie über ein privates Subnetz mit ausgehendem Internetzugang verfügen. Anweisungen finden Sie unter VPC mit Servern in privaten Subnetzen und NAT in der Dokumentation zu Amazon Virtual Private Cloud (Amazon VPC). Sie können den Internetzugang mithilfe eines NAT-Gateways einrichten, das in einem öffentlichen Subnetz bereitgestellt wird.
- Zugriff auf das AWS Organizations Verwaltungskonto oder ein Konto, für das delegierte Administratorrechte erteilt wurden. CloudFormation Anweisungen finden Sie in der Dokumentation unter Registrieren eines delegierten Administrators. CloudFormation
- Aktivieren Sie den vertrauenswürdigen Zugriff zwischen AWS Organizations und CloudFormation. Anweisungen finden Sie AWS Organizations in der CloudFormation Dokumentation unter Vertrauenswürdigen Zugriff aktivieren mit.

Einschränkungen

- Das Ziel AWS-Konten muss als Organisation in verwaltet werden AWS Organizations. Wenn Sie die Vorlage nicht verwenden AWS Organizations, können Sie die CloudFormation Vorlage IAM- ProwlerExecRole .yaml und das Skript prowler_scan.sh für Ihre Umgebung aktualisieren. Stattdessen geben Sie eine Liste der AWS-Konto IDs Regionen an, in denen Sie das Skript ausführen möchten.
- Die CloudFormation Vorlage ist für die Bereitstellung der Amazon Elastic Compute Cloud (Amazon EC2) -Instance in einem privaten Subnetz mit ausgehendem Internetzugang konzipiert. Der AWS Systems Manager Agent (SSM Agent) benötigt ausgehenden Zugriff, um den AWS Systems Manager Service-Endpunkt zu erreichen, und Sie benötigen ausgehenden Zugriff, um das Code-Repository zu klonen und Abhängigkeiten zu installieren. Wenn Sie ein öffentliches Subnetz

verwenden möchten, müssen Sie die Vorlage prowler-resources.yaml ändern, um der Instance eine Elastic IP-Adresse zuzuordnen. EC2

Produktversionen

- Prowler Version 4.0 oder höher

Architektur

Das Diagramm zeigt den folgenden Prozess:

1. Mithilfe von Session Manager, einer Fähigkeit von AWS Systems Manager, authentifiziert sich der Benutzer bei der EC2 Instanz und führt das Skript prowler_scan.sh aus. Dieses Shell-Skript führt die Schritte 2 bis 8 aus.
2. Die EC2 Instanz übernimmt die `ProwlerEC2Role` IAM-Rolle, die Berechtigungen für den Zugriff auf den S3-Bucket und für die Übernahme der `ProwlerExecRole` IAM-Rollen in den anderen Konten in der Organisation gewährt.
3. Die EC2 Instanz übernimmt die `ProwlerExecRole` IAM-Rolle im Verwaltungskonto der Organisation und generiert eine Liste der Konten in der Organisation.
4. Die EC2 Instanz übernimmt die `ProwlerExecRole` IAM-Rolle in den Mitgliedskonten der Organisation (im Architekturdiagramm als Workload-Konten bezeichnet) und führt für jedes Konto eine Sicherheitsbewertung durch. Die Ergebnisse werden als CSV- und HTML-Dateien auf der EC2 Instanz gespeichert.

   > **Note**
   >
   > HTML-Dateien sind ein Ergebnis des Prowler-Assessments. Aufgrund der Natur von HTML werden sie nicht verkettet, verarbeitet oder direkt in diesem Muster verwendet. Diese können jedoch für die Überprüfung einzelner Kontoberichte nützlich sein.

5. Die EC2 Instanz verarbeitet alle CSV-Dateien, um bekannte, erwartete Fehler zu entfernen, und konsolidiert die verbleibenden Ergebnisse in einer einzigen CSV-Datei.
6. Die EC2 Instanz verpackt die einzelnen Kontoergebnisse und die aggregierten Ergebnisse in einer ZIP-Datei.
7. Die EC2 Instanz lädt die Zip-Datei in den S3-Bucket hoch.

8. Eine EventBridge Regel erkennt den Datei-Upload und verwendet ein Amazon SNS SNS-Thema, um dem Benutzer eine E-Mail zu senden, in der er darüber informiert wird, dass die Bewertung abgeschlossen ist.
9. Der Benutzer lädt die Zip-Datei aus dem S3-Bucket herunter. Der Benutzer importiert die Ergebnisse in die Excel-Vorlage und überprüft die Ergebnisse.

Tools

AWS-Services

- Amazon Elastic Compute Cloud (Amazon EC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS Lambda Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen. AWS-Konten
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Organizationsist ein Kontoverwaltungsservice, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie erstellen und zentral verwalten.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Systems Managerhilft Ihnen bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der AWS Cloud ausgeführt werden. Es vereinfacht das Anwendungs- und Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme und hilft Ihnen, Ihre AWS Ressourcen sicher und in großem Umfang zu verwalten. Dieses Muster verwendet Session Manager, eine Funktion von Systems Manager.

Andere Tools

- Prowler ist ein Open-Source-Befehlszeilentool, mit dem Sie Ihre Konten bewerten, prüfen und überwachen können, um sicherzustellen, dass sie bewährte AWS Sicherheitsmethoden und andere Sicherheitsrahmen und -standards einhalten.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub Multi-Account Security Assessment via Prowler verfügbar. Das Code-Repository enthält die folgenden Dateien:

- prowler_scan.sh — Dieses Bash-Skript wird verwendet, um eine Prowler-Sicherheitsbewertung von mehreren gleichzeitig AWS-Konten zu parallel. Wie in der Datei Prowler-Resources.yaml definiert CloudFormationtemplate, wird dieses Skript automatisch im Ordner auf der Instanz bereitgestellt. `usr/local/prowler` EC2
- prowler-resources.YAML — Sie verwenden diese CloudFormation Vorlage, um einen Stack im Sicherheitskonto der Organisation zu erstellen. Diese Vorlage stellt alle erforderlichen Ressourcen für dieses Konto bereit, um die Lösung zu unterstützen. Dieser Stack muss vor der Vorlage IAM-ProwlerExecRole .yaml bereitgestellt werden. Es wird nicht empfohlen, diese Ressourcen in einem Konto bereitzustellen, das kritische Produktionsworkloads hostet.

  > **Note**
  >
  > Wenn dieser Stack gelöscht und erneut bereitgestellt wird, müssen Sie den `ProwlerExecRole` Stacksatz neu erstellen, um die kontenübergreifenden Abhängigkeiten zwischen den IAM-Rollen wiederherzustellen.

- IAM- ProwlerExecRole .yaml — Sie verwenden diese CloudFormation Vorlage, um ein Stack-Set zu erstellen, das die `ProwlerExecRole` IAM-Rolle in allen Konten der Organisation, einschließlich des Verwaltungskontos, bereitstellt.
- prowler-report-template.xlsm — Sie verwenden diese Excel-Vorlage, um die Ergebnisse von Prowler zu verarbeiten. Die Pivot-Tabellen im Bericht bieten Suchfunktionen, Diagramme und konsolidierte Ergebnisse.

Epen

Bereite dich auf den Einsatz vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Code-Repo sitory.	1. Ändern Sie in einer Befehlszeilenschnittstelle Ihr Arbeitsverzeichnis in das Verzeichnis, in dem Sie die Beispieldateien speichern möchten. 2. Geben Sie den folgenden Befehl ein: `git clone https://github.com/aws-samples/multi-account-security-assessment-via-prowler.git`	AWS DevOps
Überprüfen Sie die Vorlagen.	1. Öffnen Sie im geklonten Repository die Dateien Prowler-Resources.yaml und IAM- .yaml. ProwlerExecRole 2. Überprüfen Sie die mit diesen Vorlagen erstellten Ressourcen und passen Sie die Vorlagen nach Bedarf an Ihre Umgebung an. Weitere Informationen finden Sie in der CloudFormation Dokumentation unter Arbeiten mit Vorlagen. 3. Speichern und schließen Sie die Dateien Prowler-	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Resources.yaml und IAM- .yaml. ProwlerEx ecRole	

Erstellen Sie die CloudFormation Stapel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Ressourcen im Sicherheitskonto bereit.	Mithilfe der Vorlage prowler-resources.yaml erstellen Sie einen CloudFormation Stack, der alle erforderl ichen Ressourcen im Sicherheitskonto bereitstellt. Anweisungen finden Sie in der Dokumentation unter Einen Stack erstellen. CloudForm ation Beachten Sie bei der Bereitstellung dieser Vorlage Folgendes: 1. Wählen Sie auf der Seite „Vorlage angeben“ die Option Vorlage ist bereit aus und laden Sie dann die Datei prowler-resources. yaml hoch. 2. Geben Sie auf der Seite „Stack-Details angeben“ im Feld Stack-Name Folgendes ein. `Prowler-R esources` 3. Geben Sie im Abschnitt Parameter Folgendes ein:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	• `VPCId`— Wählen Sie eine VPC im Konto aus.
	• `SubnetId`— Wählen Sie ein privates Subnetz mit Internetzugang aus.
	
	Hinweis: Wenn Sie ein öffentliches Subnetz auswählen, wird der EC2 Instance keine öffentliche IP-Adresse zugewiesen, da die CloudFormation Vorlage standardmäßig keine Elastic IP-Adresse bereitstellt und anfügt.
	• `InstanceType` — Wählen Sie eine Instanzgröße basierend auf der Anzahl der parallel Bewertungen aus:
	  • Für 10 wählen Sie `r6i.large` .
	  • Für 12 wählen Sie `r6i.xlarge` .
	  • Wählen Sie für 14—18. `r6i.2xlarge`
	• `InstanceImageId` — Behalten Sie die Standardeinstellung für Amazon Linux bei.
	• `KeyPairName` — Wenn Sie SSH für den Zugriff	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	verwenden, geben Sie den Namen eines vorhandenen key pair an. • `PermittedSSHInbound` — Wenn Sie SSH für den Zugriff verwenden, geben Sie einen zulässigen CIDR-Block an. Wenn Sie SSH nicht verwenden, behalten Sie den Standardwert von bei. `127.0.0.1` • `BucketName` — Der Standardwert ist`prowler-output-<accountID>-<region>` . Sie können dies nach Bedarf ändern. Wenn Sie einen benutzerdefinierten Wert angeben, werden die Konto-ID und die Region automatisch an den angegebenen Wert angehängt. • `EmailAddress` — Geben Sie eine E-Mail-Adresse für eine Amazon SNS SNS-Benachrichtigung an, wenn Prowler die Bewertung abgeschlossen und die ZIP-Datei in den S3-Bucket hochlädt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Hinweis: Die Konfiguration des SNS-Abonnements muss bestätigt werden, bevor Prowler die Bewertung abschließt. Andernfalls wird keine Benachrichtigung gesendet. • `IAMProwlerEC2Role` — Behalten Sie die Standardeinstellung bei, es sei denn, Ihre Benennungskonventionen erfordern einen anderen Namen für diese IAM-Rolle. • `IAMProwlerExecRole` — Behalten Sie die Standardeinstellung bei, es sei denn, bei der Bereitstellung der Datei IAM- ProwlerExecRole .yaml wird ein anderer Name verwendet. • `Parallelism` — Geben Sie die Anzahl der parallel Prüfungen an, die durchgeführt werden sollen. Stellen Sie sicher, dass der Wert im `InstanceType` Parameter diese Anzahl	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	parallel Bewertungen unterstützt. • `FindingOutput` — Wenn Sie bestandene Ergebnisse ausschließen möchten, wählen Sie `FailOnly`. Dadurch wird die Ausgabegröße erheblich reduziert und der Schwerpunkt liegt auf den Prüfungen, die möglicherweise behoben werden müssen. Wenn Sie bestandene Ergebnisse einbeziehen möchten, wählen Sie `FailAndPass` . 4. Wählen Sie auf der Seite Überprüfen die Option Die folgenden Ressourcen erfordern Fähigkeiten: [AWS::IAM::Role] und wählen Sie dann Stack erstellen aus. 5. Nachdem der Stack erfolgreich erstellt wurde, kopieren Sie in der CloudFormation Konsole auf der Registerkarte Outputs den `ProwlerEC2Role` Amazon-Ressourcennamen (ARN). Sie verwenden diesen ARN später, wenn Sie	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Datei IAM- ProwlerEx ecRole .yaml bereitstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die IAM-Rolle in den Mitgliedskonten bereit.	Verwenden Sie im AWS Organizations Verwaltungskonto oder einem Konto mit delegierten Administratorrechten für die Vorlage IAM- ProwlerExecRole .yaml CloudFormation, um ein Stack-Set zu erstellen. CloudFormation Das Stack-Set stellt die `ProwlerExecRole` IAM-Rolle in allen Mitgliedskonten der Organisation bereit. Anweisungen finden Sie in der Dokumentation unter Erstellen eines Stack-Sets mit vom Service verwalteten Berechtigungen. CloudFormation Beachten Sie bei der Bereitstellung dieser Vorlage Folgendes: 1. Wählen Sie unter Vorlage vorbereiten die Option Vorlage ist bereit aus und laden Sie dann die Datei IAM- ProwlerExecRole .yaml hoch. 2. Geben Sie auf der Seite „ StackSet Details angeben“ dem Stack-Set einen Namen. `IAM-ProwlerExecRole` 3. Geben Sie im Abschnitt Parameter Folgendes ein:	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `AuthorizedARN` — Geben Sie den `ProwlerEC2Role` ARN ein, den Sie bei der Erstellung des `Prowler-Resources` Stacks kopiert haben. • `ProwlerExecRoleNam e` — Behalten Sie den Standardwert von bei, `ProwlerExecRole` sofern bei der Bereitste llung der Datei Prowler-Resources.yaml kein anderer Name verwendet wurde. 4. Wählen Sie unter Permissio ns (Berechtigungen) die Option Service-managed permissions (Servicev erwaltete Berechtigungen) aus. 5. Wählen Sie auf der Seite Bereitstellungsoptionen festlegen unter Bereitste llungsziele die Option Für die Organisation bereitste llen aus und akzeptieren Sie alle Standardeinstellun gen. Hinweis: Wenn Sie möchten, dass die Stacks für alle Mitgliedskonten	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	gleichzeitig bereitgestellt werden, legen Sie „Maximale Anzahl gleichzeitiger Konten“ und „Fehlertoleranz“ auf einen hohen Wert fest, z. B. `100` 6. Wählen Sie unter Bereitstellungsregionen die Region aus, AWS-Region in der die EC2 Instanz für Prowler bereitgestellt wird. Da es sich bei den IAM-Ressourcen um globale und nicht um regionale Ressourcen handelt, wird dadurch die IAM-Rolle in allen aktiven Regionen bereitgestellt. 7. Wählen Sie auf der Seite Überprüfen die Option Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen mit benutzerdefinierten Namen erstellt werden, und wählen Sie dann Erstellen aus. StackSet 8. Überwachen Sie die Registerkarte Stack-Instances (für den Status einzelner Konten) und die Registerkarte Operationen (für den Gesamtstatus), um festzustellen, wann die	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bereitstellung abgeschlossen ist.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die IAM-Rolle im Verwaltungskonto bereit.	Mithilfe der Vorlage IAM-ProwlerExecRole .yaml erstellen Sie einen CloudFormation Stack, der die `ProwlerExecRole` IAM-Rolle im Verwaltungskonto der Organisation bereitstellt. Das Stack-Set, das Sie zuvor erstellt haben, stellt die IAM-Rolle nicht im Verwaltungskonto bereit. Anweisungen finden Sie in der CloudFormation Dokumentation unter Einen Stack erstellen. Beachten Sie bei der Bereitstellung dieser Vorlage Folgendes: 1. Wählen Sie auf der Seite „Vorlage angeben“ die Option Vorlage ist bereit aus und laden Sie dann die Datei IAM- ProwlerExecRole .yaml hoch. 2. Geben Sie auf der Seite „Stack-Details angeben“ im Feld Stackname Folgendes ein. `IAM-ProwlerExecRole` 3. Geben Sie im Abschnitt Parameter Folgendes ein: • `AuthorizedARN` — Geben Sie den `ProwlerEC2Role`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ARN ein, den Sie bei der Erstellung des `Prowler-Resources` Stacks kopiert haben. • `ProwlerExecRoleName` — Behalten Sie den Standardwert von bei, `ProwlerExecRole` sofern bei der Bereitstellung der Datei Prowler-Resources.yaml kein anderer Name verwendet wurde. 4. Wählen Sie auf der Seite „Überprüfen“ die Option Die folgenden Ressourcen erfordern Fähigkeiten: [AWS::IAM::Role] und wählen Sie dann Stapel erstellen aus.	

Führen Sie die Prowler-Sicherheitsbewertung durch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den Scan aus.	1. Melden Sie sich mit dem Sicherheitskonto in der Organisation an. 2. Stellen Sie mithilfe von Session Manager eine Verbindung zu der EC2 Instanz für Prowler her, die Sie zuvor bereitgestellt haben. Anweisungen	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	finden Sie unter Connect zu Ihrer Linux-Instance mithilfe von Session Manager. Wenn Sie keine Verbindung herstellen können, lesen Sie den Abschnitt zur Fehlerbehebung in diesem Muster. 3. Navigieren Sie zu der Datei prowler_scan.sh **`usr/local/prowler`** , und öffnen Sie sie. 4. Überprüfen und ändern Sie die einstellbaren Parameter und Variablen in diesem Skript nach Bedarf für Ihre Umgebung. Weitere Informationen zu Anpassungsoptionen finden Sie in den Kommentaren am Anfang des Skripts. Anstatt beispielsweise eine Liste aller Mitglieds konten in der Organisation aus dem Verwaltungskonto abzurufen, können Sie das Skript ändern, um das AWS-Konto IDs oder anzugeben, AWS-Regionen das Sie scannen möchten, oder Sie können auf eine externe Datei verweisen, die diese Parameter enthält.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	5. Speichern und schließen Sie die Datei prowler_scan.sh.
	6. Geben Sie die folgenden Befehle ein. Dadurch wird das Skript prowler_scan.sh ausgeführt.
	`sudo -i`
	`screen`
	`cd /usr/local/prowler`
	`./prowler_scan.sh`
	Beachten Sie Folgendes:
	• Der Befehl screen ermöglicht die weitere Ausführung des Skripts für den Fall, dass die Verbindung unterbrochen wird oder Sie den Konsolenzugriff verlieren.
	• Nach dem Start des Scans können Sie das Trennen des Bildschirms erzwingen, indem Sie Strg+A D drücken. Der Bildschirm wird getrennt, und Sie können die Instanzverbindung schließen und die Bewertung fortsetzen.
	• Um eine getrennte Sitzung wieder aufzunehmen, stellen	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie eine Verbindung zur Instanz her, geben Sie ein und geben Sie `sudo -i` dann die Eingabetaste ein`screen -r`. • Um den Fortschritt der einzelnen Kontoprüf ungen zu überwachen, können Sie zum `usr/local/prowler` Verzeichnis navigiere n und den Befehl eingeben`tail -f output/stdout-<account-id>` . 7. Warten Sie, bis Prowler die Scans aller Konten abgeschlossen hat. Das Skript bewertet mehrere Konten gleichzeitig. Wenn die Bewertung für alle Konten abgeschlossen ist, erhalten Sie eine Benachrichtigung, falls Sie bei der Bereitstellung der Datei Prowler-Resources. yaml eine E-Mail-Adresse angegeben haben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Rufen Sie die Ergebnisse von Prowler ab.	1. Laden Sie die `prowler-output-<assessDate>.zip` Datei aus dem Bucket herunter. `prowler-output-<accountID>-<region>` Anweisungen finden Sie in der Amazon S3 S3-Dokumentation unter Objekt herunterladen. 2. Löschen Sie alle Objekte im Bucket, einschließlich der Datei, die Sie heruntergeladen haben. Dies ist eine bewährte Methode zur Kostenoptimierung und um sicherzustellen, dass Sie den `Prowler-Resources` CloudFormation Stapel jederzeit löschen können. Anweisungen finden Sie in der Amazon S3 S3-Dokumentation unter Objekte löschen.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stoppen Sie die EC2 Instanz.	Um zu verhindern, dass die Instance abgerechnet wird, während sich die Instance im Leerlauf befindet, beenden Sie die EC2 Instance, auf der Prowler ausgeführt wird. Anweisungen finden Sie in der EC2 Amazon-Dokumentation unter Stoppen und Starten Ihrer Instances.	AWS DevOps

Erstellen Sie einen Bericht über die Ergebnisse

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Importieren Sie die Ergebnisse.	1. Öffnen Sie in Excel die prowler-report-templateXLSX-Datei und wählen Sie dann das Prowler CSV-Arbeitsblatt aus. 2. Löschen Sie alle Beispieldaten, einschließlich der Kopfzeile. Wenn Sie gefragt werden, ob Sie die Abfrage löschen möchten, die mit den zu entfernenden Daten verknüpft ist, wählen Sie Nein. Das Löschen der Abfrage kann sich auf die Funktionalität der Pivot-Tabellen in der Excel-Vorlage auswirken.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Extrahieren Sie den Inhalt der Zip-Datei, die Sie aus dem S3-Bucket heruntergeladen haben. 4. Öffnen Sie in Excel die prowler-fullorgresults-accessdeniedfilteredDatei .txt. Es wird empfohlen, diese Datei zu verwenden, da die häufigsten Fehler, die nicht behoben werden können, bereits behoben wurden, z. B. `Access Denied` Fehler im Zusammenhang mit versuchten Scans von Ressourcen. AWS Control Tower Wenn Sie die ungefilterten Ergebnisse erhalten möchten, öffnen Sie stattdessen die Datei prowler-fullorgresults.txt. 5. Wählen Sie Spalte A aus. 6. Wenn Sie Windows verwenden, geben Sie Strg+C ein, oder wenn Sie macOS verwenden, geben Sie Cmd+C ein. Dadurch werden alle Daten in die Zwischenablage kopiert. 7. Wählen Sie in der Excel-Berichtsvorlage im CSV-Arbeitsblatt Prowler die Zelle A1 aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Wenn Sie Windows verwenden, geben Sie Strg+V ein, oder wenn Sie macOS verwenden, geben Sie Cmd+V ein. Dadurch werden die Ergebnisse in den Bericht eingefügt. 9. Vergewissern Sie sich, dass alle Zellen mit eingefügt en Daten ausgewählt sind. Wenn nicht, wählen Sie Spalte A aus. 10. Wählen Sie auf der Registerkarte Daten die Option Text in Spalten aus. 11. Gehen Sie im Assistenten wie folgt vor: • Wählen Sie für Schritt 1 die Option Delimited aus. • Wählen Sie für Schritt 2 für Trennzeichen die Option Semikolon aus. Vergewissern Sie sich im Bereich Datenvorschau, dass die Daten in Spalten aufgeteilt sind. • Wählen Sie für Schritt 3 die Option Fertig stellen aus. 12. Vergewissern Sie sich, dass die Textdaten über mehrere Spalten getrennt sind.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	13. Speichern Sie den Excel-Bericht unter einem neuen Namen. 14. Suchen und löschen Sie alle `Access Denied` Fehler in den Ergebnissen. Anweisungen zum programmgesteuerten Entfernen von Fehlern finden Sie unter Programmgesteuertes Entfernen von Fehlern im Abschnitt Zusätzliche Informationen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Finalisieren Sie den Bericht.	1. Wählen Sie das Arbeitsblatt Ergebnisse und dann Zelle A17 aus. Diese Zelle ist die Überschrift der Pivot-Tab elle. 2. Wählen Sie in der Multifunk tionsleiste unter PivotTable Tools die Option Analysier en und anschließend unter Aktualisieren die Option Alle aktualisieren aus. Dadurch werden die Pivot-Tabellen mit dem neuen Datensatz aktualisiert. 3. Standardmäßig zeigt Excel AWS-Konto Zahlen nicht richtig an. Gehen Sie wie folgt vor, um die Zahlenfor matierung zu korrigieren: • Öffnen Sie auf dem Arbeitsblatt Ergebnisse das Kontextmenü (mit der rechten Maustaste) für Spalte A, und wählen Sie dann Zellen formatieren aus. • Wählen Sie Zahl und geben Sie im Feld Dezimalstellen den Wert ein`0`. • Wählen Sie OK aus. Hinweis: Wenn eine AWS-Konto Zahl mit einer oder	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	mehreren Nullen beginnt, entfernt Excel die Nullen automatisch. Wenn Sie im Bericht eine Kontonummer mit weniger als 12 Ziffern sehen, sind die fehlenden Ziffern Nullen am Anfang der Zahl. 4. (Optional) Sie können Felder reduzieren, um die Ergebnisse leichter lesbar zu machen. Gehen Sie wie folgt vor: • Wenn Sie auf dem Arbeitsblatt Ergebnisse den Cursor auf die Zeile zwischen den Zeilen 18 und 19 bewegen (den Raum zwischen der kritischen Überschrift und dem ersten Ergebnis), ändert sich das Cursorsymbol in einen kleinen Pfeil, der nach unten zeigt. • Klicken Sie hier, um alle Suchfelder auszuwählen. • Öffnen Sie das Kontextmenü (Rechtsklick), suchen Sie nach Erweiteren/Reduzieren und wählen Sie dann Reduzieren.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Einzelheiten zur Bewertung finden Sie in den Arbeitsbl ättern „Ergebnisse“, „Schweregrad“ und „Nicht bestanden“.	

(Optional) Aktualisieren Sie Prowler oder die Ressourcen im Code-Repository

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Aktualisiere Prowler.	Wenn Sie Prowler auf die neueste Version aktualisieren möchten, gehen Sie wie folgt vor:
	1. Stellen Sie mithilfe von Session Manager eine Connect zur EC2 Instanz für Prowler her. Anweisung en finden Sie unter Connect zu Ihrer Linux-Instance mithilfe von Session Manager.
	2. Geben Sie den folgenden Befehl ein.
	`sudo -i`
	`pip3 install --upgrade prowler`
		Allgemeines AWS

Aktualisieren Sie das Skript prowler_scan.sh.	Wenn Sie das Skript prowler_s can.sh auf die neueste Version im Repository aktualisi eren möchten, gehen Sie wie folgt vor:	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	1. Stellen Sie mithilfe von Session Manager eine Connect zur EC2 Instanz für Prowler her. Anweisung en finden Sie unter Connect zu Ihrer Linux-Instance mithilfe von Session Manager.
	2. Geben Sie den folgenden Befehl ein.
	`sudo -i`
	3. Navigieren Sie zum Prowler-Skriptverzeichnis.
	`cd /usr/local/prowler`
	4. Geben Sie den folgenden Befehl ein, um das lokale Skript zu speichern, sodass Sie benutzerd efinierte Änderungen in der neuesten Version zusammenführen können.
	`git stash`
	5. Geben Sie den folgenden Befehl ein, um die neueste Version des Skripts abzurufen.
	`git pull`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	6. Geben Sie den folgenden Befehl ein, um das benutzerdefinierte Skript mit der neuesten Version des Skripts zusammenzuführen. `git stash pop` **Note** Möglicherweise erhalten Sie Warnungen im Zusammenhang mit lokal generierten Dateien, die sich nicht im GitHub Repository befinden, z. B. beim Suchen nach Berichten. Sie können diese ignorieren, solange in der Datei prowler_scan.sh angezeigt wird, dass die lokal gespeicherten Änderungen wieder zusammengeführt wurden.	

(Optional) Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Löschen Sie alle bereitgestellten Ressourcen.	Sie können die bereitgestellten Ressourcen in den Konten belassen. Wenn Sie die EC2 Instance herunterfahren, wenn sie nicht verwendet wird, und den S3-Bucket leer lassen, reduziert dies die Kosten für die Wartung der Ressourcen für future Scans. Wenn Sie die Bereitstellung aller Ressourcen aufheben möchten, gehen Sie wie folgt vor: 1. Löschen Sie den `IAM-ProwlerExecRole` Stack, der im Verwaltungskonto bereitgestellt wurde. Anweisungen finden Sie in der CloudFormation Dokumentation unter Löschen eines Stacks. 2. Löschen Sie das `IAM-ProwlerExecRole` Stack-Set, das im Verwaltungskonto der Organisation oder im delegierten Administratorkonto bereitgestellt wurde. Anweisungen finden Sie in der Dokumentation	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	unter Löschen eines Stack-Sets. CloudFormation 3. Löschen Sie alle Objekte im `prowler-output` S3-Bucket. Anweisungen finden Sie in der Amazon S3 S3-Dokumentation unter Objekte löschen. 4. Löschen Sie den `Prowler-Resources` Stack, der im Sicherheitskonto bereitgestellt wurde. Anweisungen finden Sie in der CloudFormation Dokumentation unter Löschen eines Stacks.	

Fehlerbehebung

Problem	Lösung
Es konnte keine Verbindung mit der EC2 Instance mithilfe von Session Manager hergestellt werden.	Der SSM-Agent muss in der Lage sein, mit dem Systems Manager Manager-Endpunkt zu kommunizieren. Gehen Sie wie folgt vor: 1. Stellen Sie sicher, dass das Subnetz, in dem die EC2 Instanz bereitgestellt wird, über Internetzugang verfügt. 2. Starten Sie die EC2 Instanz neu.
Bei der Bereitstellung des Stack-Sets werden Sie von der CloudFormation Konsole dazu aufgefordert. `Enable trusted access`	Dies weist darauf hin, dass der vertrauenswürdige Zugriff zwischen AWS Organizations und CloudFormation nicht aktiviert wurde. Für die Bereitstellung des vom Service verwaltet

Problem	Lösung
`with AWS Organizations to use service-managed permissions`	en Stack-Sets ist ein vertrauenswürdiger Zugriff erforderlich. Wählen Sie die Schaltfläche, um den vertrauenswürdigen Zugriff zu aktivieren. Weitere Informationen finden Sie in der CloudFormation Dokumentation unter Vertrauenswürdigen Zugriff aktivieren.

Zugehörige Ressourcen

AWS Dokumentation

- Implementierung von Sicherheitskontrollen am AWS (AWS Präskriptive Leitlinien)

Sonstige Ressourcen

- Prowler () GitHub

Zusätzliche Informationen

Programmgesteuertes Entfernen von Fehlern

Wenn die Ergebnisse `Access Denied` Fehler enthalten, sollten Sie diese aus den Ergebnissen entfernen. Diese Fehler sind in der Regel auf externe Einflussberechtigungen zurückzuführen, die Prowler daran hindern, eine bestimmte Ressource zu bewerten. Beispielsweise schlagen einige Prüfungen fehl, wenn S3-Buckets überprüft werden, die über bereitgestellt wurden. AWS Control Tower Sie können diese Ergebnisse programmgesteuert extrahieren und die gefilterten Ergebnisse als neue Datei speichern.

Mit den folgenden Befehlen werden Zeilen entfernt, die eine einzelne Textzeichenfolge (ein Muster) enthalten, und die Ergebnisse werden dann in einer neuen Datei ausgegeben.

- Für Linux oder macOS (Grep)

```
grep -v -i "Access Denied getting bucket" myoutput.csv > myoutput_modified.csv
```

- Für Windows () PowerShell

```
Select-String -Path myoutput.csv -Pattern 'Access Denied getting bucket' -NotMatch >
 myoutput_modified.csv
```

Mit den folgenden Befehlen werden Zeilen entfernt, die mehr als einer Textzeichenfolge entsprechen, und die Ergebnisse werden dann in einer neuen Datei ausgegeben.

- Für Linux oder macOS (verwendet eine Escape-Pipe zwischen Zeichenketten)

```
grep -v -i 'Access Denied getting bucket\|Access Denied Trying to Get' myoutput.csv >
 myoutput_modified.csv
```

- Für Windows (verwendet ein Komma zwischen Zeichenketten)

```
Select-String -Path myoutput.csv -Pattern 'Access Denied getting bucket', 'Access
 Denied Trying to Get' -NotMatch > myoutput_modified.csv
```

Beispiele melden

Die folgende Abbildung zeigt ein Beispiel für das Arbeitsblatt „Ergebnisse“ im Bericht über die konsolidierten Ergebnisse von Prowler.

Die folgende Abbildung zeigt ein Beispiel für das Arbeitsblatt „Pass Fail“ im Bericht über die konsolidierten Ergebnisse von Prowler. (Standardmäßig werden erfolgreiche Ergebnisse von der Ausgabe ausgeschlossen.)

Die folgende Abbildung zeigt ein Beispiel für das Arbeitsblatt „Schweregrad“ im Bericht über die konsolidierten Ergebnisse von Prowler.

Löschen Sie ungenutzte Amazon EBS-Volumes mit AWS Config und AWS Systems Manager

Erstellt von Sankar Sangubotla (AWS)

Übersicht

Der Lebenszyklus eines Amazon Elastic Block Store (Amazon EBS) -Volumes ist in der Regel unabhängig vom Lebenszyklus der Amazon Elastic Compute Cloud (Amazon EC2) -Instance, an die es angehängt ist. Sofern Sie beim Start nicht die Option Bei Kündigung löschen ausgewählt haben, wird beim Beenden der EC2 Amazon-Instance das Amazon EBS-Volume zwar getrennt, aber nicht gelöscht. Insbesondere in Entwicklungs- und Testumgebungen, in denen es üblich ist, EC2 Amazon-Instances zu starten und zu beenden, kann dies zu einer großen Anzahl ungenutzter Amazon EBS-Volumes führen. Bei Amazon EBS-Volumes fallen Gebühren in Ihrem an AWS-Konto, unabhängig davon, ob sie verwendet werden. Das Löschen dieser Volumes kann Ihnen helfen, die Kosten für Ihre zu optimieren. AWS-Konten Darüber hinaus ist das Löschen ungenutzter Amazon EBS-Volumes eine bewährte Sicherheitsmethode, um den Zugriff auf ungenutzte, potenziell sensible Daten in diesen Volumes zu verhindern.

AWS Config kann Ihnen helfen, Ressourcen, die nicht den Vorschriften entsprechen, manuell oder automatisch zu beheben. Dieses Muster beschreibt, wie eine AWS Config Regel und eine automatische Korrekturmaßnahme konfiguriert werden, mit der ungenutzte Amazon EBS-Volumes im Konto gelöscht werden. Bei der Behebungsaktion handelt es sich um ein vordefiniertes Runbook für Automation, eine Funktion von. AWS Systems Manager Sie können das Runbook so konfigurieren, dass vor dem Löschen ein Snapshot des Volumes erstellt wird.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto.
- AWS Identity and Access Management (IAM) -Berechtigungen zum Ausführen des `AWSConfigRemediation-DeleteUnusedEBSVolume` Runbooks for Automation, einer Funktion von Systems Manager. Weitere Informationen finden Sie unter Erforderliche IAM-Berechtigungen in. AWSConfigRemediation-DeleteUnusedEBSVolume
- Ein oder mehrere ungenutzte Amazon EBS-Volumes.

Einschränkungen

- Die ungenutzten Amazon EBS-Volumes müssen sich im `available` Bundesstaat befinden.

Architektur

Zielarchitektur

1. Die AWS Config Regel bewertet die Amazon EBS-Volumes.
2. Die Regel gibt eine Liste mit konformen und nicht konformen Ressourcen zurück. Amazon EBS-Volumes im `available` Bundesstaat, bei denen es sich um ungenutzte Volumes handelt, gelten als nicht konform.
3. AWS Config startet automatisch das Automation-Runbook.
4. Falls konfiguriert, erstellt Systems Manager Snapshots der ungenutzten Volumes, bevor sie gelöscht werden.
5. Systems Manager löscht die ungenutzten Amazon EBS-Volumes.

Automatisierung und Skalierung

Sie können diese Lösung auf alle Konten in Ihrem Unternehmen anwenden. Weitere Informationen finden Sie in der AWS Config Dokumentation unter Regeln für alle Konten in Ihrer Organisation verwalten.

Tools

- AWS Configbietet einen detaillierten Überblick über die Ressourcen in Ihrem Unternehmen AWS-Konto und deren Konfiguration. Es hilft Ihnen zu erkennen, wie Ressourcen miteinander zusammenhängen und wie sich ihre Konfigurationen im Laufe der Zeit geändert haben.
- AWS Systems Managerhilft Ihnen bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der ausgeführt AWS Cloud werden. Es vereinfacht das Anwendungs- und Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme und hilft Ihnen, Ihre AWS Ressourcen sicher und in großem Umfang zu verwalten.
- AWS Systems Manager Die Automatisierung vereinfacht häufig auftretende Wartungs-, Bereitstellungs- und Problembehebungsaufgaben für viele. AWS-Services

Epen

Konfigurieren Sie die Regel AWS Config

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Rolle für das Automation-Runbook.	Erstellen Sie eine Rolle namens `AssumeRole` . Systems Manager Automation verwendet diese Rolle, um das Runbook auszuführen. Anweisungen finden Sie in der Systems Manager Manager-Dokumentation unter Konfiguration eines Zugriffs auf eine Servicerolle (Rolle übernehmen) für Automatisierungen.	AWS-Systemadministrator
Schalten Sie den AWS Config Rekorder ein.	Folgen Sie den Anweisungen unter Einrichtung AWS Config mit der Konsole in der AWS Config Dokumentation, um sicherzustellen, dass diese AWS Config läuft und für die Aufzeichnung von Amazon EBS-Volumes konfiguriert ist.	AWS-Systemadministrator
Führen Sie die Regel aus.	1. Folgen Sie den Anweisungen in der AWS Config Dokumentation unter Evaluieren Ihrer Ressourcen, um die `ec2-volume-inuse-check` Regel auszuführen. Warten Sie, bis die Evaluierung abgeschlossen ist.	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Wählen Sie auf der Seite Regeln die `ec2-volume-inuse-check` Regel aus, und wählen Sie dann für Ressourcen im Geltungsbereich die Option Nicht konform aus. 3. Vergewissern Sie sich, dass die Evaluierungsergebnisse ein oder mehrere ungenutzte Amazon EBS-Volumes enthalten.	

Automatische Behebung ungenutzter Amazon EBS-Volumes konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie die automatische Abhilfemaßnahme hinzu.	1. Wählen Sie auf der Seite Regeln die `ec2-volume-inuse-check` Regel aus. 2. Folgen Sie den Anweisungen in der AWS Config Dokumentation unter Automatische Problembehebung einrichten. Beachten Sie Folgendes: 3. Wählen Sie im Abschnitt Details zur Behebungsaktion die Option. `AWSConfigRemediation-DeleteUnusedEBSVolume`	AWS-Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	• Wählen Sie den Parameter Ressource n-ID aus, und wählen VolumeIdSie dann in der Liste die Option. Zur Laufzeit wird dieser Parameter durch die ID des nicht konformen Amazon EBS-Volumes ersetzt.
	• Geben Sie im Abschnitt Parameter Werte für die folgenden Parameter an:
	  • `CreateSnapshot` — (Optional) Wenn auf gesetzt`true`, erstellt die Automatisierung einen Snapshot des Amazon EBS-Volumes, bevor es gelöscht wird.
	  • `AutomationAssumeRole` — Geben Sie den Amazon-Ressourcennamen (ARN) der `AssumeRole` Servicerolle ein, die Sie zuvor erstellt haben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die automatische Problembehebung für die AWS Config Regel.	1. Wählen Sie in der AWS Config Konsole auf der Seite Regeln die `ec2-volume-inuse-check` Regel aus. 2. Wählen Sie im Menü Aktionen die Option Erneut auswerten aus. 3. Erlauben Sie der Regel, die nicht konformen Ressourcen zu bewerten, und bestätigen Sie dann, dass die ungenutzten Amazon EBS-Volumes gelöscht wurden.	AWS-Systemadministrator

Fehlerbehebung

Problem	Lösung
AWS Config spiegelt den Zustand der Ressource nicht genau wider.	Manchmal aktualisiert es den Status der Ressourcen AWS Config nicht. Schalten Sie den Rekorder auf der AWS Config Einstellungsseite aus und dann wieder ein. Der Rekorder erfasst den Status der Ressourcen. Bei neu erstellten oder gelöschten Ressourcen kann es einige Zeit dauern, bis der Rekorder den aktuellen Status wiedergibt. Weitere Informationen zu Amazon EBS-Volumenstatus finden Sie unter Volumenstatus in der Amazon EBS-Dokumentation.

Zugehörige Ressourcen

- AWSConfigRemediation-DeleteUnusedEBSVolume Runbook
- ec2-Regel volume-inuse-check
- Behebung von Ressourcen, die nicht den Vorschriften entsprechen, mithilfe AWS von Regeln AWS Config

Implementieren und verwalten Sie AWS Control Tower Kontrollen mithilfe von AWS CDK und CloudFormation

Erstellt von Iker Reina Fuente (AWS) und Ivan Girardi (AWS)

Übersicht

Dieses Muster beschreibt, wie präventive, detektive AWS CloudFormation und AWS Cloud Development Kit (AWS CDK) proaktive AWS Control Tower Kontrollen als Infrastructure as Code (IaC) verwendet, implementiert und verwaltet werden. Eine Kontrolle (auch als Leitplanke bezeichnet) ist eine Regel auf hoher Ebene, die eine kontinuierliche Steuerung Ihrer gesamten Umgebung gewährleistet. AWS Control Tower Sie können beispielsweise Kontrollen verwenden, um eine Protokollierung für Ihr System vorzuschreiben AWS-Konten und dann automatische Benachrichtigungen zu konfigurieren, wenn bestimmte sicherheitsrelevante Ereignisse eintreten.

AWS Control Tower unterstützt Sie bei der Implementierung präventiver, detektiver und proaktiver Kontrollen, mit denen Sie Ihre AWS Ressourcen steuern und die Einhaltung der Vorschriften in mehreren Bereichen überwachen können. AWS-Konten Jede Kontrolle erzwingt eine einzige Regel. In diesem Muster verwenden Sie eine bereitgestellte IaC-Vorlage, um anzugeben, welche Steuerelemente Sie in Ihrer Umgebung bereitstellen möchten.

AWS Control Tower Kontrollen gelten für eine gesamte Organisationseinheit (OU), und die Steuerung wirkt sich auf alle AWS-Konto innerhalb der Organisationseinheit aus. Wenn Benutzer eine Aktion in einem Konto in Ihrer landing zone ausführen, unterliegt diese Aktion daher den Kontrollen, die für die Organisationseinheit gelten.

Die Implementierung von AWS Control Tower Kontrollen trägt dazu bei, eine solide Sicherheitsgrundlage für Ihre AWS landing zone zu schaffen. Indem Sie dieses Muster verwenden, um die Steuerungen als IaC über CloudFormation und bereitzustellen AWS CDK, können Sie die Steuerungen in Ihrer landing zone standardisieren und sie effizienter einsetzen und verwalten. Diese Lösung verwendet cdk_nag, um die Anwendung während der Bereitstellung zu scannen. AWS CDK Dieses Tool überprüft, ob die Anwendung den bewährten Methoden entspricht. AWS

Um AWS Control Tower Steuerelemente als IaC bereitzustellen, können Sie stattdessen auch HashiCorp Terraform verwenden. AWS CDK Weitere Informationen finden Sie unter Bereitstellen und Verwalten von AWS Control Tower Steuerelementen mithilfe von Terraform.

Beabsichtigte Zielgruppe

Dieses Muster wird Benutzern empfohlen, die Erfahrung mit AWS Control Tower, CloudFormation AWS CDK, und haben AWS Organizations.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Aktiv AWS-Konten geführt als Organisation in AWS Organizations und als AWS Control Tower landing zone. Anweisungen finden Sie in der AWS Control Tower Dokumentation unter Erste Schritte.
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert.
- Node Package Manager (npm), installiert und konfiguriert für. AWS CDK
- Voraussetzungen für AWS CDK.
- Berechtigungen zur Übernahme einer vorhandenen AWS Identity and Access Management (IAM-) Rolle in einem Bereitstellungskonto.
- Berechtigungen zur Übernahme einer IAM-Rolle im Verwaltungskonto der Organisation, die für das Bootstrap verwendet werden kann. AWS CDK Die Rolle muss über Berechtigungen zum Ändern und Bereitstellen CloudFormation von Ressourcen verfügen. Weitere Informationen finden Sie in der Dokumentation unter Bootstrapping. AWS CDK
- Berechtigungen zum Erstellen von IAM-Rollen und -Richtlinien im Verwaltungskonto der Organisation. Weitere Informationen finden Sie in der IAM-Dokumentation unter Erforderliche Berechtigungen für den Zugriff auf IAM-Ressourcen.

Einschränkungen

- Dieses Muster enthält Anweisungen für die Bereitstellung dieser Lösung in AWS-Konten einem Bereitstellungskonto bis hin zum Verwaltungskonto der Organisation. Zu Testzwecken können Sie diese Lösung direkt im Verwaltungskonto bereitstellen, Anweisungen für diese Konfiguration werden jedoch nicht explizit bereitgestellt.
- Für AWS Control Tower Steuerelemente erfordert dieses Muster die Verwendung globaler Bezeichner im folgenden Format:

```
arn:<PARTITION>:controlcatalog:::control/<CONTROL_CATALOG_OPAQUE_ID>
```

  In früheren Versionen dieses Musters wurden regionale Identifikatoren verwendet, die nicht mehr unterstützt werden. Wir empfehlen, dass Sie von regionalen Kennungen zu globalen Kennungen

migrieren. Globale Kennungen helfen Ihnen dabei, Kontrollen zu verwalten und die Anzahl der Kontrollen, die Sie verwenden können, zu erweitern.

> **Note**
>
> In den meisten Fällen `<PARTITION>` ist `aws` der Wert für.

Versionen der Produkte

- AWS Control Tower Version 3.2 oder höher
- Python-Version 3.9 oder höher
- npm Version 8.9.0 oder höher

Architektur

Dieser Abschnitt bietet einen allgemeinen Überblick über diese Lösung und die Architektur, die durch den Beispielcode festgelegt wurde. Das folgende Diagramm zeigt die Steuerelemente, die für die verschiedenen Konten in der Organisationseinheit eingesetzt werden.

AWS Control Tower Die Kontrollen werden nach ihrem Verhalten und ihren Leitlinien kategorisiert.

Es gibt drei Haupttypen von Kontrollverhalten:

1. Präventive Kontrollen sollen verhindern, dass Maßnahmen ergriffen werden. Diese werden mithilfe von Dienststeuerungsrichtlinien (SCPs) oder Ressourcenkontrollrichtlinien (RCPs) implementiert AWS Organizations. Der Status einer präventiven Kontrolle ist entweder erzwungen oder nicht aktiviert. Präventive Kontrollen werden in allen AWS-Regionen Bereichen unterstützt.
2. Detective Controls sind so konzipiert, dass sie bestimmte Ereignisse erkennen, wenn sie auftreten, und die Aktion protokollieren AWS CloudTrail. Diese werden mit AWS Config Regeln implementiert. Der Status einer detektiven Kontrolle ist entweder „Ungültig“, „Verstoß“ oder „Nicht aktiviert“. Detective Controls gelten nur für diejenigen, die von AWS-Regionen unterstützt werden AWS Control Tower.
3. Proaktive Kontrollen scannen Ressourcen, die von bereitgestellt werden würden, AWS CloudFormation und prüfen, ob sie den Richtlinien und Zielen Ihres Unternehmens entsprechen. Ressourcen, die nicht den Vorschriften entsprechen, werden nicht bereitgestellt. Diese werden mit

AWS CloudFormation Hooks implementiert. Der Status einer proaktiven Kontrolle ist PASS, FAIL oder SKIP.

Die Anleitung zur Kontrolle bezieht sich auf die empfohlene Vorgehensweise zur Anwendung der einzelnen Kontrollen auf Sie OUs. AWS Control Tower bietet drei Kategorien von Leitlinien: verpflichtend, dringend empfohlen und fakultativ. Die Leitlinien einer Kontrolle sind unabhängig von ihrem Verhalten. Weitere Informationen finden Sie unter Verhalten und Steuerung der Steuerung.

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK)ist ein Softwareentwicklungs-Framework, das Sie dabei unterstützt, AWS Cloud Infrastruktur im Code zu definieren und bereitzustellen. Das AWS CDK Toolkit ist das wichtigste Tool für die Interaktion mit Ihrer AWS CDK App.
- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und AWS-Regionen zu verwalten.
- AWS Configbietet einen detaillierten Überblick über die Ressourcen in Ihrem System AWS-Konto und darüber, wie sie konfiguriert sind. Es hilft Ihnen zu erkennen, wie Ressourcen miteinander zusammenhängen und wie sich ihre Konfigurationen im Laufe der Zeit geändert haben.
- AWS Control Towerhilft Ihnen bei der Einrichtung und Verwaltung einer Umgebung AWS mit mehreren Konten und folgt dabei den vorgeschriebenen Best Practices.
- AWS Organizationsist ein Kontoverwaltungsservice, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie erstellen und zentral verwalten.

Andere Tools

- cdk_nag ist ein Open-Source-Tool, das eine Kombination von Regelpaketen verwendet, um AWS CDK Anwendungen auf Einhaltung von Best Practices zu überprüfen.
- npm ist eine Softwareregistrierung, die in einer Node.js -Umgebung ausgeführt wird und verwendet wird, um Pakete gemeinsam zu nutzen oder auszuleihen und die Bereitstellung von privaten Paketen zu verwalten.
- Python ist eine Allzweck-Computerprogrammiersprache.

Code-Repository

Der Code für dieses Muster ist im AWS CDK Repository GitHub Deploy AWS Control Tower controls using verfügbar. Sie verwenden die Datei cdk.json, um mit der AWS CDK App zu interagieren, und Sie verwenden die Datei package.json, um die npm-Pakete zu installieren.

Bewährte Methoden

- Folgen Sie dem Prinzip der geringsten Rechte (IAM-Dokumentation). Die in diesem Muster enthaltenen Beispiele für die IAM-Richtlinie und die Vertrauensrichtlinie enthalten die erforderlichen Mindestberechtigungen, und die im Verwaltungskonto erstellten AWS CDK Stacks sind durch diese Berechtigungen eingeschränkt.
- Folgen Sie den Best Practices für AWS Control Tower Administratoren (AWS Control Tower Dokumentation).
- Folgen Sie den Best Practices für die Entwicklung und Bereitstellung der Cloud-Infrastruktur mit der AWS CDK (AWS CDK Dokumentation).
- Passen Sie beim Bootstrapping die Bootstrap-Vorlage an AWS CDK, um Richtlinien und vertrauenswürdige Konten zu definieren, die Lese- und Schreibzugriff auf alle Ressourcen im Verwaltungskonto haben sollen. Weitere Informationen finden Sie unter Bootstrapping anpassen.
- Verwenden Sie Tools zur Codeanalyse wie cfn_nag, um die generierten Vorlagen zu scannen. CloudFormation Das Tool cfn-nag sucht in CloudFormation Vorlagen nach Mustern, die darauf hinweisen könnten, dass die Infrastruktur nicht sicher ist. Sie können auch cdk-nag verwenden, um Ihre CloudFormation Vorlagen mithilfe des Cloudformation-include-Moduls zu überprüfen.

Epen

Bereite dich darauf vor, die Steuerungen zu aktivieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Rolle im Verwaltungskonto.	1. Erstellen Sie eine IAM-Richtlinie im Verwaltungskonto mit den in der IAM-Richtlinie im Abschnitt Zusätzliche Informationen definierten Berechtigungen. Anweisungen finden Sie in der IAM-Dokumentation unter	DevOps Ingenieur, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Erstellen von IAM-Richtlinien. Notieren Sie sich den Amazon-Ressourcennamen (ARN) der Richtlinie. Das Folgende ist ein Beispiel für einen ARN.
	
	`arn:aws:iam::<MANAGEMENT-ACCOUNT-ID>:policy/<POLICY-NAME>`
	
	2. Erstellen Sie eine IAM-Rolle im Verwaltungskonto, fügen Sie die IAM-Berechtigungsrichtlinie an, die Sie im vorherigen Schritt erstellt haben, und fügen Sie die benutzerdefinierte Vertrauensrichtlinie unter Vertrauensrichtlinie im Abschnitt Zusätzliche Informationen an. Anweisungen finden Sie in der IAM-Dokumentation unter Erstellen einer Rolle mithilfe benutzerdefinierter Vertrauensrichtlinien. Im Folgenden finden Sie ein Beispiel für einen ARN für die neue Rolle.
	
	`arn:aws:iam::<MANAGEMENT-ACCOUNT-ID>:role/<ROLE-NAME>`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bootstrap. AWS CDK	1. Nehmen Sie im Verwaltungskonto eine Rolle an, die über AWS CDK Bootstrap-Berechtigungen verfügt. 2. Geben Sie den folgenden Befehl ein und ersetzen Sie den folgenden: • `<MANAGEMENT-ACCOUNT-ID>` ist die ID des Verwaltungskontos der Organisation. • `<AWS-CONTROL-TOWER-REGION>` ist der AWS-Region Ort, an dem AWS Control Tower es eingesetzt wird. Eine vollständige Liste der Regionscodes finden Sie unter Regionale Endpunkte in der AWS allgemeinen Referenz. • `<DEPLOYMENT-ACCOUNT-ID>` ist die ID des Bereitstellungskontos. • `<DEPLOYMENT-ROLE-NAME>` ist der Name der IAM-Rolle, die Sie für das Bereitstellungskonto verwenden. • `<POLICY-NAME>` ist der Name der Richtlinie, die Sie im Verwaltungskonto erstellt haben.	DevOps Ingenieur, General AWS, Python

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`$ npx cdk bootstrap aws://<MANAGEMENT-ACCOUNT-ID>/<AWS-CONTROL-TOWER-REGION> \ --trust arn:aws:iam::<DEPLOYMENT-ACCOUNT-ID>:role/<DEPLOYMENT-ROLE-NAME> \ --cloudformation-execution-policies arn:aws:iam::<MANAGEMENT-ACCOUNT-ID>:policy/<POLICY-NAME>`	
Klonen Sie das Repository	Geben Sie in einer Bash-Shell den folgenden Befehl ein. Dadurch werden die AWS Control Tower Deploy-Steuerelemente mithilfe des AWS CDK Repositorys von geklont. GitHub `git clone https://github.com/aws-samples/aws-control-tower-controls-cdk.git`	DevOps Ingenieur, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bearbeiten Sie die AWS CDK Konfigurationsdatei.	1. Öffnen Sie im geklonten Repository die Datei constants.py. 2. Geben Sie im `ACCOUNT_ID` Parameter die ID Ihres Verwaltungskontos ein. 3. Geben Sie im `<AWS-CONTROL-TOWER-REGION>` Parameter den Ort ein, AWS-Region an dem das AWS Control Tower Gerät bereitgestellt wird. 4. Geben Sie im `ROLE_ARN` Parameter den ARN der Rolle ein, die Sie im Verwaltungskonto erstellt haben. 5. Öffnen Sie Alle globalen Identifikatoren in der AWS Control Tower Dokumentation. 6. Suchen Sie in der Liste im JSON-Format das Steuerelement, das Sie implementieren möchten, und kopieren Sie dann seinen globalen Bezeichner (auch bekannt als der Wert {CONTROL_CATALOG_OPAQUE_ID}). Der globale Bezeichner für das AWS-GR_AUDIT_BUCKET_ENCRYPTION_ENABL	DevOps Ingenieur, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ED-Steuerelement lautet beispielsweise. `k4izcjxhukijhajp6ks5mjxk` 7. Geben Sie im `GUARDRAILS_CONFIGURATION` Abschnitt im Parameter den globalen Bezeichner ein, den Sie kopiert haben. `Enable-Control` Geben Sie den Bezeichner in doppelte Anführungszeichen ein und trennen Sie mehrere Bezeichner durch Kommas. 8. Geben Sie in dem `GUARDRAILS_CONFIGURATION` Abschnitt im `OrganizationalUnitIds` Parameter die ID der Organisationseinheit ein, für die Sie das Steuerelement aktivieren möchten, z. B. `ou-1111-11111111` Geben Sie die ID in doppelte Anführungszeichen ein und trennen Sie mehrere IDs durch Kommas. Weitere Informationen zum Abrufen der Organisationseinheit IDs finden Sie unter Die Details einer Organisationseinheit anzeigen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	9. Speichern und schließen Sie die Datei constants .py. Ein Beispiel für eine aktualisierte Datei constants .py finden Sie im Abschnitt Zusätzliche Informationen dieses Musters.	

Aktivieren Sie die Kontrollen im Verwaltungskonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Nehmen Sie die IAM-Rolle im Bereitstellungskonto an.	Nehmen Sie im Bereitste llungskonto die IAM-Rolle an, die über die Berechtig ungen zum Bereitstellen der AWS CDK Stacks im Verwaltungskonto verfügt. Weitere Informationen zur Übernahme einer IAM-Rolle in der AWS CLI finden Sie unter Verwenden einer IAM-Rolle in der. AWS CLI	DevOps Ingenieur, General AWS
Aktivieren Sie die Umgebung.	Wenn Sie Linux oder macOS verwenden: 1. Geben Sie den folgenden Befehl ein, um eine virtuelle Umgebung zu erstellen. `$ python3 -m venv .venv` 2. Nachdem die virtuelle Umgebung erstellt wurde,	DevOps Ingenieur, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	geben Sie den folgenden Befehl ein, um sie zu aktivieren.
	`$ source .venv/bin/activate`
	Wenn Sie Windows verwenden:
	1. Geben Sie den folgenden Befehl ein, um eine virtuelle Umgebung zu aktivieren.
	`% .venv\Scripts\activate.bat`	

Installieren Sie die Abhängigkeiten.	Geben Sie nach der Aktivierung der virtuellen Umgebung den folgenden Befehl ein, um das Skript install_deps.sh auszuführen. Dieses Skript installiert die erforderlichen Abhängigkeiten. `$ ./scripts/install_deps.sh`	DevOps Ingenieur, General AWS, Python

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie den Stack bereit.	Geben Sie die folgenden Befehle ein, um den CloudFormation Stack zu synthetisieren und bereitzustellen.
	`$ npx cdk synth`
	`$ npx cdk deploy`
		DevOps Ingenieur, General AWS, Python

Zugehörige Ressourcen

AWS Dokumentation

- Über Kontrollen (AWS Control Tower Dokumentation)
- Bibliothek für Steuerungen (AWS Control Tower Dokumentation)
- AWS CDK Toolkit-Befehle (AWS CDK Dokumentation)
- Implementieren und verwalten Sie AWS Control Tower Kontrollen mithilfe von Terraform (Prescriptive Guidance)AWS

Sonstige Ressourcen

- Python

Zusätzliche Informationen

Beispiel für eine Datei constants.py

Im Folgenden finden Sie ein Beispiel für eine aktualisierte Datei constants.py. Dieses Beispiel aktiviert das AWS-GR_DISALLOW_CROSS_REGION_NETWORKING-Steuerelement (globale ID:) und das AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED-Steuerelement (globale ID:**`dvuaav61i5cnfazfelmvn9m6k`**). `50z1ot237wl8u1lv5ufau6qqo` Eine Liste der globalen Bezeichner finden IDs Sie in AWS Control Tower der Dokumentation unter Alle globalen Bezeichner.

```
ACCOUNT_ID = 111122223333
```

```
AWS_CONTROL_TOWER_REGION = us-east-2
ROLE_ARN = "arn:aws:iam::111122223333:role/CT-Controls-Role"
GUARDRAILS_CONFIGURATION = [
    {
        "Enable-Control": {
            "dvuaav61i5cnfazfelmvn9m6k": {  # AWS-GR_DISALLOW_CROSS_REGION_NETWORKING
                "Parameters": {
                    "ExemptedPrincipalArns": ["arn:aws:iam::111122223333:role/
RoleName"]
                },
                "Tags": [{"key": "Environment", "value": "Production"}]
            },
            ...
        },
        "OrganizationalUnitIds": ["ou-1111-11111111", "ou-2222-22222222"...],
    },
    {
        "Enable-Control": {
            "50z1ot237wl8u1lv5ufau6qqo",  # AWS-
GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED
            ...
        },
        "OrganizationalUnitIds": ["ou-2222-22222222"...],
    },
]
```

IAM-Richtlinie

Die folgende Beispielrichtlinie ermöglicht die Mindestaktionen, die erforderlich sind, um AWS Control Tower Kontrollen zu aktivieren oder zu deaktivieren, wenn AWS CDK Stacks von einem Bereitstellungskonto auf das Verwaltungskonto verteilt werden.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "controltower:EnableControl",
                "controltower:DisableControl",
                "controltower:GetControlOperation",
                "controltower:ListEnabledControls",
                "organizations:AttachPolicy",
```

```
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DetachPolicy",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
                "organizations:UpdatePolicy",
                "ssm:GetParameters"
            ],
            "Resource": "*"
        }
    ]
}
```

Vertrauensrichtlinie

Mit der folgenden benutzerdefinierten Vertrauensrichtlinie kann eine bestimmte IAM-Rolle im Bereitstellungskonto die IAM-Rolle im Verwaltungskonto übernehmen. Ersetzen Sie Folgendes:

- <DEPLOYMENT-ACCOUNT-ID>ist die ID des Bereitstellungskontos
- <DEPLOYMENT-ROLE-NAME>ist der Name der Rolle im Bereitstellungskonto, die die Rolle im Verwaltungskonto übernehmen darf

```
{
    “Version”: “2012-10-17”,
    “Statement”: [
        {
            “Effect”: “Allow”,
            “Principal”: {
                “AWS”: “arn:aws:iam::<DEPLOYMENT-ACCOUNT-ID>:role/<DEPLOYMENT-ROLE-
NAME>”
            },
            “Action”: “sts:AssumeRole”,
            “Condition”: {}
        }
    ]
```

```
}
```

Stellen Sie AWS Control Tower Kontrollen mithilfe von Terraform bereit und verwalten Sie sie

Erstellt von Iker Reina Fuente (AWS) und Ivan Girardi (AWS)

Übersicht

Dieses Muster beschreibt, wie AWS Control Tower Controls, HashiCorp Terraform und Infrastructure as Code (IaC) verwendet werden, um präventive, detektive und proaktive Sicherheitskontrollen zu implementieren und zu verwalten. Eine Kontrolle (auch als Guardrail bezeichnet) ist eine Regel auf hoher Ebene, die eine kontinuierliche Steuerung Ihrer gesamten Umgebung gewährleistet. AWS Control Tower Sie können beispielsweise Kontrollen verwenden, um eine Protokollierung für Ihr System vorzuschreiben AWS-Konten und dann automatische Benachrichtigungen zu konfigurieren, wenn bestimmte sicherheitsrelevante Ereignisse eintreten.

AWS Control Tower unterstützt Sie bei der Implementierung präventiver, detektiver und proaktiver Kontrollen, mit denen Sie Ihre AWS Ressourcen steuern und die Einhaltung der Vorschriften in mehreren Bereichen überwachen können. AWS-Konten Jede Kontrolle erzwingt eine einzige Regel. In diesem Muster verwenden Sie eine bereitgestellte IaC-Vorlage, um anzugeben, welche Steuerelemente Sie in Ihrer Umgebung bereitstellen möchten.

AWS Control Tower Kontrollen gelten für eine gesamte Organisationseinheit (OU), und die Steuerung wirkt sich auf alle AWS-Konto innerhalb der Organisationseinheit aus. Wenn Benutzer eine Aktion in einem Konto in Ihrer landing zone ausführen, unterliegt diese Aktion daher den Kontrollen, die für die Organisationseinheit gelten.

Die Implementierung von AWS Control Tower Kontrollen trägt dazu bei, eine solide Sicherheitsgrundlage für Ihre AWS landing zone zu schaffen. Indem Sie dieses Muster verwenden, um die Steuerungen als IaC über Terraform bereitzustellen, können Sie die Steuerungen in Ihrer landing zone standardisieren und sie effizienter einsetzen und verwalten.

Um AWS Control Tower Steuerelemente als IaC bereitzustellen, können Sie anstelle von Terraform auch Terraform verwenden. AWS Cloud Development Kit (AWS CDK) Weitere Informationen finden Sie unter Bereitstellen und Verwalten von AWS Control Tower Steuerelementen mithilfe von und. AWS CDK AWS CloudFormation

Beabsichtigte Zielgruppe

Dieses Muster wird Benutzern empfohlen, die Erfahrung mit AWS Control Tower Terraform und haben. AWS Organizations

Voraussetzungen und Einschränkungen

Voraussetzungen

- Aktiv AWS-Konten geführt als Organisation in AWS Organizations und als AWS Control Tower landing zone. Anweisungen finden Sie in der AWS Control Tower Dokumentation unter Erste Schritte.
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert.
- Eine AWS Identity and Access Management (IAM-) Rolle im Verwaltungskonto, die berechtigt ist, dieses Muster bereitzustellen. Weitere Informationen zu den erforderlichen Berechtigungen und eine Beispielrichtlinie finden Sie unter Berechtigungen mit den geringsten Rechten für die IAM-Rolle im Abschnitt Zusätzliche Informationen dieses Musters.
- Berechtigungen zur Übernahme der IAM-Rolle im Verwaltungskonto.
- Terraform CLI, installiert (Terraform-Dokumentation).
- Terraform AWS Provider, konfiguriert (Terraform-Dokumentation).
- Terraform-Backend, konfiguriert (Terraform-Dokumentation).

Einschränkungen

- Für AWS Control Tower Steuerelemente erfordert dieses Muster die Verwendung globaler Bezeichner im folgenden Format:

```
arn:<PARTITION>:controlcatalog:::control/<CONTROL_CATALOG_OPAQUE_ID>
```

  In früheren Versionen dieses Musters wurden regionale Identifikatoren verwendet, die nicht mehr unterstützt werden. Wir empfehlen, dass Sie von regionalen Kennungen zu globalen Kennungen migrieren. Globale Kennungen helfen Ihnen dabei, Kontrollen zu verwalten und die Anzahl der Kontrollen, die Sie verwenden können, zu erweitern.

> **Note**
>
> In den meisten Fällen `<PARTITION>` ist `aws` der Wert für.

Versionen der Produkte

- AWS Control Tower Version 3.2 oder höher
- Terraform Version 1.5 oder höher
- Terraform AWS Provider Version 4.67 oder höher

Architektur

Dieser Abschnitt bietet einen allgemeinen Überblick über diese Lösung und die durch den Beispielcode geschaffene Architektur. Das folgende Diagramm zeigt die Steuerelemente, die für die verschiedenen Konten in der Organisationseinheit eingesetzt werden.

AWS Control Tower Die Kontrollen werden nach ihrem Verhalten und ihren Leitlinien kategorisiert.

Es gibt drei Haupttypen von Kontrollverhalten:

1. Präventive Kontrollen sollen verhindern, dass Maßnahmen ergriffen werden. Diese werden mithilfe von Dienststeuerungsrichtlinien (SCPs) oder Ressourcenkontrollrichtlinien (RCPs) implementiert AWS Organizations. Der Status einer präventiven Kontrolle ist entweder erzwungen oder nicht aktiviert. Präventive Kontrollen werden in allen AWS-Regionen Bereichen unterstützt.
2. Detective Controls sind so konzipiert, dass sie bestimmte Ereignisse erkennen, wenn sie auftreten, und die Aktion protokollieren AWS CloudTrail. Diese werden mit AWS Config Regeln implementiert. Der Status einer detektiven Kontrolle ist entweder „Ungültig“, „Verstoß“ oder „Nicht aktiviert“. Detective Controls gelten nur für diejenigen, die von AWS-Regionen unterstützt werden AWS Control Tower.
3. Proaktive Kontrollen scannen Ressourcen, die von bereitgestellt werden würden, AWS CloudFormation und prüfen, ob sie den Richtlinien und Zielen Ihres Unternehmens entsprechen. Ressourcen, die nicht den Vorschriften entsprechen, werden nicht bereitgestellt. Diese werden mit AWS CloudFormation Hooks implementiert. Der Status einer proaktiven Kontrolle ist PASS, FAIL oder SKIP.

Es wird empfohlen, die einzelnen Kontrollen auf Ihr System anzuwenden OUs. AWS Control Tower bietet drei Kategorien von Leitlinien: verpflichtend, dringend empfohlen und fakultativ. Die Leitlinien einer Kontrolle sind unabhängig von ihrem Verhalten. Weitere Informationen finden Sie unter Verhalten und Steuerung der Steuerung.

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend AWS-Konten zu verwalten.
- AWS Configbietet einen detaillierten Überblick über die Ressourcen in Ihrem System AWS-Konto und darüber, wie sie konfiguriert sind. Es hilft Ihnen zu erkennen, wie Ressourcen miteinander zusammenhängen und wie sich ihre Konfigurationen im Laufe der Zeit geändert haben.
- AWS Control Towerhilft Ihnen bei der Einrichtung und Verwaltung einer Umgebung AWS mit mehreren Konten und folgt dabei den vorgeschriebenen Best Practices.
- AWS Organizationsist ein Kontoverwaltungsservice, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie erstellen und zentral verwalten.

Andere Tools

- HashiCorp Terraform ist ein Infrastructure-as-Code-Tool (IaC), mit dem Sie mithilfe von Code Cloud-Infrastruktur und -Ressourcen bereitstellen und verwalten können.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub Deploy and Manage AWS Control Tower Controls by Using Terraform verfügbar.

Bewährte Methoden

- Die für die Bereitstellung dieser Lösung verwendete IAM-Rolle sollte dem Prinzip der geringsten Rechte entsprechen (IAM-Dokumentation).
- Folgen Sie den Best Practices für AWS Control Tower Administratoren (Dokumentation).AWS Control Tower

Epen

Aktivieren Sie die Steuerelemente im Verwaltungskonto

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Geben Sie in einer Bash-Shell den folgenden Befehl ein. Dadurch werden die AWS Control Tower Steuerelemente Deploy und Manage mithilfe des Terraform-Repositorys von geklont. GitHub `git clone https://github.com/aws-samples/aws-control-tower-controls-terraform.git`	DevOps Ingenieur
Bearbeiten Sie die Terraform-Backend-Konfigurationsdatei.	1. Öffnen Sie im geklonten Repository die Datei backend.tf. 2. Bearbeiten Sie die Datei, um die Terraform-Backend-Konfiguration festzulegen. Die Konfiguration, die Sie in dieser Datei definieren, hängt von Ihrer Umgebung ab. Weitere Informationen finden Sie unter Backend-Konfiguration (Terraform-Dokumentation). 3. Speichern und schließen Sie die Datei backend.tf.	DevOps Ingenieur, Terraform

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bearbeiten Sie die Konfigurationsdatei des Terraform-Anbieters.	1. Öffnen Sie im geklonten Repository die Datei provider.tf. 2. Bearbeiten Sie die Datei, um die Terraform-Anbieterkonfiguration festzulegen. Weitere Informationen finden Sie unter Provider-Konfiguration (Terraform-Dokumentation). Stellen Sie die AWS-Region als Region ein, in der die AWS Control Tower API verfügbar ist. 3. Speichern und schließen Sie die Datei provider.tf.	DevOps Ingenieur, Terraform

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bearbeiten Sie die Konfigurationsdatei.	1. Öffnen Sie im geklonten Repository die Datei variables.tfvars. 2. Öffnen Sie Alle globalen Bezeichner in der Dokumentation. AWS Control Tower 3. Suchen Sie in der Liste im JSON-Format das Steuerelement, das Sie implementieren möchten, und kopieren Sie dann seinen globalen Bezeichner (auch bekannt als der Wert {CONTROL_CATALOG_OPAQUE_ID}). Der globale Bezeichner für das AWS-GR_AUDIT_BUCKET_ENCRYPTION_ENABLED-Steuerelement lautet beispielsweise. `k4izcjxhukijhajp6ks5mjxk` 4. Geben Sie im `controls` Abschnitt im Parameter den globalen Bezeichner ein, den Sie kopiert haben. `control_names` 5. Geben Sie in dem `controls` Abschnitt im `organizational_unit_ids` Parameter die ID der Organisationseinheit ein, für die Sie das Steuerelement aktivieren	DevOps Ingenieur, General AWS, Terraform

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	möchten, z. `ou-1111-1111111` B. Geben Sie die ID in doppelte Anführungszeichen ein und trennen Sie mehrere IDs durch Kommas. Weitere Informationen zum Abrufen der Organisationseinheit IDs finden Sie unter Die Details einer Organisationseinheit anzeigen. 6. Speichern und schließen Sie die Datei variables.tfvars. Ein Beispiel für eine aktualisierte Datei variables.tfvars finden Sie im Abschnitt Zusätzliche Informationen dieses Musters.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Nehmen Sie die IAM-Rolle im Verwaltungskonto an.	Nehmen Sie im Verwaltungskonto die IAM-Rolle an, die über die Berechtigungen zur Bereitstellung der Terraform-Konfigurationsdatei verfügt. Weitere Informationen zu den erforderlichen Berechtigungen und eine Beispielrichtlinie finden Sie unter Berechtigungen mit den geringsten Rechten für die IAM-Rolle im Abschnitt Zusätzliche Informationen. Weitere Informationen zur Übernahme einer IAM-Rolle in der AWS CLI finden Sie unter Verwenden einer IAM-Rolle in der. AWS CLI	DevOps Ingenieur, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die Konfigurationsdatei bereit.	1. Geben Sie den folgenden Befehl ein, um Terraform zu initialisieren.
	`$ terraform init -upgrade`
	2. Geben Sie den folgenden Befehl ein, um eine Vorschau der Änderungen im Vergleich zum aktuellen Status anzuzeigen.
	`$ terraform plan -var-file="variables.tfvars"`
	3. Überprüfen Sie die Konfigurationsänderungen im Terraform-Plan und bestätigen Sie, dass Sie diese Änderungen in der Organisation implementieren möchten.
	4. Geben Sie den folgenden Befehl ein, um die Ressourcen bereitzustellen.
	`$ terraform apply -var-file="variables.tfvars"`
		DevOps Ingenieur, General AWS, Terraform

(Optional) Deaktivieren Sie die Kontrollen im Verwaltungskonto AWS Control Tower

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie den Befehl `destroy` aus.	Geben Sie den folgenden Befehl ein, um die nach diesem Muster bereitgestellten Ressourcen zu entfernen. `$ terraform destroy -var-file="variables.tfvars"`	DevOps Ingenieur, General AWS, Terraform

Fehlerbehebung

Problem	Lösung
`Error: creating ControlTower Control ValidationException: Guardrail <control ID> is already enabled on organizational unit <OU ID>`-Fehler	Das Steuerelement, das Sie aktivieren möchten, ist in der Ziel-OU bereits aktiviert . Dieser Fehler kann auftreten, wenn ein Benutzer das Steuerelement manuell über AWS Management Console, durch AWS Control Tower oder durch aktiviert hat AWS Organizations. Um die Terraform-Konfigur ationsdatei bereitzustellen, können Sie eine der folgenden Optionen verwenden. Option 1: Aktualisieren Sie die aktuelle Terraform-Statusdatei Sie können die Ressource in die aktuelle Terraform-Statusdatei importieren. Wenn Sie den `apply` Befehl erneut ausführen, übersprin gt Terraform diese Ressource. Gehen Sie wie folgt vor, um die Ressource in den aktuellen Terraform-Status zu importieren:

Problem	Lösung

	1. Geben Sie im AWS Control Tower Verwaltungskonto den folgenden Befehl ein, um eine Liste der Amazon-Ressourcennamen (ARNs) für OUs, wo `<root-ID>` ist der Organisationsstamm, abzurufen. Weitere Informationen zum Abrufen dieser ID finden Sie unter Stammdaten anzeigen.
	`aws organizations list-organizational-units-for-parent --parent-id <root-ID>`
	2. Geben Sie für jede im vorherigen Schritt zurückgegebene OU den folgenden Befehl ein, wobei der ARN der OU angegeben `<OU-ARN>` ist.
	`aws controltower list-enabled-controls --target-identifier <OU-ARN>`
	3. Kopieren Sie das ARNs und führen Sie den Terraform-Import im erforderlichen Modul durch, sodass es im Terraform-Status enthalten ist. Anweisungen finden Sie unter Import (Terraform-Dokumentation).
	4. Wiederholen Sie die Schritte unter Konfiguration bereitstellen im Abschnitt Epics.
	
	Option 2: Deaktivieren Sie die Steuerung
	
	Wenn Sie nicht in einer Produktionsumgebung arbeiten, können Sie die Steuerung in der Konsole deaktivieren. Aktivieren Sie es erneut, indem Sie die Schritte unter Konfiguration bereitstellen im Abschnitt Epics wiederholen. Dieser Ansatz wird für Produktionsumgebun

Problem	Lösung
	gen nicht empfohlen, da die Steuerung für einen bestimmten Zeitraum deaktiviert wird. Wenn Sie diese Option in einer Produktio nsumgebung verwenden möchten, können Sie temporäre Kontrollen implementieren, z. B. die vorübergehende Anwendung eines SCP in AWS Organizations.

Zugehörige Ressourcen

AWS Dokumentation

- Über Kontrollen (AWS Control Tower Dokumentation)
- Bibliothek für Steuerungen (AWS Control Tower Dokumentation)
- Implementieren und verwalten Sie AWS Control Tower Kontrollen mithilfe von AWS CDK und AWS CloudFormation (AWS Prescriptive Guidance)

Sonstige Ressourcen

- Terraform
- Terraform CLI-Dokumentation

Zusätzliche Informationen

Beispiel für eine Datei variables.tfvars

Im Folgenden finden Sie ein Beispiel für eine aktualisierte Variables.tfvars-Datei. Dieses Beispiel aktiviert das AWS-GR_ENCRYPTED_VOLUMES-Steuerelement (globale ID:) und das AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED-Steuerelement (globale ID:`503uicglhjkokaajywfpt6ros`). `50z1ot237wl8u1lv5ufau6qqo` Eine Liste der globalen IDs Bezeichner finden Sie in AWS Control Tower der Dokumentation unter Alle globalen Bezeichner.

Das folgende Beispiel aktiviert auch Steuerelemente mit Parametern wie CT.S3.PV.5 (globale ID:**`7mo7a2h2ebsq71l8k6uzr96ou`**) und CT.SECRETSMANAGER.PV.1 (globale ID:).

dvhe47fxg5o6lryqrq9g6sxg4 Eine Liste der Steuerelemente mit Parametern finden Sie in der Dokumentation unter Steuerelemente mit Parametern. AWS Control Tower

```
controls = [
    {
        control_names = [
            "503uicglhjkokaajywfpt6ros", # AWS-GR_ENCRYPTED_VOLUMES
            ...
        ],
        organizational_unit_ids = ["ou-1111-11111111", "ou-2222-22222222"...],
    },
    {
        control_names = [
            "50z1ot237wl8u1lv5ufau6qqo", # AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED
            ...
        ],
        organizational_unit_ids = ["ou-1111-11111111"...],
    },
]

controls_with_params = [
  {
    control_names = [
      { "7mo7a2h2ebsq71l8k6uzr96ou" = { # CT.S3.PV.5
        parameters = {
          "ExemptedPrincipalArns" : ["arn:aws:iam::*:role/RoleName"],
          "ExemptedResourceArns" : [],
        }
      } },
      { "dvhe47fxg5o6lryqrq9g6sxg4" = { # CT.SECRETSMANAGER.PV.1
        parameters = {
          "ExemptedPrincipalArns" : ["arn:aws:iam::*:role/RoleName"],
        }
      } },
      ...
    ],
    organizational_unit_ids = ["ou-1111-11111111"...]
  },
  {
    control_names = [
      { "dvuaav61i5cnfazfelmvn9m6k" = { # AWS-GR_DISALLOW_CROSS_REGION_NETWORKING
        parameters = {
          "ExemptedPrincipalArns" : ["arn:aws:iam::*:role/RoleName"],
```

```
        }
      } },
      { "41ngl8m5c4eb1myoz0t707n7h" = { # AWS-GR_DISALLOW_VPC_INTERNET_ACCESS
        parameters = {
          "ExemptedPrincipalArns" : ["arn:aws:iam::*:role/RoleName"],
        }
      } },
      ...
    ],
    organizational_unit_ids = ["ou-2222-22222222"...]
  }
]
```

Berechtigungen mit den geringsten Rechten für die IAM-Rolle

Dieses Muster erfordert, dass Sie eine IAM-Rolle im Verwaltungskonto annehmen. Es hat sich bewährt, eine Rolle mit temporären Berechtigungen anzunehmen und die Berechtigungen nach dem Prinzip der geringsten Rechte einzuschränken. Die folgende Beispielrichtlinie ermöglicht die Mindestaktionen, die zum Aktivieren oder Deaktivieren von AWS Control Tower Steuerelementen erforderlich sind.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "controltower:EnableControl",
                "controltower:DisableControl",
                "controltower:GetControlOperation",
                "controltower:ListEnabledControls",
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeOrganization",
                "organizations:DetachPolicy",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
```

```
                "organizations:UpdatePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Stellen Sie eine Pipeline bereit, die Sicherheitsprobleme in mehreren Codeergebnissen gleichzeitig erkennt

Erstellt von Benjamin Morris (AWS), Dina Odum (AWS), Isaiah Schisler (AWS), Sapeksh Madan (AWS) und Tim Hahn (AWS)

Übersicht

Hinweis: ist für Neukunden nicht mehr verfügbar. AWS CodeCommit Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen.

Die Simple Code Scanning Pipeline (SCSP) ermöglicht die Erstellung einer Codeanalysepipeline mit zwei Klicks, in der branchenübliche Open-Source-Sicherheitstools parallel ausgeführt werden. Auf diese Weise können Entwickler die Qualität und Sicherheit ihres Codes überprüfen, ohne Tools installieren oder auch nur verstehen zu müssen, wie sie ausgeführt werden. Auf diese Weise können Sie Sicherheitslücken und Fehlkonfigurationen in den Code-Ergebnissen reduzieren. Es reduziert auch den Zeitaufwand, den Ihr Unternehmen mit der Installation, Recherche und Konfiguration von Sicherheitstools verbringt.

Vor SCSP mussten Entwickler beim Scannen von Code mithilfe dieser speziellen Toolsuite die Softwareanalysetools ausfindig machen, manuell installieren und konfigurieren. Selbst lokal installierte all-in-one Tools wie Automated Security Helper (ASH) erfordern die Konfiguration eines Docker-Containers, damit sie ausgeführt werden können. Mit SCSP wird jedoch eine Suite von branchenüblichen Codeanalyse-Tools automatisch im ausgeführt. AWS Cloud Bei dieser Lösung verwenden Sie Git, um Ihre Codeergebnisse zu pushen. Anschließend erhalten Sie eine visuelle Ausgabe mit at-a-glance Informationen darüber, welche Sicherheitsüberprüfungen fehlgeschlagen sind.

Voraussetzungen und Einschränkungen

- Ein aktiver AWS-Konto
- Ein oder mehrere Codeergebnisse, die Sie auf Sicherheitsprobleme überprüfen möchten
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert
- Python Version 3.0 oder höher und Pip-Version 9.0.3 oder höher, installiert
- Git, installiert
- Installieren Sie es git-remote-codecommitauf Ihrer lokalen Workstation

Architektur

Zieltechnologie-Stack

- AWS CodeCommit Endlager
- AWS CodeBuild Projekt
- AWS CodePipeline Pipeline
- Amazon Simple Storage Service (Amazon S3)-Bucket
- AWS CloudFormation Vorlage

Zielarchitektur

Das SCSP für die statische Codeanalyse ist ein DevOps Projekt, das darauf abzielt, Sicherheitsfeedback zu lieferbarem Code zu geben.

1. Melden Sie AWS Management Console sich in der beim Ziel AWS-Konto an. Vergewissern Sie sich, dass Sie sich an dem AWS-Region Ort befinden, an dem Sie die Pipeline bereitstellen möchten.
2. Verwenden Sie die CloudFormation Vorlage im Code-Repository, um den SCSP-Stack bereitzustellen. Dadurch werden ein neues CodeCommit Repository und ein neues CodeBuild Projekt erstellt.

> **Note**
>
> Als alternative Bereitstellungsoption können Sie ein vorhandenes CodeCommit Repo verwenden, indem Sie den Amazon-Ressourcennamen (ARN) des Repositorys während der Stack-Bereitstellung als Parameter angeben.

3. Klonen Sie das Repository auf Ihre lokale Workstation und fügen Sie dann alle Dateien zu den entsprechenden Ordnern im geklonten Repository hinzu.
4. Verwende Git, um die Dateien hinzuzufügen, zu übertragen und in das CodeCommit Repository zu übertragen.
5. Durch das Pushen in das CodeCommit Repository wird ein CodeBuild Job initiiert. Das CodeBuild Projekt verwendet die Sicherheitstools, um die im Code enthaltenen Ergebnisse zu scannen.

6. Überprüfen Sie die Ausgabe der Pipeline. Sicherheitstools, die Probleme auf Fehlerebene gefunden haben, führen zu fehlgeschlagenen Aktionen in der Pipeline. Korrigieren Sie diese Fehler oder unterdrücken Sie sie als Fehlalarme. Überprüfen Sie die Details der Tool-Ausgabe in den Aktionsdetails im CodePipeline oder im S3-Bucket der Pipeline.

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend AWS-Konten zu verwalten.
- AWS CodeBuildist ein vollständig verwalteter Build-Service, der Ihnen hilft, Quellcode zu kompilieren, Komponententests durchzuführen und Artefakte zu erstellen, die sofort einsatzbereit sind.
- AWS CodeCommitist ein Versionskontrolldienst, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.

Andere Tools

Eine vollständige Liste der Tools, die SCSP zum Scannen von Codeergebnissen verwendet, finden Sie in der SCSP-Readme-Datei unter. GitHub

Code-Repository

Der Code für dieses Muster ist im Simple Code Scanning Pipeline (SCSP) -Repository unter verfügbar. GitHub

Epen

Stellen Sie das SCSP bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie den CloudFormation Stapel.	1. Melden Sie sich an der AWS Management Console an.	AWS DevOps, AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Vergewissern Sie sich in der Konsole, dass Sie sich in der Zielregion befinden, in der Sie die Lösung bereitstellen möchten. Weitere Informationen finden Sie unter Region auswählen. 3. Wählen Sie den folgenden Link. Dadurch wird der Assistent zum schnellen Erstellen von Stacks in geöffnet CloudFormation. https://console.aws.amazon.com/cloudformation/Zuhause?#/ stacks/create/review?templateURL=https://proservetools.s3.amazonaws.com/cft/scsp -pipeline-stack.template.json&stackName=SimpleCodeScanPipeline 4. Überprüfen Sie im Assistenten zum schnellen Erstellen von Stacks die Parametereinstellungen für Ihren Stack und nehmen Sie die für Ihren Anwendungsfall erforderlichen Änderungen vor. 5. Wählen Sie Ich bestätige, dass AWS CloudFormation	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	möglicherweise IAM-Resso urcen erstellt, und wählen Sie dann Stack erstellen aus. Dadurch werden ein CodeCommit Repository, eine CodePipeline Pipeline, mehrere CodeBuild Jobdefini tionen und ein S3-Bucket erstellt. Build-Läufe und Scan-Ergebnisse werden in diesen Bucket kopiert. Nachdem der CloudFormation Stack vollständig bereitgestellt wurde, ist SCSP einsatzbereit.	

Verwenden Sie die Pipeline

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Untersuchen Sie die Ergebnisse des Scans.	1. Wählen Sie in der Amazon S3 S3-Konsole unter Buckets den Bucket simplecodescanpipeline-deleteresourcespipelineeso aus. 2. Wählen Sie das Verzeichn is scan_results und dann den Ordner mit dem letzten Scandatumsstempel. 3. Überprüfen Sie die Protokoll dateien in diesem Ordner, um alle Probleme zu	App-Entwickler, AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	überprüfen, die von den in der Pipeline verwendeten Sicherheitstools entdeckt wurden. Sicherheitstools, die Probleme auf Fehlerebene gefunden haben, führen zu `failed` laufenden Aktionen. Diese müssen behoben oder unterdrückt werden, wenn es sich um Fehlalarme handelt. **Note** Sie können sich auch Details der Tool-Ausgabe (sowohl für erfolgreiche als auch für fehlgeschlagene Scans) in der CodePipeline Konsole im Abschnitt Aktionsdetails ansehen.	

Fehlerbehebung

Problem	Lösung
HashiCorp Terraform oder AWS CloudFormation Dateien werden nicht gescannt.	Stellen Sie sicher, dass Terraform-Dateien (.tf) und CloudFormation (.yml, .yaml oder .json) in

Problem	Lösung
	den entsprechenden Ordnern des geklonten Repositorys abgelegt werden. CodeCommit
Der `git clone` Befehl schlägt fehl.	Stellen Sie sicher, dass Sie die Installation installiert haben `git-remote-codecommit` und dass Ihre CLI Zugriff auf AWS Anmeldeinformationen hat, die zum Lesen des CodeCommit Repositorys berechtigt sind.
Ein Parallelitätsfehler, wie z. `Project-level concurrent build limit cannot exceed the account-level concurrent build limit of 1`	Führen Sie die Pipeline erneut aus, indem Sie in der Konsole auf die CodePipeline Schaltfläche Release Change klicken. Dies ist ein bekanntes Problem, das bei den ersten Versuchen, in denen die Pipeline ausgeführt wird, offenbar am häufigsten auftritt.

Zugehörige Ressourcen

Geben Sie Feedback zum SCSP-Projekt.

Zusätzliche Informationen

HÄUFIG GESTELLTE FRAGEN

Ist das SCSP-Projekt dasselbe wie Automated Security Helper (ASH)?

Nein. Verwenden Sie ASH, wenn Sie ein CLI-Tool benötigen, das Code-Scan-Tools mithilfe von Containern ausführt. Automated Security Helper (ASH) ist ein Tool, mit dem die Wahrscheinlichkeit einer Sicherheitsverletzung in einer neuen Code-, Infrastruktur- oder IAM-Ressourcenkonfiguration verringert werden soll. ASH ist ein Befehlszeilenprogramm, das lokal ausgeführt werden kann. Für die lokale Verwendung muss eine Container-Umgebung auf dem System installiert und betriebsbereit sein.

Verwenden Sie SCSP, wenn Sie eine einfachere Setup-Pipeline als ASH benötigen. SCSP erfordert keine lokalen Installationen. SCSP ist so konzipiert, dass Prüfungen einzeln in einer Pipeline ausgeführt und die Ergebnisse nach Tools angezeigt werden. SCSP vermeidet außerdem einen Großteil des Aufwands bei der Einrichtung von Docker und ist betriebssystemunabhängig (OS).

Ist SCSP nur für Sicherheitsteams gedacht?

Nein, jeder kann die Pipeline einsetzen, um festzustellen, welche Teile seines Codes die Sicherheitsüberprüfungen nicht bestehen. Benutzer, die keine Sicherheitsprobleme haben, können beispielsweise SCSP verwenden, um ihren Code zu überprüfen, bevor sie ihn mit ihren Sicherheitsteams überprüfen.

Kann ich SCSP verwenden, wenn ich mit einem anderen Repository-Typ wie GitLab GitHub, oder Bitbucket arbeite?

Du kannst ein lokales Git-Repository so konfigurieren, dass es auf zwei verschiedene Remote-Repositorys verweist. Sie könnten beispielsweise ein vorhandenes GitLab Repository klonen, eine SCSP-Instanz erstellen (mit Angabe CloudFormation von Terraform- und AWS RDK-Ordnern (AWS Config Rules Development Kit), falls erforderlich) und dann das lokale Repository auch auf das SCSP-Repository verweisen. `git remote add upstream <SCSPGitLink>` CodeCommit Auf diese Weise können Codeänderungen zuerst an SCSP gesendet, validiert und dann, nachdem weitere Aktualisierungen vorgenommen wurden, um die Ergebnisse zu korrigieren, in das, ,- oder Bitbucket-Repository übertragen werden. GitLab GitHub Weitere Informationen zu mehreren Remotes finden Sie unter Push Commits to an ein zusätzliches Git-Repository (AWS Blogbeitrag).

> **Note**
>
> Achten Sie auf Abweichungen, z. B. vermeiden Sie es, Änderungen über Weboberflächen vorzunehmen.

Tragen Sie Ihre eigenen Aktionen bei und fügen Sie sie hinzu

Das SCSP-Setup wird als GitHub Projekt verwaltet, das den Quellcode für die AWS Cloud Development Kit (AWS CDK) SCSP-Anwendung enthält. Um der Pipeline zusätzliche Prüfungen hinzuzufügen, muss die AWS CDK Anwendung aktualisiert und anschließend synthetisiert oder in AWS-Konto dem Ziel bereitgestellt werden, auf dem die Pipeline ausgeführt werden soll. Klonen Sie dazu zunächst das GitHub SCSP-Projekt und suchen Sie dann die Stack-Definitionsdatei im Ordner. `lib`

Wenn Sie eine zusätzliche Prüfung hinzufügen möchten, macht es die `StandardizedCodeBuildProject` Klasse im AWS CDK Code sehr einfach, Aktionen hinzuzufügen. Geben Sie den Namen, die Beschreibung und/oder `install` die `build` Befehle ein. AWS CDK erstellt das CodeBuild Projekt unter Verwendung sinnvoller Standardwerte. Sie müssen

das Build-Projekt nicht nur erstellen, sondern es auch zu den CodePipeline Aktionen in der Build-Phase hinzufügen. Beim Entwerfen einer neuen Prüfung sollte die Aktion erfolgen, `FAIL` wenn das Scan-Tool Probleme feststellt oder nicht ausgeführt werden kann. Die Aktion sollte `PASS` erfolgen, wenn das Scan-Tool keine Probleme erkennt. Ein Beispiel für die Konfiguration eines Tools finden Sie im Code für die `Bandit` Aktion.

Weitere Informationen zu den erwarteten Eingaben und Ausgaben finden Sie in der Repository-Dokumentation.

Wenn Sie benutzerdefinierte Aktionen hinzufügen, müssen Sie SCSP mithilfe von `cdk deploy` oder `cdk synth + CloudFormation deploy` bereitstellen. Das liegt daran, dass die Quick CloudFormation Create-Stack-Vorlage von den Repo-Besitzern verwaltet wird.

Stellen Sie detektivattributebasierte Zugriffskontrollen für öffentliche Subnetze bereit, indem Sie AWS Config

Erstellt von Alberto Menendez (AWS)

Übersicht

Distributed-Edge-Netzwerkarchitekturen verlassen sich auf die Sicherheit am Netzwerkrand, die parallel zu den Workloads in ihren virtuellen privaten Clouds ausgeführt wird (). VPCs Dies bietet eine beispiellose Skalierbarkeit im Vergleich zum üblicheren, zentralisierten Ansatz. Die Bereitstellung öffentlicher Subnetze in Workload-Konten kann zwar Vorteile bieten, bringt aber auch neue Sicherheitsrisiken mit sich, da dadurch die Angriffsfläche vergrößert wird. Wir empfehlen, nur Elastic Load Balancing Balancing-Ressourcen wie Application Load Balancers oder NAT-Gateways in deren öffentlichen Subnetzen bereitzustellen. VPCs Die Verwendung von Load Balancern und NAT-Gateways in dedizierten öffentlichen Subnetzen hilft Ihnen dabei, eine differenzierte Steuerung für eingehenden und ausgehenden Datenverkehr zu implementieren.

Wir empfehlen, sowohl präventive als auch detektive Kontrollen zu implementieren, um die Arten von Ressourcen zu begrenzen, die in öffentlichen Subnetzen eingesetzt werden können. Weitere Informationen zur Verwendung der attributebasierten Zugriffskontrolle (ABAC) zur Bereitstellung präventiver Kontrollen für öffentliche Subnetze finden Sie unter Bereitstellen präventiver attributebasierter Zugriffskontrollen für öffentliche Subnetze. Diese präventiven Kontrollen sind zwar in den meisten Situationen wirksam, decken aber möglicherweise nicht alle möglichen Anwendungsfälle ab. Daher baut dieses Muster auf dem ABAC-Ansatz auf und hilft Ihnen bei der Konfiguration von Warnmeldungen über nicht konforme Ressourcen, die in öffentlichen Subnetzen bereitgestellt werden. Die Lösung prüft, ob Elastic Network-Schnittstellen zu einer Ressource gehören, die in öffentlichen Subnetzen nicht zulässig ist.

Um dies zu erreichen, verwendet dieses Muster AWS Config benutzerdefinierte Regeln und ABAC. Die benutzerdefinierte Regel verarbeitet die Konfiguration einer elastic network interface, wann immer sie erstellt oder geändert wird. Auf einer übergeordneten Ebene führt diese Regel zwei Aktionen durch, um festzustellen, ob die Netzwerkschnittstelle konform ist:

1. Um festzustellen, ob die Netzwerkschnittstelle in den Geltungsbereich der Regel fällt, überprüft die Regel, ob das Subnetz über bestimmte AWS Tags verfügt, die darauf hinweisen, dass es sich um ein öffentliches Subnetz handelt. Dieses Tag könnte beispielsweise sein. `IsPublicFacing=True`

2. Wenn die Netzwerkschnittstelle in einem öffentlichen Subnetz bereitgestellt wird, überprüft die Regel, wer diese Ressource AWS-Service erstellt hat. Wenn es sich bei der Ressource nicht um eine Elastic Load Balancing Balancing-Ressource oder kein NAT-Gateway handelt, wird die Ressource als nicht konform markiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- AWS Config, im Workload-Konto eingerichtet
- Berechtigungen zur Bereitstellung der erforderlichen Ressourcen im Workload-Konto
- Eine VPC mit öffentlichen Subnetzen
- Ordnungsgemäß angewendete Tags zur Identifizierung der öffentlichen Zielsubnetze
- (Optional) Eine Organisation in AWS Organizations
- (Optional) Ein zentrales Sicherheitskonto, das als delegierter Administrator für AWS Config und AWS Security Hub

Architektur

Zielarchitektur

Das Diagramm veranschaulicht folgende Vorgänge:

1. Wenn eine elastic network interface Network-Schnittstellenressource (`AWS::EC2::NetworkInterface`) bereitgestellt oder geändert wird, AWS Config erfasst sie das Ereignis und die Konfiguration.
2. AWS Config gleicht dieses Ereignis mit der benutzerdefinierten Regel ab, die zur Auswertung der Konfiguration verwendet wurde.
3. Die mit dieser benutzerdefinierten Regel verknüpfte AWS Lambda Funktion wird aufgerufen. Die Funktion wertet die Ressource aus und wendet die angegebene Logik an, um zu ermittelnCOMPLIANT, NON_COMPLIANT ob die Ressourcenkonfiguration oder ist. NOT_APPLICABLE

4. Wenn bei einer Ressource festgestellt wird, dass dies der Fall ist`NON_COMPLIANT`, wird eine Warnung über Amazon Simple Notification Service (Amazon SNS) AWS Config gesendet.

> **Note**
>
> Wenn es sich bei diesem Konto um ein Mitgliedskonto handelt AWS Organizations, können Sie Compliance-Daten über AWS Config oder AWS Security Hub an ein zentrales Sicherheitskonto senden.

Bewertungslogik für Lambda-Funktionen

Das folgende Diagramm zeigt die Logik, die von der Lambda-Funktion angewendet wird, um die Konformität der elastic network interface zu bewerten.

Automatisierung und Skalierung

Dieses Muster ist eine detektivische Lösung. Sie können es auch durch eine Behebungsregel ergänzen, um automatisch alle Ressourcen zu beheben, die den Anforderungen nicht entsprechen. Weitere Informationen finden Sie unter Korrigieren nicht konformer Ressourcen mithilfe von Regeln. AWS Config

Sie können diese Lösung wie folgt skalieren:

- Erzwingung der Anwendung der entsprechenden AWS Tags, die Sie einrichten, um öffentlich zugängliche Subnetze zu identifizieren. Weitere Informationen finden Sie in der Dokumentation unter Tag-Richtlinien. AWS Organizations
- Konfiguration eines zentralen Sicherheitskontos, das die AWS Config benutzerdefinierte Regel auf jedes Workload-Konto in der Organisation anwendet. Weitere Informationen finden Sie unter Automatisieren Sie die Einhaltung von Konfigurationen im großen Maßstab in AWS (AWS Blogbeitrag).
- Integration AWS Config mit, AWS Security Hub um die Erfassung, Zentralisierung und Benachrichtigung in großem Umfang zu ermöglichen. Weitere Informationen finden Sie AWS Config in der AWS Security Hub Dokumentation unter Konfiguration.

Tools

- AWS Configbietet einen detaillierten Überblick über die Ressourcen in Ihrem AWS-Konto und darüber, wie sie konfiguriert sind. Es hilft Ihnen zu erkennen, wie Ressourcen miteinander zusammenhängen und wie sich ihre Konfigurationen im Laufe der Zeit geändert haben.
- Elastic Load Balancing verteilt den eingehenden Anwendungs- oder Netzwerkverkehr auf mehrere Ziele. Sie können beispielsweise den Traffic auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Container und IP-Adressen in einer oder mehreren Availability Zones verteilen.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk bereitzustellen. Dieses virtuelle Netzwerk entspricht einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben würden, mit den Vorteilen der Verwendung der skalierbaren Infrastruktur von AWS.

Bewährte Methoden

Weitere Beispiele und bewährte Methoden für die Entwicklung benutzerdefinierter AWS Config Regeln finden Sie im offiziellen AWS Config Regel-Repository unter GitHub.

Epen

Stellen Sie die Lösung bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
So erstellen Sie die Lambda-Funktion:	1. Melden Sie sich bei der an AWS Management Console, und öffnen Sie dann die AWS Lambda Konsole.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Klicken Sie auf der Seite Functions (Funktionen) auf Create function (Funktion erstellen). 3. Wählen Sie Verfassen von Grund auf aus. 4. Geben Sie im Bereich Grundinformationen für Funktionsname einen Namen ein. 5. Wählen Sie für Runtime (Laufzeit) die Option Python 3.12 aus. 6. Lassen Sie die Architektur auf x86_64 eingestellt. 7. Wählen Sie Funktion erstellen. 8. Wählen Sie die Registerkarte Code. 9. Wählen Sie im Datei-Explorer lambda_function.py. 10. Fügen Sie den Beispielcode aus dem Abschnitt Zusätzliche Informationen dieses Musters in die Registerkarte lambda_function.py ein. Passen Sie den Beispielcode an, um jede benutzerdefinierte Bewertungslogik in der `evaluate_change_notification_complia`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	nce Funktion zu identifizieren. 11. Wählen Sie Bereitstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie der Ausführungsrolle der Lambda-Funktion Berechtigungen hinzu.	1. Wählen Sie im Navigationsbereich Funktionen aus. 2. Wählen Sie die Funktion aus, die Sie gerade erstellt haben. 3. Wählen Sie Configuration (Konfiguration) und anschließend Permissions (Berechtigungen) aus. 4. Wählen Sie den Rollennamen, um die Rolle in der AWS Identity and Access Management (IAM-) Konsole zu öffnen. 5. Wählen Sie unter Berechtigungsrichtlinien die Option Berechtigungen hinzufügen und dann Inline-Richtlinie erstellen aus. 6. Wählen Sie JSON. 7. Fügen Sie die folgende Richtlinie in den Richtlinien-Editor ein. Dadurch kann die Lambda-Funktion: • Rufen Sie die Details der Subnetz-Tags ab. • Senden Sie das Konformitätsergebnis zurück an AWS Config. `{`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Action": [
	"config:PutEvaluations",
	"ec2:DescribeSubnets"
	],
	"Resource": "*",
	"Effect": "Allow"
	}
	]
	}</pre>
	8. Wählen Sie Weiter aus.
	9. Geben Sie einen Namen für die Richtlinie ein und wählen Sie dann Create policy (Richtlinie erstellen) aus.	

Rufen Sie die Lambda-Funktion Amazon Resource Name (ARN) ab.	1. Öffnen Sie die Lambda-Konsole. 2. Wählen Sie im Navigationsbereich Funktionen aus. 3. Wählen Sie die Funktion aus, die Sie gerade erstellt haben. 4. Kopieren Sie im Abschnitt Funktionsübersicht unter Function ARN den Wert.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die AWS Config benutzerdefinierte Regel.	1. Öffnen Sie die AWS Config -Konsole. 2. Wählen Sie auf der Seite Rules (Regeln) die Option Add Rule (Regel hinzufügen) aus. 3. Wählen Sie auf der Seite Regeltyp angeben die Option Benutzerdefinierte Lambda-Regel erstellen und dann Weiter aus. 4. Gehen Sie auf der Seite Regel konfigurieren wie folgt vor: a. Geben Sie einen Namen und eine Beschreibung ein. b. Fügen Sie für die AWS Lambda Funktion ARN den ARN ein, den Sie zuvor kopiert haben. c. Als Triggertyp wählen Sie Wenn sich die Konfiguration ändert aus. d. Wählen Sie unter Umfang der Änderungen die Option Ressourcen aus. e. Wählen Sie als Ressourcentyp AWS aus EC2 NetworkInterface. f. Wählen Sie Weiter aus.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	5. Überprüfen Sie auf der Seite Überprüfen und erstellen Ihre Regel und wählen Sie dann Speichern aus.	
Benachrichtigungen konfigurieren.	1. Folgen Sie den Anweisungen unter Ein Amazon SNS SNS-Thema erstellen, um ein Amazon SNS SNS-Thema zu erstellen. 2. Folgen Sie den Anweisungen unter Amazon SNS SNS-Thema abonnieren, um einen Endpunkt zu konfigurieren, der Benachrichtigungen für das Amazon SNS SNS-Thema empfängt. 3. Folgen Sie den Anweisungen unter Wie kann ich benachrichtigt werden, wenn eine AWS Ressource nicht konform ist, AWS Config um eine benutzerdefinierte EventBridge Amazon-Regel für Ihre nicht konformen Ressourcen zu konfigurieren.	Allgemeines AWS

Testen der Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine konforme Ressource.	1. Verwenden Sie die folgenden Anweisungen, um eine der unterstützten Ressourcen in einem öffentlichen Subnetz zu erstellen: • Erstellen Sie ein NAT-Gateway • Erste Schritte mit Network Load Balancern • Erstellen Sie einen Application Load Balancer 2. Nachdem die Ressource erstellt wurde, bewertet die AWS Config benutzerdefinierte Regel die Elastic Network-Schnittstellen, die der Ressource zugeordnet sind. Sie kennzeichnet diese Netzwerkschnittstellen als `COMPLIANT`. Sie können die Ressourcen anzeigen, AWS Config indem Sie die folgenden Schritte ausführen: a. Öffnen Sie die AWS Config -Konsole. b. Wählen Sie auf der Seite Regeln Ihre Regel aus.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	c. Gehen Sie auf der Seite mit den Regeldetails zum Ende der Seite. d. Wählen Sie unter Ressourcen im Geltungsbereich die Option Konformität aus. Vergewissern Sie sich, dass Sie IDs die Netzwerkschnittste llen sehen, die erstellt wurden. e. Wählen Sie die Ressourcen-ID aus, um weitere Informationen zur Konfiguration der Netzwerkschnittstelle zu erhalten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine nicht konforme Ressource.	1. Verwenden Sie die folgenden Anweisungen, um eine nicht konforme Ressource in einem öffentlichen Subnetz zu erstellen: • Starten Sie eine EC2 Amazon-Instance • Erstellen einer Amazon Relational Database Service (Amazon RDS) - Datenbank-Instance • Erstellen Sie einen VPC-Endpunkt 2. Nachdem die Ressource erstellt wurde, bewertet die AWS Config benutzerdefinierte Regel die Elastic Network-Schnittstellen, die der Ressource zugeordnet sind. Sie kennzeichnet diese Netzwerkschnittstellen als `NON_COMPLIANT`. Sie können die Ressourcen anzeigen, AWS Config indem Sie die folgenden Schritte ausführen: a. Öffnen Sie die AWS Config -Konsole. b. Wählen Sie auf der Seite Regeln Ihre Regel aus.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	c. Gehen Sie auf der Seite mit den Regeldetails zum Ende der Seite. d. Wählen Sie unter Ressourcen im Geltungsbereich die Option aus NonCompli ant. Vergewissern Sie sich, dass Sie IDs die Netzwerkschnittste llen sehen, die erstellt wurden. e. Wählen Sie die Ressourcen-ID aus, um weitere Informationen zur Konfiguration der Netzwerkschnittstelle zu erhalten. 3. Vergewissern Sie sich, dass Sie die Benachrichtigung an dem Endpunkt erhalten, den Sie in Amazon SNS konfiguriert haben.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Ressource, die nicht zutrifft.	1. Erstellen Sie in einem privaten Subnetz jede Ressource, die eine elastic network interface benötigt. 2. Nachdem die Ressource erstellt wurde, bewertet die AWS Config benutzerdefinierte Regel die Elastic Network-Schnittstellen, die der Ressource zugeordnet sind. Sie kennzeichnet diese Netzwerkschnittstellen als `NOT_APPLICABLE`. Diese Ressourcen werden in der AWS Config Konsole nicht angezeigt.	Allgemeines AWS

Zugehörige Ressourcen

AWS Dokumentation

- Einrichtung AWS Config
- AWS Config benutzerdefinierte Regeln
- ABAC für AWS
- Implementieren Sie präventive, auf Attributen basierende Zugriffskontrollen für öffentliche Subnetze

AWS Andere Ressourcen

- Automatisieren Sie die Einhaltung von Konfigurationen im großen Maßstab in AWS
- Verteilte Inspektionsarchitekturen mit Gateway Load Balancer

Zusätzliche Informationen

Im Folgenden finden Sie ein Beispiel für eine Lambda-Funktion, die zu Demonstrationszwecken bereitgestellt wird.

```
import boto3
import json
import os

# Init clients
config_client = boto3.client('config')
ec2_client = boto3.client('ec2')

def lambda_handler(event, context):

    # Init values
    compliance_value = 'NOT_APPLICABLE'
    invoking_event = json.loads(event['invokingEvent'])
    configuration_item = invoking_event['configurationItem']

    status = configuration_item['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']

    # First check if the event configuration applies. Ex. resource event is not delete
    if (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope:
        compliance_value = evaluate_change_notification_compliance(configuration_item)


    config_client.put_evaluations(
       Evaluations=[
           {
               'ComplianceResourceType': invoking_event['configurationItem']
['resourceType'],
               'ComplianceResourceId': invoking_event['configurationItem']
['resourceId'],
               'ComplianceType': compliance_value,
               'OrderingTimestamp': invoking_event['configurationItem']
['configurationItemCaptureTime']
           },
       ],
       ResultToken=event['resultToken'])

# Function with the logs to evaluate the resource
```

```
def evaluate_change_notification_compliance(configuration_item):
    is_in_scope = is_in_scope_subnet(configuration_item['configuration']['subnetId'])

    if (configuration_item['resourceType'] != 'AWS::EC2::NetworkInterface') or not
 is_in_scope:
        return 'NOT_APPLICABLE'

    else:
        alb_condition = configuration_item['configuration']['requesterId'] in ['amazon-
elb']
        nlb_condition = configuration_item['configuration']['interfaceType'] in
 ['network_load_balancer']
        nat_gateway_condition = configuration_item['configuration']['interfaceType'] in
 ['nat_gateway']

        if alb_condition or nlb_condition or nat_gateway_condition:
            return 'COMPLIANT'
    return 'NON_COMPLIANT'

# Function to check if elastic network interface is in public subnet
def is_in_scope_subnet(eni_subnet):

    subnet_description = ec2_client.describe_subnets(
        SubnetIds=[eni_subnet]
    )

    for subnet in subnet_description['Subnets']:
        for tag in subnet['Tags']:
            if tag['Key'] == os.environ.get('TAG_KEY') and tag['Value'] ==
 os.environ.get('TAG_VALUE'):
                return True

    return False
```

Implementieren Sie präventive attributebasierte Zugriffskontrollen für öffentliche Subnetze

Erstellt von Joel Alfredo Nunez Gonzalez (AWS) und Samuel Ortega Sancho (AWS)

Übersicht

In zentralisierten Netzwerkarchitekturen konzentrieren Inspection und Edge Virtual Private Clouds (VPCs) den gesamten eingehenden und ausgehenden Verkehr, z. B. den Verkehr zum und vom Internet. Dies kann jedoch zu Engpässen führen oder dazu führen, dass die Grenzen der AWS-Servicekontingenten erreicht werden. Die Bereitstellung von Netzwerksicherheit zusammen mit den Workloads VPCs bietet eine beispiellose Skalierbarkeit im Vergleich zum üblicheren, zentralisierten Ansatz. Dies wird als Distributed-Edge-Architektur bezeichnet.

Die Bereitstellung öffentlicher Subnetze in Workload-Konten kann zwar Vorteile bieten, bringt aber auch neue Sicherheitsrisiken mit sich, da dadurch die Angriffsfläche vergrößert wird. Wir empfehlen, dass Sie nur Elastic Load Balancing (ELB) -Ressourcen wie Application Load Balancer oder NAT-Gateways in deren öffentlichen Subnetzen bereitstellen. VPCs Die Verwendung von Load Balancern und NAT-Gateways in dedizierten öffentlichen Subnetzen hilft Ihnen dabei, eine differenzierte Steuerung für eingehenden und ausgehenden Datenverkehr zu implementieren.

Bei der attributebasierten Zugriffskontrolle (ABAC) werden detaillierte Berechtigungen auf der Grundlage von Benutzerattributen wie Abteilung, Aufgabenrolle und Teamname erstellt. Weitere Informationen finden Sie unter ABAC for AWS. ABAC kann Leitplanken für öffentliche Subnetze in Workload-Konten bereitstellen. Dies hilft Anwendungsteams, agil zu sein, ohne die Sicherheit der Infrastruktur zu gefährden.

Dieses Muster beschreibt, wie Sie zur Sicherung öffentlicher Subnetze beitragen können, indem ABAC über eine Service Control Policy (SCP) in AWS Organizations und Richtlinien in AWS Identity and Access Management (IAM) implementiert wird. Sie wenden das SCP entweder auf ein Mitgliedskonto einer Organisation oder auf eine Organisationseinheit (OU) an. Diese ABAC-Richtlinien ermöglichen es Benutzern, NAT-Gateways in den Zielsubnetzen bereitzustellen und sie daran zu hindern, andere Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen wie EC2 Instances und elastische Netzwerkschnittstellen bereitzustellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Organisation in AWS Organizations
- Administratorzugriff auf das Root-Konto von AWS Organizations
- In der Organisation ein aktives Mitgliedskonto oder eine Organisationseinheit zum Testen des SCP

Einschränkungen

- Das SCP in dieser Lösung verhindert nicht, dass AWS-Services, die eine serviceverknüpfte Rolle verwenden, Ressourcen in den Zielsubnetzen bereitstellen. Beispiele für diese Dienste sind Elastic Load Balancing (ELB), Amazon Elastic Container Service (Amazon ECS) und Amazon Relational Database Service (Amazon RDS). Weitere Informationen finden Sie unter SCP-Auswirkungen auf Berechtigungen in der Dokumentation zu AWS Organizations. Implementieren Sie Sicherheitskontrollen, um diese Ausnahmen zu erkennen.

Architektur

Zieltechnologie-Stack

- SCP wurde auf ein AWS-Konto oder eine Organisationseinheit in AWS Organizations angewendet
- Die folgenden IAM-Rollen:
  - `AutomationAdminRole`— Wird verwendet, um Subnetz-Tags zu ändern und VPC-Ressourcen nach der Implementierung des SCP zu erstellen
  - `TestAdminRole`— Wird verwendet, um zu testen, ob der SCP andere IAM-Prinzipale, einschließlich derer mit Administratorzugriff, daran hindert, die Aktionen auszuführen, die für `AutomationAdminRole`

Zielarchitektur

1. Sie erstellen die `AutomationAdminRole` IAM-Rolle im Zielkonto. Diese Rolle verfügt über Berechtigungen zur Verwaltung von Netzwerkressourcen. Beachten Sie die folgenden Berechtigungen, die ausschließlich für diese Rolle gelten:
   - Mit dieser Rolle können Subnetze erstellt VPCs und öffentlich zugänglich gemacht werden.
   - Diese Rolle kann die Tag-Zuweisungen für die Zielsubnetze ändern.
   - Diese Rolle kann ihre eigenen Berechtigungen verwalten.

2. In AWS Organizations wenden Sie den SCP auf das AWS-Zielkonto oder die Organisationseinheit an. Eine Beispielrichtlinie finden Sie unter Zusätzliche Informationen in diesem Muster.
3. Ein Benutzer oder ein Tool in der CI/CD-Pipeline kann die `AutomationAdminRole` Rolle übernehmen, das `SubnetType` Tag auf die Zielsubnetze anzuwenden.
4. Durch die Übernahme anderer IAM-Rollen können autorisierte IAM-Prinzipale in Ihrer Organisation NAT-Gateways in den Zielsubnetzen und andere zulässige Netzwerkressourcen im AWS-Konto verwalten, z. B. Routing-Tabellen. Verwenden Sie IAM-Richtlinien, um diese Berechtigungen zu gewähren. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für Amazon VPC.

Automatisierung und Skalierung

Um öffentliche Subnetze zu schützen, müssen die entsprechenden AWS-Tags angewendet werden. Nach der Anwendung des SCP sind NAT-Gateways die einzige Art von EC2 Amazon-Ressource, die autorisierte Benutzer in Subnetzen mit diesem Tag erstellen können. `SubnetType:IFA` (`IFA`bedeutet Ressourcen, die mit dem Internet verbunden sind.) Das SCP verhindert die Erstellung anderer EC2 Amazon-Ressourcen wie Instances und Elastic Network Interfaces. Es wird empfohlen, eine CI/CD-Pipeline zu verwenden, die die `AutomationAdminRole` Rolle beim Erstellen von VPC-Ressourcen übernimmt, sodass diese Tags ordnungsgemäß auf öffentliche Subnetze angewendet werden.

Tools

AWS-Services

- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten. In AWS Organizations können Sie Service-Kontrollrichtlinien (SCPs) implementieren. Dabei handelt es sich um eine Art von Richtlinie, mit der Sie Berechtigungen in Ihrer Organisation verwalten können.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk zu starten. Dieses virtuelle Netzwerk ähnelt einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, mit den Vorteilen der skalierbaren Infrastruktur von AWS.

Epen

Wenden Sie das SCP an

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Test-Admin-Rolle.	Erstellen Sie eine IAM-Rolle mit dem Namen `TestAdminRole` des AWS-Zielkontos. Hängen Sie die von AdministratorAccessAWS verwaltete IAM-Richtlinie an die neue Rolle an. Anweisungen finden Sie in der IAM-Dokumentation unter Eine Rolle erstellen, um Berechtigungen an einen IAM-Benutzer zu delegieren.	AWS-Administrator
Erstellen Sie die Automatisierungs-Admin-Rolle.	1. Erstellen Sie eine IAM-Rolle mit dem Namen `AutomationAdminRole` des AWS-Zielkontos. 2. Hängen Sie die von AdministratorAccessAWS verwaltete IAM-Richtlinie an die neue Rolle an. Im Folgenden finden Sie ein Beispiel für eine Vertrauensrichtlinie, mit der Sie die Rolle vom `000000000000` Konto aus testen können. `{ "Version": "2012-10-17", "Statement": [`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	{ "Effect": "Allow", "Principal": { "AWS": ["arn:aws:iam::000000000000:root"] }, "Action": "sts:AssumeRole", "Condition": {} }] }	
Erstellen Sie das SCP und hängen Sie es an.	1. Erstellen Sie mithilfe des im Abschnitt Zusätzliche Informationen bereitgestellten Beispielcodes eine Richtlinie zur Sicherheitskontrolle. Anweisungen finden Sie in der Dokumentation zu AWS Organizations unter Creating an SCP. 2. Ordnen Sie den SCP dem AWS-Zielkonto oder der Organisationseinheit zu. Anweisungen finden Sie in der Dokumentation zu AWS Organizations unter Servicesteuerungsrichtlinien anhängen und trennen.	AWS-Administrator

Testen Sie das SCP

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine VPC oder ein Subnetz.	1. Nehmen Sie die `TestAdminRole` Rolle im AWS-Zielkonto an. 2. Versuchen Sie, eine VPC oder ein neues öffentlic hes Subnetz in einer vorhandenen VPC zu erstellen. Anweisungen finden Sie unter Erstellen einer VPC, Subnetze und anderer VPC-Ressourcen in der Amazon VPC-Dokum entation. Sie sollten nicht in der Lage sein, diese Ressourcen zu erstellen. 3. Nehmen Sie die `AutomationAdminRol e` Rolle an und wiederhol en Sie den vorherige n Schritt. Jetzt sollten Sie in der Lage sein, die Netzwerkressourcen zu erstellen.	AWS-Administrator
Tags verwalten.	1. Nehmen Sie die `TestAdminRole` Rolle im AWS-Zielkonto an. 2. Fügen Sie einem verfügbar en öffentlichen Subnetz ein `SubnetType:IFA` Tag hinzu. Sie sollten in der Lage sein, dieses Tag	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	hinzuzufügen. Anweisungen zum Hinzufügen von Tags über die AWS-Befehlszeilenschnittstelle (AWS CLI) finden Sie unter create-tags in der AWS CLI Command Reference. 3. Versuchen Sie, das diesem Subnetz zugewiesene `SubnetType:IFA` Tag zu ändern, ohne Ihre Anmeldeinformationen zu ändern. Sie sollten dieses Tag nicht ändern können. 4. Nehmen Sie die `AutomationAdminRole` Rolle an und wiederholen Sie die vorherigen Schritte. Diese Rolle sollte in der Lage sein, dieses Tag hinzuzufügen und zu ändern.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Ressourcen in den Zielsubnetzen bereit.	1. Übernehmen Sie die `TestAdminRole` Rolle. 2. Versuchen Sie für ein öffentliches Subnetz, das das `SubnetType:IFA` Tag hat, eine EC2 Instanz zu erstellen. Anweisungen finden Sie in der EC2 Amazon-Dokumentation unter Eine Instance starten. In diesem Subnetz sollten Sie keine EC2 Amazon-Ressourcen außer NAT-Gateways erstellen, ändern oder löschen können. 3. Erstellen Sie im selben Subnetz ein NAT-Gateway. Anweisungen finden Sie unter Erstellen eines NAT-Gateways in der Amazon VPC-Dokumentation. Sie sollten in der Lage sein, NAT-Gateways in diesem Subnetz zu erstellen, zu ändern oder zu löschen.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwalte die AutomationAdminRole Rolle.	1. Übernimm die `TestAdminRole` Rolle. 2. Versuchen Sie, die `AutomationAdminRole` Rolle zu ändern. Anweisungen finden Sie in der IAM-Dokumentation unter Eine Rolle ändern. Sie sollten diese Rolle nicht ändern können. 3. Nehmen Sie die `AutomationAdminRole` Rolle an und wiederholen Sie den vorherigen Schritt. Jetzt sollten Sie in der Lage sein, die Rolle zu ändern.	AWS-Administrator

Bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Säubern Sie die eingesetzten Ressourcen.	1. Trennen Sie das SCP vom AWS-Konto oder der Organisationseinheit. Anweisungen finden Sie unter Trennen eines SCP in der Dokumentation zu AWS Organizations. 2. Löschen Sie die SCP. Anweisungen finden Sie unter Löschen eines SCP	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(Dokumentation zu AWS Organizations). 3. Löschen Sie die `AutomationAdminRole` Rolle und die `TestAdminRole` Rolle. Anweisungen finden Sie in der IAM-Dokumentation unter Rollen löschen. 4. Löschen Sie alle Netzwerkressourcen wie VPCs Subnetze, die Sie für diese Lösung erstellt haben.	

Zugehörige Ressourcen

AWS-Dokumentation

- Anhängen und Trennen SCPs
- Erstellen, Aktualisieren und Löschen SCPs
- Stellen Sie mithilfe von AWS Config detektivattributebasierte Zugriffskontrollen für öffentliche Subnetze bereit
- Detektivische Kontrollen
- Referenz zur Serviceautorisierung
- Tagging von AWS-Ressourcen
- Was ist ABAC für AWS?

Zusätzliche AWS-Referenzen

- Sicherung von Ressourcen-Tags, die für die Autorisierung verwendet werden, mithilfe einer Service Control-Richtlinie in AWS Organizations (AWS-Blogbeitrag)

Zusätzliche Informationen

Die folgende Service Control-Richtlinie ist ein Beispiel, mit dem Sie diesen Ansatz in Ihrer Organisation testen können.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyVPCActions",
      "Effect": "Deny",
      "Action": [
        "ec2:CreateVPC",
        "ec2:CreateRoute",
        "ec2:CreateSubnet",
        "ec2:CreateInternetGateway",
        "ec2:DeleteVPC",
        "ec2:DeleteRoute",
        "ec2:DeleteSubnet",
        "ec2:DeleteInternetGateway"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:*"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN": ["arn:aws:iam::*:role/AutomationAdminRole"]
        }
      }
    },
    {
      "Sid": "AllowNATGWOnIFASubnet",
      "Effect": "Deny",
      "NotAction": [
        "ec2:CreateNatGateway",
        "ec2:DeleteNatGateway"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition": {
        "ForAnyValue:StringEqualsIfExists": {
          "aws:ResourceTag/SubnetType": "IFA"
```

```
        },
        "StringNotLike": {
          "aws:PrincipalARN": ["arn:aws:iam::*:role/AutomationAdminRole"]
        }
      }
    },
    {
      "Sid": "DenyChangesToAdminRole",
      "Effect": "Deny",
      "NotAction": [
        "iam:GetContextKeysForPrincipalPolicy",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Resource": [
        "arn:aws:iam::*:role/AutomationAdminRole"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN": ["arn:aws:iam::*:role/AutomationAdminRole"]
        }
      }
    },
    {
      "Sid": "allowbydefault",
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```

Stellen Sie die Security Automations for AWS WAF Solution mithilfe von Terraform bereit

Erstellt von Dr. Rahul Sharad Gaikwad (AWS) und Tamilselvan P (AWS)

Übersicht

AWS WAF ist eine Firewall für Webanwendungen, die mithilfe anpassbarer Regeln, die Sie in Web-Zugriffskontrolllisten () definieren und bereitstellen, zum Schutz von Anwendungen vor häufigen Exploits beiträgt. ACLs Die Konfiguration von AWS WAF Regeln kann eine Herausforderung sein, insbesondere für Unternehmen, die keine eigenen Sicherheitsteams haben. Um diesen Prozess zu vereinfachen, bietet Amazon Web Services (AWS) die AWS WAF Lösung Security Automations for an, die automatisch eine einzige Web-ACL mit einer Reihe von AWS WAF Regeln bereitstellt, die webbasierte Angriffe filtern. Während der Terraform-Bereitstellung können Sie angeben, welche Schutzfunktionen enthalten sein sollen. Nachdem Sie diese Lösung bereitgestellt haben, AWS WAF überprüft sie Webanfragen an bestehende CloudFront Amazon-Distributionen oder Application Load Balancer und blockiert alle Anfragen, die nicht den Regeln entsprechen.

Die AWS WAF Lösung Security Automations for kann AWS CloudFormation gemäß den Anweisungen im Security Automations for Implementation Guide bereitgestellt werden. AWS WAF Dieses Muster bietet eine alternative Bereitstellungsoption für Unternehmen, die HashiCorp Terraform als bevorzugtes Infrastructure-as-Code-Tool (IaC) für die Bereitstellung und Verwaltung ihrer Cloud-Infrastruktur verwenden. Wenn Sie diese Lösung bereitstellen, wendet Terraform die Änderungen automatisch in der Cloud an und stellt die Einstellungen und Schutzfunktionen bereit und konfiguriert sie. AWS WAF

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver. AWS-Konto
- AWS Command Line Interface (AWS CLI) Version 2.4.25 oder höher, mit den erforderlichen Berechtigungen installiert und konfiguriert. Weitere Informationen finden Sie unter Erste Schritte (AWS CLI Dokumentation).
- Terraform Version 1.1.9 oder höher, installiert und konfiguriert. Weitere Informationen finden Sie unter Terraform installieren (Terraform-Dokumentation).

Architektur

Zielarchitektur

Dieses Muster stellt die Sicherheitsautomatisierungen als Lösung bereit AWS WAF . Weitere Informationen zur Zielarchitektur finden Sie unter Überblick über die Architektur im Leitfaden zur AWS WAF Implementierung von Sicherheitsautomatisierungen. Weitere Informationen zu den AWS Lambda Automatisierungen in dieser Bereitstellung, dem Anwendungsprotokollparser, dem Protokollparser, dem AWS WAF IP-Listen-Parser und dem Zugriffshandler finden Sie unter Komponentendetails im Security Automations for Implementation Guide. AWS WAF

Terraform-Bereitstellung

Wenn Sie es ausführen`terraform apply`, macht Terraform Folgendes:

1. Terraform erstellt AWS Identity and Access Management (IAM) -Rollen und Lambda-Funktionen auf der Grundlage der Eingaben aus der Datei testing.tfvars.
2. Terraform erstellt AWS WAF ACL-Regeln und IP-Sets basierend auf den Eingaben aus der Datei testing.tfvars.
3. Terraform erstellt die Amazon Simple Storage Service (Amazon S3) -Buckets, EventBridge Amazon-Regeln, AWS Glue Datenbanktabellen und Amazon Athena-Arbeitsgruppen auf der Grundlage der Eingaben aus der Datei testing.tfvars.
4. Terraform stellt den Stack bereit, um die benutzerdefinierten Ressourcen bereitzustellen. AWS CloudFormation
5. Terraform erstellt die Amazon API Gateway Gateway-Ressourcen auf der Grundlage der angegebenen Eingaben aus der Datei testing.tfvars.

Automatisierung und Skalierung

Sie können dieses Muster verwenden, um AWS WAF Regeln für mehrere AWS-Regionen zu erstellen AWS-Konten und die Security Automations for AWS WAF -Lösung in Ihrer gesamten AWS Cloud Umgebung bereitzustellen.

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie AWS-Services über Befehle in Ihrer Befehlszeilen-Shell interagieren können.

- AWS WAFist eine Firewall für Webanwendungen, mit der Sie HTTP- und HTTPS-Anfragen überwachen können, die an Ihre geschützten Webanwendungsressourcen weitergeleitet werden.

Andere Dienste

- Git ist ein verteiltes Open-Source-Versionskontrollsystem.
- HashiCorp Terraform ist eine Befehlszeilenschnittstellenanwendung, mit der Sie mithilfe von Code Cloud-Infrastruktur und -Ressourcen bereitstellen und verwalten können.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub AWS WAF Automation Using Terraform verfügbar.

Bewährte Methoden

- Platzieren Sie statische Dateien in separaten Amazon S3 S3-Buckets.
- Vermeiden Sie hartcodierte Variablen.
- Beschränken Sie die Verwendung von benutzerdefinierten Skripten.
- Nehmen Sie eine Namenskonvention an.

Epen

Richten Sie Ihre lokale Workstation ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Git.	Folgen Sie den Anweisungen unter Erste Schritte (Git-Website), um Git auf Ihrer lokalen Workstation zu installieren.	DevOps Ingenieur
Klonen Sie das Repository	Geben Sie auf Ihrer lokalen Workstation den folgenden Befehl ein, um das Code-Repository zu klonen:	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`git clone https://github.com/aws-samples/aws-waf-automation-terraform-samples.git`	
Aktualisieren Sie die Variablen.	1. Navigieren Sie in das geklonte Verzeichnis, indem Sie den folgenden Befehl eingeben: `cd terraform-aws-waf-automation` 2. Öffnen Sie in einem beliebigen Texteditor die Datei testing.tfvars. 3. Aktualisieren Sie die Werte der Variablen in der Datei testing.tfvars. 4. Speichern und schließen Sie die Datei.	DevOps Ingenieur

Stellen Sie die Zielarchitektur mit Terraform bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Initialisieren Sie die Terraform-Konfiguration.	Geben Sie den folgenden Befehl ein, um Ihr Arbeitsverzeichnis zu initialisieren, das die Terraform-Konfigurationsdateien enthält: `terraform init`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich eine Vorschau des Terraform-Plans an.	Geben Sie den folgenden Befehl ein. Terraform wertet die Konfigurationsdateien aus, um den Zielstatus für die deklarierten Ressource n zu ermitteln. Anschließend wird der Zielstatus mit dem aktuellen Status verglichen und ein Plan erstellt: `terraform plan -var-file ="testing.tfvars"`	DevOps Ingenieur
Überprüfen Sie den Plan.	Überprüfen Sie den Plan und stellen Sie sicher, dass er die erforderliche Architekt ur in Ihrem Ziel AWS-Konto konfiguriert.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Lösung bereit.	1. Geben Sie den folgenden Befehl ein, um den Plan anzuwenden: `terraform apply -var-file="testing.tfvars"` 2. Geben Sie `yes` zur Bestätigung ein. Terraform erstellt, aktualisiert oder zerstört die Infrastruktur, um den in den Konfigurationsdateien angegebenen Zielstatus zu erreichen. Weitere Informationen zur Reihenfolge finden Sie unter Terraform-Bereitstellung im Abschnitt Architektur dieses Musters.	DevOps Ingenieur

Validieren und bereinigen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Überprüfen Sie die Änderungen.	1. Stellen Sie in der Terraform-Konsole sicher, dass die Ausgaben den erwarteten Ergebnissen entsprechen. 2. Melden Sie sich bei der an. AWS Management Console 3. Stellen Sie sicher, dass die Ausgaben in der Terraform-Konsole erfolgreich in Ihrer	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	bereitgestellt wurden. AWS-Konto	
(Optional) Säubern Sie die Infrastruktur.	Wenn Sie alle Ressourcen und Konfigurationsänderungen, die durch diese Lösung vorgenommen wurden, entfernen möchten, gehen Sie wie folgt vor: 1. Geben Sie in der Terraform-Konsole den folgenden Befehl ein: `terraform destroy -var-file="testing.tfvars”` 2. Geben Sie `yes` zur Bestätigung ein.	DevOps Ingenieur

Fehlerbehebung

Problem	Lösung
`WAFV2 IPSet: WAFOptimisticLockException` -Fehler	Wenn Sie diesen Fehler bei der Ausführung des `terraform destroy` Befehls erhalten, müssen Sie die IP-Sätze manuell löschen. Anweisungen finden Sie unter Löschen eines IP-Sets (AWS WAF Dokumentation).

Zugehörige Ressourcen

AWS Verweise

- Leitfaden zur AWS WAF Implementierung von Sicherheitsautomatisierungen
- Sicherheitsautomatisierungen für AWS WAF (AWS Lösungsbibliothek)
- Häufig gestellte Fragen zu Sicherheitsautomatisierungen AWS WAF

Terraform-Referenzen

- Terraform-Backend-Konfiguration
- Terraform AWS Provider — Dokumentation und Verwendung
- Terraform Provider AWS (Repository) GitHub

Erkennen Sie Amazon RDS- und Aurora-Datenbank-Instances mit ablaufenden CA-Zertifikaten

Erstellt von Stephen DiCato (AWS) und Eugene Shifer (AWS)

Übersicht

Aus Sicherheitsgründen wird empfohlen, Daten bei der Übertragung zwischen Anwendungsservern und relationalen Datenbanken zu verschlüsseln. Sie können SSL oder TLS verwenden, um eine Verbindung zu einer Datenbank-Instance oder einem Cluster zu verschlüsseln. Diese Protokolle tragen dazu bei, Vertraulichkeit, Integrität und Authentizität zwischen einer Anwendung und einer Datenbank zu gewährleisten. Die Datenbank verwendet ein Serverzertifikat, das von einer Zertifizierungsstelle (CA) ausgestellt wird und zur Überprüfung der Serveridentität verwendet wird. SSL oder TLS verifiziert die Echtheit des Zertifikats, indem es seine digitale Signatur validiert und sicherstellt, dass es nicht abgelaufen ist.

In der AWS Management Console bieten Amazon Relational Database Service (Amazon RDS) und Amazon Aurora Benachrichtigungen über DB-Instances, für die Zertifikatsaktualisierungen erforderlich sind. Um nach diesen Benachrichtigungen zu suchen, müssen Sie sich jedoch bei jeder Benachrichtigung anmelden AWS-Konto und zur jeweiligen Servicekonsole navigieren. AWS-Region Diese Aufgabe wird komplexer, wenn Sie die Gültigkeit von Zertifikaten für viele Zertifikate überprüfen müssen AWS-Konten , die als Organisation verwaltet werden AWS Organizations.

Durch die Bereitstellung der Infrastruktur als Code (IaC), die in diesem Muster bereitgestellt wird, können Sie ablaufende CA-Zertifikate für alle Amazon RDS- und Aurora-DB-Instances in Ihrem Unternehmen oder Ihrer AWS-Konto Organisation erkennen. AWS Die AWS CloudFormationVorlage enthält eine AWS Config Regel, eine AWS Lambda Funktion und die erforderlichen Berechtigungen. Sie können sie als Stack in einem einzigen Konto oder als Stack-Set in der gesamten AWS Organisation bereitstellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Wenn Sie die Bereitstellung in einem einzigen System durchführen AWS-Konto:
  - Stellen Sie sicher, dass Sie über die Berechtigungen zum Erstellen von CloudFormation Stacks verfügen.

  - AWS Config Im Zielkonto aktivieren.
  - (Optional) AWS Security Hub Im Zielkonto aktivieren.
- Wenn Sie die Bereitstellung in einer AWS Organisation durchführen:
  - Stellen Sie sicher, dass Sie über die Berechtigungen zum Erstellen von CloudFormation Stack-Sets verfügen.
  - Aktivieren Sie Security Hub mit AWS Organizations Integration.
  - Aktivieren Sie diese Option AWS Config in den Konten, in denen Sie diese Lösung bereitstellen.
  - Benennen Sie AWS-Konto einen als delegierten Administrator für einen Security AWS Config Hub.

Einschränkungen

- Wenn Sie die Installation für ein einzelnes Konto durchführen, für das Security Hub nicht aktiviert ist, können Sie es verwenden, AWS Config um die Ergebnisse auszuwerten.
- Wenn Sie die Bereitstellung in einer Organisation durchführen, die keinen delegierten Administrator für AWS Config und Security Hub hat, müssen Sie sich bei den einzelnen Mitgliedskonten anmelden, um die Ergebnisse einzusehen.
- Wenn Sie die Konten in Ihrer Organisation verwalten und verwalten, stellen Sie IaC AWS Control Tower nach diesem Muster bereit, indem Sie Customizations for AWS Control Tower (cFcT) verwenden. Die Verwendung der CloudFormation Konsole führt dazu, dass die Konfiguration von den AWS Control Tower Vorgaben abweicht und Sie die Organisationseinheiten () oder verwalteten Konten erneut registrieren müssen. OUs
- Einige AWS-Services sind nicht in allen verfügbar. AWS-Regionen Informationen zur regionalen Verfügbarkeit finden Sie auf der Seite Dienstendpunkte und Kontingente. Wählen Sie dort den Link für den Dienst aus.

Architektur

Bereitstellung für eine Einzelperson AWS-Konto

Das folgende Architekturdiagramm zeigt den Einsatz der AWS Ressourcen innerhalb einer einzigen AWS-Konto. Es wird mithilfe einer CloudFormation Vorlage direkt über die CloudFormation Konsole implementiert. Wenn Security Hub aktiviert ist, können Sie die Ergebnisse entweder in Security Hub AWS Config oder in Security Hub anzeigen. Wenn Security Hub nicht aktiviert ist, können Sie die Ergebnisse nur in der AWS Config Konsole anzeigen.

Das Diagramm zeigt die folgenden Schritte:

1. Sie erstellen einen CloudFormation Stapel. Dadurch werden eine Lambda-Funktion und eine AWS Config Regel bereitgestellt. Sowohl die Regel als auch die Funktion sind mit den AWS Identity and Access Management (IAM-) Berechtigungen eingerichtet, die für die Veröffentlichung von Ressourcenbewertungen in AWS Config und Protokollen erforderlich sind.
2. Die AWS Config Regel arbeitet im Modus Detective Evaluation und wird alle 24 Stunden ausgeführt.
3. Security Hub erhält alle AWS Config Ergebnisse.
4. Sie können die Ergebnisse je nach Konfiguration des Kontos im Security Hub oder in AWS Config einsehen.

Bereitstellung in einer AWS Organisation

Das folgende Diagramm zeigt die Bewertung des Ablaufs von Zertifikaten für mehrere Konten, die über AWS Organizations und verwaltet werden AWS Control Tower. Sie stellen die CloudFormation Vorlage über CfCT bereit. Die Bewertungsergebnisse werden in Security Hub im delegierten Administratorkonto zentralisiert. Der im Diagramm dargestellte AWS CodePipeline Arbeitsablauf zeigt die Hintergrundschritte, die während der cFCT-Bereitstellung ablaufen.

Das Diagramm zeigt die folgenden Schritte:

1. Je nach Konfiguration für CfCT übertragen Sie den IaC im Verwaltungskonto in ein AWS CodeCommit Repository oder laden eine komprimierte (ZIP-) Datei des IaC in einen Amazon Simple Storage Service (Amazon S3) -Bucket hoch.
2. Die CfCT-Pipeline entpackt die Datei, führt cfn-nag (GitHub) -Prüfungen durch und stellt sie als Stack-Set bereit. CloudFormation
3. Abhängig von der Konfiguration, die in der CFCT-Manifestdatei angegeben ist, CloudFormation StackSets werden Stacks für einzelne Konten bereitgestellt oder angegeben. OUs Dadurch werden eine Lambda-Funktion und eine AWS Config Regel in den Zielkonten bereitgestellt. Sowohl die Regel als auch die Funktion sind mit den IAM-Berechtigungen eingerichtet, die für die Veröffentlichung von Ressourcenbewertungen und Protokollen erforderlich sind. AWS Config
4. Die AWS Config Regel arbeitet im Modus Detective Evaluation und wird alle 24 Stunden ausgeführt.

5. AWS Config leitet alle Ergebnisse an Security Hub weiter.
6. Die Ergebnisse von Security Hub werden im delegierten Administratorkonto zusammengefasst.
7. Sie können die Ergebnisse in Security Hub im delegierten Administratorkonto einsehen.

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend AWS-Konten zu verwalten.
- AWS Configbietet einen detaillierten Überblick über die Ressourcen in Ihrem System AWS-Konto und deren Konfiguration. Es hilft Ihnen zu erkennen, wie Ressourcen miteinander zusammenhängen und wie sich ihre Konfigurationen im Laufe der Zeit geändert haben. Eine AWS Config Regel definiert Ihre idealen Konfigurationseinstellungen für eine Ressource und AWS Config kann bewerten, ob Ihre AWS Ressourcen die Bedingungen in Ihren Regeln erfüllen.
- AWS Control Towerhilft Ihnen dabei, eine Umgebung mit AWS mehreren Konten einzurichten und zu verwalten und dabei die vorgeschriebenen Best Practices zu befolgen. Customizations for AWS Control Tower (cFCT) hilft dir dabei, deine AWS Control Tower landing zone individuell anzupassen und dich an bewährte Methoden zu AWS halten. Anpassungen werden mithilfe von CloudFormation Vorlagen und Richtlinien zur Servicesteuerung () implementiert. SCPs
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Organizationsist ein Kontoverwaltungsservice, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie erstellen und zentral verwalten.
- AWS Security Hubbietet einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS. Es hilft Ihnen auch dabei, Ihre AWS Umgebung anhand der Sicherheitsstandards und bewährten Verfahren der Branche zu überprüfen.

Andere Tools

- Python ist eine Allzweck-Computerprogrammiersprache.

Code-Repository

Der Code für dieses Muster ist im Repository GitHub Detect Amazon RDS-Instances with Expiring CA Certificates verfügbar.

Bewährte Methoden

Wir empfehlen Ihnen, sich an die bewährten Methoden in den folgenden Ressourcen zu halten:

- Bewährte Methoden für Organisationseinheiten mit AWS Organizations (AWS Cloud Operations & Migrations Blog)
- Leitfaden für die Einrichtung einer ersten Grundlage mithilfe von AWS Control Tower on AWS (AWS Solutions Library)
- Anleitung zum Erstellen und Ändern von AWS Control Tower Ressourcen (AWS Control Tower Dokumentation)
- Überlegungen zur CfCT-Bereitstellung (AWS Control Tower Dokumentation)

Epen

Überprüfe die Lösung und den Code

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestimmen Sie Ihre Bereitstellungsstrategie.	Prüfen Sie die Lösung und den Code, um festzustellen, wie Sie sie in Ihrer AWS Umgebung einsetzen werden. Stellen Sie fest, ob Sie die Implementierung in einem einzelnen Konto oder in einer AWS Organisation durchführen möchten.	Inhaber der App, General AWS
Klonen Sie das Repository	Geben Sie den folgenden Befehl ein, um das Repository Detect Amazon RDS-Instances mit ablaufenden CA-Zertifikaten zu klonen.	App-Entwickler, App-Besitzer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`git clone https://github.com/aws-samples/config-rds-ca-expiry.git`	
Validieren Sie die Python-Version.	1. Navigieren Sie in das Verzeichnis der obersten Ebene im geklonten Repository. `cd config-rds-ca-expiry` 2. Öffnen Sie .yamlconfig-rds-ca-expiry. 3. Vergewissern Sie sich in der `CertExpirationCheckLambdaFunction` Ressource, dass die Python-Version mit Ihrem Ziel kompatibel ist AWS-Regionen. Standardmäßig verwendet diese Funktion Python 3.12. Weitere Informationen finden Sie unter AWS Lambda Fügt Unterstützung für Python 3.12 hinzu. Aktualisieren Sie bei Bedarf die Python-Version. 4. Speichern und schließen Sie config-rds-ca-expiry.yaml.	App-Entwickler, App-Besitzer

Stellen Sie die Lösung bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudForm ation Vorlage bereit.	Stellen Sie die CloudForm ation Vorlage in Ihrer AWS Umgebung bereit. Führen Sie eine der folgenden Aktionen aus: • Wenn Sie die Bereitstellung in einer einzelnen Datei durchführen AWS-Konto, folgen Sie den Anweisungen unter Erstellen eines Stacks. • Wenn Sie die Bereitste llung in einer Organisat ion durchführen, die nicht von verwaltet wird AWS Control Tower, folgen Sie den Anweisungen unter Erstellen eines Stack-Sets. • Wenn Sie die Bereitste llung in einer Organisat ion durchführen, die von verwaltet wird AWS Control Tower, lesen Sie die Anweisungen im Abschnitt Eigene Anpassungen erstellen.	App-Entwickler, AWS-Admin istrator, Allgemeines AWS
Überprüfen Sie die Bereitste llung.	Stellen Sie in der CloudForm ation Konsole sicher, dass der Stack oder das Stack-Set erfolgreich bereitgestellt wurde.	AWS-Administrator, App-Besit zer

Überprüfen Sie die Ergebnisse

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sehen Sie sich die Ergebnisse AWS Config der Regel an.	Gehen Sie in Security Hub wie folgt vor, um eine Liste der einzelnen Ergebnisse anzuzeigen: 1. Öffnen Sie die Security Hub Hub-Konsole. 2. Wählen Sie im Navigatio nsbereich Findings aus. 3. Fügen Sie im Feld Filter hinzufügen die folgenden Filter hinzu: • Der Konformitätsstatus ist `FAILED` • Titel ist `rds-has-e xpiring-ca` 4. Wählen Sie Anwenden aus. Gehen Sie in Security Hub wie folgt vor, um eine Liste der Gesamtergebnisse anzuzeige n, gruppiert nach AWS-Konto: 1. Öffnen Sie die Security Hub Hub-Konsole. 2. Wählen Sie im Navigatio nsbereich Insights aus. 3. Wählen Sie Create Insight (Insight erstellen) aus.	AWS-Administrator, AWS-Systemadministrator, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. So wählen Sie das Gruppierungsattribut für den Insight aus: a. Wählen Sie das Suchfeld, um die Filteroptionen anzuzeige n. b. Wählen Sie Group by (Gruppieren nach). c. Wählen Sie AwsAccoun tId. d. Wählen Sie Anwenden aus. 5. Fügen Sie im Feld Filter hinzufügen die folgenden Filter hinzu: • Der Titel lautet `rds-has-expiring-ca` • Der Compliance-Status ist `FAILED` 6. Wählen Sie Create Insight (Insight erstellen) aus. 7. Geben Sie einen Insight-N amen ein und wählen Sie dann Create Insight aus.	
	Um eine Liste der Ergebniss e einzusehen, folgen Sie den Anweisungen unter Konformitätsinformationen und Bewertungsergebnisse	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	anzeigen in der AWS Config Dokumentation. AWS Config	

Fehlerbehebung

Problem	Lösung
CloudFormation Das Erstellen oder Löschen von Stack-Sets schlägt fehl	Wenn es bereitgestellt AWS Control Tower wird, setzt es die erforderlichen Schutzmaß nahmen durch und übernimmt die Kontrolle über AWS Config Aggregatoren und Regeln. Dazu gehört auch die Verhinderung direkter Änderungen durch. CloudFormation Um diese CloudFormation Vorlage, einschließlich aller zugehörigen Ressourcen, ordnungsgemäß bereitzustellen oder zu entfernen, müssen Sie CfCT verwenden.
CfCT kann die Vorlage nicht löschen CloudFormation	Wenn die CloudFormation Vorlage auch nach den erforderlichen Änderungen an der Manifestdatei und dem Entfernen der Vorlagendateien weiterhin besteht, stellen Sie sicher, dass die Manifestdatei den `enable_stack_set_deletion` Parameter enthält und dass der Wert auf gesetzt ist. `false` Weitere Informationen finden Sie in der CfCt-Dokumentation unter Löschen eines Stack-Sets.

Zugehörige Ressourcen

- Verwenden von SSL/TLS zur Verschlüsselung einer Verbindung zu einer DB-Instance oder einem Cluster (Amazon RDS-Dokumentation)
- AWS Config Benutzerdefinierte Regeln (Dokumentation)AWS Config

Dynamisches Generieren einer IAM-Richtlinie mit IAM Access Analyzer mithilfe von Step Functions

Erstellt von Thomas Scott (AWS), Adil El Kanabi (AWS), Koen van Blijderveen (AWS) und Rafal Pawlaszek (AWS)

Übersicht

AWS CodeCommit Hinweis: ist für Neukunden nicht mehr verfügbar. Bestandskunden von AWS CodeCommit können den Service weiterhin wie gewohnt nutzen. Weitere Informationen.

Least-Privilege ist die bewährte Sicherheitsmethode, bei der nur die für die Ausführung einer Aufgabe erforderlichen Mindestberechtigungen gewährt werden. Die Implementierung des Zugriffs mit den geringsten Rechten in einem bereits aktiven Amazon Web Services (AWS) -Konto kann schwierig sein, da Sie Benutzer nicht ungewollt daran hindern möchten, ihre Aufgaben zu erfüllen, indem Sie ihre Berechtigungen ändern. Bevor Sie AWS Identity and Access Management (IAM) -Richtlinienänderungen implementieren können, müssen Sie die Aktionen und Ressourcen verstehen, die die Kontonutzer ausführen.

Dieses Muster soll Ihnen helfen, das Prinzip des Zugriffs mit den geringsten Rechten anzuwenden, ohne die Teamproduktivität zu blockieren oder zu beeinträchtigen. Es beschreibt, wie Sie IAM Access Analyzer verwenden und AWS Step Functions dynamisch eine up-to-date IAM-Richtlinie für Ihre Rolle generieren, die auf den Aktionen basiert, die derzeit im Konto ausgeführt werden. Die neue Richtlinie ist so konzipiert, dass sie die aktuelle Aktivität zulässt, aber alle unnötigen, erhöhten Rechte entfernt. Sie können die generierte Richtlinie anpassen, indem Sie Regeln zum Zulassen und Verweigern definieren. Die Lösung integriert Ihre benutzerdefinierten Regeln.

Dieses Muster beinhaltet Optionen für die Implementierung der Lösung mit AWS Cloud Development Kit (AWS CDK) oder HashiCorp CDK for Terraform (CDKTF). Anschließend können Sie die neue Richtlinie mithilfe einer CI/CD-Pipeline (Continuous Integration and Continuous Delivery) der Rolle zuordnen. Wenn Sie über eine Architektur mit mehreren Konten verfügen, können Sie diese Lösung in jedem Konto bereitstellen, für das Sie aktualisierte IAM-Richtlinien für die Rollen generieren möchten, wodurch die Sicherheit Ihrer gesamten Umgebung erhöht wird. AWS Cloud

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein Aktiv AWS-Konto mit aktiviertem AWS CloudTrail Trail.
- IAM-Berechtigungen für Folgendes:
  - Erstellen und implementieren Sie Step Functions Functions-Workflows. Weitere Informationen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Step Functions (Dokumentation zu Step Functions).
  - AWS Lambda Funktionen erstellen. Weitere Informationen finden Sie unter Ausführungsrolle und Benutzerberechtigungen (Lambda-Dokumentation).
  - Erstellen Sie IAM-Rollen. Weitere Informationen finden Sie unter Erstellen einer Rolle zur Delegierung von Berechtigungen an einen IAM-Benutzer (IAM-Dokumentation).
- npm ist installiert. Weitere Informationen finden Sie unter Node.js und npm herunterladen und installieren (npm-Dokumentation).
- Wenn Sie diese Lösung mit AWS CDK (Option 1) bereitstellen:
  - AWS CDK Toolkit, installiert und konfiguriert. Weitere Informationen finden Sie unter Installieren von AWS CDK(AWS CDK Dokumentation).
- Wenn Sie diese Lösung mit CDKTF (Option 2) bereitstellen:
  - CDKTF, installiert und konfiguriert. Weitere Informationen finden Sie unter CDK for Terraform installieren (CDKTF-Dokumentation).
  - Terraform, installiert und konfiguriert. Weitere Informationen finden Sie unter Erste Schritte (Terraform-Dokumentation).
- AWS Command Line Interface (AWS CLI) lokal installiert und konfiguriert für Ihren. AWS-Konto Weitere Informationen finden Sie unter Installation oder Aktualisierung der neuesten Version von AWS CLI (AWS CLI Dokumentation).

Einschränkungen

- Dieses Muster wendet die neue IAM-Richtlinie nicht auf die Rolle an. Am Ende dieser Lösung wird die neue IAM-Richtlinie in einem AWS CodeCommit Repository gespeichert. Sie können eine CI/CD-Pipeline verwenden, um Richtlinien auf die Rollen in Ihrem Konto anzuwenden.

Architektur

Zielarchitektur

1. Eine regelmäßig geplante EventBridge Amazon-Ereignisregel startet einen Step Functions Functions-Workflow. Sie definieren diesen Regenerierungsplan im Rahmen der Einrichtung dieser Lösung.
2. Im Step Functions Functions-Workflow generiert eine Lambda-Funktion die Datumsbereiche, die bei der Analyse der Kontoaktivitäten in den CloudTrail Protokollen verwendet werden sollen.
3. Im nächsten Workflow-Schritt wird die IAM Access Analyzer-API aufgerufen, um mit der Generierung der Richtlinie zu beginnen.
4. Mithilfe des Amazon-Ressourcennamens (ARN) der Rolle, die Sie bei der Einrichtung angegeben haben, analysiert IAM Access Analyzer die CloudTrail Protokolle auf Aktivitäten innerhalb der angegebenen Datumsrate. Basierend auf der Aktivität generiert IAM Access Analyzer eine IAM-Richtlinie, die nur die Aktionen und Dienste zulässt, die von der Rolle im angegebenen Zeitraum genutzt wurden. Wenn dieser Schritt abgeschlossen ist, generiert dieser Schritt eine Job-ID.
5. Im nächsten Workflow-Schritt wird alle 30 Sekunden nach der Job-ID gesucht. Wenn die Job-ID erkannt wird, verwendet dieser Schritt die Job-ID, um die IAM Access Analyzer-API aufzurufen und die neue IAM-Richtlinie abzurufen. IAM Access Analyzer gibt die Richtlinie als JSON-Datei zurück.
6. Der nächste Workflow-Schritt platziert die **<**IAM role name**>**Datei /policy.json in einem Amazon Simple Storage Service (Amazon S3) -Bucket. Sie definieren diesen S3-Bucket im Rahmen der Einrichtung dieser Lösung.
7. Eine Amazon S3 S3-Ereignisbenachrichtigung startet eine Lambda-Funktion.
8. Die Lambda-Funktion ruft die Richtlinie aus dem S3-Bucket ab, integriert die benutzerdefinierten Regeln, die Sie in den Dateien allow.json und deny.json definieren, und überträgt dann die aktualisierte Richtlinie an. CodeCommit Sie definieren das CodeCommit Repository, den Branch und den Ordnerpfad im Rahmen der Einrichtung dieser Lösung.

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK)ist ein Softwareentwicklungs-Framework, das Ihnen hilft, AWS Cloud Infrastruktur im Code zu definieren und bereitzustellen.
- AWS CDK Toolkit ist ein Cloud-Entwicklungskit für die Befehlszeile, mit dem Sie mit Ihrer AWS Cloud Development Kit (AWS CDK) App interagieren können.
- AWS CloudTrailhilft Ihnen bei der Prüfung der Unternehmensführung, der Einhaltung von Vorschriften und der betrieblichen Risiken Ihres AWS-Konto.

- AWS CodeCommitist ein Versionskontrolldienst, mit dem Sie Git-Repositorys privat speichern und verwalten können, ohne Ihr eigenes Quellcodeverwaltungssystem verwalten zu müssen.
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie AWS-Services über Befehle in Ihrer Befehlszeilen-Shell interagieren können.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem es kontrolliert, wer authentifiziert und autorisiert ist, diese zu verwenden. Dieses Muster verwendet IAM Access Analyzer, eine Funktion von IAM, um Ihre CloudTrail Protokolle zu analysieren, um Aktionen und Dienste zu identifizieren, die von einer IAM-Entität (Benutzer oder Rolle) verwendet wurden, und generiert dann eine IAM-Richtlinie, die auf dieser Aktivität basiert.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Step Functionsist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Funktionen und andere Funktionen kombinieren können, um geschäftskritische AWS-Services Anwendungen zu erstellen. In diesem Muster verwenden Sie AWS SDK-Dienstintegrationen in Step Functions, um Service-API-Aktionen aus Ihrem Workflow aufzurufen.

Andere Tools

- CDK for Terraform (CDKTF) unterstützt Sie bei der Definition von Infrastructure as Code (IaC) mithilfe gängiger Programmiersprachen wie Python und Typescript.
- Lerna ist ein Build-System zum Verwalten und Veröffentlichen mehrerer Pakete aus demselben Repository. JavaScript TypeScript
- Node.js ist eine ereignisgesteuerte JavaScript Laufzeitumgebung, die für die Erstellung skalierbarer Netzwerkanwendungen entwickelt wurde.
- npm ist eine Softwareregistrierung, die in einer Node.js -Umgebung ausgeführt wird und verwendet wird, um Pakete gemeinsam zu nutzen oder auszuleihen und die Bereitstellung von privaten Paketen zu verwalten.

Code-Repository

Der Code für dieses Muster ist im GitHub Automated IAM Access Analyzer Role Policy Generator Repository verfügbar.

Epen

Bereite dich auf den Einsatz vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repo.	Mit dem folgenden Befehl wird das Automated IAM Access Analyzer Role Policy Generator () GitHub -Repository geklont. `git clone https://github.com/aws-samples/automated-iam-access-analyzer.git`	App-Developer
Installieren Sie Lerna.	Der folgende Befehl installiert Lerna. `npm i -g lerna`	App-Developer

Richten Sie die Abhängigkeiten ein.	Der folgende Befehl installiert die Abhängigkeiten für das Repository.
	`cd automated-iam-access-analyzer/`
	`npm install && npm run bootstrap`
		App-Developer

Erstellen Sie den Code.	Der folgende Befehl testet, erstellt und bereitet die Zip-Pakete der Lambda-Funktionen vor.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`npm run test:code`
	`npm run build:code`
	`npm run pack:code`	

Erstellen Sie die Konstrukte.	Der folgende Befehl erstellt die Infrastruktur, die Anwendungen synthetisiert, sowohl für CDKTF als auch für CDKTF AWS CDK . `npm run build:infra`	
Konfigurieren Sie alle benutzerdefinierten Berechtigungen.	Bearbeiten Sie im Repo-Ordner des geklonten Repositorys die Dateien allow.json und deny.json, um alle benutzerdefinierten Berechtigungen für die Rolle zu definieren. Wenn die Dateien allow.json und deny.json dieselbe Berechtigung enthalten, wird die Berechtigung „Deny“ angewendet.	AWS-Administrator, App-Entwickler

Option 1 — Stellen Sie die Lösung bereit mit AWS CDK

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den AWS CDK Stack bereit.	Der folgende Befehl stellt die Infrastruktur bereit über AWS CloudFormation. Legen Sie die folgenden Parameter fest:	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	• <NAME_OF_ROLE> — Der ARN der IAM-Rolle, für die Sie eine neue Richtlinie erstellen.
	• <TRAIL_ARN> — Der ARN des CloudTrail Trails, in dem die Rollenaktivität gespeichert ist.
	• <CRON_EXPRESSION_TO_RUN_SOLUTION> — Der Cron-Ausdruck, der den Regenerierungsplan für die Richtlinie definiert. Der Step Functions Functions-Workflow wird nach diesem Zeitplan ausgeführt.
	• <TRAIL_LOOKBACK> — Der Zeitraum in Tagen, für den Sie bei der Bewertung der Rollenberechtigungen zurückblicken müssen.
	
	`cd infra/cdk`
	`cdk deploy –-parameters roleArn=<NAME_OF_ROLE> \`
	`–-parameters trailArn=<TRAIL_ARN> \`
	`--parameters schedule=<CRON_EXPRESSION_TO_RUN_SOLUTION> \`
	`[ --parameters trailLookBack=<TRAIL_LOOKBACK> ]`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Die eckigen Klammern stehen für optionale Parameter.	
(Optional) Warten Sie auf die neue Richtlinie.	Wenn der Trail keine angemessene Menge an historischen Aktivitäten für die Rolle enthält, warten Sie, bis Sie sicher sind, dass genügend protokoll ierte Aktivitäten vorhanden sind, damit IAM Access Analyzer eine genaue Richtlini e generieren kann. Wenn die Rolle für einen ausreichenden Zeitraum im Konto aktiv war, ist diese Wartezeit möglicher weise nicht erforderlich.	AWS-Administrator
Überprüfen Sie die generierte Richtlinie manuell.	Überprüfen Sie in Ihrem CodeCommit Repositor y die generierte JSON-Datei<ROLE_ARN>, um sicherzustellen, dass die Berechtigungen Zulassen und Verweigern für die Rolle geeignet sind.	AWS-Administrator

Option 2 — Stellen Sie die Lösung mit CDKTF bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Synthetisieren Sie die Terraform-Vorlage.	Der folgende Befehl synthetisiert die Terraform-Vorlage. `lerna exec cdktf synth --scope @aiaa/tfm`	App-Developer
Stellen Sie die Terraform-Vorlage bereit.	Der folgende Befehl navigiert zu dem Verzeichnis, das die von CDKTF definierte Infrastruktur enthält. `cd infra/cdktf` Mit dem folgenden Befehl wird die Infrastruktur im Ziel bereitgestellt. AWS-Konto Legen Sie die folgenden Parameter fest: • `<account_ID>` — Die ID des Zielkontos. • `<region>`- Das Ziel AWS-Region. • `<selected_role_ARN>` — Der ARN der IAM-Rolle, für die Sie eine neue Richtlinie erstellen. • `<trail_ARN>` — Der ARN des CloudTrail Trails, in dem die Rollenaktivität gespeichert ist.	App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `<schedule_expression>` — Der Cron-Ausdruck, der den Regenerierungsplan für die Richtlinie definiert. Der Step Functions Functions-Workflow wird nach diesem Zeitplan ausgeführt. • `<trail_look_back>` — Der Zeitraum in Tagen, für den Sie bei der Bewertung der Rollenberechtigungen zurückblicken müssen. `TF_VAR_accountId=<account_ID> \ TF_VAR_region=<region> \ TF_VAR_roleArns=<selected_role_ARN> \ TF_VAR_trailArn=<trail_ARN> \ TF_VAR_schedule=<schedule_expression> \ [ TF_VAR_trailLookBack=<trail_look_back> ] \ cdktf deploy` **Note** Die eckigen Klammern stehen für optionale Parameter.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Warten Sie auf die neue Richtlinie.	Wenn der Trail keine angemessene Menge an historischen Aktivitäten für die Rolle enthält, warten Sie, bis Sie sicher sind, dass genügend protokoll ierte Aktivitäten vorhanden sind, damit IAM Access Analyzer eine genaue Richtlini e generieren kann. Wenn die Rolle für einen ausreichenden Zeitraum im Konto aktiv war, ist diese Wartezeit möglicher weise nicht erforderlich.	AWS-Administrator
Überprüfen Sie die generierte Richtlinie manuell.	Überprüfen Sie in Ihrem CodeCommit Repositor y die generierte JSON-Datei<ROLE_ARN>, um sicherzustellen, dass die Berechtigungen Zulassen und Verweigern für die Rolle geeignet sind.	AWS-Administrator

Zugehörige Ressourcen

AWS Ressourcen

- Endpunkte und Kontingente von IAM Access Analyzer
- Konfiguration der AWS CLI
- Erste Schritte mit dem AWS CDK
- Berechtigungen mit den geringsten Rechten

Sonstige Ressourcen

- CDK für Terraform (Terraform-Website)

Aktivieren Sie Amazon GuardDuty unter bestimmten Bedingungen mithilfe von Vorlagen AWS CloudFormation

Erstellt von Ram Kandaswamy (AWS)

Übersicht

Sie können GuardDuty Amazon mithilfe einer AWS CloudFormation Vorlage für ein Amazon Web Services (AWS) -Konto aktivieren. Standardmäßig schlägt die Stack-Bereitstellung fehl, wenn es bereits aktiviert GuardDuty ist, wenn Sie versuchen, es CloudFormation zu aktivieren. Sie können jedoch Bedingungen in Ihrer CloudFormation Vorlage verwenden, um zu überprüfen, ob sie bereits aktiviert GuardDuty ist. CloudFormation unterstützt die Verwendung von Bedingungen, die statische Werte vergleichen; die Verwendung der Ausgabe einer anderen Ressourceneigenschaft innerhalb derselben Vorlage wird nicht unterstützt. Weitere Informationen finden Sie in der CloudFormation Dokumentation unter Bedingungen.

In diesem Muster verwenden Sie eine CloudFormation benutzerdefinierte Ressource, die von einer AWS Lambda Funktion zur bedingten Aktivierung unterstützt wird, GuardDuty sofern sie nicht bereits aktiviert ist. Wenn GuardDuty aktiviert, erfasst der Stack den Status und zeichnet ihn im Ausgabebereich des Stacks auf. Wenn nicht GuardDuty aktiviert, aktiviert der Stack es.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Eine AWS Identity and Access Management (IAM-) Rolle, die über Berechtigungen zum Erstellen, Aktualisieren und Löschen CloudFormation von Stacks verfügt
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert

Einschränkungen

Wenn dieses Muster für ein AWS-Konto oder manuell deaktiviert GuardDuty wurde AWS-Region, wird es GuardDuty für dieses Zielkonto oder diese Region nicht aktiviert.

Architektur

Zieltechnologie-Stack

Das Muster wird CloudFormation für Infrastructure as Code (IaC) verwendet. Sie verwenden eine CloudFormation benutzerdefinierte Ressource, die von einer Lambda-Funktion unterstützt wird, um die dynamische Service-Enablement-Funktion zu erreichen.

Zielarchitektur

Das folgende Architekturdiagramm auf hoher Ebene zeigt den Prozess der Aktivierung GuardDuty durch die Bereitstellung einer CloudFormation Vorlage:

1. Sie stellen eine CloudFormation Vorlage bereit, um einen CloudFormation Stack zu erstellen.
2. Der Stack erstellt eine IAM-Rolle und eine Lambda-Funktion.
3. Die Lambda-Funktion übernimmt die IAM-Rolle.
4. Wenn GuardDuty es auf dem Ziel noch nicht aktiviert ist AWS-Konto, aktiviert es die Lambda-Funktion.

Automatisierung und Skalierung

Sie können die AWS CloudFormation StackSet Funktion verwenden, um diese Lösung auf mehrere AWS-Konten und auszudehnen AWS-Regionen. Weitere Informationen finden Sie AWS CloudFormation StackSets in der CloudFormation Dokumentation unter Arbeiten mit.

Tools

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie AWS-Services über Befehle in Ihrer Befehlszeilen-Shell interagieren können.
- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend AWS-Konten zu verwalten.
- Amazon GuardDuty ist ein Dienst zur kontinuierlichen Sicherheitsüberwachung, der Protokolle analysiert und verarbeitet, um unerwartete und potenziell nicht autorisierte Aktivitäten in Ihrer AWS Umgebung zu identifizieren.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.

- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.

Epen

Erstellen Sie die CloudFormation Vorlage und stellen Sie den Stack bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die CloudFormation Vorlage.	1. Kopieren Sie den Code in der CloudFormation Vorlage im Abschnitt Zusätzliche Informationen. 2. Fügen Sie den Code in einen Texteditor ein. 3. Speichern Sie die Datei wie `sample.yaml` auf Ihrer Workstation.	AWS DevOps
Erstellen Sie den CloudFormation Stack.	1. Geben Sie im AWS CLI den folgenden Befehl ein. Dadurch wird mithilfe der `sample.yaml` Datei ein neuer CloudFormation Stapel erstellt. Weitere Informationen finden Sie in der CloudFormation Dokumentation unter Einen Stack erstellen. `aws cloudformation create-stack \ --stack-name guardduty-cf-stack \ --template-body file://sample.yaml`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Vergewissern Sie sich, dass der folgende Wert in der erscheint AWS CLI, was darauf hinweist, dass der Stack erfolgreich erstellt wurde. Die Zeit, die zum Erstellen des Stacks benötigt wird, kann variieren . `"StackStatus": "CREATE_COMPLETE",`	
Überprüfen Sie, ob dies für aktiviert GuardDuty ist AWS-Konto.	1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole. 2. Stellen Sie sicher, dass der GuardDuty Dienst aktiviert ist.	Cloud-Administrator, AWS-Administrator
Konfigurieren Sie zusätzliche Konten oder Regionen.	Verwenden Sie die CloudFormation StackSet Funktion je nach Bedarf für Ihren Anwendungsfall, um diese Lösung auf mehrere AWS-Konten und auszudehnen AWS-Regionen. Weitere Informationen finden Sie AWS CloudFormation StackSets in der CloudFormation Dokumentation unter Arbeiten mit.	Cloud-Administrator, AWS-Administrator

Zugehörige Ressourcen

Referenzen

- AWS CloudFormation Dokumentation
- AWS Lambda Referenz zum Ressourcentyp
- CloudFormation Ressourcentyp: AWS: :IAM: :Rolle
- CloudFormation Ressourcentyp::: AWS: Detector GuardDuty
- Vier Möglichkeiten zum Abrufen beliebiger AWS Service-Eigenschaften mithilfe von AWS CloudFormation (Blogbeitrag)

Tutorials und Videos

- Vereinfachen Sie Ihr Infrastrukturmanagement mithilfe von AWS CloudFormation (Tutorial)
- Verwenden Sie Amazon GuardDuty und sichern AWS Security Hub Sie mehrere Konten (AWS re:Invent 2020)
- Bewährte Methoden für die Inhaltserstellung (re:Invent AWS CloudFormation 2019)AWS
- Bedrohungserkennung auf AWS: Eine Einführung in Amazon GuardDuty (AWS re:INFORCE 2019)

Zusätzliche Informationen

CloudFormation Vorlage

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  rLambdaLogGroup:
    Type: 'AWS::Logs::LogGroup'
    DeletionPolicy: Delete
    Properties:
      RetentionInDays: 7
      LogGroupName: /aws/lambda/resource-checker
  rLambdaCheckerLambdaRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: !Sub 'resource-checker-lambda-role-${AWS::Region}'
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
```

```
          - Effect: Allow
            Principal:
              Service: lambda.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: /
      Policies:
        - PolicyName: !Sub 'resource-checker-lambda-policy-${AWS::Region}'
          PolicyDocument:
            Version: 2012-10-17
            Statement:
              - Sid: CreateLogGroup
                Effect: Allow
                Action:
                  - 'logs:CreateLogGroup'
                  - 'logs:CreateLogStream'
                  - 'logs:PutLogEvents'
                  - 'iam:CreateServiceLinkedRole'
                  - 'cloudformation:CreateStack'
                  - 'cloudformation:DeleteStack'
                  - 'cloudformation:Desc*'
                  - 'guardduty:CreateDetector'
                  - 'guardduty:ListDetectors'
                  - 'guardduty:DeleteDetector'
                Resource: '*'
  resourceCheckerLambda:
    Type: 'AWS::Lambda::Function'
    Properties:
      Description: Checks for resource type enabled and possibly name to exist
      FunctionName: resource-checker
      Handler: index.lambda_handler
      Role: !GetAtt
        - rLambdaCheckerLambdaRole
        - Arn
      Runtime: python3.13
      MemorySize: 128
      Timeout: 180
      Code:
        ZipFile: |
          import boto3
          import os
          import json
          from botocore.exceptions import ClientError
          import cfnresponse
```

```
          guardduty=boto3.client('guardduty')
          cfn=boto3.client('cloudformation')


          def lambda_handler(event, context):
              print('Event: ', event)
              if 'RequestType' in event:
                if event['RequestType'] in ["Create","Update"]:
                    enabled=False
                    try:
                      response=guardduty.list_detectors()
                      if "DetectorIds" in response and len(response["DetectorIds"])>0:
                        enabled="AlreadyEnabled"
                      elif "DetectorIds" in response and
 len(response["DetectorIds"])==0:
                        cfn_response=cfn.create_stack(
                          StackName='guardduty-cfn-stack',
                          TemplateBody='{ "AWSTemplateFormatVersion": "2010-09-09",
 "Description": "A sample template",    "Resources": { "IRWorkshopGuardDutyDetector": {
  "Type": "AWS::GuardDuty::Detector",    "Properties": {   "Enable": true  }   } } }'
                          )
                        enabled="True"
                    except Exception as e:
                        print("Exception: ",e)
                    responseData = {}
                    responseData['status'] = enabled
                    cfnresponse.send(event, context, cfnresponse.SUCCESS, responseData,
 "CustomResourcePhysicalID" )
                elif event['RequestType'] == "Delete":
                    cfn_response=cfn.delete_stack(
                            StackName='guardduty-cfn-stack')
                    cfnresponse.send(event, context, cfnresponse.SUCCESS, {})
  CheckResourceExist:
    Type: 'Custom::LambdaCustomResource'
    Properties:
      ServiceToken: !GetAtt
        - resourceCheckerLambda
        - Arn
Outputs:
  status:
    Value: !GetAtt
      - CheckResourceExist
```

```
      - status
```

Alternative Codeoption für die Lambda-Ressource

Die bereitgestellte CloudFormation Vorlage verwendet Inline-Code, um auf die Lambda-Ressource zu verweisen, um die Referenz und Anleitung zu erleichtern. Alternativ können Sie den Lambda-Code in einem Amazon Simple Storage Service (Amazon S3) -Bucket platzieren und in der CloudFormation Vorlage darauf verweisen. Inline-Code unterstützt keine Paketabhängigkeiten oder Bibliotheken. Sie können diese unterstützen, indem Sie den Lambda-Code in einem Amazon S3 S3-Bucket platzieren und in der CloudFormation Vorlage darauf verweisen.

Ersetzen Sie die folgenden Codezeilen:

```
Code:
         ZipFile: |
```

durch die folgenden Codezeilen:

```
Code:
      S3Bucket: <bucket name>
      S3Key: <python file name>
      S3ObjectVersion: <version>
```

Die `S3ObjectVersion` Eigenschaft kann weggelassen werden, wenn Sie in Ihrem Amazon S3 S3-Bucket keine Versionierung verwenden. Weitere Informationen finden Sie unter Verwenden der Versionierung in Amazon S3 S3-Buckets in der Amazon S3 S3-Dokumentation.

Aktivieren Sie die transparente Datenverschlüsselung in Amazon RDS for SQL Server

Erstellt von Ranga Cherukuri (AWS)

Übersicht

Dieses Muster beschreibt, wie transparente Datenverschlüsselung (TDE) in Amazon Relational Database Service (Amazon RDS) für SQL Server implementiert wird, um Daten im Ruhezustand zu verschlüsseln.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine Amazon RDS for SQL Server Server-DB-Instance

Produktversionen

Amazon RDS unterstützt derzeit TDE für die folgenden SQL Server-Versionen und -Editionen:

- SQL Server 2016 Enterprise Edition
- SQL Server 2017 Enterprise Edition
- SQL Server 2019: Standard- und Enterprise Editions
- SQL Server 2022 Standard- und Enterprise-Editionen

Aktuelle Informationen zu unterstützten Versionen und Editionen finden Sie unter Support for Transparent Data Encryption in SQL Server in der Amazon RDS-Dokumentation.

Architektur

Technologie-Stack

- Amazon RDS für SQL Server

Architektur

Tools

- Microsoft SQL Server Management Studio (SSMS) ist eine integrierte Umgebung für die Verwaltung einer SQL Server-Infrastruktur. Es bietet eine Benutzeroberfläche und eine Gruppe von Tools mit umfangreichen Skripteditoren, die mit SQL Server interagieren.

Epen

Erstellen Sie eine Optionsgruppe in der Amazon RDS-Konsole

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Öffnen Sie die Amazon RDS-Konsole.	Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon RDS-Konsole.	Entwickler, DBA
Erstellen Sie eine Optionsgruppe.	Wählen Sie im Navigationsbereich Optionsgruppen, Gruppe erstellen aus. Wählen Sie sqlserver-ee als DB-Engine und wählen Sie dann die Engine-Version aus.	Entwickler, DBA
Fügen Sie die Option TRANSPARENT_DATA_ENCRYPTION hinzu.	Bearbeiten Sie die Optionsgruppe, die Sie erstellt haben, und fügen Sie die angegebene Option hinzu. `TRANSPARENT_DATA_ENCRYPTION`	Entwickler, DBA

Zuordnen der Optionsgruppe zu einer DB-Instance

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Wählen Sie die DB-Instance aus.	Wählen Sie in der Amazon RDS-Konsole im Navigationsbereich Datenbanken und dann die DB-Instance aus, die Sie der Optionsgruppe zuordnen möchten.	Entwickler, DBA
Ordnen Sie die DB-Instance der Optionsgruppe zu.	Wählen Sie Ändern aus, und verwenden Sie dann die Einstellung Optionsgruppe, um die SQL Server-DB-Instance der Optionsgruppe zuzuordnen, die Sie zuvor erstellt haben.	Entwickler, DBA
Wenden Sie die Änderungen an.	Wenden Sie die Änderungen je nach Bedarf sofort oder während des nächsten Wartungsfensters an.	Entwickler, DBA

Holen Sie sich den Namen des Zertifikats.	Rufen Sie den Namen des Standardzertifikats mithilfe der folgenden Abfrage ab.
	`USE [master]`
	`GO`
	`SELECT name FROM sys.certificates WHERE name LIKE 'RDSTDECertificate%'`
	`GO`
		Entwickler, DBA

Erstellen Sie den Datenbank-Verschlüsselungsschlüssel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie mithilfe von SSMS eine Connect zur Amazon RDS for SQL Server-DB-Instance her.	Anweisungen finden Sie in der Microsoft-Dokumentation unter SSMS verwenden.	Entwickler, DBA

Erstellen Sie den Datenbank-Verschlüsselungsschlüssel mithilfe des Standardzertifikats.	Erstellen Sie einen Verschlüsselungsschlüssel für die Datenbank, indem Sie den Standardnamen des Zertifikats verwenden, den Sie zuvor erhalten haben. Verwenden Sie die folgende T-SQL-Abfrage, um einen Datenbank-Verschlüsselungsschlüssel zu erstellen. Sie können den AES_256-Algorithmus anstelle von AES_128 angeben.
	`USE [Databasename]`
	`GO`
	`CREATE DATABASE`
	`ENCRYPTION KEY`
	`WITH ALGORITHM = AES_128`
	`ENCRYPTION BY SERVER`
	`CERTIFICATE [certificatename]`
	`GO`
		Entwickler, DBA

Aktivieren Sie die Verschlüsselung in der Datenbank.	Verwenden Sie die folgende T-SQL-Abfrage, um die Datenbankverschlüsselung zu aktivieren. `ALTER DATABASE [Database Name]`	Entwickler, DBA

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`SET ENCRYPTION ON` `GO`	
Überprüfen Sie den Status der Verschlüsselung.	Verwenden Sie die folgende T-SQL-Abfrage, um den Status der Verschlüsselung zu überprüfen. `SELECT DB_NAME(database_id) AS DatabaseName, encryption_state, percent_complete FROM sys.dm_database_encryption_keys`	Entwickler, DBA

Zugehörige Ressourcen

- Support für transparente Datenverschlüsselung in SQL Server (Amazon RDS-Dokumentation)
- Arbeiten mit Optionsgruppen (Amazon RDS-Dokumentation)
- Ändern einer Amazon RDS-DB-Instance (Amazon RDS-Dokumentation)
- Transparente Datenverschlüsselung für SQL Server (Microsoft-Dokumentation)
- SSMS verwenden (Microsoft-Dokumentation)

Stellen Sie sicher, dass AWS-Load Balancer sichere Listener-Protokolle (HTTPS, SSL/TLS) verwenden

Erstellt von Chandini Penmetsa (AWS) und Purushotham G K (AWS)

Übersicht

In der Amazon Web Services (AWS) -Cloud verteilt Elastic Load Balancing den eingehenden Anwendungsdatenverkehr automatisch auf mehrere Ziele, z. B. Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Container, IP-Adressen und AWS Lambda Lambda-Funktionen. Die Load Balancer verwenden Listener, um die Ports und Protokolle zu definieren, die der Load Balancer verwendet, um Traffic von Benutzern anzunehmen. Application Load Balancer treffen Routing-Entscheidungen auf Anwendungsebene und verwenden die. HTTP/HTTPS protocols. Network Load Balancers make routing decisions at the transport layer and use the Transmission Control Protocol (TCP), Transport Layer Security (TLS), User Datagram Protcol (UDP), or TCP_UDP protocols. Classic Load Balancers make routing decisions at either the transport layer, using TCP or Secure Sockets Layer (SSL) protocols, or at the application layer, using HTTP/HTTPS

In Ihrer Organisation besteht möglicherweise eine Sicherheits- oder Compliance-Anforderung, dass Load Balancer Datenverkehr von Benutzern nur über sichere Protokolle wie HTTPS oder SSL/TLS akzeptieren.

Dieses Muster bietet eine Sicherheitskontrolle, die eine EventBridge Amazon-Regel verwendet, um die `CreateListener` und `ModifyListener` API-Aufrufe für Application Load Balancer und Network Load Balancer sowie die `CreateLoadBalancerListeners` und `CreateLoadBalancer` API-Aufrufe für Classic Load Balancers zu überwachen. Wenn HTTP, TCP/UDP oder TCP_UDP für das Listener-Protokoll des Load Balancers verwendet wird, ruft das Steuerelement eine Lambda-Funktion auf. Die Lambda-Funktion veröffentlicht eine Nachricht an ein Amazon Simple Notification Service (Amazon SNS) -Thema, um eine Benachrichtigung zu senden, die die Load Balancer-Details enthält.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Eine E-Mail-Adresse, an die Sie die Benachrichtigung über den Verstoß erhalten möchten

- Ein Amazon Simple Storage Service (Amazon S3) -Bucket zum Speichern der Lambda-Code-ZIP-Datei

Einschränkungen

- Diese Sicherheitskontrolle sucht nicht nach vorhandenen Load Balancers, es sei denn, die Load Balancer-Listener werden aktualisiert.
- Diese Sicherheitskontrolle ist regional und muss in den AWS-Regionen eingesetzt werden, die Sie überwachen möchten.

Architektur

Zieltechnologie-Stack

- Lambda-Funktion
- Amazon SNS-Thema
- EventBridge Regel

Zielarchitektur

Automatisierung und Skalierung

- Wenn Sie AWS Organizations verwenden, können Sie AWS Cloudformation verwenden, StackSets um diese Vorlage in mehreren Konten bereitzustellen, die überwacht werden sollen.

Tools

- AWS CloudFormation — AWS CloudFormation ist ein Service, der Sie bei der Modellierung und Einrichtung von AWS-Ressourcen unterstützt, indem Infrastruktur als Code verwendet wird.
- Amazon EventBridge — Amazon EventBridge liefert einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, SaaS-Anwendungen (Software as a Service) und AWS-Services und leitet diese Daten an Ziele wie Lambda-Funktionen weiter.
- AWS Lambda — Lambda unterstützt die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern.

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice, der für eine Vielzahl von Speicherlösungen verwendet werden kann, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Bewährte Methoden

Stellen Sie sicher, dass das verwendete SNS-Thema nicht öffentlich zugänglich ist. Weitere Informationen finden Sie in der AWS-Dokumentation.

Epen

Laden Sie den Lambda-Code hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Wählen oder erstellen Sie auf der Amazon S3 S3-Konsole einen S3-Bucket mit einem eindeutigen Namen, der keine führenden Schrägstr iche enthält. Ein S3-Bucket-Name ist weltweit eindeutig , und der Namespace wird von allen AWS-Konten gemeinsam genutzt. Ihr S3-Bucket muss sich in derselben Region befinden wie der Load Balancer, der evaluiert wird.	Cloud-Architekt
Laden Sie den Lambda-Code in den S3-Bucket hoch.	Laden Sie die Lambda-Code-ZIP-Datei, die im Abschnitt „Anlagen“ bereitgestellt wird,	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	in den definierten S3-Bucket hoch.	
Stellen Sie die CloudFormation AWS-Vorlage bereit.	Stellen Sie auf der CloudFormation AWS-Konsole, in derselben AWS-Region wie der S3-Bucket, die Vorlage bereit, die im Abschnitt „Anlagen“ bereitgestellt wird. Geben Sie im nächsten Epic die Werte für die Parameter an.	Cloud-Architekt

CloudFormation Parameter

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Nennen Sie den S3-Bucket.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epic erstellt haben.	Cloud-Architekt
Geben Sie das Amazon S3 S3-Präfix an.	Geben Sie den Speicherort der Lambda-Code-ZIP-Datei in Ihrem S3-Bucket an, ohne vorangestellte Schrägstriche (z. B.). `<directory>/<file-name>.zip`	Cloud-Architekt
Geben Sie den ARN des SNS-Themas an.	Geben Sie das SNS-Thema Amazon Resource Name (ARN) an, wenn Sie ein vorhandenes SNS-Thema für Benachrichtigungen über Verstöße verwenden möchten. Um ein neues SNS-Thema	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	zu erstellen, behalten Sie den Wert `None` (Standardwert) bei.	
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine aktive E-Mail-Adresse an, um Amazon SNS SNS-Benachrichtigungen zu erhalten.	Cloud-Architekt
Definieren Sie die Protokollierungsebene.	Definieren Sie die Protokollierungsebene und die Häufigkeit für Ihre Lambda-Funktion. `Info`bezeichnet detaillierte Informationsmeldungen über den Fortschritt der Anwendung. `Error`bezeichnet Fehlerereignisse, die es der Anwendung dennoch ermöglichen könnten, weiter zu laufen. `Warning`bezeichnet potenziell schädliche Situationen.	Cloud-Architekt

Stellen Sie die CloudFormation Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die Vorlage für herunter.	Laden Sie die CloudFormation Vorlage herunter, die im Abschnitt Anlagen bereitgestellt wird.	Cloud-Architekt
Erstellen Sie den Stack.	Navigieren Sie in derselben Region wie der S3-Bucket zur CloudFormation Servicekonsole und stellen Sie die	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	heruntergeladene Vorlage bereit. Einzelheiten zu den Parametern finden Sie im vorherigen Epos.	
Überprüfen Sie die Ressourcen.	Nachdem der Stack vollständig erstellt wurde, navigieren Sie zur Registerkarte Ressourcen und überprüfen Sie die Ressourcen. Mit der Vorlage werden die folgenden Ressourcen erstellt: • EventBridge Regel • Lambda-Funktion • Lambda-Ausführungsrolle • Lambda-Zugriffsberechtigung	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die Vorlage erfolgreich bereitgestellt wurde und ein neues SNS-Thema erstellt wurde, wird eine Abonnement-E-Mail-Nachricht an die in den Parametern angegebene E-Mail-Adresse gesendet. Sie müssen dieses E-Mail-Abonnement bestätigen, um Benachrichtigungen über Verstöße zu erhalten.	Cloud-Architekt

Fehlerbehebung

Problem	Lösung
Die Erstellung des Stacks ist fehlgeschlagen. Während ist ein Fehler aufgetreten GetObject. S3-Fehlercode: PermanentRedirect. S3-Fehler meldung: Der Bucket befindet sich in dieser Region: xx-xxxx-1. Bitte verwenden Sie diese Region, um die Anfrage erneut zu versuchen.	Stellen Sie sicher, dass die S3-Bucket-Region und die Region, in der der Stack bereitgestellt wird, identisch sind.
Die Erstellung des Stacks ist fehlgeschlagen. Der Laufzeitparameter von Python3.6 wird für die Erstellung oder Aktualisierung von AWS Lambda Lambda-Funktionen nicht mehr unterstützt.	Aktualisieren Sie die heruntergeladene Vorlage in Zeile 186 von Python-Version 3.6 auf 3.9.

Zugehörige Ressourcen

- Einen Stack auf der CloudFormation AWS-Konsole erstellen
- AWS Lambda
- Was ist ein Classic Load Balancer?
- Was ist ein Application Load Balancer?
- Was ist ein Network Load Balancer?
- Bewährte Methoden für die Arbeit mit AWS Lambda Lambda-Funktionen
- CloudFormation Bewährte AWS-Methoden

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Stellen Sie sicher, dass die Verschlüsselung für Amazon EMR-Daten im Ruhezustand beim Start aktiviert ist

Erstellt von Priyanka Chaudhary (AWS)

Übersicht

Dieses Muster bietet eine Sicherheitskontrolle für die Überwachung der Verschlüsselung von Amazon EMR-Clustern auf Amazon Web Services (AWS).

Die Datenverschlüsselung verhindert, dass nicht autorisierte Benutzer Daten auf einem Cluster und in den dazugehörigen Datenspeichersystemen lesen können. Dazu gehören Daten, die während der Übertragung durch das Netzwerk abgefangen werden können (sogenannte Daten während der Übertragung), und Daten, die auf persistenten Medien gespeichert werden, sogenannte Daten im Ruhezustand. Daten im Ruhezustand in Amazon Simple Storage Service (Amazon S3) können auf zwei Arten verschlüsselt werden.

- Serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3)
- Serverseitige Verschlüsselung mit AWS Key Management Service (AWS KMS) -Schlüsseln (SSE-KMS), eingerichtet mit Richtlinien, die für Amazon EMR geeignet sind.

Diese Sicherheitskontrolle überwacht API-Aufrufe und initiiert ein Amazon CloudWatch Events-Ereignis am RunJobFlow. Der Trigger ruft AWS Lambda auf, das ein Python-Skript ausführt. Die Funktion ruft die EMR-Cluster-ID aus der JSON-Eingabe des Ereignisses ab und ermittelt anhand der folgenden Prüfungen, ob eine Sicherheitsverletzung vorliegt.

1. Prüfen Sie, ob ein EMR-Cluster mit einer Amazon EMR-spezifischen Sicherheitskonfiguration verknüpft ist.
2. Wenn dem EMR-Cluster eine Amazon EMR-spezifische Sicherheitskonfiguration zugeordnet ist, überprüfen Sie, ob sie aktiviert Encryption-at-Rest ist.
3. Wenn nicht Encryption-at-Rest aktiviert, senden Sie eine Amazon Simple Notification Service (Amazon SNS) -Benachrichtigung, die den EMR-Clusternamen, Details zum Verstoß, die AWS-Region, das AWS-Konto und den Lambda Amazon Resource Name (ARN) enthält, von dem diese Benachrichtigung stammt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein S3-Bucket für die Lambda-Code-.zip-Datei
- Eine E-Mail-Adresse, an die Sie die Benachrichtigung über den Verstoß erhalten möchten
- Die Amazon EMR-Protokollierung ist deaktiviert, sodass alle API-Protokolle abgerufen werden können

Einschränkungen

- Diese Detective Control ist regional und muss in den AWS-Regionen eingesetzt werden, die Sie überwachen möchten.

Produktversionen

- Amazon EMR Version 4.8.0 und höher

Architektur

Zieltechnologie-Stack

- Amazon EMR
- Veranstaltung Amazon CloudWatch Events
- Lambda-Funktion
- Amazon SNS

Zielarchitektur

Automatisierung und Skalierung

Wenn Sie AWS Organizations verwenden, können Sie AWS Cloudformation verwenden, StackSets um diese Vorlage in mehreren Konten bereitzustellen, die Sie überwachen möchten.

Tools

Tools

- AWS CloudFormation ist ein Service, mit dem Sie AWS-Ressourcen mithilfe von Infrastructure as Code modellieren und einrichten können.
- Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit.
- Amazon EMR ist eine verwaltete Cluster-Plattform, die die Ausführung von Big-Data-Frameworks vereinfacht.
- AWS Lambda unterstützt die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern.
- Amazon S3 ist ein hoch skalierbarer Objektspeicherservice, der für eine Vielzahl von Speicherlösungen verwendet werden kann, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon SNS koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Code

- Die EMREncryption AtRest .zip- und EMREncryption AtRest .yml-Dateien für dieses Projekt sind als Anhang verfügbar.

Epen

Definieren Sie den S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Wählen oder erstellen Sie auf der Amazon S3 S3-Konsole einen S3-Bucket mit einem eindeutigen Namen, der keine führenden Schrägstriche	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	enthält. Ein S3-Bucket-Name ist weltweit eindeutig, und der Namespace wird von allen AWS-Konten gemeinsam genutzt. Ihr S3-Bucket muss sich in derselben Region befinden wie der Amazon EMR-Cluster, der bewertet wird.	

Laden Sie den Lambda-Code in den S3-Bucket hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Lambda-Code in den S3-Bucket hoch.	Laden Sie die Lambda-Code-ZIP-Datei, die im Abschnitt „Anlagen“ bereitgestellt wird, in den definierten S3-Bucket hoch.	Cloud-Architekt

Stellen Sie die CloudFormation AWS-Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation AWS-Vorlage bereit.	Stellen Sie auf der CloudFormation AWS-Konsole, in derselben Region wie Ihr S3-Bucket, die CloudFormation AWS-Vorlage bereit, die als Anlage zu diesem Muster bereitgestellt wird. Geben Sie im nächsten Epic die Werte für die Parameter an. Weitere Informationen zur	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bereitstellung von CloudFormation AWS-Vorlagen finden Sie im Abschnitt „Verwandte Ressourcen“.	

Vervollständigen Sie die Parameter in der CloudFormation AWS-Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Nennen Sie den S3-Bucket.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epic erstellt haben.	Cloud-Architekt
Geben Sie den Amazon S3 S3-Schlüssel ein.	<file-name>Geben Sie den Speicherort der Lambda-Code-ZIP-Datei in Ihrem S3-Bucket ohne führende Schrägstriche an (z. B.<directory>/.zip).	Cloud-Architekt
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine aktive E-Mail-Adresse an, um Amazon SNS SNS-Benachrichtigungen zu erhalten.	Cloud-Architekt
Definieren Sie die Protokollierungsebene.	Definieren Sie die Protokollierungsebene und die Häufigkeit für Ihre Lambda-Funktion. „Info“ bezeichnet detaillierte Informationsmeldungen zum Fortschritt der Anwendung. „Fehler“ bezeichnet Fehlerereignisse, die dazu führen könnten, dass die Anwendung weiterhin	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ausgeführt werden kann. „Warnung“ steht für potenziell schädliche Situationen.	

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail-Nachricht an die angegebene E-Mail-Adresse. Sie müssen dieses E-Mail-Abonnement bestätigen, um Benachric htigungen über Verstöße zu erhalten.	Cloud-Architekt

Zugehörige Ressourcen

- Einen Stack auf der CloudFormation AWS-Konsole erstellen
- AWS Lambda
- Amazon EMR-Verschlüsselungsoptionen

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Stellen Sie sicher, dass ein IAM-Profil mit einer EC2 Instance verknüpft ist

Erstellt von Mansi Suratwala (AWS)

Übersicht

Dieses Muster stellt eine CloudFormation AWS-Sicherheitskontrollvorlage bereit, die eine automatische Benachrichtigung einrichtet, wenn eine Verletzung des AWS Identity and Access Management (IAM) -Profilverstoßes für eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance auftritt.

Ein Instance-Profil ist ein Container für eine IAM-Rolle, den Sie verwenden können, um Rolleninformationen an eine EC2 Instance zu übergeben, wenn die Instance gestartet wird.

Amazon CloudWatch Events leitet diese Prüfung ein, wenn AWS EC2 Amazon-API-Aufrufe auf der Grundlage der `ReplaceIamInstanceProfileAssociation` Aktionen `RunInstancesAssociateIamInstanceProfile`, und CloudTrail protokolliert. Der Trigger ruft eine AWS-Lambda-Funktion auf, die mithilfe eines Amazon CloudWatch Events-Ereignisses nach einem IAM-Profil sucht.

Wenn kein IAM-Profil vorhanden ist, initiiert die Lambda-Funktion eine Amazon Simple Notification Service (Amazon SNS) -E-Mail-Benachrichtigung, die die Amazon Web Services (AWS) -Konto-ID und die AWS-Region enthält.

Wenn ein IAM-Profil vorhanden ist, sucht die Lambda-Funktion nach Platzhaltereinträgen in den Richtliniendokumenten. Wenn die Platzhaltereinträge vorhanden sind, wird eine Amazon SNS SNS-Benachrichtigung ausgelöst, die Ihnen hilft, erweiterte Sicherheit zu implementieren. Die Benachrichtigung enthält den Namen des IAM-Profils, das Ereignis, die EC2 Instance-ID, den Namen der verwalteten Richtlinie, den Verstoß, die Konto-ID und die Region.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives Konto
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket für die Lambda-Code-.zip-Datei

Einschränkungen

- Die CloudFormation AWS-Vorlage darf nur für die `ReplaceIamInstanceProfileAssociation` Aktionen `RunInstancesAssociateIamInstanceProfile`, und bereitgestellt werden.
- Die Sicherheitskontrolle überwacht nicht die Trennung von IAM-Profilen.
- Die Sicherheitskontrolle überprüft nicht, ob die IAM-Richtlinien, die mit dem IAM-Profil der Instanz verknüpft sind, geändert wurden. EC2
- Die Sicherheitskontrolle berücksichtigt nicht unterstützte Berechtigungen auf Ressourcenebene, für die die Verwendung von erforderlich ist. `"Resource":*`

Architektur

Zieltechnologie-Stack

- Amazon EC2
- AWS CloudTrail
- Amazon CloudWatch
- AWS Lambda
- Amazon S3
- Amazon SNS

Zielarchitektur

Automatisierung und Skalierung

Sie können die CloudFormation AWS-Vorlage mehrfach für verschiedene AWS-Regionen und Konten verwenden. Sie müssen die Vorlage für jedes Konto oder jede Region nur einmal starten.

Tools

Tools

- Amazon EC2 — Amazon EC2 bietet skalierbare Rechenkapazität (virtuelle Server) in der AWS-Cloud.
- AWS CloudTrail — AWS CloudTrail unterstützt Sie bei der Steuerung, Einhaltung von Vorschriften sowie Betriebs- und Risikoprüfungen Ihres AWS-Kontos. Aktionen, die von einem Benutzer,

einer Rolle oder einem AWS-Service ausgeführt werden, werden als Ereignisse in aufgezeichnet CloudTrail.

- Amazon CloudWatch Events — Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit.
- AWS Lambda — AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon S3 — Amazon S3 bietet hoch skalierbaren Objektspeicher, den Sie für eine Vielzahl von Speicherlösungen verwenden können, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon SNS — Amazon SNS ermöglicht es Anwendungen und Geräten, Benachrichtigungen aus der Cloud zu senden und zu empfangen.

Code

- Eine ZIP-Datei des Projekts ist als Anhang verfügbar.

Epen

Definieren Sie den S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Um die Lambda-Code-ZIP-Datei zu hosten, wählen oder erstellen Sie einen S3-Bucket mit einem eindeutigen Namen, der keine führenden Schrägstriche enthält. Ein S3-Bucket-Name ist weltweit eindeutig, und der Namespace wird von allen AWS-Konten gemeinsam genutzt. Ihr S3-Bucket muss sich in derselben	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Region befinden wie die EC2 Instance, die evaluiert wird.	

Laden Sie den Lambda-Code in den S3-Bucket hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Lambda-Code in den S3-Bucket hoch.	Laden Sie den Lambda-Code, der im Abschnitt Anlagen bereitgestellt wird, in den S3-Bucket hoch. Der S3-Bucket muss sich in derselben Region befinden wie die EC2 Instanz, die ausgewertet wird.	Cloud-Architekt

Stellen Sie die CloudFormation AWS-Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation AWS-Vorlage bereit.	Stellen Sie die CloudFormation AWS-Vorlage bereit, die als Anlage zu diesem Muster bereitgestellt wird. Geben Sie im nächsten Epos die Werte für die Parameter an.	Cloud-Architekt

Vervollständigen Sie die Parameter in der CloudFormation AWS-Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Nennen Sie den S3-Bucket.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epic erstellt haben.	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den S3-Schlüssel ein.	Geben Sie den Speicherort der Lambda-Code-ZIP-Datei in Ihrem S3-Bucket an, ohne vorangestellte Schrägstriche (z. B.). `<directory>/<file-name>.zip`	Cloud-Architekt
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine aktive E-Mail-Adresse an, um Amazon SNS SNS-Benachrichtigungen zu erhalten.	Cloud-Architekt
Definieren Sie die Protokollierungsebene.	Definieren Sie die Protokollierungsebene und die Häufigkeit für Ihre Lambda-Funktion. `Info`bezeichnet detaillierte Informationsmeldungen über den Fortschritt der Anwendung. `Error`bezeichnet Fehlerereignisse, die es der Anwendung dennoch ermöglichen könnten, weiter zu laufen. `Warning`bezeichnet potenziell schädliche Situationen.	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail-Nachricht an die angegebene	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	E-Mail-Adresse. Sie müssen dieses E-Mail-Abonnement bestätigen, um Benachric htigungen über Verstöße zu erhalten.	

Zugehörige Ressourcen

- Erstellen eines S3-Buckets
- Dateien in einen S3-Bucket hochladen
- Instanzprofile verwenden
- Erstellen einer CloudWatch Ereignisregel, die bei einem AWS-API-Aufruf mit AWS ausgelöst wird CloudTrail

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Stellen Sie sicher, dass ein Amazon Redshift Redshift-Cluster bei der Erstellung verschlüsselt ist

Erstellt von Mansi Suratwala (AWS)

Übersicht

Dieses Muster stellt eine CloudFormation AWS-Vorlage bereit, die Sie automatisch benachrichtigt, wenn ein neuer Amazon Redshift Redshift-Cluster ohne Verschlüsselung erstellt wird.

Die CloudFormation AWS-Vorlage erstellt ein Amazon CloudWatch Events-Ereignis und eine AWS-Lambda-Funktion. Das Ereignis überwacht, ob ein Amazon Redshift Redshift-Cluster erstellt oder aus einem Snapshot über AWS CloudTrail wiederhergestellt wird. Wenn der Cluster ohne Verschlüsselung mit dem AWS Key Management Service (AWS KMS) oder dem Cloud Hardware Security Model (HSM) im AWS-Konto erstellt wird, wird eine Lambda-Funktion CloudWatch initiiert, die Ihnen eine Amazon Simple Notification Service (Amazon SNS) -Benachrichtigung sendet, die Sie über den Verstoß informiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine Virtual Private Cloud (VPC) mit einer Cluster-Subnetzgruppe und einer zugehörigen Sicherheitsgruppe.

Einschränkungen

- Die CloudFormation AWS-Vorlage kann nur für die `RestoreFromClusterSnapshot` Aktionen `CreateCluster` und bereitgestellt werden.

Architektur

Zieltechnologie-Stack

- Amazon Redshift
- AWS CloudTrail

- Amazon CloudWatch
- AWS Lambda
- Amazon Simple Storage Service (Amazon-S3)
- Amazon SNS

Zielarchitektur

Automatisierung und Skalierung

Sie können die CloudFormation AWS-Vorlage mehrfach für verschiedene AWS-Regionen und Konten verwenden. Sie müssen sie in jeder Region oder jedem Konto nur einmal ausführen.

Tools

Tools

- Amazon Redshift — Amazon Redshift ist ein vollständig verwalteter Data-Warehouse-Service im Petabyte-Bereich in der Cloud. Amazon Redshift ist in Ihren Data Lake integriert, sodass Sie Ihre Daten nutzen können, um neue Erkenntnisse für Ihr Unternehmen und Ihre Kunden zu gewinnen.
- AWS CloudTrail — AWS CloudTrail ist ein AWS-Service, der Sie bei der Implementierung von Governance, Compliance sowie Betriebs- und Risikoprüfungen Ihres AWS-Kontos unterstützt. Aktionen, die von einem Benutzer, einer Rolle oder einem AWS-Service ausgeführt werden, werden als Ereignisse in aufgezeichnet CloudTrail.
- Amazon CloudWatch Events — Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit.
- AWS Lambda — AWS Lambda unterstützt die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern. AWS Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon S3 — Amazon S3 ist ein hoch skalierbarer Objektspeicherservice, den Sie für eine Vielzahl von Speicherlösungen verwenden können, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon SNS — Amazon SNS ist ein Webservice, der die Zustellung oder den Versand von Nachrichten zwischen Herausgebern und Kunden koordiniert und verwaltet, einschließlich Webservern und E-Mail-Adressen.

Code

- Eine ZIP-Datei des Projekts ist als Anhang verfügbar.

Epen

Definieren Sie den S3-Bucket

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Wählen oder erstellen Sie auf der Amazon S3 S3-Konsole einen S3-Bucket. Dieser S3-Bucket hostet die Lambda-Co de-.zip-Datei. Ihr S3-Bucket muss sich in derselben Region befinden wie der Amazon Redshift Redshift-Cluster, der evaluiert wird. Der Name des S3-Buckets darf keine führenden Schrägstriche enthalten.	Cloud-Architekt

Laden Sie den Lambda-Code in den S3-Bucket hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Lambda-Code in den S3-Bucket hoch.	Laden Sie den im Abschnitt Anlagen bereitgestellten Lambda-Code in den S3-Bucket hoch. Der S3-Bucket muss sich in derselben Region befinden wie der Amazon Redshift Redshift-Cluster, der evaluiert wird.	Cloud-Architekt

Stellen Sie die CloudFormation AWS-Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation AWS-Vorlage bereit.	Stellen Sie die CloudFormation AWS-Vorlage bereit, die als Anlage zu diesem Muster bereitgestellt wird. Geben Sie im nächsten Epos die Werte für die Parameter an.	Cloud-Architekt

Vervollständigen Sie die Parameter in der CloudFormation AWS-Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Nennen Sie den S3-Bucket.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epic erstellt haben.	Cloud-Architekt
Geben Sie den S3-Schlüssel ein.	Geben Sie den Speicherort der Lambda-Code-ZIP-Datei in Ihrem S3-Bucket an, ohne vorangestellte Schrägstriche (z. B.). `<directory>/<file-name>.zip`	Cloud-Architekt
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine aktive E-Mail-Adresse an, um Amazon SNS SNS-Benachrichtigungen zu erhalten.	Cloud-Architekt
Definieren Sie die Protokollierungsebene.	Definieren Sie die Protokollierungsebene und die Häufigkeit für Ihre Lambda-Funktion. `Info`bezeichnet detaillierte Informationsmeldungen über den Fortschritt der	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anwendung. `Error`bezeichnet Fehlerereignisse, die es der Anwendung dennoch ermöglichen könnten, weiter zu laufen. `Warning`bezeichnet potenziell schädliche Situationen.	

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail an die angegebene E-Mail-Adresse. Sie müssen dieses E-Mail-Abonnement bestätigen, um Benachrichtigungen über Verstöße zu erhalten.	Cloud-Architekt

Zugehörige Ressourcen

- Erstellen eines S3-Buckets
- Dateien in einen S3-Bucket hochladen
- Erstellen einer CloudWatch Ereignisregel, die bei einem AWS-API-Aufruf mit AWS ausgelöst wird CloudTrail
- Einen Amazon Redshift Redshift-Cluster erstellen

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Exportieren Sie einen Bericht über AWS IAM Identity Center-Identitäten und deren Zuweisungen mithilfe von PowerShell

Erstellt von Jorge Pava (AWS), Tschad Miles (AWS), Frank Allotta (AWS) und Manideep Reddy Gillela (AWS)

Übersicht

Wenn Sie AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) verwenden, um den Single Sign-On (SSO) -Zugriff auf all Ihre Amazon Web Services (AWS) -Konten und Cloud-Anwendungen zentral zu verwalten, kann das Melden und Prüfen dieser Zuweisungen über die AWS-Managementkonsole mühsam und zeitaufwändig sein. Dies gilt insbesondere, wenn Sie über Berechtigungen für einen Benutzer oder eine Gruppe für Dutzende oder Hunderte von AWS-Konten berichten.

Für viele wäre das ideale Tool zum Anzeigen dieser Informationen eine Tabellenkalkulationsanwendung wie Microsoft Excel. Dies kann Ihnen helfen, die von AWS Organizations verwalteten Daten für Ihre gesamte Organisation zu filtern, zu suchen und zu visualisieren.

Dieses Muster beschreibt, wie AWS-Tools verwendet werden PowerShell , um einen Bericht über SSO-Identitätskonfigurationen im IAM Identity Center zu generieren. Der Bericht ist als CSV-Datei formatiert und enthält den Identitätsnamen (Principal), den Identitätstyp (Benutzer oder Gruppe), Konten, auf die die Identität zugreifen kann, und die Berechtigungssätze. Nachdem Sie diesen Bericht generiert haben, können Sie ihn in Ihrer bevorzugten Anwendung öffnen, um die Daten nach Bedarf zu suchen, zu filtern und zu prüfen. Die folgende Abbildung zeigt Beispieldaten in einer Tabellenkalkulationsanwendung.

> **Important**
>
> Da dieser Bericht vertrauliche Informationen enthält, empfehlen wir Ihnen dringend, ihn sicher zu speichern und nur auf einer bestimmten need-to-know Grundlage weiterzug eben.

Voraussetzungen und Einschränkungen

Voraussetzungen

- IAM Identity Center und AWS Organizations, konfiguriert und aktiviert.
- PowerShell, installiert und konfiguriert. Weitere Informationen finden Sie unter Installation PowerShell (Microsoft-Dokumentation).
- AWS-Tools für PowerShell, installiert und konfiguriert. Aus Leistungsgründen empfehlen wir dringend, die modularisierte Version von AWS Tools for zu installieren PowerShell, genannt`AWS.Tools`. Jeder AWS-Service wird von einem eigenen, kleinen Modul unterstützt. Geben Sie in der PowerShell Shell die folgenden Befehle ein, um die für dieses Muster benötigten Module zu installieren: `AWS.Tools.Installer`Organizations,`SSOAdmin`, und`IdentityStore`.

  ```
  Install-Module AWS.Tools.Installer
  Install-AWSToolsModule -Name Organizations, SSOAdmin, IdentityStore
  ```

  Weitere Informationen finden Sie unter AWS.Tools unter Windows installieren oder AWS.Tools unter Linux oder macOS installieren (AWS-Tools für die Dokumentation). PowerShell Wenn Sie bei der Installation der Module eine Fehlermeldung erhalten, lesen Sie den Abschnitt zur Fehlerbehebung in diesem Muster.
- Die AWS-Befehlszeilenschnittstelle (AWS CLI) oder das AWS-SDK müssen zuvor mit funktionierenden Anmeldeinformationen konfiguriert werden, indem Sie einen der folgenden Schritte ausführen:
  - Verwenden Sie die AWS-CLI `aws configure` Weitere Informationen finden Sie unter Schnellkonfiguration (AWS-CLI-Dokumentation).
  - Konfigurieren Sie AWS CLI oder AWS Cloud Development Kit (AWS CDK), um temporären Zugriff über eine AWS Identity and Access Management (IAM) -Rolle zu erhalten. Weitere Informationen finden Sie unter Abrufen von IAM-Rollenanmeldedaten für den CLI-Zugriff (IAM Identity Center-Dokumentation).
- Ein benanntes Profil für die AWS-CLI, das Anmeldeinformationen für einen IAM-Prinzipal gespeichert hat, der:
  - Hat Zugriff auf das Verwaltungskonto von AWS Organizations oder das delegierte Administratorkonto für IAM Identity Center

- Wurden die `AWSSSOReadOnly` und von `AWSSSODirectoryReadOnly` AWS verwalteten Richtlinien darauf angewendet?

Weitere Informationen finden Sie unter Verwenden von benannten Profilen (AWS-CLI-Dokumentation) und AWS-verwaltete Richtlinien (IAM-Dokumentation).

Einschränkungen

- Die AWS-Zielkonten müssen als Organisation in AWS Organizations verwaltet werden.

Produktversionen

- Für alle Betriebssysteme wird empfohlen, PowerShell Version 7.0 oder höher zu verwenden.

Architektur

Zielarchitektur

1. Der Benutzer führt das Skript in einer PowerShell Befehlszeile aus.
2. Das Skript geht von dem benannten Profil für AWS CLI aus. Dadurch wird Zugriff auf das IAM Identity Center gewährt.
3. Das Skript ruft die SSO-Identitätskonfigurationen aus dem IAM Identity Center ab.
4. Das Skript generiert eine CSV-Datei in demselben Verzeichnis auf der lokalen Workstation, in dem das Skript gespeichert ist.

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Mit AWS IAM Identity Center können Sie den Single Sign-On (SSO) -Zugriff auf all Ihre AWS-Konten und Cloud-Anwendungen zentral verwalten.

- Bei den AWS-Tools für PowerShell handelt es sich um eine Reihe von PowerShell Modulen, die Ihnen helfen, Operationen auf Ihren AWS-Ressourcen von der PowerShell Befehlszeile aus zu skripten.

Andere Tools

- PowerShellist ein Automatisierungs- und Konfigurationsverwaltungsprogramm von Microsoft, das unter Windows, Linux und macOS läuft.

Epen

Generieren Sie den Bericht

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereite das Drehbuch vor.	1. Kopieren Sie das PowerShell Skript im Abschnitt Zusätzliche Informationen dieses Musters. 2. Definieren Sie im `Param` Abschnitt für Ihre AWS-Umgebung die Werte für die folgenden Variablen: • `OutputFile` — Der Dateiname des Berichts. • `ProfileName` — Das benannte AWS-CLI-Profil, das Sie zum Generieren des Berichts verwenden möchten. • `Region`— Die AWS-Region, in der IAM Identity Center bereitgestellt wird. Eine vollständige Liste der Regionen	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	und ihrer Codes finden Sie unter Regionale Endpunkte. 3. Speichern Sie das Skript mit dem Dateinamen `SSO-Report.ps1` .	

Führen Sie das Skript aus.	Es wird empfohlen, dass Sie Ihr benutzerdefiniertes Skript in der PowerShell Shell mit dem folgenden Befehl ausführen.
	`.\SSO-Report.ps1`
	Sie können das Skript auch von einer anderen Shell aus ausführen, indem Sie den folgenden Befehl eingeben.
	`pwsh .\SSO-Report.ps1`
	Das Skript generiert eine CSV-Datei im selben Verzeichnis wie die Skriptdatei.
		Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Analysieren Sie Berichtsdaten.	Die CSV-Ausgabedatei enthält die Header AccountNa mePermissionSet, Principal und Type. Öffnen Sie diese Datei in Ihrer bevorzugt en Tabellenkalkulatio nsanwendung. Sie können eine Datentabelle erstellen, um die Ausgabe zu filtern und zu sortieren.	Cloud-Administrator

Fehlerbehebung

Problem	Lösung

`The term 'Get-<parameter>' is not recognized as the name of a cmdlet, function, script file, or operable program.`-Fehler	Die AWS-Tools für PowerShell oder ihre Module sind nicht installiert. Geben Sie in der PowerShell Shell die folgenden Befehle ein, um die AWS-Tools für PowerShell und die für dieses Muster benötigten Module zu installie ren: `AWS.Tools.Installer` `Organizat ions` ,`SSOAdmin`, und`IdentityStore` .
	`Install-Module AWS.Tools.Installer`
	`Install-AWSToolsModule -Name Organizations, SSOAdmin, IdentityS tore`

`No credentials specified or obtained from persisted/shell defaults`-Fehler	Vergewissern Sie sich im Abschnitt Prepare the script in the Epics, dass Sie die `Region` Variablen `ProfileName` und korrekt eingegeben haben. Stellen Sie sicher, dass die Einstellungen und Anmeldeinformationen im genannten Profil über ausreichende Berechtig

Problem	Lösung
	ungen für die Verwaltung von IAM Identity Center verfügen.
`Authenticode Issuer …` Fehler bei der Installation der AWS.Tools-Module	Fügen Sie den `-SkipPublisherCheck` Parameter am Ende des `Install-AWSToolsModule` Befehls hinzu.

`Get-ORGAccountList : Assembly AWSSDK.SSO could not be found or loaded.`-Fehler	Dieser Fehler kann auftreten, wenn benannte AWS-CLI-Profile angegeben werden, AWS CLI für die Authentifizierung von Benutzern mit IAM Identity Center konfiguriert ist und AWS CLI so konfiguriert ist, dass aktualisierte Authentifizierungstoken automatisch abgerufen werden. Gehen Sie wie folgt vor, um diesen Fehler zu beheben:
	1. Geben Sie den folgenden Befehl ein, um zu bestätigen, dass die `SSOOIDC` Module `SSO` und installiert sind.
	`Install-AWSToolsModule SSO, SSOOIDC`
	2. Fügen Sie die folgenden Zeilen in das Skript unter dem `param()` Block ein.
	`Import-Module AWS.Tools.SSO`
	`Import-Module AWS.Tools.SSOOIDC`

Zugehörige Ressourcen

- Wo werden die Konfigurationseinstellungen gespeichert? (AWS-CLI-Dokumentation)
- Konfiguration der AWS-CLI für die Verwendung von AWS IAM Identity Center (AWS-CLI-Dokumentation)

- Benannte Profile verwenden (AWS-CLI-Dokumentation)

Zusätzliche Informationen

Stellen Sie im folgenden Skript fest, ob Sie die Werte für die folgenden Parameter aktualisieren müssen:

- Wenn Sie ein benanntes Profil in AWS CLI verwenden, um auf das Konto zuzugreifen, in dem IAM Identity Center konfiguriert ist, aktualisieren Sie den `$ProfileName` Wert.
- Wenn IAM Identity Center in einer anderen AWS-Region als der Standardregion für Ihre AWS-CLI- oder AWS-SDK-Konfiguration bereitgestellt wird, aktualisieren Sie den `$Region` Wert, sodass die Region verwendet wird, in der IAM Identity Center bereitgestellt wird.
- Wenn keine dieser Situationen zutrifft, ist kein Skript-Update erforderlich.

```
param (
    # The name of the output CSV file
    [String] $OutputFile  = "SSO-Assignments.csv",
    # The AWS CLI named profile
    [String] $ProfileName = "",
    # The AWS Region in which IAM Identity Center is configured
    [String] $Region      = ""
)
$Start = Get-Date; $OrgParams = @{}
If ($Region){ $OrgParams.Region = $Region}
if ($ProfileName){$OrgParams.ProfileName = $ProfileName}
$SSOParams   = $OrgParams.Clone(); $IdsParams = $OrgParams.Clone()
$AccountList = Get-ORGAccountList @OrgParams | Select-Object Id, Name
$SSOinstance = Get-SSOADMNInstanceList @OrgParams
$SSOParams['InstanceArn']       = $SSOinstance.InstanceArn
$IdsParams['IdentityStoreId']   = $SSOinstance.IdentityStoreId
$PSsets       = @{}; $Principals   = @{}
$Assignments  = @(); $AccountCount = 1; Write-Host ""
foreach ($Account in $AccountList) {
    $Duration = New-Timespan -Start $Start -End (Get-Date) | ForEach-Object
 {[Timespan]::New($_.Days, $_.Hours, $_.Minutes, $_.Seconds)}
    Write-Host "`r$Duration - Account $AccountCount of $($AccountList.Count)
 (Assignments:$($Assignments.Count))        " -NoNewline
    $AccountCount++
    foreach ($PS in Get-SSOADMNPermissionSetsProvisionedToAccountList -AccountId
 $Account.Id @SSOParams) {
```

```
        if (-not $PSsets[$PS]) {$PSsets[$PS] = (Get-SSOADMNPermissionSet @SSOParams -
PermissionSetArn $PS).Name;$APICalls++}
        $AssignmentsResponse = Get-SSOADMNAccountAssignmentList @SSOParams -
PermissionSetArn $PS -AccountId $Account.Id
        if ($AssignmentsResponse.NextToken) {$AccountAssignments =
 $AssignmentsResponse.AccountAssignments}
        else {$AccountAssignments = $AssignmentsResponse}
        While ($AssignmentsResponse.NextToken) {
            $AssignmentsResponse = Get-SSOADMNAccountAssignmentList @SSOParams -
PermissionSetArn $PS -AccountId $Account.Id -NextToken $AssignmentsResponse.NextToken
            $AccountAssignments += $AssignmentsResponse.AccountAssignments}
        foreach ($Assignment in $AccountAssignments) {
            if (-not $Principals[$Assignment.PrincipalId]) {
                $AssignmentType = $Assignment.PrincipalType.Value
                $Expression     = "Get-IDS"+$AssignmentType+" @IdsParams -"+
$AssignmentType+"Id "+$Assignment.PrincipalId
                $Principal      = Invoke-Expression $Expression
                if ($Assignment.PrincipalType.Value -eq "GROUP")
 { $Principals[$Assignment.PrincipalId] = $Principal.DisplayName }
                else { $Principals[$Assignment.PrincipalId] = $Principal.UserName }
            }
            $Assignments += [PSCustomObject]@{
                AccountName     = $Account.Name
                PermissionSet   = $PSsets[$PS]
                Principal       = $Principals[$Assignment.PrincipalId]
                Type            = $Assignment.PrincipalType.Value}
        }
    }
}
$Duration = New-Timespan -Start $Start -End (Get-Date) | ForEach-Object
 {[Timespan]::New($_.Days, $_.Hours, $_.Minutes, $_.Seconds)}
Write-Host "`r$($AccountList.Count) accounts done in $Duration. Outputting result to
 $OutputFile"
$Assignments | Sort-Object Account | Export-CSV -Path $OutputFile -Force
```

Überwachen und korrigieren Sie das geplante Löschen von AWS-KMS-Schlüsseln

Erstellt von Mikesh Khanal (AWS) und Ramya Pulipaka (AWS)

Übersicht

In der Amazon Web Services (AWS) -Cloud kann das Löschen eines AWS Key Management Services (AWS KMS) -Schlüssels zu Datenverlust führen. Durch das Löschen werden das Schlüsselmaterial und alle mit dem AWS-KMS-Schlüssel verknüpften Metadaten entfernt, und der Vorgang kann nicht rückgängig gemacht werden. Nachdem ein AWS-KMS-Schlüssel gelöscht wurde, können Sie die Daten, die unter diesem AWS-KMS-Schlüssel verschlüsselt wurden, nicht mehr entschlüsseln, sodass Daten nicht wiederhergestellt werden können.

Mit diesem Muster wird eine Überwachung eingerichtet, mit Benachrichtigungen, wenn eine Anwendung oder ein Benutzer einen AWS-KMS-Schlüssel zum Löschen plant. Wenn Sie eine Benachrichtigung erhalten, sollten Sie das Löschen des AWS-KMS-Schlüssels abbrechen und Ihre Entscheidung, ihn zu löschen, noch einmal überdenken. Das Muster verwendet das AWS Systems Manager Manager-Automatisierungsrunbook, AWSConfigRemediation-CancelKeyDeletionum das Abbrechen des Löschens eines AWS-KMS-Schlüssels zu erleichtern.

> **Note**
>
> Die CloudFormation Vorlage des Musters muss in allen AWS-Regionen bereitgestellt werden, in denen Sie das Löschen von AWS-KMS-Schlüsseln überwachen möchten.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Verständnis der folgenden AWS-Services:
  - Amazon EventBridge
  - AWS KMS
  - Amazon-Simple-Notification-Service (Amazon-SNS)
  - AWS Systems Manager

Einschränkungen

- Jede Anpassung der Lösung erfordert Kenntnisse der CloudFormation AWS-Vorlagen und der in diesem Muster verwendeten AWS-Services.
- Derzeit verwendet diese Lösung den Standard-Event-Bus und kann an die Anforderungen angepasst werden. Weitere Informationen zum benutzerdefinierten Event-Bus finden Sie in der AWS-Dokumentation.

Architektur

Zieltechnologie-Stack

- Amazon EventBridge
- AWS KMS
- Amazon SNS
- AWS Systems Manager
- Automatisierung mit den folgenden Methoden:
  - AWS-Befehlszeilenschnittstelle (AWS CLI) oder AWS-SDK
  - CloudFormation AWS-Stapel

Zielarchitektur

1. Das Löschen eines AWS-KMS-Schlüssels ist geplant.
2. Das geplante Löschereignis wird anhand einer Regel ausgewertet. EventBridge
3. Die EventBridge Regel bezieht sich auf das Thema Amazon SNS.
4. Die EventBridge Regel initiiert die Systems Manager Manager-Automatisierung und die Runbooks.
5. Die Runbooks brechen das Löschen ab.

Automatisierung und Skalierung

Der CloudFormation Stack stellt alle erforderlichen Ressourcen und Dienste bereit, damit diese Lösung funktioniert. Das Muster kann unabhängig in einem einzigen Konto oder mit AWS CloudFormation StackSets für mehrere unabhängige Konten oder eine Organisation ausgeführt werden.

```
aws cloudformation create-stack --stack-name  <stack-name>\
    --template-body file://<Full-Path-of-file> \
    --parameters ParameterKey=,ParameterValue= \
    --capabilities CAPABILITY_NAMED_IAM
```

Tools

Tools

- AWS CloudFormation — AWS CloudFormation ist ein Service, der Sie bei der Modellierung und Einrichtung Ihrer Amazon Web Services Services-Ressourcen unterstützt, sodass Sie weniger Zeit mit der Verwaltung dieser Ressourcen verbringen und sich mehr auf Ihre Anwendungen konzentrieren können, die auf AWS ausgeführt werden. Sie können eine CloudFormation Vorlage verwenden, um Stacks in einem AWS-Konto in einer AWS-Region zu erstellen. Die Vorlage beschreibt alle gewünschten AWS-Ressourcen und CloudFormation stellt diese Ressourcen für Sie bereit und konfiguriert sie.
- AWS CLI — Die AWS-Befehlszeilenschnittstelle (AWS CLI) ist ein Open-Source-Tool, mit dem Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.
- Amazon EventBridge — Amazon EventBridge ist ein serverloser Event-Bus-Service, der Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen verbindet. EventBridge liefert einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen und AWS-Services und leitet diese Daten an Ziele wie AWS Lambda weiter. EventBridge vereinfacht den Prozess der Erstellung ereignisgesteuerter Architekturen.
- AWS KMS — AWS Key Management Service (AWS KMS) ist ein verwalteter Service zur Erstellung und Steuerung von AWS-KMS-Schlüsseln, den Verschlüsselungsschlüsseln, die zur Verschlüsselung Ihrer Daten verwendet werden.
- AWS SDKs — Zu den AWS-Tools gehören, SDKs sodass Sie Anwendungen auf AWS in der Programmiersprache Ihrer Wahl entwickeln und verwalten können.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) ist ein verwalteter Service, der die Nachrichtenzustellung von Verlagen an Abonnenten (auch bekannt als Produzenten und Verbraucher) ermöglicht. Herausgeber kommunizieren asynchron mit Abonnenten, indem sie eine Nachricht erstellen und an ein Thema senden, bei dem es sich um einen logischen Zugriffspunkt und Kommunikationskanal handelt.
- AWS Systems Manager — AWS Systems Manager ist ein AWS-Service, mit dem Sie Ihre Infrastruktur auf AWS anzeigen und steuern können. Mithilfe der Systems Manager Manager-Konsole können Sie betriebliche Aufgaben in Ihren AWS-Ressourcen automatisieren. Systems

Manager unterstützt Sie bei der Aufrechterhaltung von Sicherheit und Compliance, indem er Ihre verwalteten Instances scannt und über festgestellte Richtlinienverstöße (oder Abhilfemaßnahmen ergreifen) berichtet.

Code

- Die `alerting_ct_logs.yaml` CloudFormation Vorlage für das Projekt ist beigefügt.

Epen

Bereiten Sie das AWS-Konto vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren und konfigurieren Sie AWS CLI.	Installieren Sie AWS CLI Version 2. Konfigurieren Sie anschließend die Einstellungen für die Sicherheitsanmeldedaten für eine Identität, das Standardausgabeformat und die AWS-Standardregion, die die AWS-CLI für die Interaktion mit AWS verwendet. Die Identität muss über die erforderlichen Berechtigungen verfügen, um die Aufgaben auszuführen.	Entwickler, Sicherheitsingenieur

Stellen Sie die CloudFormation AWS-Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie die CloudFormation Vorlage herunter.	Laden Sie den Anhang in einen lokalen Pfad auf	Entwickler, Sicherheitsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ihrem Computer herunter und extrahieren Sie die `alerting_ct_logs.yaml` Vorlagendatei.	
Stellen Sie die Vorlage bereit.	Führen Sie im Terminalfenster, in dem das AWS-Kontoprofil konfiguriert wurde, den folgenden Befehl aus. `aws cloudformation create-stack --stack-name <stack_name> \ --capabilities <Value> \ --template-body file://<Full_Path> \ --parameters ParameterKey=DestinationEmailAddress,ParameterValue=<Value> \ ParameterKey=SNSTopicName,ParameterValue=<Value> \ ParameterKey=EnableRemediation ,ParameterValue=<Value> \ ParameterKey=AutomationAssumeRole, ParameterValue=<Value>` Geben Sie im nächsten Schritt Werte für die Vorlagenparameter ein.	Entwickler, Sicherheitsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vervollständigen Sie die Vorlagenparameter.	Geben Sie die erforderlichen Werte für die Parameter ein. • `DestinationEmailAddress` — Die E-Mail-Adresse, an die eine Warnung gesendet werden soll, wenn ein AWS-KMS-Schlüssel gelöscht werden soll. • `SNSTopicName` — Der Name des Amazon SNS SNS-Themas. • `EnableRemediation` — Abbruch der geplanten Schlüssellöschung mithilfe eines Systems Manager Manager-Runbooks. Zulässige Werte sind `true` und `false`. • `AutomationAssumeRole` — Der Amazon-Ressourcenname (ARN) der Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Weitere Informationen finden Sie in der AWSConfig Remediation-Cancel KeyDeletionDokumentation im Abschnitt Erforderliche IAM-Berechtigungen. • `Capabilities` — Damit AWS CloudFormation	Entwickler, Sicherheitsingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den Stack erstellen kann, müssen Sie ausdrückl ich bestätigen, dass Ihre Stack-Vorlage bestimmte Funktionen enthält.	

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Überprüfen Sie Ihren E-Mail-Posteingang und wählen Sie in der E-Mail-Na chricht, die Sie von Amazon SNS erhalten, die Option Abonnement bestätigen aus. Ein Webbrowser-Fenster wird geöffnet und zeigt eine Abonnementbestätigung und Ihre Abonnement-ID an.	Entwickler, Sicherheitsingenie ur

Zugehörige Ressourcen

Referenzen

- Eine Regel für einen AWS-Service erstellen
- Erstellen eines CloudWatch Amazon-Alarms zur Erkennung der Verwendung eines AWS-KMS-Schlüssels, dessen Löschung noch aussteht

Tutorials und Videos

- Wie fange ich mit Amazon an EventBridge
- Tiefer Einblick in Amazon EventBridge (AWS Online Tech Talks)

AWS-Werkstatt

- Mit EventBridge Regeln arbeiten

Zusätzliche Informationen

Der folgende Code enthält Beispiele für die Erweiterung der Lösung zur Überwachung und Benachrichtigung von Änderungen an AWS. Die Beispiele umfassen vordefinierte Muster und benutzerdefinierte Muster. Weitere Informationen finden Sie unter Ereignisse und Ereignismuster in EventBridge.

```
EventPattern:
        source:
        - aws.kms
        detail-type:
        - AWS API Call via CloudTrail
        detail:
          eventSource:
          - kms.amazonaws.com
          eventName:
          - ScheduleKeyDeletion
```

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Identifizieren Sie öffentliche Amazon S3 S3-Buckets mithilfe AWS Organizations von Security Hub

Erstellt von Mourad Cherfaoui (AWS), Arun Chandapillai (AWS) und Parag Nagwekar (AWS)

Übersicht

Dieses Muster zeigt Ihnen, wie Sie einen Mechanismus zur Identifizierung öffentlicher Amazon Simple Storage Service (Amazon S3) -Buckets in Ihren AWS Organizations Konten erstellen. Der Mechanismus verwendet Kontrollen aus dem Standard AWS Foundational Security Best Practices (FSBP) AWS Security Hub zur Überwachung von Amazon S3 S3-Buckets. Sie können Amazon verwenden, EventBridge um Security Hub Hub-Ergebnisse zu verarbeiten und diese Ergebnisse dann in einem Amazon Simple Notification Service (Amazon SNS) -Thema zu veröffentlichen. Stakeholder in Ihrer Organisation können das Thema abonnieren und sofort per E-Mail über die Ergebnisse informiert werden.

Neue Amazon S3 S3-Buckets und ihre Objekte erlauben standardmäßig keinen öffentlichen Zugriff. Sie können dieses Muster in Szenarien verwenden, in denen Sie die Amazon S3 S3-Standardkonfigurationen an die Anforderungen Ihrer Organisation anpassen müssen. Dies könnte beispielsweise ein Szenario sein, in dem Sie einen Amazon S3 S3-Bucket haben, der eine öffentlich zugängliche Website hostet, oder Dateien, die jeder im Internet aus Ihrem Amazon S3 S3-Bucket lesen können muss.

Security Hub wird häufig als zentraler Dienst eingesetzt, um alle Sicherheitsfeststellungen zu konsolidieren, einschließlich solcher, die sich auf Sicherheitsstandards und Compliance-Anforderungen beziehen. Es gibt andere AWS-Services , die Sie verwenden können, um öffentliche Amazon S3 S3-Buckets zu erkennen, aber dieses Muster verwendet eine bestehende Security Hub Hub-Bereitstellung mit minimaler Konfiguration.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Einrichtung mit AWS mehreren Konten und einem eigenen Security Hub-Administratorkonto
- Security Hub und AWS Config, aktiviert in dem AWS-Region , den Sie überwachen möchten

> **Note**
>
> Sie müssen die regionsübergreifende Aggregation in Security Hub aktivieren, wenn Sie mehrere Regionen von einer einzigen Aggregationsregion aus überwachen möchten.

- Benutzerberechtigungen für den Zugriff und die Aktualisierung des Security Hub-Administratorkontos, Lesezugriff auf alle Amazon S3 S3-Buckets in der Organisation und Berechtigungen zum Deaktivieren des öffentlichen Zugriffs (falls erforderlich)

Architektur

Das folgende Diagramm zeigt eine Architektur für die Verwendung von Security Hub zur Identifizierung öffentlicher Amazon S3 S3-Buckets.

Das Diagramm zeigt den folgenden Arbeitsablauf:

1. Security Hub überwacht die Konfiguration von Amazon S3 S3-Buckets in allen AWS Organizations Konten (einschließlich des Administratorkontos) mithilfe der S3.2- und S3.3-Steuerelemente des FSBP-Sicherheitsstandards und erkennt, ob ein Bucket als öffentlich konfiguriert ist.
2. Das Security Hub-Administratorkonto greift von allen Mitgliedskonten aus auf die Ergebnisse (einschließlich der Ergebnisse für S3.2 und S3.3) zu.
3. Security Hub sendet automatisch alle neuen Ergebnisse und alle Aktualisierungen vorhandener Ergebnisse EventBridge als Security Hub Hub-Ergebnisse — Importierte Ereignisse. Dazu gehören Ereignisse für Ergebnisse sowohl aus dem Administrator- als auch aus dem Mitgliedskonto.
4. Eine EventBridge Regel filtert nach Ergebnissen aus S3.2 und S3.3, die den Workflow-Status „Von“`FAILED`, den Workflow-Status „von`NEW`“ und „Von“ haben. `ComplianceStatus` `RecordState` `ACTIVE`
5. Regeln verwenden die Ereignismuster, um Ereignisse zu identifizieren und sie nach dem Abgleich an ein Amazon SNS SNS-Thema zu senden.
6. Ein Amazon SNS SNS-Thema sendet die Ereignisse an seine Abonnenten (z. B. per E-Mail).
7. Sicherheitsanalysten, die für den Empfang der E-Mail-Benachrichtigungen bestimmt sind, überprüfen den betreffenden Amazon S3 S3-Bucket.

8. Wenn der Bucket für den öffentlichen Zugriff zugelassen ist, setzt der Sicherheitsanalyst den Workflow-Status des entsprechenden Ergebnisses in Security Hub auf`SUPPRESSED`. Andernfalls setzt der Analyst den Status auf`NOTIFIED`. Dadurch werden future Benachrichtigungen für den Amazon S3 S3-Bucket vermieden und das Benachrichtigungsrauschen reduziert.
9. Wenn der Workflow-Status auf festgelegt ist`NOTIFIED`, überprüft der Sicherheitsanalyst das Ergebnis zusammen mit dem Bucket-Besitzer, um festzustellen, ob der öffentliche Zugriff gerechtfertigt ist und den Datenschutz- und Datenschutzanforderungen entspricht. Die Untersuchung führt dazu, dass entweder der öffentliche Zugriff auf den Bucket aufgehoben oder der öffentliche Zugriff genehmigt wird. Im letzteren Fall setzt der Sicherheitsanalyst den Workflow-Status auf`SUPPRESSED`.

> **Note**
>
> Das Architekturdiagramm gilt sowohl für regionsübergreifende Aggregationsbereitstellungen als auch für regionsübergreifende Aggregationsbereitstellungen. In den Konten A, B und C im Diagramm kann Security Hub zu derselben Region gehören wie das Administratorkonto oder zu verschiedenen Regionen gehören, wenn die regionsübergreifende Aggregation aktiviert ist.

Tools

- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. EventBridge liefert einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, SaaS-Anwendungen (Software as a Service) und AWS-Services. EventBridge leitet diese Daten an Ziele wie Amazon SNS SNS-Themen und AWS Lambda -Funktionen weiter, wenn die Daten benutzerdefinierten Regeln entsprechen.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- AWS Security Hubbietet einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS. Security Hub hilft Ihnen auch dabei, Ihre AWS Umgebung anhand von Industriestandards und

Best Practices zu überprüfen. Security Hub sammelt Sicherheitsdaten von Across AWS-Konten, Services und unterstützten Produkten von Drittanbietern und hilft dann bei der Analyse von Sicherheitstrends und der Identifizierung der Sicherheitsprobleme mit der höchsten Priorität.

Epen

Security Hub Hub-Konten konfigurieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie Security Hub in AWS Organizations Konten.	Informationen zur Aktivierung von Security Hub in den Organisationskonten, in denen Sie Amazon S3 S3-Buckets überwachen möchten, finden Sie in den Richtlinien unter Security Hub-Administratorkonto (Konsole) einrichten und Mitgliedskonten verwalten, die zu einer Organisation gehören, in der Security Hub Hub-Dokumentation.	AWS-Administrator
(Optional) Aktivieren Sie die regionsübergreifende Aggregation.	Wenn Sie Amazon S3 S3-Buckets in mehreren Regionen von einer einzigen Region aus überwachen möchten, richten Sie die regionsübergreifende Aggregation ein.	AWS-Administrator
Aktivieren Sie die S3.2- und S3.3-Steuerelemente für den FSBP-Sicherheitsstandard.	Sie müssen die S3.2- und S3.3-Steuerelemente für den FSBP-Sicherheitsstandard aktivieren.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	1. Um S3.2-Steuerelemente zu aktivieren, folgen Sie den Anweisungen unter [S3.2] S3-Buckets sollten öffentlichen Lesezugriff verbieten in der Security Hub Hub-Dokumentation. 2. Um S3.3-Steuerelemente zu aktivieren, folgen Sie den Anweisungen in [3] S3-Buckets sollten öffentlichen Schreibzugriff verbieten in der Security Hub Hub-Dokumentation.	

Richten Sie die Umgebung ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie das Amazon SNS SNS-Thema und das E-Mail-Abonnement.	1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon SNS SNS-Konsole. 2. Wählen Sie im Navigationsbereich Topics (Themen) und Create topic (Thema erstellen). 3. Wählen Sie unter Type (Typ) die Option Standard aus. 4. Geben Sie unter Name einen Namen für Ihr	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Thema ein (z. B. public-s3-buckets). 5. Wählen Sie Thema erstellen aus. 6. Wählen Sie auf der Registerkarte Abonnements für Ihr Thema die Option Abonnement erstellen aus. 7. Wählen Sie unter Protocol die Option Email aus. 8. Geben Sie für Endpoint die E-Mail-Adresse ein, an die die Benachrichtigungen gesendet werden sollen. Sie können die E-Mail-Adresse eines AWS Administrators, IT-Experten oder Infosec-Experten verwenden. 9. Wählen Sie Create subscription (Abonnement erstellen) aus. Um zusätzliche E-Mail-Abonnements zu erstellen, wiederholen Sie bei Bedarf die Schritte 6—8.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die EventBridge Regel.	1. Öffnen Sie die EventBridge -Konsole. 2. Wählen Sie im Abschnitt Erste Schritte die Option EventBridge Regel und dann Regel erstellen aus. 3. Geben Sie auf der Detailseite Regel definieren unter Name einen Namen für Ihre Regel ein (z. B. public-s3-buckets). Wählen Sie Weiter aus. 4. Wählen Sie im Abschnitt Ereignismuster die Option Muster bearbeiten aus. 5. Kopieren Sie den folgenden Code, fügen Sie ihn in den Event-Pattern-Code-Editor ein und wählen Sie dann Weiter. `{ "source": ["aws.securityhub"], "detail-type": ["Security Hub Findings - Imported"], "detail": { "findings": { "Compliance": { "Status": ["FAILED"] }, "RecordState": ["ACTIVE"],`	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Workflow": {
	"Status":
	["NEW"]
	},
	"ProductF
	ields": {
	"ControlId":
	["S3.2", "S3.3"]
	}
	}
	}
	}</pre>
	6. Wählen Sie auf der Seite Ziel (e) auswählen unter Ziel auswählen die Option SNS-Thema als Ziel aus, und wählen Sie dann das Thema aus, das Sie zuvor erstellt haben.
	7. Wählen Sie Weiter, erneut Weiter und anschließend Regel erstellen aus.	

Fehlerbehebung

Problem	Lösung
Ich habe einen Amazon S3 S3-Bucket mit aktiviertem öffentlichen Zugriff, erhalte dafür aber keine E-Mail-Benachrichtigungen.	Dies könnte daran liegen, dass der Bucket in einer anderen Region erstellt wurde und die regionsübergreifende Aggregation im Security Hub-Administratorkonto nicht aktiviert ist. Um dieses Problem zu beheben, aktivieren Sie die regionsübergreifende Aggregation oder implementieren Sie die Lösung dieses Musters

Problem	Lösung
	in der Region, in der sich Ihr Amazon S3 S3-Bucket derzeit befindet.

Zugehörige Ressourcen

- Was ist? AWS Security Hub (Security Hub Hub-Dokumentation)
- AWS FSBP-Standard (Fundational Security Best Practices) (Security Hub Hub-Dokumentation)
- AWS Security Hub Skripts zur Aktivierung mehrerer Konten (Labs)AWS
- Bewährte Sicherheitsmethoden für Amazon S3 (Amazon S3 S3-Dokumentation)

Zusätzliche Informationen

Workflow für die Überwachung öffentlicher Amazon S3 S3-Buckets

Der folgende Workflow veranschaulicht, wie Sie die öffentlichen Amazon S3 S3-Buckets in Ihrer Organisation überwachen können. Der Workflow geht davon aus, dass Sie die Schritte im Thema Amazon SNS konfigurieren und in der E-Mail-Abonnementstory zu diesem Muster ausgeführt haben.

1. Sie erhalten eine E-Mail-Benachrichtigung, wenn ein Amazon S3 S3-Bucket mit öffentlichem Zugriff konfiguriert ist.
   - Wenn der Bucket für den öffentlichen Zugriff zugelassen ist, setzen Sie den Workflow-Status des entsprechenden Ergebnisses `SUPPRESSED` im Security Hub-Administratorkonto auf. Dadurch wird verhindert, dass Security Hub weitere Benachrichtigungen für diesen Bucket ausgibt, und doppelte Benachrichtigungen können vermieden werden.
   - Wenn der Bucket nicht für den öffentlichen Zugriff zugelassen ist, setzen Sie den Workflow-Status des entsprechenden Ergebnisses im Security Hub-Administratorkonto auf`NOTIFIED`. Dadurch wird verhindert, dass Security Hub weitere Benachrichtigungen für diesen Bucket von Security Hub ausgibt, und Rauschen kann vermieden werden.
2. Wenn der Bucket möglicherweise vertrauliche Daten enthält, schalten Sie den öffentlichen Zugriff sofort aus, bis die Überprüfung abgeschlossen ist. Wenn Sie den öffentlichen Zugriff deaktivieren, ändert Security Hub den Workflow-Status auf`RESOLVED`. Dann werden die E-Mail-Benachrichtigungen für den Bucket beendet.

3. Suchen Sie den Benutzer, der den Bucket als öffentlich konfiguriert hat (z. B. mithilfe von AWS CloudTrail), und starten Sie eine Überprüfung. Die Überprüfung führt dazu, dass entweder der öffentliche Zugriff auf den Bucket aufgehoben oder der öffentliche Zugriff genehmigt wird. Wenn der öffentliche Zugriff genehmigt wurde, setzen Sie den Workflow-Status des entsprechenden Ergebnisses auf`SUPPRESSED`.

Erfassung und Analyse von AWS-Sicherheitsprotokollen in Microsoft Sentinel

Erstellt von Ivan Girardi (AWS) und Sebastian Wenzel (AWS)

Übersicht

Dieses Muster beschreibt, wie die Erfassung von AWS Sicherheitsprotokollen wie AWS CloudTrail Protokollen, Amazon Logs-Daten, Amazon VPC Flow CloudWatch Logs-Daten und GuardDuty Amazon-Ergebnissen in Microsoft Sentinel automatisiert wird. Wenn Ihr Unternehmen Microsoft Sentinel als SIEM-System (Security Information and Event Management) verwendet, können Sie damit Protokolle zentral überwachen und analysieren, um sicherheitsrelevante Ereignisse zu erkennen. Sobald die Protokolle verfügbar sind, werden sie automatisch in weniger als 5 Minuten an einen Amazon Simple Storage Service (Amazon S3) -Bucket übermittelt. Dies kann Ihnen helfen, Sicherheitsereignisse in Ihrer AWS Umgebung schnell zu erkennen.

Microsoft Sentinel nimmt CloudTrail Protokolle in einem tabellarischen Format auf, das den ursprünglichen Zeitstempel für die Aufzeichnung des Ereignisses enthält. Die Struktur der aufgenommenen Protokolle ermöglicht Abfragefunktionen mithilfe der Kusto Query Language in Microsoft Sentinel.

Das Muster stellt eine Überwachungs- und Warnlösung bereit, die Aufnahmefehler in weniger als 1 Minute erkennt. Es beinhaltet auch ein Benachrichtigungssystem, das das externe SIEM überwachen kann. Sie verwenden AWS CloudFormation , um die erforderlichen Ressourcen im Protokollierungskonto bereitzustellen.

Zielpublikum

Dieses Muster wird Benutzern empfohlen, die Erfahrung mit AWS Control Tower,, AWS Organizations CloudFormation, AWS Identity and Access Management (IAM) und AWS Key Management Service (AWS KMS) haben.

Voraussetzungen und Einschränkungen

Voraussetzungen

Die folgenden Voraussetzungen müssen für die Bereitstellung dieser Lösung erfüllt sein:

- Aktiv AWS-Konten , die als Organisation in einer AWS Control Tower landing zone verwaltet werden AWS Organizations und Teil einer solchen sind. Die Organisation sollte über ein eigenes

Konto für die Protokollierung verfügen. Anweisungen finden Sie in der AWS Organizations Dokumentation unter Organisation erstellen und konfigurieren.

- Ein CloudTrail Trail, der Ereignisse für die gesamte Organisation protokolliert und Protokolle in einem Amazon S3 S3-Bucket im Logging-Konto speichert. Eine Anleitung finden Sie unter Einen Trail für eine Organisation erstellen.
- Im Logging-Konto die Berechtigungen, eine bestehende IAM-Rolle anzunehmen, die über die folgenden Berechtigungen verfügt:
  - Stellen Sie die in der bereitgestellten CloudFormation Vorlage definierten Ressourcen bereit.
  - Stellen Sie die bereitgestellte CloudFormation Vorlage bereit.
  - Ändern Sie die AWS KMS Schlüsselrichtlinie, wenn die Protokolle mit einem vom Kunden verwalteten Schlüssel verschlüsselt sind.
- AWS Command Line Interface (AWS CLI), installiert und konfiguriert.
- Ein Microsoft Azure-Konto mit einem Abonnement für die Nutzung von Microsoft Sentinel.
- Aktivieren und richten Sie Microsoft Sentinel ein. Anweisungen finden Sie unter Microsoft Sentinel aktivieren und erste Funktionen und Inhalte in der Microsoft Sentinel-Dokumentation.
- Erfüllen Sie die Voraussetzungen für die Einrichtung des Microsoft Sentinel S3-Connectors.

Einschränkungen

- Diese Lösung leitet die Sicherheitsprotokolle aus einem Amazon S3 S3-Bucket im Protokollierungskonto an Microsoft Sentinel weiter. Anweisungen zum Senden der Protokolle an Amazon S3 werden nicht ausdrücklich bereitgestellt.
- Dieses Muster enthält Anweisungen für den Einsatz in einer AWS Control Tower landing zone. Die Verwendung von AWS Control Tower ist jedoch nicht erforderlich.
- Diese Lösung ist mit einer Umgebung kompatibel, in der der Amazon S3 S3-Logging-Bucket durch Service-Kontrollrichtlinien (SCPs) eingeschränkt ist, wie z. B. Änderungen an der Bucket-Richtlinie für AWS Control Tower erstellte Amazon S3 S3-Buckets im Log Archive nicht zulassen.
- Dieses Muster enthält Anweisungen für die Weiterleitung von CloudTrail Protokollen. Sie können diese Lösung jedoch so anpassen, dass auch andere Protokolle gesendet werden, die Microsoft Sentinel unterstützt, z. B. CloudWatch Protokolle aus Logs, Amazon VPC Flow Logs und. GuardDuty
- In den Anweisungen wird AWS CLI für die Bereitstellung der CloudFormation Vorlage verwendet, Sie können aber auch die verwenden. AWS Management Console Anweisungen finden Sie unter

Die AWS CloudFormation Konsole verwenden. Wenn Sie die Konsole zum Bereitstellen des Stacks verwenden, stellen Sie den Stack genauso bereit AWS-Region wie den Logging-Bucket.

- Diese Lösung stellt eine Amazon Simple Queue Service (Amazon SQS) -Warteschlange bereit, um Amazon S3 S3-Benachrichtigungen zuzustellen. Die Warteschlange enthält Nachrichten mit den Pfaden von Objekten, die in den Amazon S3 S3-Bucket hochgeladen wurden, keine tatsächlichen Daten. Die Warteschlange verwendet SSE-SQS-Verschlüsselung, um den Inhalt der Nachrichten zu schützen. Wenn Sie die SQS-Warteschlange mit SSE-KMS verschlüsseln möchten, können Sie einen vom Kunden verwalteten KMS-Schlüssel verwenden. Weitere Informationen finden Sie unter Verschlüsselung im Ruhezustand in Amazon SQS.

Architektur

Dieser Abschnitt bietet einen allgemeinen Überblick über die Architektur, die durch den Beispielcode eingerichtet wird. Das folgende Diagramm zeigt die Ressourcen, die im Protokollierungskonto bereitgestellt werden, um Protokolle aus einem vorhandenen Amazon S3 S3-Bucket in Microsoft Sentinel aufzunehmen.

Das Architekturdiagramm zeigt die folgenden Ressourceninteraktionen:

1. Im Logging-Konto übernimmt Microsoft Sentinel über OpenID Connect (OIDC) eine IAM-Rolle, um auf Protokolle in einem bestimmten Amazon S3 S3-Bucket und einer Amazon SQS SQS-Warteschlange zuzugreifen.
2. Amazon Simple Notification Service (Amazon SNS) und Amazon S3 werden AWS KMS für die Verschlüsselung verwendet.
3. Amazon S3 sendet bei jedem Empfang neuer Protokolle Benachrichtigungen an die Amazon SQS SQS-Warteschlange.
4. Microsoft Sentinel überprüft Amazon SQS auf neue Nachrichten. Die Amazon SQS SQS-Warteschlange verwendet SSE-SQS-Verschlüsselung. Die Aufbewahrungsfrist für Nachrichten ist auf 14 Tage festgelegt.
5. Microsoft Sentinel ruft Nachrichten aus der Amazon SQS SQS-Warteschlange ab. Die Nachrichten enthalten den Pfad der hochgeladenen Amazon S3 S3-Objekte. Microsoft Sentinel nimmt diese Objekte aus dem Amazon S3 S3-Bucket in das Microsoft Azure-Konto auf.
6. Ein CloudWatch Alarm überwacht die Amazon SQS SQS-Warteschlange. Wenn innerhalb von 5 Minuten keine Nachrichten empfangen und aus der Amazon SQS SQS-Warteschlange gelöscht werden, wird eine Amazon SNS-Benachrichtigung ausgelöst, die eine E-Mail sendet.

AWS Control Tower hilft Ihnen bei der Einrichtung der grundlegenden Organisationseinheit (OU) und zentralisiert die CloudTrail Protokolle im Logging-Konto. Zum Schutz des Logging-Buckets ist außerdem SCPs eine obligatorische Implementierung erforderlich.

Wir haben die Zielarchitektur in einer AWS Control Tower landing zone bereitgestellt, dies ist jedoch nicht unbedingt erforderlich. In diesem Diagramm stellen die Ressourcen im Verwaltungskonto eine AWS Control Tower Bereitstellung und ein Protokoll dar, in CloudTrail dem Ereignisse für die gesamte Organisation protokolliert werden.

Dieses Muster konzentriert sich auf die Bereitstellung von Ressourcen im Protokollierungskonto. Wenn die in Amazon S3 in Ihrer AWS Control Tower landing zone gespeicherten Protokolle mit einem vom Kunden verwalteten KMS-Schlüssel verschlüsselt sind, müssen Sie die Schlüsselrichtlinie aktualisieren, damit Microsoft Sentinel die Protokolle entschlüsseln kann. In einer AWS Control Tower landing zone verwalten Sie die Schlüsselrichtlinie über das Verwaltungskonto, in dem der Schlüssel erstellt wurde.

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend AWS-Konten zu verwalten.
- Amazon CloudWatch hilft Ihnen dabei, die Kennzahlen Ihrer AWS Ressourcen und der Anwendungen, auf denen Sie laufen, AWS in Echtzeit zu überwachen.
- AWS Control Towerhilft Ihnen bei der Einrichtung und Verwaltung einer Umgebung AWS mit mehreren Konten und befolgt dabei bewährte Methoden.
- AWS Key Management Service (AWS KMS) hilft Ihnen dabei, kryptografische Schlüssel zu erstellen und zu kontrollieren, um Ihre Daten zu schützen.
- AWS Organizationsist ein Kontoverwaltungsdienst, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie erstellen und zentral verwalten.
- Amazon Simple Queue Service (Amazon SQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere Tools

- Microsoft Sentinel ist ein cloudnatives SIEM-System, das Sicherheitsorchestrierung, Automatisierung und Reaktion (SOAR) bietet.

Code-Repository

Der Code für dieses Muster ist in den AWS Sicherheitsprotokollen GitHub Ingest and Analyze im Microsoft Sentinel-Repository verfügbar.

Bewährte Methoden

- Folgen Sie dem Prinzip der geringsten Rechte (IAM-Dokumentation).
- Folgen Sie den Best Practices für AWS Control Tower Administratoren (Dokumentation).AWS Control Tower
- Folgen Sie den AWS CloudFormation bewährten Methoden (CloudFormation Dokumentation).
- Verwenden Sie Tools zur Codeanalyse wie cfn_nag, um die generierten Vorlagen zu scannen. CloudFormation Das Tool cfn_nag identifiziert potenzielle Sicherheitsprobleme in Vorlagen, indem es nach Mustern sucht. CloudFormation

Epen

Microsoft Sentinel mit Amazon S3 Connect

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bereiten Sie den Microsoft Sentinel S3-Connector vor.	1. Wählen Sie in Microsoft Sentinel Data Connectors aus. 2. Wählen Sie in der Data Connectors-Galerie Amazon Web Services S3 aus.	DevOps Ingenieur, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Wenn Sie den Connector nicht sehen, installieren Sie die Amazon Web Services Services-Lösung über den Content Hub in Microsoft Sentinel. 3. Wählen Sie im Detailber eich für den Connector die Option Connector-Seite öffnen aus. 4. Kopieren Sie im Abschnitt Konfiguration die externe ID. Sie benötigen diese ID später.	

Stellen Sie den CloudFormation Stack bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Geben Sie in einer Bash-Shel l den folgenden Befehl ein. Dadurch werden die Ingest- und AWS Analysesicherheits protokolle im Microsoft Sentinel-Repository geklont. `git clone https://g ithub.com/aws-samp`	DevOps Ingenieur, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`les/ingest-and-ana lyze-aws-security- logs-in-microsoft- sentinel.git`	
Nehmen Sie die IAM-Rolle im Logging-Konto an.	Nehmen Sie im Protokoll ierungskonto die IAM-Rolle an, die über die Berechtig ungen zum Bereitstellen des CloudFormation Stacks verfügt. Weitere Informationen zur Übernahme einer IAM-Rolle in der AWS CLI finden Sie unter Verwenden einer IAM-Rolle in der. AWS CLI	DevOps Ingenieur, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den Stack bereit.	Um den CloudFormation Stack bereitzustellen, geben Sie den folgenden Befehl ein, wobei: • `<Bucket name>` ist der Name des Amazon S3 S3-Buckets, der protokolliert wird. • `<Sentinel external ID>` ist die externe ID des Amazon S3 S3-Connectors in Microsoft Sentinel. • `<Email address>` ist eine gültige E-Mail-Adresse, an die Sie Benachrichtigungen erhalten möchten. • `<Customer managed key ARN>` ist der Amazon-Ressourcenname (ARN) des vom Kunden verwalteten KMS-Schlüssels. Geben Sie diesen Parameter nur an, wenn die Protokolle mit einem vom Kunden verwalteten KMS-Schlüssel verschlüsselt sind. • `<Suffix>` ist ein optionaler Parameter, um Konflikte mit Ressourcennamen zu vermeiden. • `<ARN for the OIDC provider>` ist der ARN des OIDC-Anbieters, falls er bereits existiert. Wenn	DevOps Ingenieur, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Sie diesen Parameter nicht angeben, wird der CloudFormation OIDC-Anbieter erstellt. **Important** Wenn die AWS Organisation mit Microsoft Code Defender überwacht wird, wurde der OIDC-Anbieter für Microsoft bereits bereitgestellt. Sie müssen diesen Parameter und den ARN des vorhandenen Anbieters angeben. `aws cloudformation deploy --stack-name cloudtrail-sentinel-integration \ --no-fail-on-empty-changeset \ --template-file template.yml \ --capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM CAPABILITY_AUTO_EXPAND \ --parameter-overrides \`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`ControlTowerS3BucketName="<Bucket name>" \ AzureWorkspaceID="<Sentinel external ID>" \ EmailAddress="<Email address>" \ KMSKeyArn="<Customer managed key ARN>" \ Suffix="<Suffix to avoid name conflicts>" \ OIDCProviderArn="<ARN for the OIDC provider>"`	
Ausgaben kopieren.	Kopieren Sie aus der Ausgabe des CloudFormation Stacks die Werte für `SentinelRoleArn` und `SentinelSQS`. Sie verwenden diese Werte später, um die Konfiguration in Microsoft Sentinel abzuschließen.	DevOps Ingenieur, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ändern Sie die Schlüssel richtlinie.	Wenn Sie keinen vom Kunden verwalteten KMS-Schlü ssel zum Verschlüsseln der Protokolle im Amazon S3 S3-Bucket verwenden, können Sie diesen Schritt übersprin gen. Wenn die Protokolle mit einem vom Kunden verwalteten KMS-Schlüssel verschlüsselt sind, ändern Sie die Schlüssel richtlinie, um Microsoft Sentinel die Erlaubnis zu erteilen, die Protokolle zu entschlüsseln. Es folgt eine Beispielschlüsselrichtlinie . Diese Beispielrichtlinie ermöglicht den kontoüber greifenden Zugriff, wenn sich der KMS-Schlüssel in einem anderen befindet. AWS-Konto `{ "Version": "2012-10-17", "Id": "key-policy", "Statement": [ ... { "Sid": "Grant access to decrypt", "Effect": "Allow", "Principa l": {`	DevOps Ingenieur, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"AWS": "<SentinelRoleArn>" }, "Action": "kms:Decrypt", "Resource": "<KeyArn>" }] }	

Konfigurieren Sie den Connector in Microsoft Sentinel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Schließen Sie die Konfiguration in Microsoft Sentinel ab.	1. Wählen Sie in Microsoft Sentinel Data Connectors aus. 2. Wählen Sie in der Data Connectors-Galerie Amazon Web Services S3 aus. 3. Wählen Sie im Detailbereich für den Connector die Option Connector-Seite öffnen aus. 4. Gehen Sie im Abschnitt Konfiguration wie folgt vor: a. Geben Sie im Feld Hinzuzufügende Rolle den `SentinelRoleArn` Wert ein, den Sie kopiert haben.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	b. Geben Sie im Feld SQS-URL den `SentinelSQS` Wert ein, den Sie kopiert haben. c. Wählen Sie in der Liste Zieltabelle die Option `AWSCloudTrail` . 5. Wählen Sie Add connection (Verbindung hinzufügen).	
Senden Sie Amazon S3 S3-Ereignisbenachrichtigungen an Amazon SQS.	Folgen Sie den Anweisungen unter Aktivieren und Konfigurieren von Ereignisbenachrichtigungen mithilfe der Amazon S3 S3-Konsole, um den Amazon S3 S3-Logging-Bucket so zu konfigurieren, dass Ereignisbenachrichtigungen an die Amazon SQS SQS-Warteschlange gesendet werden. Wenn es für die gesamte Organisation konfiguriert CloudTrail wurde, haben die Logs in diesem Bucket das Präfix `<OrgID>/AWSLogs/<OrgID>/` , wo sich die Organisations-ID `<OrgID>` befindet. Weitere Informationen finden Sie unter Details zu Ihrer Organisation anzeigen.	DevOps Ingenieur, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vergewissern Sie sich, dass die Protokolle aufgenommen wurden.	1. Warten Sie, bis die Protokolle in Microsoft Sentinel aufgenommen wurden. Dies kann mehrere Minuten dauern. 2. Öffnen Sie in Microsoft Sentinel die Amazon S3 Data Connector-Seite und gehen Sie dann wie folgt vor: • Vergewissern Sie sich, dass der Amazon S3 Data Connector-Status lautet`Connected` . • Überprüfen Sie das Datenvolumen im Diagramm „Empfangene Daten“. Weitere Informationen zur Überprüfung der Datenkonnektoraktivität finden Sie unter Datenkonnektor in der Microsoft-Dokumentation.	DevOps Ingenieur

Validieren Sie die Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vergleiche CloudWatch und Sentinel-Logs.	In der Standardkonfiguration von AWS Control Tower werden CloudTrail Protokolle an Amazon gesendet CloudWatch und im AWS	DevOps Ingenieur, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Control Tower Verwaltungskonto gespeichert. Weitere Informationen finden Sie unter Anmelden und Überwachen AWS Control Tower. Gehen Sie wie folgt vor, um sicherzustellen, dass Protokolle automatisch in Microsoft Sentinel aufgenommen werden: 1. Öffnen Sie die CloudWatch-Konsole. 2. Wählen Sie im Navigationsbereich Logs (Protokolle) und dann Logs Insights aus. 3. Wählen Sie unter Protokollgruppe (n) auswählen die Protokollgruppe aus, in der die CloudTrail Protokolle gespeichert werden, z. B. `aws-controltower/CloudTrailLogs` 4. Geben Sie im Feld des Abfrage-Editors ein`fields eventID`. 5. Wählen Sie Abfrage ausführen. 6. Wählen Sie Ergebnisse exportieren und anschließend Tabelle in die Zwischenablage kopieren (CSV).	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	7. Fügen Sie die Ergebnisse in einen Texteditor ein. 8. Ändern Sie das Format der Ausgabe, sodass es in einer Microsoft Sentinel-Abfrage verwendet werden kann. Im Folgenden finden Sie ein Beispiel, das die Kusto Query Language verwendet: `AWSCloudTrail	where AwsEventId in ('aa08b5fe-3bfb-391a-a14e-5fcebe14dab2', '9decd805-269c-451c-b75b-762f5dce59f9')` 9. Öffnen Sie in Microsoft Sentinel die Amazon S3 Data Connector-Seite. Wählen Sie neben dem Diagramm „Empfangene Daten“ die Option Gehe zu den Protokollanalysen aus. 10. Geben Sie im Feld des Abfrage-Editors die Abfrage ein, und wählen Sie dann Ausführen aus. 11. Stellen Sie in Microsoft Sentinel und sicher CloudWatch, dass die Anzahl der Einträge	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	identisch ist. Passen Sie den Zeitraum bei Bedarf an.	

Zugehörige Ressourcen

AWS Dokumentation und Ressourcen

- AWS CLI Befehlsreferenz (AWS CLI Dokumentation)
- Optional konfigurieren AWS KMS keys (AWS Control Tower Dokumentation)
- Verschlüsselung im Ruhezustand in Amazon SQS (Amazon SQS SQS-Dokumentation)
- Wie verhindere ich, dass Empfänger von Mailinglisten jeden auf der Liste von meinen Amazon SNS SNS-Themen-E-Mails abmelden? (Wissenszentrum)AWS

Microsoft-Dokumentation

- Connect Microsoft Sentinel mit Amazon Web Services, um Serviceprotokolldaten aufzunehmen AWS
- Kusto-Abfragesprache in Microsoft Sentinel

AWS Organizations Richtlinien mithilfe AWS CodePipeline von Amazon Bedrock als Code verwalten

Erstellt von Andre Cavalcante (AWS) und Mariana Pessoa de Queiroz (AWS)

Übersicht

Sie können Autorisierungsrichtlinien verwenden, AWS Organizations um den Zugriff für Prinzipale und Ressourcen in Ihren Mitgliedskonten zentral zu konfigurieren und zu verwalten. Richtlinien zur Servicesteuerung (SCPs) definieren die maximal verfügbaren Berechtigungen für die AWS Identity and Access Management (IAM-) Rollen und Benutzer in Ihrer Organisation. Richtlinien zur Ressourcenkontrolle (RCPs) definieren die maximal verfügbaren Berechtigungen für Ressourcen in Ihrer Organisation.

Dieses Muster hilft Ihnen bei der Verwaltung SCPs und RCPs als Infrastructure as Code (IaC), die Sie über eine CI/CD-Pipeline (Continuous Integration and Continuous Deployment) bereitstellen. Indem Sie unsere AWS CloudFormation Hashicorp Terraform zur Verwaltung dieser Richtlinien verwenden, können Sie den Aufwand reduzieren, der mit der Erstellung und Verwaltung mehrerer Autorisierungsrichtlinien verbunden ist.

Dieses Muster umfasst die folgenden Funktionen:

- Sie erstellen, löschen und aktualisieren die Autorisierungsrichtlinien mithilfe von Manifestdateien (`scp-management.jsonundrcp-management.json`).
- Sie arbeiten mit Leitplanken statt mit Richtlinien. Sie definieren Ihre Leitplanken und ihre Ziele in den Manifestdateien.
- Die Pipeline, die AWS CodeBuild und verwendet AWS CodePipeline, führt die Leitplanken in den Manifestdateien zusammen und optimiert sie. Für jede Anweisung in der Manifestdatei fasst die Pipeline die Guardrails zu einem einzigen SCP oder RCP zusammen und wendet sie dann auf die definierten Ziele an.
- AWS Organizations wendet die Richtlinien auf Ihre Ziele an. Bei einem Ziel kann es sich um eine Organisationseinheit (OU), eine Umgebung (bei der es sich um eine Gruppe von Konten handelt oder OUs die Sie in der `environments.json` Datei definieren) oder um eine Gruppe von Konten mit einem gemeinsamen AWS Tag handeln. AWS-Konto
- Amazon Bedrock liest die Pipeline-Protokolle und fasst alle Richtlinienänderungen zusammen.
- Die Pipeline erfordert eine manuelle Genehmigung. Der Genehmiger kann die von Amazon Bedrock erstellte Zusammenfassung lesen, die ihm hilft, die Änderungen zu verstehen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Mehrere AWS-Konten , die als Organisation verwaltet werden in. AWS Organizations Weitere Informationen finden Sie unter Organisation erstellen.
- Die SCP- und RCP-Funktionen sind in aktiviert. AWS Organizations Weitere Informationen finden Sie unter Einen Richtlinientyp aktivieren.
- Terraform Version 1.9.8 oder höher ist installiert.
- Wenn Sie diese Lösung nicht über eine Terraform-Pipeline bereitstellen, muss die Terraform-Statusdatei in einem Amazon Simple Storage Service (Amazon S3) -Bucket gespeichert werden, in AWS-Konto dem Sie die Policy-Management-Pipeline bereitstellen.
- Python-Version 3.13.3 oder höher ist installiert.

Einschränkungen

- Sie können dieses Muster nicht verwenden, um Objekte zu verwalten SCPs RCPs , die außerhalb dieser CI/CD-Pipeline erstellt wurden. Sie können jedoch vorhandene Richtlinien über die Pipeline neu erstellen. Weitere Informationen finden Sie unter Migrieren vorhandener Richtlinien zur Pipeline im Abschnitt Zusätzliche Informationen dieses Musters.
- Die Anzahl der Konten und die Richtlinien in jedem Konto unterliegen den Kontingenten und Dienstlimits für AWS Organizations. OUs
- Dieses Muster kann nicht zur Konfiguration von Verwaltungsrichtlinien wie Backup-Richtlinien, Tag-Richtlinien, Chat-Anwendungsrichtlinien oder deklarativen Richtlinien verwendet werden. AWS Organizations

Architektur

Das folgende Diagramm zeigt den Arbeitsablauf der Richtlinienverwaltungspipeline und der zugehörigen Ressourcen.

Das Diagramm zeigt den folgenden Workflow:

1. Ein Benutzer überträgt Änderungen an den Dateien `scp-management.json` oder den `rcp-management.json` Manifestdateien im Hauptzweig des Remote-Repositorys.

2. Durch die Änderung des `main` Zweigs wird der Pipeline-Eingang initiiert. AWS CodePipeline
3. CodePipeline startet das `Validate-Plan` CodeBuild Projekt. Dieses Projekt verwendet ein Python-Skript im Remote-Repository, um Richtlinien und die Richtlinienmanifestdateien zu validieren. Dieses CodeBuild Projekt macht Folgendes:
   a. Überprüft, ob die SCP- und RCP-Manifestdateien eine eindeutige Anweisung IDs () `Sid` enthalten.
   b. Verwendet die `rcp-policy-processor/main.py` Python-Skripte `scp-policy-processor/main.py` und, um Guardrails im Guardrails-Ordner zu einer einzigen RCP- oder SCP-Richtlinie zu verketten. Es kombiniert Leitplanken, die dieselben, und haben. `Resource` `Action` `Condition`
   c. Wird verwendet AWS Identity and Access Management Access Analyzer , um die endgültige, optimierte Richtlinie zu validieren. Falls irgendwelche Ergebnisse vorliegen, wird die Pipeline gestoppt.
   d. Erstellt `scps.json` `rcps.json` Dateien, die Terraform verwendet, um Ressourcen zu erstellen.
   e. Führt den `terraform plan` Befehl aus, der einen Terraform-Ausführungsplan erstellt.
4. (Optional) Das `Validate-Plan` CodeBuild Projekt verwendet das `bedrock-prompt/prompt.py` Skript, um eine Aufforderung an Amazon Bedrock zu senden. Sie definieren die Aufforderung in der `bedrock-prompt/prompt.txt` Datei. Amazon Bedrock verwendet Anthropic Claude Sonnet 3.5, um durch die Analyse der Terraform- und Python-Protokolle eine Zusammenfassung der vorgeschlagenen Änderungen zu generieren.
5. CodePipeline verwendet ein Amazon Simple Notification Service (Amazon SNS) -Thema, um Genehmiger darüber zu informieren, dass Änderungen überprüft werden müssen. Wenn Amazon Bedrock eine Änderungszusammenfassung generiert hat, enthält die Benachrichtigung diese Zusammenfassung.
6. Ein Policy-Genehmiger genehmigt die Maßnahme in. CodePipeline Wenn Amazon Bedrock eine Änderungszusammenfassung generiert hat, kann der Genehmiger die Zusammenfassung CodePipeline vor der Genehmigung überprüfen.
7. CodePipeline startet das Projekt. `Apply` CodeBuild Dieses Projekt verwendet Terraform, um die RCP- und SCP-Änderungen in anzuwenden. AWS Organizations

Die mit dieser Architektur verknüpfte IaC-Vorlage stellt außerdem die folgenden Ressourcen bereit, die die Richtlinienverwaltungspipeline unterstützen:

- Ein Amazon S3 S3-Bucket zum Speichern von CodePipeline Artefakten und Skripten wie `scp-policy-processor/main.py` und `bedrock-prompt/prompt.py`
- Ein AWS Key Management Service (AWS KMS) -Schlüssel, der die von dieser Lösung erstellten Ressourcen verschlüsselt

Tools

AWS-Services

- Amazon Bedrock ist ein vollständig verwalteter KI-Service, der viele leistungsstarke Basismodelle über eine einheitliche API zur Nutzung verfügbar macht.
- AWS CodeBuildist ein vollständig verwalteter Build-Service, der Ihnen hilft, Quellcode zu kompilieren, Komponententests durchzuführen und Artefakte zu erstellen, die sofort einsatzbereit sind.
- AWS CodePipelinehilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.
- AWS Organizationsist ein Kontoverwaltungsservice, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie erstellen und zentral verwalten.
- AWS SDK für Python (Boto3)ist ein Softwareentwicklungskit, mit dem Sie Ihre Python-Anwendung, -Bibliothek oder Ihr Skript integrieren können AWS-Services.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Andere Tools

- HashiCorp Terraform ist ein IaC-Tool, mit dem Sie mithilfe von Code Cloud-Infrastruktur und -Ressourcen bereitstellen und verwalten können.

Code-Repository

Der Code für dieses Muster ist im organizations-policy-pipeline GitHub Repository verfügbar. Im Folgenden sind die wichtigsten Dateien aufgeführt, die in dem `sample-repository` Ordner enthalten sind:

- `environments.json`Enthält in dem `environments` Ordner eine Liste von Umgebungen. Umgebungen sind eine Gruppe von Zielen, und sie können Organisationseinheiten (OUs) enthalten AWS-Konto IDs .
- Im `rcp-management` Ordner:
  - Der `guardrails` Ordner enthält die einzelnen Leitplanken für Ihre RCPs
  - Der `policies` Ordner enthält die einzelnen RCPs
  - Die `rcp-management.json` Manifestdatei hilft Ihnen bei der Verwaltung von RCP-Guardrails RCPs, Full und den zugehörigen Zielen.
- Im Ordner: `scp-management`
  - Der `guardrails` Ordner enthält die einzelnen Leitplanken für Ihre SCPs
  - Der `policies` Ordner enthält die einzelnen SCPs
  - Die `scp-management.json` Manifestdatei hilft Ihnen bei der Verwaltung von SCP-Guardrails SCPs, Full und den zugehörigen Zielen.
- Der `utils` Ordner enthält Skripts, mit denen Sie Ihre aktuellen Dateien migrieren SCPs und RCPs sie über die Pipeline verwalten können. Weitere Informationen finden Sie im Abschnitt Zusätzliche Informationen dieses Musters.

Bewährte Methoden

- Bevor Sie die Pipeline einrichten, empfehlen wir Ihnen, sich zu vergewissern, dass Sie die Grenzwerte Ihrer AWS Organizations Kontingente nicht erreicht haben.
- Wir empfehlen, das AWS Organizations Verwaltungskonto nur für Aufgaben zu verwenden, die in diesem Konto ausgeführt werden müssen. Weitere Informationen finden Sie unter Bewährte Methoden für das Verwaltungskonto.

Epen

Richten Sie das Zielkonto ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein -Repository.	Erstellen Sie ein Repositor y, von dem aus Ihr Security Operations Team die Richtlini	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en verwaltet. Verwenden Sie einen der Drittanbieter für Repositorys, der dies AWS CodeConnections unterstützt.	
Delegieren Sie die Richtlinienverwaltung.	Delegieren Sie die Verwaltung der AWS Organizations Richtlinien an das Mitgliedskonto, für das Sie die Pipeline bereitstellen. Anweisungen finden Sie unter Erstellen einer ressourcenbasierten Delegierungsrichtlinie mit AWS Organizations. Ein Beispiel für eine Richtlinie finden Sie unter Beispiel für eine ressourcenbasierte Delegierungsrichtlinie im Abschnitt Zusätzliche Informationen dieses Musters.	AWS-Administrator
(Optional) Aktivieren Sie das Foundation-Modell.	Wenn Sie Zusammenfassungen der Richtlinienänderungen erstellen möchten, aktivieren Sie den Zugriff auf das Anthropic Claude 3.5 Sonnet Foundation-Modell in Amazon Bedrock in dem Land, in AWS-Konto dem Sie die Pipeline bereitstellen. Anweisungen finden Sie unter Zugriff auf Amazon Bedrock Foundation-Modelle hinzufügen oder entfernen.	Allgemeines AWS

Stellen Sie die Ressourcen für die Pipeline bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Geben Sie den folgenden Befehl ein, um das organizations-policy-pipeline Repository von zu klonen GitHub: `git clone https://github.com/aws-samples/organizations-policy-pipeline.git`	DevOps Ingenieur
Definieren Sie Ihre Bereitstellungsmethode.	1. Öffnen Sie die `variables.tf` Datei im geklonten Repository. 2. Geben Sie für `project_name` das Präfix ein, das Sie auf die Namen der bereitgestellten Ressourcen anwenden möchten. 3. Geben Sie für `provider_type` den Anbieter des Remote-Repositorys ein. Gültige Werte sind in der Datei enthalten. 4. Geben Sie für `full_repository_name` den Namen des Remote-Repositorys ein. 5. Geben Sie für `branch_name` den Namen des Git-Branches ein, den Sie für die Bereitstellung von Richtlinien verwenden	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	werden. Ein Push oder Merge in diesem Branch startet die Pipeline. In der Regel ist dies der Hauptzweig. 6. Geben Sie für `terraform_version` die Version von Terraform ein, die Sie verwenden. 7. Geben Sie für ein`enable_bedrock` , `true` ob Amazon Bedrock die Änderungen zusammenfassen soll. Geben Sie ein, `false` wenn Sie keine Zusammenfassung der Änderungen generieren möchten. 8. Geben Sie für `tags` die Schlüssel-Wert-Paare ein, die Sie den bereitgestellten Ressourcen als Tags zuweisen möchten. 9. Speichern und schließen Sie die Datei `variables.tf` .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die Pipeline bereit.	1. Geben Sie den folgenden Befehl ein, um einen Plan zu erstellen und die Änderungen zu überprüfen:
	`terraform plan`
	2. Geben Sie den folgenden Befehl ein, um den Plan anzuwenden und die Pipeline-Infrastruktur zu erstellen:
	`terraform apply`
		DevOps Ingenieur, Terraform

Connect zum Remote-Repository her.	Im vorherigen Schritt hat Terraform eine CodeConnections Verbindung zum Repository eines Drittanbieters hergestellt. Ändern Sie in der AWS Developer Tools-Konsole den Status der Verbindung von `PENDING` zu. `AVAILABLE` Anweisungen finden Sie unter Aktualisieren einer ausstehenden Verbindung.	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Abonnieren Sie das Amazon-SNS-Thema.	Terraform hat ein Amazon SNS SNS-Thema erstellt. Abonnieren Sie einen Endpunkt für das Thema und bestätigen Sie das Abonnement, damit die Genehmiger Benachric htigungen über ausstehende Genehmigungsaktionen in der Pipeline erhalten. Anweisung en finden Sie unter Erstellen eines Abonnements für ein Amazon SNS SNS-Abonn ement.	Allgemeines AWS

Definieren Sie Ihre Leitplanken und Richtlinien

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Füllen Sie das Remote-Re pository auf.	Kopieren Sie den Inhalt des `sample-repository` Ordners aus dem geklonten Repository in Ihr Remote-Repository. Dazu gehören die `utils` Ordner `environments rcp-manag ement ,scp-management` , und.	DevOps Ingenieur
Definieren Sie Ihre Umgebungen.	1. Öffnen `environments` Sie die `environme nts.json` Datei in dem Ordner. Dies ist die Datei, in der Sie das Ziel AWS-Konte	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	n und OUs für Ihr RCPs und definieren SCPs. 2. Löschen Sie die Beispielu mgebungen. 3. Fügen Sie Ihre Zielumgeb ungen im folgenden Format hinzu: `[ { "ID": "<environment-name>", "Target": [ "<ou-name>:<ou-id>", "<account-name>:<account-id>" ] } ]` Wobei gilt: • `<environment-name>` ist der Name, den Sie der Gruppe von OUs AWS-Konten zuweisen. Sie können diesen Namen in der Manifestd atei verwenden, um zu definieren, wo Sie Ihre Richtlinien anwenden möchten. • `<ou-name>` ist der Name der Ziel-OU.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `<ou-id>`ist die ID der Ziel-OU. • `<account-name>` ist der Name des Ziels AWS-Konto. • `<account-id>` ist die ID des Ziels AWS-Konto. Beispiele finden Sie im Quellcode-Repository. 4. Speichern und schließen Sie die Datei `environments.json` .	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definiere deine Leitplanken.	1. Navigieren Sie zu dem `rcp-management/guardrails` Ordner in Ihrem Remote-Repository. In diesem Ordner definieren Sie die Leitplanken für Ihre RCP-Manifestdatei. Jede Leitplanke muss sich in einer eigenen Datei befinden. Guardrail-Dateien können eine oder mehrere Anweisungen enthalten. **Note** Sie können dieselbe Guardrail in mehreren Anweisungen in den Manifestdateien für und verwenden. SCPs RCPs Wenn Sie die Leitplanke ändern, sind alle Richtlinien betroffen, die diese Leitplanke enthalten. 2. Löschen Sie alle Beispiel-Guardrails, die aus dem Quellcode-Repository kopiert wurden. 3. Erstellen Sie eine neue JSON-Datei und geben Sie	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ihr einen aussagekräftigen Namen. 4. Öffnen Sie die von Ihnen erstellte JSON-Datei. 5. Definieren Sie die Leitplanke im folgenden Format: `[ { "Sid": "<guardrail-name>", "Effect": "<effect-value>", "Action": [ "<action-name>" ], "Resource": "<resource-arn>", "Condition": { "<condition-operator>": { "<condition-key>": [ "<condition-value>" ] } } } ]` Wobei gilt: • `<guardrail-name>` ist ein eindeutiger Name für die Leitplanke. Dieser Name kann nicht für	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	andere Leitplanken verwendet werden. • `<effect-value>` muss oder sein. `Allow` `Deny` Weitere Informationen finden Sie unter Wirkung. • `<action-name>` muss ein gültiger Name einer Aktion sein, die der Dienst unterstützt. Weitere Informationen finden Sie unter Aktion. • `<resource-arn>` ist der Amazon-Re ssourcenname (ARN) der Ressource, für die die Leitplanke gilt. Sie können auch Platzhalt erzeichen wie oder verwenden. `*` `?` Weitere Informationen finden Sie unter Ressource. • `<condition-operato r>` ist ein gültiger Bedingungsoperator . Weitere Informati onen finden Sie unter Bedingungsoperatoren. • `<condition-key>` ist ein gültiger globaler Bedingungskontexts chlüssel oder ein dienstspezifischer Kontextschlüssel. Weitere	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Informationen finden Sie unter Bedingung. • `<condition-value>`ist der spezifische Wert, der in einer Bedingung verwendet wird, um zu bewerten, ob eine Leitplanke zutrifft. Weitere Informationen finden Sie unter Bedingung. Ein Beispiel für RCP-Guardrails finden Sie im Quellcode-Repository. 6. Speichern und schließen Sie die JSON-Datei. 7. Wiederholen Sie diese Schritte, um so viele RCP-Leitplanken wie nötig zu erstellen. 8. Wiederholen Sie diese Schritte im `scp-management/guardrails` Ordner, um so viele Leitplanken zu erstellen, wie Sie für Ihre benötigen. SCPs Ein Beispiel für SCP-Guardrails finden Sie im Quellcode-Repository.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie Ihre Richtlinien.	1. Navigieren Sie zu dem `rcp-management/policies` Ordner in Ihrem Remote-Repository. In diesem Ordner definieren Sie die vollständigen Richtlinien für Ihre RCP-Manifestdatei. Jede Richtlinie muss eine einzelne Datei sein. **Note** Wenn Sie eine Richtlinie in diesem Ordner ändern, wirken sich die Richtlinienänderungen, wie in der Manifestdatei definiert, auf alle Konten aus oder OUs auf die diese Richtlinie angewendet wird. 2. Löschen Sie alle Beispielrichtlinien, die aus dem Quellcode-Repository kopiert wurden. 3. Erstellen Sie eine neue JSON-Datei und geben Sie ihr einen aussagekräftigen Namen.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	4. Öffnen Sie die von Ihnen erstellte JSON-Datei. 5. Definieren Sie das RCP. Sehen Sie sich RCPs beispielsweise das Quellcode-Repository oder die Beispiele für Richtlinien zur Ressourcensteuerung in der AWS Organizations Dokumentation an. 6. Speichern und schließen Sie die JSON-Datei. 7. Wiederholen Sie diese Schritte, um so viele RCPs wie nötig zu erstellen. 8. Wiederholen Sie diese Schritte im `scp-management/policies` Ordner, um so viele SCPs wie nötig zu erstellen . Sehen Sie sich SCPs beispielsweise das Quellcode-Repository oder die Beispiele für Richtlinien zur Servicesteuerung in der AWS Organizations Dokumentation an.	

Verwenden Sie die Manifestdatei, um die Richtlinien zu verwalten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie die Manifestdateien.	1. Öffnen `rcp-management` Sie die `rcp-management.json` Datei in dem Ordner. In dieser Datei definieren Sie, welche RCP-Guardrails und welche RCP-Richtlinien für Ihre RCPs Zielumgebungen gelten. Ein Beispiel für diese Datei finden Sie im Quellcode-Repository. 2. Löschen Sie die Beispielanweisung. 3. Fügen Sie eine neue Anweisung im folgenden Format hinzu: `[ { "SID": "<statement-name>", "Target": { "Type": "<target-type>", "ID": "<target-name>" }, "Guardrails": [ "<guardrail-name>" ], "Policy": "<policy-name>",`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	<pre>"Comments": "<comment-text>" }]</pre> Wobei gilt: • `<statement-name>` ist ein eindeutiger Name für die Anweisung. • `<target-type>` ist der Zieltyp, auf den Sie die Richtlinie anwenden möchten. Gültige Werte sind `Account`, `OU`, `Environment` oder `Tag`. • `<target-name>` ist der Bezeichner des Ziels, auf das Sie die Richtlini e anwenden möchten. Machen Sie eine der folgenden Eingaben: • Geben Sie für eine AWS-Konto den Bezeichner als ein`<account-name>:<account-id>` . • Geben Sie für eine Organisationseinhe it den Bezeichner als ein`<OU-name>:<ou-id>`.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Geben Sie für eine Umgebung den eindeutigen Namen ein, den Sie in der `environments.json` Datei definiert haben. • Geben Sie für ein Tag das Schlüssel-Wert-Paar als ein. `<tag-key>:<tag-value>` • `<guardrail-name>` ist der eindeutige Name der RCP-Leitplanke, die Sie im Ordner definiert haben. `rcp-management/guardrails` Sie können diesem Element mehrere Leitplanken hinzufügen. Sie können dieses Feld leer lassen, wenn Sie keine Leitplanke anwenden möchten. • `<policy-name>` ist der eindeutige Name des RCP, den Sie im Ordner definiert haben. `rcp-management/policies` Sie können diesem Element nur eine Richtlinie hinzufügen. Sie können dieses Feld leer	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	lassen, wenn Sie keine Richtlinie anwenden möchten. • `<comment-text>` ist eine Beschreibung, die Sie zu Dokumentationszwecken eingeben können. Dieses Feld wird bei der Pipelineverarbeitung nicht verwendet. Sie können dieses Feld leer lassen, wenn Sie keinen Kommentar hinzufügen möchten. 4. Wiederholen Sie diese Schritte, um so viele Anweisungen hinzuzufügen, wie für die Konfiguration RCPs für Ihre Organisation erforderlich sind. 5. Speichern und schließen Sie die Datei `rcp-management.json` . 6. Wiederholen Sie diese Schritte im `scp-management` Ordner in der `scp-management.json` Datei. In dieser Datei definieren Sie, welche SCP-Guardrails und welche SCP-Richtlinien für Ihre SCPs Zielumgebungen gelten. Ein Beispiel für	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	diese Datei finden Sie im Quellcode-Repository.	
Starte die Pipeline.	Übernehmen Sie die Änderungen und übertragen Sie sie in den Zweig des Remote-Repositorys, den Sie in der `variables.tf` Datei definiert haben. In der Regel ist dies der `main` Branch. Die CI/CD-Pipeline wird automatisch gestartet. Falls Pipeline-Fehler auftreten, finden Sie weitere Informationen im Abschnitt zur Fehlerbehebung in diesem Muster.	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Genehmigen Sie die Änderungen.	Wenn das `Validate-Plan` CodeBuild Projekt abgeschlossen ist, erhalten die Richtlinengenehmiger eine Benachrichtigung über das Amazon SNS SNS-Thema, das Sie zuvor konfiguriert haben. Gehen Sie wie folgt vor: 1. Öffnen Sie die Benachrichtigungsnachricht. 2. Falls verfügbar, überprüfen Sie die Zusammenfassung der Richtlinienänderungen. 3. Folgen Sie den Anweisungen unter Genehmigungsaktion genehmigen oder ablehnen unter CodePipeline.	Allgemeines AWS, Richtliniengenehmiger

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die Bereitstellung.	1. Melden Sie sich bei der AWS Organizations Konsole mit dem Konto an, für AWS Organizations das Sie der delegierte Administrator ist. 2. Vergewissern Sie sich auf der Seite mit den Richtlinien zur Dienststeuerung, SCPs dass die von Ihnen erstellten Richtlinien aufgeführt sind. 3. Wählen Sie einen SCP aus, der über die Pipeline verwaltet wird, und vergewissern Sie sich, dass er für die vorgesehenen Ziele gilt. 4. Vergewissern Sie sich auf der Seite Resource Control Policies, RCPs dass die, die Sie erstellt haben, aufgeführt sind. 5. Wählen Sie ein RCP aus, das über die Pipeline verwaltet wird, und vergewissern Sie sich, dass es für die vorgesehenen Ziele gilt.	Allgemeines AWS

Fehlerbehebung

Problem	Lösung
Manifeste Dateifehler in der `Validate-Plan` Phase der Pipeline	Wenn die ODER-Dateien Fehler enthalten , wird in der Pipeline-Ausgabe die Meldung „Pipeline-Fehler in der Überprüfungs `scp-management.json` - und Planungsphase für `rcp-management.json` Manifestd ateien“ angezeigt. Zu den möglichen Fehlern gehören ein falscher Umgebungsname SIDs, doppelte oder ungültige Felder oder Werte. Gehen Sie wie folgt vor: 1. Folgen Sie den Anweisungen unter Build-Details anzeigen unter AWS CodeBuild. 2. Suchen Sie im Build-Log nach dem Validierungsfehler. Der Fehler enthält weitere Informationen darüber, was zum Fehlschlagen des Builds geführt hat. 3. Aktualisieren Sie die entsprechende JSON-Datei. 4. Übergeben Sie die aktualisierte Datei und übertragen Sie sie in das Remote-Repository. Die Pipeline wird neu gestartet. 5. Überwachen Sie den Status, um sicherzustellen, dass der Validierungsfehler behoben wurde.
Ergebnisse des IAM Access Analyzer in der `Validate-Plan` Pipeline-Phase	Die Meldung „Ergebnisse in IAM Access Analyzer während der Überprüfungs- und Planungsphase“ wird in der Pipeline-Ausgabe angezeigt, wenn Fehler in der Guardrail- oder Policy-Definition vorliegen. Dieses Muster verwendet IAM Access Analyzer, um die

Problem	Lösung
	endgültige Richtlinie zu validieren. Gehen Sie wie folgt vor: 1. Folgen Sie den Anweisungen unter Build-Details anzeigen unter AWS CodeBuild. 2. Suchen Sie im Build-Log nach dem IAM Access Analyzer-Validierungsfehler. Der Fehler enthält weitere Informationen darüber, was zum Fehlschlagen des Builds geführt hat. Weitere Informationen zu den Findetypen finden Sie in der Referenz zur Überprüfung der IAM-Richtlinienvalidierung. 3. Aktualisieren Sie die entsprechende .json-Datei für die Leitplanke oder Richtlinie. 4. Übergeben Sie die aktualisierte Datei und übertragen Sie sie in das Remote-Repository. Die Pipeline wird neu gestartet. 5. Überwachen Sie den Status, um sicherzustellen, dass der Validierungsfehler behoben wurde.

Zugehörige Ressourcen

- Referenz zum JSON-Richtlinienelement (IAM-Dokumentation)
- Richtlinien zur Ressourcenkontrolle (AWS Organizations Dokumentation)
- Richtlinien zur Servicesteuerung (AWS Organizations Dokumentation)
- Zugriff auf Amazon Bedrock Foundation-Modelle hinzufügen oder entfernen (Amazon Bedrock-Dokumentation)
- Genehmigen oder lehnen Sie eine Genehmigungsaktion in CodePipeline (Dokumentation) CodePipeline ab

Zusätzliche Informationen

Beispiel für eine ressourcenbasierte Delegierungsrichtlinie

Im Folgenden finden Sie ein Beispiel für eine ressourcenbasierte Delegierungsrichtlinie für. AWS Organizations Sie ermöglicht dem delegierten Administratorkonto die Verwaltung SCPs und RCPs für die Organisation. Ersetzen Sie den Wert in der folgenden Beispielrichtlinie `<MEMBER_ACCOUNT_ID>` durch die ID des Kontos, für das Sie die Richtlinienverwaltungspipeline bereitstellen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegationToAudit",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<MEMBER_ACCOUNT_ID>:root"
      },
      "Action": [
        "organizations:ListTargetsForPolicy",
        "organizations:CreatePolicy",
        "organizations:DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:DisablePolicyType",
        "organizations:EnablePolicyType",
        "organizations:UpdatePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Migrieren vorhandener Richtlinien in die Pipeline

Wenn Sie bereits über diese Pipeline verfügen SCPs oder RCPs die Sie über diese Pipeline migrieren und verwalten möchten, können Sie die Python-Skripte im `sample-repository/utils` Ordner des Code-Repositorys verwenden. Zu diesen Skripten gehören:

- `check-if-scp-exists-in-env.py`— Dieses Skript prüft, ob eine angegebene Richtlinie für Ziele in einer bestimmten Umgebung gilt, die Sie in der `environments.json` Datei definieren. Geben Sie den folgenden Befehl ein, um dieses Skript auszuführen:

  ```
  python3 check-if-scp-exists-in-env.py \
     --policy-type <POLICY_TYPE> \
     --policy-name <POLICY_NAME> \
     --env-id <ENV_ID>
  ```

  Ersetzen Sie in diesem Befehl Folgendes:

  - `<POLICY_TYPE>` ist `scp` oder `rcp`
  - `<POLICY_NAME>`ist der Name des SCP oder RCP
  - `<ENV_ID>`ist die ID der Umgebung, die Sie in der Datei definiert haben `environments.json`
- `create-environments.py`— Dieses Skript erstellt eine environments.json-Datei, die auf der aktuellen SCPs und RCPs in Ihrer Umgebung basiert. Es schließt Richtlinien aus, die über bereitgestellt werden. AWS Control Tower Geben Sie den folgenden Befehl ein, um dieses Skript auszuführen, wobei `<POLICY_TYPE>` es sich um `scp` oder `rcp` handelt:

  ```
  python create-environments.py --policy-type <POLICY_TYPE>
  ```
- `verify-policies-capacity.py`— Dieses Skript überprüft jede von Ihnen definierte Umgebung, um festzustellen, wie viel Kapazität für jedes AWS Organizations richtlinienbezogene Kontingent noch übrig ist. Sie definieren die Umgebungen, in die die Datei eingecheckt werden soll. `environments.json` Geben Sie den folgenden Befehl ein, um dieses Skript auszuführen, wobei `<POLICY_TYPE>` es sich um `scp` oder handelt`rcp`:

  ```
  python verify-policies-capacity.py --policy-type <POLICY_TYPE>
  ```

Verwalten Sie AWS IAM Identity Center Berechtigungssätze als Code, indem Sie AWS CodePipeline

Erstellt von Andre Cavalcante (AWS) und Claison Amorim (AWS)

Übersicht

AWS IAM Identity Center hilft Ihnen dabei, den Single Sign-On (SSO) -Zugriff auf all Ihre Anwendungen zentral zu verwalten. AWS-Konten Sie können Benutzeridentitäten in IAM Identity Center erstellen und verwalten, oder Sie können eine Verbindung zu einer vorhandenen Identitätsquelle herstellen, z. B. einer Microsoft Active Directory-Domäne oder einem externen Identitätsanbieter (IdP). IAM Identity Center bietet eine einheitliche Administrationserfahrung, mit der Sie mithilfe von Berechtigungssätzen einen detaillierten Zugriff auf Ihre AWS Umgebung definieren, anpassen und zuweisen können. Berechtigungssätze gelten für die verbundenen Benutzer und Gruppen aus Ihrem IAM Identity Center-Identitätsspeicher oder Ihrem externen IdP.

Dieses Muster hilft Ihnen dabei, IAM Identity Center-Berechtigungssätze als Code in Ihrer Umgebung mit mehreren Konten zu verwalten, die als Organisation in verwaltet wird. AWS Organizations Mit diesem Muster können Sie Folgendes erreichen:

- Berechtigungssätze erstellen, löschen und aktualisieren
- Erstellen, aktualisieren oder löschen Sie Berechtigungssatz-Zuweisungen zum Ziel AWS-Konten, zu den Organisationseinheiten (OUs) oder zum Stammverzeichnis Ihrer Organisation.

Um IAM Identity Center-Berechtigungen und -Zuweisungen als Code zu verwalten, stellt diese Lösung eine CI/CD-Pipeline (Continuous Integration and Continuous Delivery) bereit, die und verwendet. AWS CodeBuild AWS CodePipeline Sie verwalten die Berechtigungssätze und Zuweisungen in JSON-Vorlagen, die Sie in einem Remote-Repository speichern. Wenn EventBridge Amazon-Regeln eine Änderung am Repository oder Änderungen an den Konten in der Ziel-OU erkennen, wird eine AWS Lambda Funktion gestartet. Die Lambda-Funktion initiiert die CI/CD-Pipeline, die die Berechtigungssätze und Zuweisungen in IAM Identity Center aktualisiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Umgebung mit mehreren Konten, die als Organisation in verwaltet wird. AWS Organizations Weitere Informationen finden Sie unter Organisation erstellen.

- IAM Identity Center, aktiviert und konfiguriert mit einer Identitätsquelle. Weitere Informationen finden Sie unter Erste Schritte in der IAM Identity Center-Dokumentation.
- Ein Mitgliedskonto, das als delegierter Administrator für Folgendes registriert ist: AWS-Services
  - IAM Identity Center — Anweisungen finden Sie in der IAM Identity Center-Dokumentation unter Ein Mitgliedskonto registrieren.
  - AWS Organizations — Anweisungen finden Sie unter Delegierter Administrator für. AWS Organizations Dieses Konto muss berechtigt sein, Konten aufzulisten und zu beschreiben und OUs.

> **Note**
>
> Sie müssen für beide Dienste dasselbe Konto wie der delegierte Administrator verwenden.

- Berechtigungen zum Bereitstellen von AWS CloudFormation Stacks im delegierten Administratorkonto von IAM Identity Center und im Verwaltungskonto der Organisation. Weitere Informationen finden Sie in der Dokumentation unter Zugriffskontrolle. CloudFormation
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket im delegierten Administratorkonto von IAM Identity Center. Sie laden den Artefaktcode in diesen Bucket hoch. Anweisungen finden Sie in der Amazon S3 S3-Dokumentation unter Bucket erstellen.
- Die Konto-ID des Verwaltungskontos der Organisation. Anweisungen finden Sie unter Ihre AWS-Konto ID finden.
- Ein Repository auf Ihrem Quellcode-Host, z. GitHub B.

Einschränkungen

- Dieses Muster kann nicht zur Verwaltung oder Zuweisung von Berechtigungssätzen für Umgebungen mit nur einem Konto oder für Konten verwendet werden, die nicht als Organisation in AWS Organizations verwaltet werden.
- Die Namen der Berechtigungssätze, die Zuweisung IDs und die IAM Identity Center-Prinzipaltypen können nach der Bereitstellung IDs nicht geändert werden.
- Dieses Muster hilft Ihnen bei der Erstellung und Verwaltung benutzerdefinierter Berechtigungen. Sie können dieses Muster nicht verwenden, um vordefinierte Berechtigungen zu verwalten oder zuzuweisen.
- Dieses Muster kann nicht verwendet werden, um einen Berechtigungssatz für das Verwaltungskonto der Organisation zu verwalten.

Architektur

Zielarchitektur

Das Diagramm zeigt den folgenden Workflow:

1. Ein Benutzer nimmt eine der folgenden Änderungen vor:
   - Übergibt eine oder mehrere Änderungen an das Remote-Repository, z. B. GitHub
   - Ändert die Konten in der Organisationseinheit in AWS Organizations
2. Wenn der Benutzer eine Änderung am Remote-Repository in den Hauptzweig übernommen hat, wird die Pipeline gestartet.

   Wenn der Benutzer die Konten in der Organisationseinheit geändert hat, erkennt die `MoveAccount` EventBridge Regel die Änderung und startet eine Lambda-Funktion im Verwaltungskonto der Organisation.
3. Die initiierte Lambda-Funktion startet die CI/CD-Pipeline in. CodePipeline
4. CodePipeline startet das Projekt. `TemplateValidation` CodeBuild Das `TemplateValidation` CodeBuild Projekt verwendet ein Python-Skript im Remote-Repository, um die Berechtigungssatz-Vorlagen zu validieren. CodeBuild validiert Folgendes:
   - Die Namen der Berechtigungssätze sind eindeutig.
   - Die Zuweisungsanweisung IDs (`Sid`) ist einzigartig.
   - Richtliniendefinitionen sind im `CustomPolicy` Parameter enthalten und gültig. (Diese Überprüfung verwendet AWS Identity and Access Management Access Analyzer.)
   - Die Amazon-Ressourcennamen (ARNs) der verwalteten Richtlinien sind gültig.
5. Die `PermissionSet` Aktionsgruppe im `Deploy` CodeBuild Projekt wird verwendet, AWS SDK für Python (Boto3) um die Berechtigungssätze im IAM Identity Center zu löschen, zu erstellen oder zu aktualisieren. Nur Berechtigungssätze mit dem `SSOPipeline:true` Tag sind betroffen. Alle Berechtigungssätze, die über diese Pipeline verwaltet werden, haben dieses Tag.
6. Die `Assignments` Aktionsgruppe im `Deploy` CodeBuild Projekt verwendet Terraform, um die Aufgaben im IAM Identity Center zu löschen, zu erstellen oder zu aktualisieren. Die Terraform-Backend-Statusdateien werden in einem Amazon S3 S3-Bucket im selben Konto gespeichert.
7. CodeBuild aktualisiert die Berechtigungssätze und Zuweisungen im IAM Identity Center.

Automatisierung und Skalierung

Da alle neuen Konten in einer Umgebung mit mehreren Konten in eine bestimmte Organisationseinheit verschoben werden AWS Organizations, wird diese Lösung automatisch ausgeführt und gewährt allen Konten, die Sie in den Zuweisungsvorlagen angeben, die erforderlichen Berechtigungssätze. Es sind keine zusätzlichen Automatisierungen oder Skalierungsaktionen erforderlich.

In großen Umgebungen kann die Anzahl der API-Anfragen an IAM Identity Center dazu führen, dass diese Lösung langsamer ausgeführt wird. Terraform und Boto3 verwalten die Drosselung automatisch, um Leistungseinbußen zu minimieren.

Tools

AWS-Services

- AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über und zu verwalten. AWS-Konten AWS-Regionen
- AWS CodeBuildist ein vollständig verwalteter Build-Service, der Ihnen hilft, Quellcode zu kompilieren, Komponententests durchzuführen und Artefakte zu erstellen, die sofort einsatzbereit sind.
- AWS CodePipelinehilft Ihnen dabei, die verschiedenen Phasen einer Softwareversion schnell zu modellieren und zu konfigurieren und die Schritte zu automatisieren, die für die kontinuierliche Veröffentlichung von Softwareänderungen erforderlich sind.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS Lambda Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen. AWS-Konten
- AWS IAM Identity Centerhilft Ihnen dabei, den Single Sign-On (SSO) -Zugriff auf all Ihre Anwendungen AWS-Konten und Cloud-Anwendungen zentral zu verwalten.
- AWS Organizationsist ein Kontoverwaltungsdienst, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie erstellen und zentral verwalten.
- AWS SDK für Python (Boto3)ist ein Softwareentwicklungskit, mit dem Sie Ihre Python-Anwendung, -Bibliothek oder Ihr Skript integrieren können AWS-Services.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Code-Repository

Der Code für dieses Muster ist im Repository aws-iam-identity-center-pipeline verfügbar. Der Vorlagenordner im Repository enthält Beispielvorlagen für Berechtigungssätze und Zuweisungen. Er enthält auch AWS CloudFormation Vorlagen für die Bereitstellung der CI/CD-Pipeline und der AWS Ressourcen in den Zielkonten.

Bewährte Methoden

- Bevor Sie mit der Änderung des Berechtigungssatzes und der Zuweisungsvorlagen beginnen, empfehlen wir Ihnen, die Berechtigungssätze für Ihre Organisation zu planen. Überlegen Sie, wie die Berechtigungen aussehen sollen, für welche Konten oder OUs welcher Berechtigungssatz gelten soll und für welche IAM Identity Center-Prinzipale (Benutzer oder Gruppen) der Berechtigungssatz gelten soll. Die Namen des Berechtigungssatzes, die Zuordnung IDs und die IAM Identity Center-Prinzipaltypen können nach der IDs Bereitstellung nicht geändert werden.
- Halten Sie sich an das Prinzip der geringsten Rechte und gewähren Sie nur die für die Ausführung einer Aufgabe erforderlichen Mindestberechtigungen. Weitere Informationen finden Sie in der AWS Identity and Access Management (IAM-) Dokumentation unter Gewährung der geringsten Rechte und bewährte Methoden zur Sicherheit.

Epen

Planen Sie Berechtigungssätze und Zuweisungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Geben Sie in einer Bash-Shell den folgenden Befehl ein. Dadurch wird das aws-iam-identity-center-pipeline Repository von geklont. GitHub `git clone https://github.com/aws-samples/aws-iam-identity-center-pipeline.git`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie die Berechtigungssätze.	1. Navigieren Sie im geklonten Repository zu dem `templates/permissionsets` Ordner und öffnen Sie dann eine der verfügbaren Vorlagen. 2. Geben Sie im `Name` Parameter einen Namen für den Berechtigungssatz ein. Dieser Wert muss eindeutig sein und kann nach der Bereitstellung nicht geändert werden. 3. Beschreiben Sie im `Description` Parameter kurz den Berechtigungssatz, z. B. seinen Anwendungsfall. 4. Geben Sie im `SessionDuration` Parameter an, wie lange ein Benutzer angemeldet sein kann AWS-Konto. Verwenden Sie das ISO-8601-Dauerformat (Wikipedia), z. B. `PT4H` für 4 Stunden. Wenn kein Wert definiert ist, ist der Standardwert in IAM Identity Center 1 Stunde. 5. Geben Sie im `RelayState` Parameter die URL an, die einen schnellen Zugriff auf die Konsole ermöglicht und für die Rolle	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	des Benutzers am besten geeignet ist. 6. Passen Sie die Richtlinien im Berechtigungssatz an. Alle folgenden Parameter sind optional und können nach der Bereitstellung geändert werden. Sie müssen mindestens einen der Parameter verwenden , um die Richtlinien im Berechtigungssatz zu definieren: • Geben Sie im `ManagedPolicies` Parameter die ARNs aller AWS verwalteten Richtlinien ein, die Sie zuweisen möchten. • Geben Sie im `CustomerManagedPolicies` Parameter die Namen aller vom Kunden verwalteten Richtlinien ein, die Sie zuweisen möchten. Verwenden Sie den ARN nicht. • Gehen Sie im `PermissionBoundary` Parameter wie folgt vor, um eine Berechtigungsgrenze zuzuweisen: • Wenn Sie eine AWS verwaltete Richtlinie als	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Berechtigungsgrenze verwendenPolicyTyp e , geben Sie inAWS, und inPolicy, den ARN der Richtlinie ein. • Wenn Sie eine vom Kunden verwaltete Richtlinie als Berechtig ungsgrenze verwenden PolicyType , geben Sie inCustomer, und inPolicy, den Namen der Richtlinie ein. Verwenden Sie den ARN nicht. • Definieren Sie im CustomPolicy Parameter alle benutzerd efinierten Richtlinien im JSON-Format, die Sie zuweisen möchten. Weitere Informationen zur JSON-Richtlinienstruktur finden Sie unter Überblick über JSON-Richtlinien. 7. Speichern und schließen Sie die Vorlage für den Berechtigungssatz. Es wird empfohlen, die Datei unter einem Namen zu speichern, der dem Namen des Berechtigungssatzes entspricht.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	8. Wiederholen Sie diesen Vorgang, um so viele Berechtigungssätze wie nötig für Ihre Organisation zu erstellen, und löschen Sie alle Beispielvorlagen, die nicht benötigt werden.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie die Aufgaben.	1. Navigieren Sie im geklonten Repository zu dem `templates/assignments` Ordner, und öffnen `iam-identitycenter-assigments.json` Sie ihn. In dieser Datei wird beschrieben, wie Sie die Berechtigungssätze AWS-Konten oder OUs zuweisen möchten. 2. Geben Sie im `SID` Parameter einen Bezeichner für die Zuweisung ein. Dieser Wert muss eindeutig sein und kann nach der Bereitstellung nicht geändert werden. 3. Definieren Sie im `Target` Parameter die Konten oder Organisationen, auf die Sie den Berechtigungssatz anwenden möchten. Gültige Werte sind Konto IDs OUs, oder`root`. `root`weist den Berechtigungssatz allen Mitgliedskonten in der Organisation zu, mit Ausnahme des Verwaltungskontos. Geben Sie die Werte in doppelte Anführungszeichen ein und trennen Sie mehrere Werte durch Kommas. Konto	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	IDs und OUs sollte dem Muster folgen: `{{account_name}}:{{account_id}}` oder`{{ou_name}}:{{ou_id}}` . Wenn Sie Nested rekursiv Berechtigungen zuweisen möchten OUs, verwenden Sie das OU-Muster mit einem Platzhalter am Ende. Beispiel: `{{ou_name}}:{{ou_id}}:*` 4. Geben Sie im `PrincipalType` Parameter den Typ des IAM Identity Center-Principals ein, auf den sich der Berechtigungssatz auswirkt. Gültige Werte sind `USER` oder `GROUP`. Dieser Wert kann nach der Bereitstellung nicht geändert werden. 5. Geben Sie im `PrincipalID` Parameter den Namen des Benutzers oder der Gruppe im IAM Identity Center-Identitätsspeicher ein, für den der Berechtigungssatz gilt. Dieser Wert kann nach der Bereitstellung nicht geändert werden. 6. Geben Sie im `PermissionSetName` Parameter	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den Namen des Berechtigungssatzes ein, den Sie zuweisen möchten. 7. Wiederholen Sie die Schritte 2—6, um in dieser Datei so viele Aufgaben wie nötig zu erstellen. In der Regel gibt es für jeden Berechtigungssatz eine Zuweisung. Löschen Sie alle Beispielzuweisungen, die nicht erforderlich sind. 8. Speichern und schließen Sie die Datei `iam-identitycenter-assigments.json` .	

Stellen Sie die Berechtigungssätze und Zuweisungen bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Ressourcen im delegierten IAM Identity Center-Administratorkonto bereit.	1. Öffnen Sie im delegierten IAM Identity Center-Administratorkonto die Konsole.AWS CloudFormation 2. Stellen Sie die Vorlage bereit. `iam-identitycenter-pipeline.yaml` Geben Sie dem Stack einen klaren und aussagekräftigen Namen und aktualisieren Sie die Parameter gemäß den	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Anweisungen. Anweisungen finden Sie in der Dokumentation unter Einen Stack erstellen. CloudFormation	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie Ressourcen im AWS Organizations Verwaltungskonto bereit.	1. Melden Sie sich beim Verwaltungskonto der Organisation an. 2. Öffnen Sie die AWS CloudFormation -Konsole. 3. Wählen Sie in der Navigationsleiste den Namen der aktuell angezeigten Datei aus AWS-Region. Wählen Sie dann die `us-east-1` Region aus. Diese Region ist erforderlich, damit die `MoveAccount` EventBridge Regel AWS CloudTrail Ereignisse im Zusammenhang mit Organisationsänderungen erkennen kann. 4. Stellen Sie die `iam-identitycenter-organization` Vorlage bereit. Geben Sie dem Stack einen klaren und aussagekräftigen Namen und aktualisieren Sie die Parameter gemäß den Anweisungen. Anweisungen finden Sie in der Dokumentation unter Einen Stack erstellen. CloudFormation	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Beenden Sie die Einrichtung des Remote-Repositorys.	Ändern Sie den Status der AWS CodeConnections Verbindung von `PENDING` zu`AVAILABLE` . Diese Verbindung wurde erstellt, als Sie den CloudFormation Stack bereitgestellt haben. Anweisungen finden Sie in der CodeConnections Dokumentation unter Aktualisieren einer ausstehenden Verbindung.	DevOps Ingenieur
Laden Sie Dateien in das Remote-Repository hoch.	Laden Sie alle Dateien, die Sie aus dem `aws-samples` Repository heruntergeladen und in den vorherigen Schritten bearbeitet haben, in das Remote-Repository hoch. Änderungen am `main` Zweig starten die Pipeline, die die Berechtigungssätze und Zuweisungen erstellt oder aktualisiert.	DevOps Ingenieur

Aktualisierung der Berechtigungssätze und Zuweisungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktualisieren Sie die Berechtigungssätze und Zuweisungen.	Wenn die `MoveAccount` EventBridge Amazon-Regel Änderungen an den Konten in der Organisation feststellt, wendet die CI/CD pipeline automatically starts and	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	updates the permission sets. For example, if you add an account to an OU specified in the assignments JSON file, then the CI/CD Pipeline den Berechtigungssatz auf das neue Konto an. Wenn Sie die bereitges tellten Berechtigungssätze und Zuweisungen ändern möchten, aktualisieren Sie die JSON-Dateien und übertrage n Sie sie dann in das Remote-Repository. Beachten Sie Folgendes , wenn Sie die CI/CD-Pip eline verwenden, um zuvor bereitgestellte Berechtig ungssätze und Zuordnungen zu verwalten: • Wenn Sie den Namen eines Berechtigungssatze s ändern, löscht die CI/CD-Pipeline den ursprünglichen Berechtigungssatz und erstellt einen neuen. • Diese Pipeline verwaltet nur Berechtigungssätze, die das Tag enthalten. `SSOPipeli ne:true` • Sie können mehrere Berechtigungssätze und	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Vorlagen für Zuweisungen in demselben Ordner im Repository haben. • Wenn Sie eine Vorlage löschen, löscht die Pipeline die Zuweisung oder den Berechtigungssatz. • Wenn Sie einen gesamten JSON-Block für eine Zuweisung löschen, löscht die Pipeline die Zuweisung aus dem IAM Identity Center. • Sie können keinen Berechtigungssatz löschen, der einem zugewiesen ist. AWS-Konto Zunächst müssen Sie die Zuweisung des Berechtigungssatzes aufheben.	

Fehlerbehebung

Problem	Lösung
Fehler aufgrund einer Zugriffsverweigerung	Vergewissern Sie sich, dass Sie über die erforderlichen Berechtigungen verfügen, um die CloudFormation Vorlagen und die darin definierten Ressourcen bereitzustellen. Weitere Informationen finden Sie in der CloudFormation Dokumentation unter Zugriffskontrolle.

Problem	Lösung
Pipeline-Fehler in der Validierungsphase	Dieser Fehler tritt auf, wenn der Berechtigungssatz oder die Zuweisungsvorlagen Fehler enthalten. 1. Sehen Sie CodeBuild sich unter die Build-Details an. 2. Suchen Sie im Build-Log nach dem Validierungsfehler, der weitere Informationen darüber enthält, was zum Fehlschlagen des Builds geführt hat. 3. Aktualisieren Sie den Berechtigungssatz oder die Zuweisungsvorlagen, und übertragen Sie sie anschließend in das Repository. 4. Die CI/CD-Pipeline startet das Projekt neu. CodeBuild Überwachen Sie den Status, um sicherzustellen, dass der Validierungsfehler behoben wurde.

Zugehörige Ressourcen

- Berechtigungssätze (IAM Identity Center-Dokumentation)

Anmeldeinformationen mit AWS Secrets Manager verwalten

Erstellt von Durga Prasad Cheepuri (AWS)

Übersicht

Dieses Muster führt Sie durch die Verwendung von AWS Secrets Manager zum dynamischen Abrufen von Datenbankanmeldedaten für eine Java Spring-Anwendung.

Wenn Sie eine angepasste Anwendung erstellt haben, die Informationen aus einer Datenbank abruft, mussten Sie bisher normalerweise die Anmeldeinformationen (das Secret) für den Zugriff auf die Datenbank direkt in die Anwendung einbetten. Als es an der Zeit war, die Anmeldeinformationen zu wechseln, mussten Sie Zeit investieren, um die Anwendung so zu aktualisieren, dass sie die neuen Anmeldeinformationen verwendet, und dann die aktualisierte Anwendung verteilen. Wenn Sie über mehrere Anwendungen mit gemeinsamen Anmeldeinformationen verfügten und Sie es versäumten, eine davon zu aktualisieren, schlug die Anwendung fehl. Aufgrund dieses Risikos entschieden sich viele Benutzer dafür, ihre Anmeldeinformationen nicht regelmäßig zu wechseln, wodurch ein Risiko durch ein anderes ersetzt wurde.

Secrets Manager ermöglicht es Ihnen, hartcodierte Anmeldeinformationen in Ihrem Code (einschließlich Kennwörtern) durch einen API-Aufruf zu ersetzen, um das Geheimnis programmgesteuert abzurufen. Dadurch wird sichergestellt, dass das Geheimnis nicht von jemandem, der Ihren Code untersucht, kompromittiert werden kann, da das Geheimnis einfach nicht vorhanden ist. Sie können Secrets Manager auch so konfigurieren, dass das Secret automatisch nach einem von Ihnen angegebenen Zeitplan rotiert wird. Auf diese Weise können Sie langfristige Geheimnisse durch kurzfristige ersetzen, wodurch das Risiko von Kompromissen erheblich reduziert wird. Weitere Informationen finden Sie in der Dokumentation zu AWS Secrets Manager.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein AWS-Konto mit Zugriff auf Secrets Manager
- Eine Java Spring-Anwendung

Architektur

Quelltechnologie-Stack

- Eine Java Spring-Anwendung mit Code, der auf eine Datenbank zugreift, wobei die DB-Anmeldeinformationen über die Datei application.properties verwaltet werden.

Zieltechnologie-Stack

- Eine Java Spring-Anwendung mit Code, der auf eine Datenbank zugreift, wobei die DB-Anmeldeinformationen in Secrets Manager verwaltet werden. Die Datei application.properties enthält die Geheimnisse von Secrets Manager.

Secrets Manager Manager-Integration mit einer Anwendung

Tools

- Secrets Manager — AWS Secrets Manager ist ein AWS-Service, der Ihnen die Verwaltung von Geheimnissen erleichtert. Bei den Secrets kann es sich um Datenbank-Anmeldeinformationen, Passwörter, API-Schlüssel von Drittanbietern und sogar beliebigen Text handeln. Sie können diese Secrets zentral speichern und den Zugriff darauf kontrollieren, indem Sie die Secrets Manager Manager-Konsole, die Secrets Manager Manager-Befehlszeilenschnittstelle (CLI) oder die Secrets Manager Manager-API und verwenden. SDKs

Epen

Geheimnis im Secrets Manager speichern

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Speichern Sie die DB-Anmeld einformationen als geheim in Secrets Manager.	Speichern Sie Amazon Relational Database Service (Amazon RDS) oder andere DB-Anmeldeinformationen als geheim in Secrets Manager, indem Sie die Schritte unter Creating a Secret in der Secrets Manager-Dokumentat ion befolgen.	Systemadministrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie die Berechtigungen für die Spring-Anwendung für den Zugriff auf Secrets Manager fest.	Legen Sie die entsprechenden Berechtigungen fest, je nachdem, wie die Java Spring-Anwendung Secrets Manager verwendet. Um den Zugriff auf den Secret zu kontrollieren, erstellen Sie eine Richtlinie auf der Grundlage der Informationen in der Secrets Manager-Dokumentation in den Abschnitten Verwenden identitätsbasierter Richtlinien (IAM-Richtlinien) und ABAC für Secrets Manager und Verwenden ressourcenbasierter Richtlinien für Secrets Manager. Folgen Sie den Schritten im Abschnitt Abrufen des geheimen Werts in der Secrets Manager-Dokumentation.	Sys-Admin

Aktualisieren Sie die Spring-Anwendung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie JAR-Abhängigkeiten hinzu, um Secrets Manager zu verwenden.	Einzelheiten finden Sie im Abschnitt Zusätzliche Informationen.	Java-Entwickler
Fügen Sie die Details des Geheimnisses zur Spring-Anwendung hinzu.	Aktualisieren Sie die Datei application.properties mit dem geheimen Namen, den Endpunkten und der AWS-	Java-Entwickler

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Region. Ein Beispiel finden Sie im Abschnitt Zusätzliche Informationen.	
Aktualisieren Sie den Code zum Abrufen von DB-Anmeld einformationen in Java.	Aktualisieren Sie in der Anwendung den Java-Code, der die DB-Anmeldeinformat ionen abruft, um diese Details aus Secrets Manager abzurufen. Beispielcode finden Sie im Abschnitt Zusätzliche Informationen.	Java-Entwickler

Zugehörige Ressourcen

- Dokumentation zu AWS Secrets Manager
- Verwendung identitätsbasierter Richtlinien (IAM-Richtlinien) und ABAC für Secrets Manager
- Verwendung ressourcenbasierter Richtlinien für Secrets Manager
- Beispielcode

Zusätzliche Informationen

Hinzufügen von JAR-Abhängigkeiten für die Verwendung von Secrets Manager

Maven:

```
<groupId>com.amazonaws</groupId>
    <artifactId>aws-java-sdk-secretsmanager</artifactId>
    <version>1.11. 355 </version>
```

Gradle:

```
compile group: 'com.amazonaws', name: 'aws-java-sdk-secretsmanager', version:
 '1.11.355'
```

Aktualisierung der Datei application.properties mit den Details des Geheimnisses

```
spring.aws.secretsmanager.secretName=postgres-local
spring.aws.secretsmanager.endpoint=secretsmanager.us-east-1.amazonaws.com
spring.aws.secretsmanager.region=us-east-1
```

Aktualisierung des Codes zum Abrufen von DB-Anmeldeinformationen in Java

```
String  secretName  =  env.getProperty("spring.aws.secretsmanager.secretName");
String  endpoints  =  env.getProperty("spring.aws.secretsmanager.endpoint");
String  AWS Region  =  env.getProperty("spring.aws.secretsmanager.region");
AwsClientBuilder.EndpointConfiguration  config  =  new
  AwsClientBuilder.EndpointConfiguration(endpoints, AWS Region);
AWSSecretsManagerClientBuilder  clientBuilder  =
  AWSSecretsManagerClientBuilder.standard();
clientBuilder.setEndpointConfiguration(config);
AWSSecretsManager  client  =  clientBuilder.build();

ObjectMapper  objectMapper  =  new  ObjectMapper();

JsonNode  secretsJson  =  null;

ByteBuffer  binarySecretData;

GetSecretValueRequest  getSecretValueRequest  =  new
  GetSecretValueRequest().withSecretId(secretName);

GetSecretValueResult  getSecretValueResponse  =  null;

try  {
     getSecretValueResponse  =  client.getSecretValue(getSecretValueRequest);
    }

catch  (ResourceNotFoundException  e)  {
     log.error("The requested secret "  +  secretName  +  " was not found");
    }

catch  (InvalidRequestException  e)  {
     log.error("The request was invalid due to: "  +  e.getMessage());
     }

catch  (InvalidParameterException  e)  {
```

```
     log.error("The request had invalid params: "  +  e.getMessage());
     }
if  (getSecretValueResponse  ==  null)  {
     return  null;
     }  // Decrypted secret using the associated KMS key // Depending on whether the
 secret was a string or binary, one of these fields will be populated


String secret = getSecretValueResponse.getSecretString();

if (secret != null) {
     try {
                secretsJson  =  objectMapper.readTree(secret);
           }

     catch  (IOException  e)  {
                log.error("Exception while retrieving secret values: "  +
  e.getMessage());
           }
}

else  {
     log.error("The Secret String returned is null");

     return null;

     }
     String  host  =  secretsJson.get("host").textValue();
     String  port  =  secretsJson.get("port").textValue();
     String  dbname  =  secretsJson.get("dbname").textValue();
     String  username  =  secretsJson.get("username").textValue();
     String  password  =  secretsJson.get("password").textValue();
}
```

ElastiCache Cluster für Sicherheitsgruppen überwachen

Erstellt von Susanne Kangnoh (AWS) und Archit Mathur (AWS)

Übersicht

Amazon ElastiCache ist ein Service von Amazon Web Services (AWS), der eine leistungsstarke, skalierbare und kostengünstige Caching-Lösung für die Verteilung eines In-Memory-Datenspeichers oder einer Cache-Umgebung in der Cloud bietet. Er ruft Daten aus speicherinternen Datenspeichern mit hohem Durchsatz und niedriger Latenz ab. Diese Funktionalität macht sie zu einer beliebten Wahl für Echtzeit-Anwendungsfälle wie Caching, Sitzungsspeicher, Spiele, Geodatendienste, Echtzeitanalysen und Warteschlangen. ElastiCache bietet Redis- und Memcached-Datenspeicher, die beide Reaktionszeiten unter einer Millisekunde bieten.

Eine Sicherheitsgruppe fungiert als virtuelle Firewall für Ihre ElastiCache Instances, indem sie den eingehenden und ausgehenden Datenverkehr kontrolliert. Sicherheitsgruppen agieren auf Instanzebene, nicht auf Subnetzebene. Für jede Sicherheitsgruppe fügen Sie einen Regelsatz hinzu, der den eingehenden Datenverkehr zu Instances steuert, und einen separaten Regelsatz, der den ausgehenden Datenverkehr steuert. Sie können Regeln zum Zulassen, aber keine Regeln zum Ablehnen angeben.

Dieses Muster bietet eine Sicherheitskontrolle, die API-Aufrufe überwacht und in Amazon CloudWatch Events ein Ereignis für die ModifyReplicationGroupOperationen CreateReplicationGroupCreateCacheCluster, ModifyCacheCluster, und generiert. Dieses Ereignis ruft eine AWS Lambda Funktion auf, die ein Python-Skript ausführt. Die Funktion ruft die Replikationsgruppen-ID aus der JSON-Eingabe des Ereignisses ab und führt die folgenden Prüfungen durch, um festzustellen, ob eine Sicherheitsverletzung vorliegt:

- Überprüft, ob die Sicherheitsgruppe des Clusters mit der Sicherheitsgruppe übereinstimmt, die in der Lambda-Funktion konfiguriert ist.
- Wenn die Sicherheitsgruppe des Clusters nicht übereinstimmt, sendet die Funktion mithilfe einer Amazon Simple Notification Service (Amazon SNS) -Benachrichtigung eine Verstoßmeldung an eine von Ihnen angegebene E-Mail-Adresse.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS Konto.
- Ein Amazon Simple Storage Service (Amazon S3) -Bucket zum Hochladen des bereitgestellten Lambda-Codes.
- Eine E-Mail-Adresse, an die Sie Benachrichtigungen über Verstöße erhalten möchten.
- ElastiCache Protokollierung aktiviert, für den Zugriff auf alle API-Protokolle.

Einschränkungen

- Diese Detective Control ist regional und muss in allen Bereichen eingesetzt werden AWS-Region , die Sie überwachen möchten.
- Das Steuerelement unterstützt Replikationsgruppen, die in einer Virtual Private Cloud (VPC) ausgeführt werden.

Architektur

Workflow-Architektur

Automatisierung und Skalierung

- Wenn Sie diese Vorlage verwenden AWS Organizations, können Sie AWS CloudFormation StackSetssie verwenden, um sie für mehrere Konten bereitzustellen, die Sie überwachen möchten.

Tools

AWS Dienste

- Amazon ElastiCache macht es einfach, verteilte In-Memory-Cache-Umgebungen in der einzurichten, zu verwalten und zu skalieren. AWS Cloud Es bietet einen leistungsstarken, in der Größe anpassbaren und kostengünstigen In-Memory-Cache und verringert gleichzeitig die Komplexität, die mit der Bereitstellung und Verwaltung einer verteilten Cache-Umgebung verbunden ist. ElastiCache funktioniert sowohl mit der Redis- als auch mit der Memcached-Engine.
- AWS CloudFormationhilft Ihnen dabei, Ihre AWS Ressourcen zu modellieren und einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus zu verwalten. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben und sie zusammen als Stapel zu starten und zu konfigurieren, anstatt Ressourcen

einzeln zu verwalten. Sie können Stacks über mehrere und hinweg verwalten AWS-Konten und AWS-Regionen bereitstellen.

- Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS Ressourcen beschreiben, nahezu in Echtzeit. CloudWatch Events erkennt betriebliche Änderungen, sobald sie eintreten, und ergreift bei Bedarf Korrekturmaßnahmen, indem es Nachrichten sendet, um auf die Umgebung zu reagieren, Funktionen aktiviert, Änderungen vornimmt und Statusinformationen erfasst.
- AWS Lambdaist ein Rechendienst, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch von wenigen Anfragen pro Tag auf Tausende pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.
- Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet den Versand von Nachrichten zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Code

Dieses Muster beinhaltet einen Anhang mit zwei Dateien:

- `ElastiCacheAllowedSecurityGroup.zip`ist eine komprimierte Datei, die die Sicherheitskontrolle (Lambda-Code) enthält.
- `ElastiCacheAllowedSecurityGroup.yml`ist eine CloudFormation Vorlage, die die Sicherheitskontrolle bereitstellt.

Informationen zur Verwendung dieser Dateien finden Sie im Abschnitt Epics.

Epen

Stellen Sie die Sicherheitskontrolle bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Code in einen S3-Bucket hoch.	Erstellen Sie einen neuen S3-Bucket oder verwenden Sie einen vorhandenen S3-	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bucket, um die angehängte `ElastiCacheAllowedSecurityGroup.zip` Datei hochzuladen (Lambda-Code). Dieser Bucket muss sich in demselben Bereich befinden AWS-Region wie die Ressourcen, die Sie auswerten möchten.	
Stellen Sie die CloudFormation Vorlage bereit.	Öffnen Sie die CloudFormation Konsole genauso AWS-Region wie der S3-Bucket und stellen Sie die `ElastiCacheAllowedSecurityControl.yml` Datei bereit, die im Anhang enthalten ist. Geben Sie im nächsten Epic Werte für die Vorlagenparameter an.	Cloud-Architekt

Vervollständigen Sie die Parameter in der CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den S3-Bucket-Namen an.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epic erstellt oder ausgewählt haben. Dieser S3-Bucket enthält die ZIP-Datei für den Lambda-Code und muss sich in derselben Datei AWS-Region wie die CloudFormation Vorlage und	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	die Ressource befinden, die ausgewertet werden.	
Geben Sie den S3-Schlüssel an.	Geben Sie den Speicherort der Lambda-Code-ZIP-Datei in Ihrem S3-Bucket an, ohne vorangestellte Schrägstriche (z. B. `ElasticCacheAllowedSecurityGroup.zip` oder). `controls/ElasticCacheAllowedSecurityGroup.zip`	Cloud-Architekt
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine aktive E-Mail-Adresse an, unter der Sie Benachrichtigungen über Verstöße erhalten möchten.	Cloud-Architekt
Geben Sie eine Protokollierungsebene an.	Geben Sie die Protokollierungsebene und die Ausführlichkeit an. `Info`bezeichnet detaillierte Informationsmeldungen über den Fortschritt der Anwendung und sollte nur zum Debuggen verwendet werden. `Error`bezeichnet Fehlerereignisse, die es der Anwendung dennoch ermöglichen könnten, weiter zu laufen. `Warning`bezeichnet potenziell schädliche Situationen.	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das E-Mail-Abonnement.	Wenn die CloudFormation Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail-Nachricht an die von Ihnen angegebene E-Mail-Adresse. Um Benachrichtigungen zu erhalten, müssen Sie dieses E-Mail-Abonnement bestätigen.	Cloud-Architekt

Zugehörige Ressourcen

- Einen Stack auf der AWS CloudFormation Konsole erstellen (AWS CloudFormation Dokumentation)
- Amazon VPCs und ElastiCache Sicherheit (ElastiCache Amazon-Dokumentation)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Überwachen Sie Amazon EMR-Cluster beim Start auf Verschlüsselung während der Übertragung

Erstellt von Susanne Kangnoh (AWS)

Übersicht

Dieses Muster bietet eine Sicherheitskontrolle, die Amazon EMR-Cluster beim Start überwacht und eine Warnung sendet, wenn die Verschlüsselung während der Übertragung nicht aktiviert wurde.

Amazon EMR ist ein Webservice, mit dem Sie auf einfache Weise Big-Data-Frameworks wie Apache Hadoop ausführen können, um Daten zu verarbeiten und zu analysieren. Amazon EMR ermöglicht es Ihnen, riesige Datenmengen auf kostengünstige Weise zu verarbeiten, indem Sie Mapping- und Reduction-Schritte parallel ausführen.

Die Datenverschlüsselung verhindert, dass unbefugte Benutzer auf Daten im Ruhezustand oder Daten während der Übertragung zugreifen oder diese lesen. Daten im Ruhezustand beziehen sich auf Daten, die auf Medien wie einem lokalen Dateisystem auf jedem Knoten, Hadoop Distributed File System (HDFS) oder dem EMR File System (EMRFS) über Amazon Simple Storage Service (Amazon S3) gespeichert sind. Bei der Übertragung von Daten handelt es sich um Daten, die über das Netzwerk übertragen werden und zwischen Aufträgen übertragen werden. Die Verschlüsselung während der Übertragung unterstützt Open-Source-Verschlüsselungsfunktionen für Apache Spark, Apache TEZ, Apache Hadoop, Apache und Presto. HBase Sie aktivieren die Verschlüsselung, indem Sie über die AWS-Befehlszeilenschnittstelle (AWS CLI), die Konsole oder AWS SDKs eine Sicherheitskonfiguration erstellen und die Datenverschlüsselungseinstellungen angeben. Sie können die Verschlüsselungsartefakte für die Verschlüsselung während der Übertragung auf zwei Arten bereitstellen:

- Durch Hochladen einer komprimierten Zertifikatsdatei auf Amazon S3.
- Durch Verweisen auf eine benutzerdefinierte Java-Klasse, die Verschlüsselungsartefakte bereitstellt.

Die in diesem Muster enthaltene Sicherheitskontrolle überwacht API-Aufrufe und generiert ein Amazon CloudWatch Events-Ereignis für die RunJobFlowAktion. Das Ereignis ruft eine AWS-Lambda-Funktion auf, die ein Python-Skript ausführt. Die Funktion ruft die EMR-Cluster-ID aus der JSON-Eingabe des Ereignisses ab und führt die folgenden Prüfungen durch, um festzustellen, ob eine Sicherheitsverletzung vorliegt:

- Überprüft, ob der EMR-Cluster über eine Amazon EMR-spezifische Sicherheitskonfiguration verfügt.
- Wenn der Cluster über eine Sicherheitskonfiguration verfügt, wird geprüft, ob die Verschlüsselung bei der Übertragung aktiviert ist.
- Wenn der Cluster nicht über eine Sicherheitskonfiguration verfügt, sendet er mithilfe von Amazon Simple Notification Service (Amazon SNS) eine Warnung an eine von Ihnen angegebene E-Mail-Adresse. In der Benachrichtigung werden der EMR-Clustername, Einzelheiten zum Verstoß, AWS-Regions- und Kontoinformationen sowie der AWS-Lambda-ARN (Amazon-Ressourcenname) angegeben, von dem die Benachrichtigung stammt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein S3-Bucket zum Hochladen des Lambda-Codes, der mit diesem Muster bereitgestellt wird.
- Eine E-Mail-Adresse, an die Sie Benachrichtigungen über Verstöße erhalten möchten.
- Amazon EMR-Protokollierung aktiviert, für den Zugriff auf alle API-Protokolle.

Einschränkungen

- Diese Detective Control ist regional und muss in jeder AWS-Region eingesetzt werden, die Sie überwachen möchten.

Produktversionen

- Amazon EMR Version 4.8.0 oder höher.

Architektur

Workflow-Architektur

Automatisierung und Skalierung

- Wenn Sie AWS Organizations verwenden, können Sie AWS Cloudformation verwenden, StackSets um die Vorlage in mehreren Konten bereitzustellen, die Sie überwachen möchten.

Tools

AWS-Services

- Amazon EMR — Amazon EMR ist eine verwaltete Cluster-Plattform, die die Ausführung von Big-Data-Frameworks wie Apache Hadoop und Apache Spark auf AWS vereinfacht, um riesige Datenmengen zu verarbeiten und zu analysieren. Durch die Verwendung dieser Frameworks und verwandter Open-Source-Projekte können Sie Daten zu Analysezwecken und Business-Intelligence-Workloads verarbeiten. Darüber hinaus können Sie Amazon EMR verwenden, um große Datenmengen in und aus anderen AWS-Datenspeichern und Datenbanken wie Amazon S3 und Amazon DynamoDB zu transformieren und zu verschieben.
- AWS Cloudformation — AWS CloudFormation hilft Ihnen dabei, Ihre AWS-Ressourcen zu modellieren und einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus zu verwalten. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben und sie zusammen als Stack zu starten und zu konfigurieren, anstatt Ressourcen einzeln zu verwalten. Sie können Stacks für mehrere AWS-Konten und AWS-Regionen verwalten und bereitstellen.
- AWS Cloudwatch Events — Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit. CloudWatch Events erkennt betriebliche Änderungen, sobald sie eintreten, und ergreift bei Bedarf Korrekturmaßnahmen, indem es Nachrichten sendet, um auf die Umgebung zu reagieren, Funktionen aktiviert, Änderungen vornimmt und Statusinformationen erfasst.
- AWS Lambda — AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch von wenigen Anfragen pro Tag auf Tausende pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.
- AWS SNS — Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet den Versand von Nachrichten zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Code

Dieses Muster beinhaltet einen Anhang mit zwei Dateien:

- `EMRInTransitEncryption.zip`ist eine komprimierte Datei, die die Sicherheitskontrolle (Lambda-Code) enthält.
- `EMRInTransitEncryption.yml`ist eine CloudFormation Vorlage, die die Sicherheitskontrolle bereitstellt.

Informationen zur Verwendung dieser Dateien finden Sie im Abschnitt Epics.

Epen

Stellen Sie die Sicherheitskontrolle bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Code in einen S3-Bucket hoch.	Erstellen Sie einen neuen S3-Bucket oder verwenden Sie einen vorhandenen S3-Bucket, um die angehängte `EMRInTransitEncryption.zip` Datei hochzuladen (Lambda-Code). Dieser Bucket muss sich in derselben AWS-Region befinden wie die CloudFormation Vorlage und die Ressourcen, die Sie bewerten möchten.	Cloud-Architekt
Stellen Sie die CloudFormation Vorlage bereit.	Öffnen Sie die Cloudformation-Konsole in derselben AWS-Region wie der S3-Bucket und stellen Sie die `EMRInTransitEncryption.yml` Datei bereit, die im Anhang bereitgestellt wird. Geben Sie im nächsten	Cloud-Architekt,

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Epic Werte für die Vorlagenp arameter an.	

Vervollständigen Sie die Parameter in der CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den S3-Bucket-Namen an.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epic erstellt oder ausgewählt haben. Dieser S3-Bucket enthält die ZIP-Datei für den Lambda-Code und muss sich in derselben AWS-Region befinden wie die CloudFormation Vorlage und die Ressource, die ausgewert et werden.	Cloud-Architekt
Geben Sie den S3-Schlüssel an.	Geben Sie den Speicherort der Lambda-Code-ZIP-Da tei in Ihrem S3-Bucket ohne führende Schrägstriche an (z. B. `EMRInTransitEncryp tion.zip` oder). `controls/EMRInTran sitEncryption.zip`	Cloud-Architekt
Geben Sie eine E-Mail-Ad resse an.	Geben Sie eine aktive E-Mail-Adresse an, an die Sie Benachrichtigungen über Verstöße erhalten möchten.	Cloud-Architekt
Geben Sie eine Protokoll ierungsebene an.	Geben Sie die Protokoll ierungsebene und die	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ausführlichkeit für die Lambda-Protokolle an. `Info`bezeichnet detaillierte Informationsmeldungen über den Fortschritt der Anwendung und sollte nur zum Debuggen verwendet werden. `Error`bezeichnet Fehlerereignisse, die es der Anwendung dennoch ermöglichen könnten, weiter zu laufen. `Warning`bezeichnet potenziell schädliche Situationen.	

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das E-Mail-Abonnement.	Wenn die CloudFormation Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail-Nachricht an die von Ihnen angegebene E-Mail-Adresse. Um Benachrichtigungen zu erhalten, müssen Sie dieses E-Mail-Abonnement bestätigen.	Cloud-Architekt

Zugehörige Ressourcen

- Einen Stack auf der CloudFormation AWS-Konsole erstellen (CloudFormation AWS-Dokumentation)

- Verschlüsselungsoptionen (Amazon EMR-Dokumentation)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

ElastiCache Amazon-Cluster auf Verschlüsselung im Ruhezustand überwachen

Erstellt von Susanne Kangnoh (AWS)

Übersicht

Amazon ElastiCache ist ein Service von Amazon Web Services (AWS), der eine leistungsstarke, skalierbare und kostengünstige Caching-Lösung für die Verteilung eines In-Memory-Datenspeichers oder einer Cache-Umgebung in der Cloud bietet. Er ruft Daten aus In-Memory-Datenspeichern mit hohem Durchsatz und niedriger Latenz ab. Diese Funktionalität macht sie zu einer beliebten Wahl für Echtzeit-Anwendungsfälle wie Caching, Sitzungsspeicher, Spiele, Geodatendienste, Echtzeitanalysen und Warteschlangen. ElastiCache bietet Redis- und Memcached-Datenspeicher, die beide Reaktionszeiten unter einer Millisekunde bieten.

Datenverschlüsselung verhindert, dass unbefugte Benutzer sensible Daten lesen, die auf Ihren Redis-Clustern und den zugehörigen Cache-Speichersystemen verfügbar sind. Dazu gehören Daten, die auf persistenten Medien gespeichert sind (sogenannte Data at Rest), und Daten, die auf ihrem Weg durch das Netzwerk zwischen Clients und Cache-Servern abgefangen werden können (sogenannte Daten während der Übertragung).

Sie können die Verschlüsselung im Ruhezustand ElastiCache für Redis aktivieren, wenn Sie eine Replikationsgruppe erstellen, indem Sie den AtRestEncryptionEnabledParameter auf true setzen. Wenn dieser Parameter aktiviert ist, verschlüsselt er die Festplatte bei Synchronisierungs-, Sicherungs- und Swap-Vorgängen und verschlüsselt Backups, die in Amazon Simple Storage Service (Amazon S3) gespeichert sind. Sie können die Verschlüsselung im Ruhezustand nicht für eine bestehende Replikationsgruppe aktivieren. Wenn Sie eine Replikationsgruppe erstellen, können Sie die Verschlüsselung im Ruhezustand auf zwei Arten aktivieren:

- Indem Sie die Standardoption wählen, bei der vom Service verwaltete Verschlüsselung im Ruhezustand verwendet wird.
- Indem Sie einen vom Kunden verwalteten Schlüssel verwenden und die Schlüssel-ID oder den Amazon-Ressourcennamen (ARN) von AWS Key Management Service (AWS KMS) angeben.

Dieses Muster bietet eine Sicherheitskontrolle, die API-Aufrufe überwacht und bei diesem CreateReplicationGroupVorgang ein Amazon CloudWatch Events-Ereignis generiert. Dieses Ereignis ruft eine AWS-Lambda-Funktion auf, die ein Python-Skript ausführt. Die Funktion ruft

die Replikationsgruppen-ID aus der JSON-Eingabe des Ereignisses ab und führt die folgenden Prüfungen durch, um festzustellen, ob eine Sicherheitsverletzung vorliegt:

- Prüft, ob der AtRestEncryptionEnabledSchlüssel existiert.
- Falls AtRestEncryptionEnabledvorhanden, wird der Wert überprüft, um festzustellen, ob er wahr ist.
- Wenn der AtRestEncryptionEnabledWert auf False gesetzt ist, wird eine Variable festgelegt, die Verstöße verfolgt und mithilfe einer Amazon Simple Notification Service (Amazon SNS) - Benachrichtigung eine Verstoßmeldung an eine von Ihnen angegebene E-Mail-Adresse sendet.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Ein S3-Bucket zum Hochladen des bereitgestellten Lambda-Codes.
- Eine E-Mail-Adresse, an die Sie Benachrichtigungen über Verstöße erhalten möchten.
- ElastiCache Protokollierung aktiviert, für den Zugriff auf alle API-Protokolle.

Einschränkungen

- Diese Detective Control ist regional und muss in jeder AWS-Region eingesetzt werden, die Sie überwachen möchten.
- Das Steuerelement unterstützt Replikationsgruppen, die in einer Virtual Private Cloud (VPC) ausgeführt werden.
- Das Steuerelement unterstützt Replikationsgruppen, auf denen die folgenden Knotentypen ausgeführt werden:
  - R5, R4, R3
  - M5, M4, M3
  - T3, T2

Produktversionen

- ElastiCache für Redis Version 3.2.6 oder höher

Architektur

Workflow-Architektur

Automatisierung und Skalierung

- Wenn Sie AWS Organizations verwenden, können Sie AWS Cloudformation verwenden, StackSets um diese Vorlage in mehreren Konten bereitzustellen, die Sie überwachen möchten.

Tools

AWS-Services

- Amazon ElastiCache — Amazon ElastiCache macht es einfach, verteilte In-Memory-Cache-Umgebungen in der AWS-Cloud einzurichten, zu verwalten und zu skalieren. Es bietet einen leistungsstarken, in der Größe anpassbaren und kostengünstigen In-Memory-Cache und verringert gleichzeitig die Komplexität, die mit der Bereitstellung und Verwaltung einer verteilten Cache-Umgebung verbunden ist. ElastiCache funktioniert sowohl mit der Redis- als auch mit der Memcached-Engine.
- AWS CloudFormation — AWS CloudFormation hilft Ihnen dabei, Ihre AWS-Ressourcen zu modellieren und einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus zu verwalten. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben und sie zusammen als Stapel zu starten und zu konfigurieren, anstatt Ressourcen einzeln zu verwalten. Sie können Stacks für mehrere AWS-Konten und AWS-Regionen verwalten und bereitstellen.
- AWS Cloudwatch Events — Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit. CloudWatch Events erkennt betriebliche Änderungen, sobald sie eintreten, und ergreift bei Bedarf Korrekturmaßnahmen, indem es Nachrichten sendet, um auf die Umgebung zu reagieren, Funktionen aktiviert, Änderungen vornimmt und Statusinformationen erfasst.
- AWS Lambda — AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch von wenigen Anfragen pro Tag auf Tausende pro Sekunde. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird.

- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet den Versand von Nachrichten zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Code

Dieses Muster beinhaltet einen Anhang mit zwei Dateien:

- `ElasticCache-EncryptionAtRest.zip`ist eine komprimierte Datei, die die Sicherheitskontrolle (Lambda-Code) enthält.
- `elasticache_encryption_at_rest.yml`ist eine CloudFormation Vorlage, die die Sicherheitskontrolle bereitstellt.

Informationen zur Verwendung dieser Dateien finden Sie im Abschnitt Epics.

Epen

Stellen Sie die Sicherheitskontrolle bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Code in einen S3-Bucket hoch.	Erstellen Sie einen neuen S3-Bucket oder verwenden Sie einen vorhandenen S3-Bucket, um die angehängte `ElastiCache-EncryptionAtRest.zip` Datei hochzuladen (Lambda-Code). Dieser Bucket muss sich in derselben AWS-Region befinden wie die Ressourcen, die Sie bewerten möchten.	Cloud-Architekt
Stellen Sie die CloudFormation Vorlage bereit.	Öffnen Sie die Cloudformation-Konsole in derselben AWS-Region wie der S3-	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bucket und stellen Sie die `elasticache_encryption_at_rest.yml` Datei bereit, die im Anhang bereitgestellt wird. Geben Sie im nächsten Epic Werte für die Vorlagenparameter an.	

Vervollständigen Sie die Parameter in der CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den S3-Bucket-Namen an.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epic erstellt oder ausgewählt haben. Dieser S3-Bucket enthält die ZIP-Datei für den Lambda-Code und muss sich in derselben AWS-Region befinden wie die CloudFormation Vorlage und die Ressource, die ausgewertet werden.	Cloud-Architekt
Geben Sie den S3-Schlüssel an.	Geben Sie den Speicherort der Lambda-Code-ZIP-Datei in Ihrem S3-Bucket an, ohne vorangestellte Schrägstriche (z. B. `ElasticCache-EncryptionAtRest.zip` oder). `controls/ElasticCache-EncryptionAtRest.zip`	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine aktive E-Mail-Adresse an, unter der Sie Benachrichtigungen über Verstöße erhalten möchten.	Cloud-Architekt
Geben Sie eine Protokollierungsebene an.	Geben Sie die Protokollierungsebene und die Ausführlichkeit an. `Info`bezeichnet detaillierte Informationsmeldungen über den Fortschritt der Anwendung und sollte nur zum Debuggen verwendet werden. `Error`bezeichnet Fehlerereignisse, die es der Anwendung dennoch ermöglichen könnten, weiter zu laufen. `Warning`bezeichnet potenziell schädliche Situationen.	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das E-Mail-Abonnement.	Wenn die CloudFormation Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail-Nachricht an die von Ihnen angegebene E-Mail-Adresse. Um Benachrichtigungen zu erhalten, müssen Sie dieses E-Mail-Abonnement bestätigen.	Cloud-Architekt

Zugehörige Ressourcen

- Einen Stack auf der CloudFormation AWS-Konsole erstellen (CloudFormation AWS-Dokumentation)
- Verschlüsselung im Ruhezustand ElastiCache für Redis (ElastiCache Amazon-Dokumentation)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Überwachen Sie EC2 Instanzschlüsselpaare mit AWS Config

Erstellt von Wassim Benhallam (AWS), Sergio Bilbao Lopez (AWS) und Vikrant Telkar (AWS)

Übersicht

Beim Starten einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance in der Amazon Web Services (AWS) -Cloud empfiehlt es sich, ein vorhandenes key pair zu erstellen oder zu verwenden, um eine Verbindung mit der Instance herzustellen. Das key pair, das aus einem in der Instanz gespeicherten öffentlichen Schlüssel und einem privaten Schlüssel besteht, der dem Benutzer zur Verfügung gestellt wird, ermöglicht den sicheren Zugriff über Secure Shell (SSH) auf die Instanz und vermeidet die Verwendung von Passwörtern. Manchmal können Benutzer jedoch versehentlich Instances starten, ohne ein key pair anzuhängen. Da Schlüsselpaare nur beim Start einer Instance zugewiesen werden können, ist es wichtig, Instances, die ohne Schlüsselpaare gestartet wurden, schnell zu identifizieren und als nicht konform zu kennzeichnen. Dies ist besonders nützlich, wenn Sie in Konten oder Umgebungen arbeiten, die die Verwendung von Schlüsselpaaren für den Instanzzugriff vorschreiben.

Dieses Muster beschreibt, wie Sie in AWS Config eine benutzerdefinierte Regel zur Überwachung von EC2 Instance-Schlüsselpaaren erstellen. Wenn Instances als nicht konform identifiziert werden, wird eine Warnung mithilfe von Amazon Simple Notification Service (Amazon SNS) - Benachrichtigungen gesendet, die durch ein EventBridge Amazon-Ereignis ausgelöst wurden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- AWS Config ist für die AWS-Region aktiviert, die Sie überwachen möchten, und ist so konfiguriert, dass alle AWS-Ressourcen aufgezeichnet werden

Einschränkungen

- Diese Lösung ist regionsspezifisch. Alle Ressourcen sollten in derselben AWS-Region erstellt werden.

Architektur

Zieltechnologie-Stack

- AWS Config
- Amazon EventBridge
- AWS Lambda
- Amazon SNS

Zielarchitektur

1. AWS Config initiiert die Regel.
2. Die Regel ruft die Lambda-Funktion auf, um die Konformität von EC2 Instanzen zu bewerten.
3. Die Lambda-Funktion sendet den aktualisierten Konformitätsstatus an AWS Config.
4. AWS Config sendet ein Ereignis an EventBridge.
5. EventBridge veröffentlicht Benachrichtigungen über Compliance-Änderungen zu einem SNS-Thema.
6. Amazon SNS sendet eine Warnung per E-Mail.

Automatisierung und Skalierung

Die Lösung kann eine beliebige Anzahl von EC2 Instanzen innerhalb einer Region überwachen.

Tools

Tools

- AWS Config — AWS Config ist ein Service, mit dem Sie die Konfigurationen Ihrer AWS-Ressourcen bewerten, prüfen und bewerten können. AWS Config überwacht und zeichnet Ihre AWS-Ressourcenkonfigurationen kontinuierlich auf und ermöglicht Ihnen, die Auswertung aufgezeichneter Konfigurationen anhand der gewünschten Konfigurationen zu automatisieren.
- Amazon EventBridge — Amazon EventBridge ist ein serverloser Event-Bus-Service, der Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen verbindet.

- AWS Lambda — AWS Lambda ist ein serverloser Rechenservice, der die Ausführung von Code ohne Bereitstellung oder Verwaltung von Servern, die Erstellung einer auslastungsorientierten Cluster-Skalierungslogik, die Verwaltung von Eventintegrationen oder die Verwaltung von Laufzeiten unterstützt.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) ist ein vollständig verwalteter Messaging-Dienst sowohl für application-to-application (A2A) als auch für (A2P application-to-person) Kommunikation.

Code

Der Code für die Lambda-Funktion ist angehängt.

Epen

Erstellen Sie eine Lambda-Funktion zur Bewertung der Amazon-Compliance EC2

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine AWS Identity and Access Management (IAM) -Rolle für Lambda.	Wählen Sie in der AWS-Managementkonsole IAM und erstellen Sie dann die Rolle. Verwenden Sie Lambda als vertrauenswürdige Entität und fügen Sie die `AmazonEventBridgeFullAccess` Berechtigungen und hinzu. `AWSConfigRulesExecutionRole` Weitere Informationen finden Sie in der AWS-Dokumentation.	DevOps
Erstellen und implementieren Sie die Lambda-Funktion.	1. Erstellen Sie auf der Lambda-Konsole mithilfe von Author von Grund auf eine Funktion mit Python 3.6 als Laufzeit und der zuvor erstellten IAM-Rolle.	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Notieren Sie den Amazon-Ressourcennamen (ARN). 2. Wählen Sie auf der Registerkarte Code den Code aus`lambda_function.py`, der an dieses Muster angehängt ist, und fügen Sie ihn ein. 3. Um Ihre Änderungen zu speichern, wählen Sie Bereitstellen.	

Erstellen Sie eine benutzerdefinierte AWS Config-Regel

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie eine benutzerdefinierte AWS Config-Regel hinzu.	Fügen Sie in der AWS Config-Konsole eine benutzerdefinierte Regel mit den folgenden Einstellungen hinzu: • ARN — Der ARN der zuvor erstellten Lambda-Funktion • Triggertyp — Konfigurationsänderungen • Umfang der Änderungen — Ressourcen • Ressourcentyp — EC2 Amazon-Instance Weitere Informationen finden Sie in der AWS-Dokumentation.	DevOps

Konfigurieren Sie E-Mail-Benachrichtigungen, wenn ein Compliance-Änderungsereignis erkannt wird

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das SNS-Thema und das Abonnement.	Erstellen Sie in der Amazon SNS SNS-Konsole ein Thema mit dem Typ Standard und anschließend ein Abonnement mit E-Mail als Protokoll. Wenn Sie die Bestätigungs-E-Mail erhalten, wählen Sie den Link zur Bestätigung des Abonnements. Weitere Informationen finden Sie in der AWS-Dokumentation.	DevOps
Erstellen Sie eine EventBridge Regel, um Amazon SNS SNS-Benachrichtigungen zu initiieren.	Erstellen Sie auf der EventBridge Konsole eine Regel mit den folgenden Einstellungen: • Dienstname — AWS Config • Ereignistyp — Änderung der Konformität der Konfigurationsregeln • Nachrichtentyp — Spezifische Nachrichtentypen, ComplianceChangeNotification • Spezifischer Regelname — Der Name Ihrer zuvor erstellten AWS Config-Regel • Ziel — SNS-Thema, Ihr zuvor erstelltes Thema	DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Weitere Informationen finden Sie in der AWS-Dokumentation.	

Überprüfen Sie die Regel und die Benachrichtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
EC2 Instanzen erstellen.	Erstellen Sie zwei EC2 Instanzen eines beliebigen Typs und hängen Sie ein key pair an, und erstellen Sie eine EC2 Instanz ohne key pair.	DevOps
Überprüfen Sie die Regel.	1. Wählen Sie in der AWS Config-Konsole auf der Seite Regeln Ihre Regel aus. 2. Um konforme und nicht konforme EC2 Instances zu sehen, ändern Sie Ressourcen im Geltungsbereich auf Alle. Stellen Sie sicher, dass zwei Instanzen als konform und eine Instanz als nicht konform aufgeführt sind. 3. Warten Sie, bis Sie die E-Mail-Benachrichtigung von Amazon SNS über den Compliance-Status der EC2 Instances erhalten.	DevOps

Zugehörige Ressourcen

- Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service
- Erstellen einer benutzerdefinierten Regel in AWS Config
- Ein Amazon SNS SNS-Thema erstellen
- Ein Amazon SNS SNS-Thema abonnieren
- Eine Regel in Amazon erstellen EventBridge

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

IAM-Root-Benutzeraktivitäten überwachen

Erstellt von Mostefa Brougui (AWS)

Übersicht

Jedes Amazon Web Services (AWS) -Konto hat einen Root-Benutzer. Als bewährte Sicherheitsmethode für AWS Identity and Access Management (IAM) empfehlen wir, dass Sie den Root-Benutzer verwenden, um die Aufgaben zu erledigen, die nur der Root-Benutzer ausführen kann. Die vollständige Liste finden Sie unter Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind, im Referenzhandbuch zur AWS-Kontoverwaltung. Da der Root-Benutzer vollen Zugriff auf all Ihre AWS-Ressourcen und Rechnungsinformationen hat, empfehlen wir Ihnen, dieses Konto nicht zu verwenden und es auf Aktivitäten zu überwachen, die darauf hindeuten könnten, dass die Root-Benutzeranmeldedaten kompromittiert wurden.

Mithilfe dieses Musters richten Sie eine ereignisgesteuerte Architektur ein, die den IAM-Root-Benutzer überwacht. Dieses Muster richtet eine hub-and-spoke Lösung ein, die mehrere AWS-Konten, die Spoke-Konten, überwacht und die Verwaltung und Berichterstattung in einem einzigen Konto, dem Hub-Konto, zentralisiert.

Wenn die IAM-Root-Benutzeranmeldedaten verwendet werden, CloudTrail zeichnen Amazon CloudWatch und AWS die Aktivität im Protokoll bzw. im Trail auf. Im Spoke-Konto sendet eine EventBridge Amazon-Regel das Ereignis an den zentralen Event-Bus im Hub-Konto. Im Hub-Konto sendet eine EventBridge Regel das Ereignis an eine AWS Lambda Lambda-Funktion. Die Funktion verwendet ein Amazon Simple Notification Service (Amazon SNS) -Thema, das Sie über die Root-Benutzeraktivität informiert.

In diesem Muster verwenden Sie eine CloudFormation AWS-Vorlage, um die Überwachungs- und Ereignisbehandlungsdienste in den Spoke-Konten bereitzustellen. Sie verwenden eine HashiCorp Terraform-Vorlage, um die Eventmanagement- und Benachrichtigungsdienste im Hub-Konto bereitzustellen.

Voraussetzungen und Einschränkungen

Voraussetzungen

1. Berechtigungen zur Bereitstellung von AWS-Ressourcen in Ihrer AWS-Umgebung.
2. Berechtigungen zur Bereitstellung von CloudFormation Stack-Sets. Weitere Informationen finden Sie unter Voraussetzungen für Stack-Set-Operationen (CloudFormation Dokumentation).

3. Terraform ist installiert und einsatzbereit. Weitere Informationen finden Sie unter Erste Schritte — AWS (Terraform-Dokumentation).
4. Ein vorhandener Trail in jedem Spoke-Konto. Weitere Informationen finden Sie unter Erste Schritte mit AWS CloudTrail (CloudTrail Dokumentation).
5. Der Trail ist so konfiguriert, dass Ereignisse an CloudWatch Logs gesendet werden. Weitere Informationen finden Sie unter Ereignisse an CloudWatch Protokolle senden (CloudTrail Dokumentation).
6. Ihre Hub-and-Spoke-Konten müssen von AWS Organizations verwaltet werden.

Architektur

Das folgende Diagramm veranschaulicht die Bausteine der Implementierung.

1. Wenn die CloudTrail IAM-Root-Benutzeranmeldedaten verwendet werden CloudWatch und die Aktivität im Protokoll bzw. im Trail aufgezeichnet wird.
2. Im Spoke-Konto sendet eine EventBridge Regel das Ereignis an den zentralen Event-Bus im Hub-Konto.
3. Im Hub-Konto sendet eine EventBridge Regel das Ereignis an eine Lambda-Funktion.
4. Die Lambda-Funktion verwendet ein Amazon SNS SNS-Thema, das Sie über die Root-Benutzeraktivität informiert.

Tools

AWS-Services

- AWS CloudFormation hilft Ihnen dabei, AWS-Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus über AWS-Konten und Regionen hinweg zu verwalten.
- AWS CloudTrail unterstützt Sie bei der Prüfung der Unternehmensführung, der Einhaltung von Vorschriften und des Betriebsrisikos Ihres AWS-Kontos.
- Amazon CloudWatch Logs hilft Ihnen dabei, die Protokolle all Ihrer Systeme, Anwendungen und AWS-Services zu zentralisieren, sodass Sie sie überwachen und sicher archivieren können.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS-Lambda-

Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen AWS-Konten.

- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Simple Notification Service (Amazon SNS) unterstützt Sie bei der Koordination und Verwaltung des Nachrichtenaustauschs zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.

Andere Tools und Dienste

- Terraform ist eine CLI-Anwendung zur Bereitstellung und Verwaltung von Cloud-Infrastruktur und -Ressourcen mithilfe von Code in Form von Konfigurationsdateien.

Code-Repository

Der Quellcode und die Vorlagen für dieses Muster sind in einem GitHub Repository verfügbar. Dieses Muster bietet zwei Vorlagen:

- Eine Terraform-Vorlage, die die Ressourcen enthält, die Sie im Hub-Konto bereitstellen
- Eine CloudFormation Vorlage, die Sie als Stackset-Instanz in den Spoke-Konten bereitstellen

Das Repository hat die folgende Gesamtstruktur.

```
.
 |__README.md
 |__spoke-stackset.yaml
 |__hub.tf
 |__root-activity-monitor-module
     |__main.tf  # contains Terraform code to deploy resources in the Hub account
     |__iam      # contains IAM policies JSON files
         |__ lambda-assume-policy.json          # contains trust policy of the IAM role
 used by the Lambda function
         |__ lambda-policy.json                 # contains the IAM policy attached to
 the IAM role used by the Lambda function
```

```
    |__outputs  # contains Lambda function zip code
```

Der Abschnitt Epics enthält step-by-step Anweisungen zum Bereitstellen der Vorlagen.

Epen

Stellen Sie Ressourcen für das Hub-Konto bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Beispielcode-Repository.	1. Öffnen Sie das AWS IAM Root User Activity Monitor-Repository. 2. Wählen Sie auf der Registerkarte Code über der Dateiliste die Option Code aus und kopieren Sie dann die HTTPS-URL. 3. Ändern Sie in einer Befehlszeilenschnittstelle Ihr Arbeitsverzeichnis in das Verzeichnis, in dem Sie die Beispieldateien speichern möchten. 4. Geben Sie den folgenden Befehl ein: `git clone <repoURL>`	Allgemeines AWS
Aktualisieren Sie die Terraform-Vorlage.	1. Rufen Sie Ihre Organisations-ID ab. Anweisungen finden Sie unter Informationen zu einer Organisation über das Verwaltungskonto anzeigen (Dokumentation zu AWS Organizations).	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	2. Öffnen `hub.tf` Sie im geklonten Repository. 3. Aktualisieren Sie Folgendes mit den entsprechenden Werten für Ihre Umgebung: • `OrganizationId` — Fügen Sie Ihre Organisations-ID hinzu. • `SNSTopicName` — Fügen Sie einen Namen für das Amazon SNS SNS-Thema hinzu. • `SNSSubscriptions` — Fügen Sie die E-Mail hinzu, an die Amazon SNS SNS-Benachrichtigungen gesendet werden sollen. • `Region`— Fügen Sie den AWS-Regionalcode hinzu, in dem Sie die Ressourcen bereitstellen. Beispiel, `eu-west-1` . • `Tags`— Fügen Sie Ihre Tags hinzu. Weitere Informationen finden Sie unter Tagging AWS-Ressourcen (AWS General Reference). 4. Speichern und schließen Sie die Datei `hub.tf`.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Stellen Sie die Ressourcen auf dem AWS-Hub-Konto bereit.	1. Navigieren Sie in der Terraform-Befehlsz eilenschnittstelle zum Stammordner des geklonten Repositorys und geben Sie dann den folgenden Befehl ein.
	`terraform init && terraform plan`
	2. Überprüfen Sie die Ausgabe und bestätigen Sie, dass Sie die beschrieb enen Ressourcen erstellen möchten.
	3. Geben Sie den folgenden Befehl ein.
	`terraform apply`
	4. Wenn Sie dazu aufgefordert werden, bestätigen Sie die Bereitstellung, indem Sie Folgendes eingeben`yes`.
		Allgemeines AWS

Stellen Sie Ressourcen für Ihre Spoke-Konten bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudForm ation Vorlage bereit.	1. Melden Sie sich bei der AWS-Managementkons ole an und öffnen Sie die CloudFormation -Konsole. 2. StackSets.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie oben auf der StackSetsSeite die Option Erstellen aus StackSet. 4. Wählen Sie unter Berechtigungen die Option Vom Dienst verwaltete Berechtigungen aus. CloudFormation konfiguriert automatisch die Berechtigungen, die für die Bereitstellung auf den von AWS Organizations verwalteten Zielkonten erforderlich sind. 5. Wählen Sie unter Voraussetzung — Vorlage vorbereiten die Option Vorlage ist bereit aus. 6. Wählen Sie unter Vorlage angeben die Option Vorlagendatei hochladen aus. 7. Wählen Sie Datei auswählen und wählen Sie dann im geklonten Repository die Option aus`spoke-stackset.yaml` . 8. Wählen Sie Weiter aus. 9. Geben Sie auf der Seite „StackSet Details angeben“ einen Namen für das StackSet ein.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	10. Geben Sie unter Parameter die Konto-ID des Hub-Kontos ein und wählen Sie dann Weiter aus. 11. Fügen Sie auf der Seite „StackSet Optionen konfigurieren“ unter Tags Ihre Tags hinzu. 12. Wählen Sie unter Ausführungskonfiguration die Option Inaktiv und dann Weiter aus. 13. Geben Sie auf der Seite Bereitstellungsoptionen festlegen die Organisationseinheiten und Regionen an, in denen Sie das Stack-Set bereitstellen möchten, und wählen Sie dann Weiter aus. 14. Wählen Sie auf der Seite Überprüfen die Option Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen erstellt, und wählen Sie dann Senden aus. CloudFormation beginnt mit der Bereitstellung Ihres Stack-Sets. Weitere Informationen und Anweisungen finden Sie unter Erstellen eines Stack-Sets	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	(CloudFormation Dokumentation).	

(Optional) Testen Sie die Benachrichtigungen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Verwenden Sie die Root-Benutzeranmeldedaten.	1. Melden Sie sich mit den Root-Benutzeranmeldedaten bei einem Spoke-Konto oder dem Hub-Konto an. 2. Vergewissern Sie sich, dass das von Ihnen angegebene E-Mail-Konto die Amazon SNS SNS-Benachrichtigung erhält.	Allgemeines AWS

Zugehörige Ressourcen

- Bewährte Sicherheitsmethoden (IAM-Dokumentation)
- Arbeiten mit StackSets (CloudFormation Dokumentation)
- Erste Schritte (Terraform-Dokumentation)

Zusätzliche Informationen

Amazon GuardDuty ist ein Dienst zur kontinuierlichen Sicherheitsüberwachung, der Protokolle analysiert und verarbeitet, um unerwartete und potenziell nicht autorisierte Aktivitäten in Ihrer AWS-Umgebung zu identifizieren. Als Alternative zu dieser Lösung können Sie, sofern Sie sie aktiviert haben GuardDuty, eine Benachrichtigung erhalten, wenn die Root-Benutzeranmeldedaten verwendet wurden. Das GuardDuty Ergebnis ist`Policy:IAMUser/RootCredentialUsage`, und der Standardschweregrad ist Niedrig. Weitere Informationen finden Sie unter GuardDuty Amazon-Ergebnisse verwalten.

Eine Benachrichtigung senden, wenn ein IAM-Benutzer erstellt wird

Erstellt von Mansi Suratwala (AWS) und Sergiy Shevchenko (AWS)

Übersicht

Auf Amazon Web Services (AWS) können Sie dieses Muster verwenden, um eine CloudFormation AWS-Vorlage bereitzustellen, um automatisch Benachrichtigungen zu erhalten, wenn Benutzer von AWS Identity and Access Management (IAM) erstellt werden.

Mit IAM können Sie den Zugriff auf AWS-Services und -Ressourcen sicher verwalten. Sie können AWS-Benutzer und -Gruppen erstellen und verwalten und Berechtigungen verwenden, um diesen Benutzern und Gruppen den Zugriff auf AWS-Ressourcen zu gewähren oder zu verweigern.

Die CloudFormation Vorlage erstellt ein Amazon CloudWatch Events-Ereignis und eine AWS-Lambda-Funktion. Die Veranstaltung verwendet AWS CloudTrail , um zu überwachen, ob alle IAM-Benutzer im AWS-Konto erstellt wurden. Wenn ein Benutzer erstellt wird, initiiert das Ereignis CloudWatch Ereignisse eine Lambda-Funktion, die Ihnen eine Amazon Simple Notification Service (Amazon SNS) -Benachrichtigung sendet, die Sie über das Ereignis zur Erstellung eines neuen Benutzers informiert.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto
- Ein CloudTrail AWS-Trail wurde erstellt und bereitgestellt

Einschränkungen

- Die CloudFormation AWS-Vorlage darf `CreateUser` nur für bereitgestellt werden.

Architektur

Zieltechnologie-Stack

- IAM
- AWS CloudTrail

- CloudWatch Amazon-Veranstaltungen
- AWS Lambda
- Amazon Simple Storage Service (Amazon-S3)
- Amazon SNS

Zielarchitektur

Automatisierung und Skalierung

Sie können die CloudFormation AWS-Vorlage mehrfach für verschiedene AWS-Regionen und Konten verwenden. Sie müssen sie in jeder Region oder jedem Konto nur einmal ausführen. Verwenden Sie AWS, um die Bereitstellung für mehrere Konten zu automatisieren CloudFormation StackSets. Die CloudFormation Vorlage wird in der Lage sein, alle erforderlichen Ressourcen in jedem Konto bereitzustellen.

Tools

Tools

- IAM — AWS Identity and Access Management (IAM) ist ein Webservice, mit dem Sie den Zugriff auf AWS-Ressourcen sicher kontrollieren können. Sie verwenden IAM, um zu steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzt) ist, Ressourcen zu nutzen.
- AWS CloudFormation — AWS CloudFormation unterstützt Sie bei der Modellierung und Einrichtung Ihrer Amazon Web Services Services-Ressourcen, sodass Sie weniger Zeit mit der Verwaltung dieser Ressourcen verbringen und sich mehr auf Ihre Anwendungen konzentrieren können, die in AWS ausgeführt werden. Sie erstellen eine Vorlage, die alle gewünschten AWS-Ressourcen beschreibt, und CloudFormation kümmert sich um die Bereitstellung und Konfiguration dieser Ressourcen für Sie.
- AWS CloudTrail — AWS CloudTrail unterstützt Sie bei der Verwaltung der Unternehmensführung, der Einhaltung von Vorschriften sowie der Betriebs- und Risikoprüfung Ihres AWS-Kontos. Aktionen, die von einem Benutzer, einer Rolle oder einem AWS-Service ausgeführt werden, werden als Ereignisse in aufgezeichnet CloudTrail. Zu den Ereignissen gehören Aktionen, die in der AWS-Managementkonsole, der AWS-Befehlszeilenschnittstelle und in AWS SDKs und durchgeführt wurden APIs.
- Amazon CloudWatch Events — Amazon CloudWatch Events liefert einen near-real-time Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben.

- AWS Lambda — AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist Speicher für das Internet. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) ist ein verwalteter Service, der die Nachrichtenzustellung über Lambda, HTTP, E-Mail, mobile Push-Benachrichtigungen und mobile Textnachrichten (SMS) ermöglicht.

Code

Eine ZIP-Datei des Projekts ist als Anhang verfügbar.

Epen

Erstellen Sie den S3-Bucket für das Lambda-Skript

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Öffnen Sie die Amazon S3 S3-Konsole und wählen oder erstellen Sie einen S3-Bucket . Dieser S3-Bucket hostet die Lambda-Code-.zip-Datei. Der S3-Bucket-Name darf keine führenden Schrägstriche enthalten.	Cloud-Architekt

Laden Sie den Lambda-Code in den S3-Bucket hoch

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie den Lambda-Code hoch.	Laden Sie die Lambda-Code-ZIP-Datei, die im Abschnitt Anlagen bereitgestellt wird, in	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den von Ihnen definierten S3-Bucket hoch.	

Stellen Sie die CloudFormation Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die CloudFormation Vorlage bereit.	Stellen Sie auf der CloudFormation Konsole die CloudFormation `createIAMuser.yaml` Vorlage bereit, die als Anlage zu diesem Muster bereitgestellt wird. Geben Sie im nächsten Epos Werte für die Vorlagenparameter an.	Cloud-Architekt

Vervollständigen Sie die Parameter in der CloudFormation Vorlage

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie den S3-Bucket-Namen an.	Geben Sie den Namen des S3-Buckets ein, den Sie im ersten Epic erstellt oder ausgewählt haben.	Cloud-Architekt
Geben Sie den S3-Schlüssel an.	Geben Sie den Speicherort der Lambda-Code-ZIP-Datei in Ihrem S3-Bucket an, ohne vorangestellte Schrägstriche (z. B.). `<directory>/<file-name>.zip`	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Geben Sie eine E-Mail-Adresse an.	Geben Sie eine aktive E-Mail-Adresse an, um Amazon SNS SNS-Benachrichtigungen zu erhalten.	Cloud-Architekt
Definieren Sie die Protokollierungsebene.	Definieren Sie die Protokollierungsebene und die Häufigkeit für Ihre Lambda-Funktion. `Info`bezeichnet detaillierte Informationsmeldungen über den Fortschritt der Anwendung. `Error`bezeichnet Fehlerereignisse, die es der Anwendung dennoch ermöglichen könnten, weiter zu laufen. `Warning`bezeichnet potenziell schädliche Situationen.	Cloud-Architekt

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die Vorlage erfolgreich bereitgestellt wurde, sendet sie eine Abonnement-E-Mail-Nachricht an die angegebene E-Mail-Adresse. Um Benachrichtigungen zu erhalten, müssen Sie dieses E-Mail-Abonnement bestätigen.	Cloud-Architekt

Zugehörige Ressourcen

- Creating a trail
- Erstellen eines S3-Buckets
- Dateien in einen S3-Bucket hochladen
- Eine CloudFormation Vorlage bereitstellen
- Einen IAM-Benutzer erstellen
- Erstellen einer CloudWatch Ereignisregel, die bei einem AWS-API-Aufruf mit AWS ausgelöst wird CloudTrail

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Verhindern Sie den Internetzugang auf Kontoebene mithilfe einer Dienststeuerungsrichtlinie

Erstellt von Sergiy Shevchenko (AWS), Sean O'Sullivan (AWS) und Victor Mazeo Whitaker (AWS)

Übersicht

Organizations möchten häufig den Internetzugang für Kontoressourcen einschränken, die privat bleiben sollten. In diesen Konten sollten die Ressourcen in virtuellen privaten Clouds (VPCs) auf keinen Fall auf das Internet zugreifen. Viele Unternehmen entscheiden sich für eine zentralisierte Inspektionsarchitektur. Für den Ost-West-Verkehr (VPC-zu-VPC) in einer zentralen Inspektionsarchitektur müssen Sie sicherstellen, dass die Spoke-Konten und ihre Ressourcen keinen Zugriff auf das Internet haben. Für Nord-Süd-Verkehr (ausgehender und lokaler Internetverkehr) möchten Sie den Internetzugang nur über die Inspektions-VPC zulassen.

Dieses Muster verwendet eine Service Control Policy (SCP), um den Internetzugang zu verhindern. Sie können dieses SCP auf Konto- oder Organisationseinheitsebene (OU) anwenden. Das SCP schränkt die Internetkonnektivität ein, indem es Folgendes verhindert:

- Erstellen oder Anhängen eines IPv4 oder IPv6 Internet-Gateways, das direkten Internetzugriff auf die VPC ermöglicht
- Erstellen oder Annehmen einer VPC-Peering-Verbindung, die möglicherweise indirekten Internetzugang über eine andere VPC ermöglicht
- Erstellen oder Aktualisieren einer AWS Global AcceleratorKonfiguration, die direkten Internetzugriff auf VPC-Ressourcen ermöglichen könnte

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine oder mehrere AWS-Konten werden als Organisation verwaltet in AWS Organizations.
- Alle Funktionen sind in aktiviert AWS Organizations.
- SCPs sind in der Organisation aktiviert.
- Berechtigungen für:
  - Greifen Sie auf das Verwaltungskonto der Organisation zu.

- Erstellen SCPs. Weitere Informationen zu den Mindestberechtigungen finden Sie unter SCP erstellen.
- Ordnen Sie den SCP den Zielkonten oder Organisationseinheiten zu ()OUs. Weitere Informationen zu den Mindestberechtigungen finden Sie unter Dienststeuerungsrichtlinien anhängen und trennen.

Einschränkungen

- SCPs wirken sich nicht auf Benutzer oder Rollen im Verwaltungskonto aus. Sie wirken sich nur auf die Mitgliedskonten Ihrer Organisation aus.
- SCPs betreffen nur AWS Identity and Access Management (IAM-) Benutzer und Rollen, die von Konten verwaltet werden, die Teil der Organisation sind. Weitere Informationen zu SCP-Auswirkungen auf Berechtigungen.

Tools

AWS-Services

- AWS Organizationsist ein Kontoverwaltungsdienst, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie erstellen und zentral verwalten. In diesem Muster verwenden Sie Richtlinien zur Dienststeuerung (SCPs) in AWS Organizations.
- Amazon Virtual Private Cloud (Amazon VPC) hilft Ihnen dabei, AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk bereitzustellen. Dieses virtuelle Netzwerk entspricht einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben würden, mit den Vorteilen der Verwendung der skalierbaren Infrastruktur von AWS.

Bewährte Methoden

Nachdem Sie dieses SCP in Ihrem Unternehmen eingerichtet haben, stellen Sie sicher, dass Sie es regelmäßig aktualisieren, um alle neuen Funktionen AWS-Services oder Funktionen zu berücksichtigen, die den Internetzugang beeinträchtigen könnten.

Epen

Erstelle das SCP und hänge es an

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie das SCP.	1. Melden Sie sich an der AWS Organizations - Konsole an. Sie müssen sich mit dem Verwaltungskonto der Organisation anmelden. 2. Wählen Sie im linken Bereich Richtlinien aus. 3. Wählen Sie auf der Seite mit den Richtlinien die Option Dienststeuerungsrichtlinien aus. 4. Wählen Sie auf der Seite Service-Kontrollrichtlinien die Option Richtlinie erstellen aus. 5. Geben Sie auf der Seite Neue Dienststeuerungsrichtlinie erstellen einen Richtliniennamen und optional eine Richtlinienbeschreibung ein. 6. (Optional) Fügen Sie Ihrer Richtlinie AWS Tags hinzu. 7. Löschen Sie im JSON-Editor die Platzhalterrichtlinie. 8. Fügen Sie die folgende - Richtlinie in den JSON-Editor ein.	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>{
	  "Version":
	 "2012-10-17",
	  "Statement": [
	  {
	  "Action": [
	  "ec2:Atta
	chInternetGateway",
	  "ec2:Crea
	teInternetGateway",
	
	  "ec2:Crea
	teVpcPeeringConnec
	tion",
	  "ec2:Acce
	ptVpcPeeringConnec
	tion",
	  "ec2:Crea
	teEgressOnlyIntern
	etGateway"
	  ],
	  "Resource":
	 "*",
	  "Effect": "Deny"
	  },
	  {
	  "Action": [
	  "globalac
	celerator:Create*",
	  "globalac
	celerator:Update*"
	  ],
	  "Resource":
	 "*",
	  "Effect": "Deny"
	  }
	  ]
	}</pre>	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	9. Wählen Sie Create Policy (Richtlinie erstellen) aus.	
Hängen Sie das SCP an.	1. Wählen Sie auf der Seite Service Control-Richtlinie n die Richtlinie aus, die Sie erstellt haben. 2. Klicken Sie in der Registerk arte Ziele auf Anfügen. 3. Wählen Sie die Organisat ionseinheit oder das Konto aus, an das Sie die Richtlinie anhängen möchten. Möglicherweise müssen Sie das erweitern , OUs um die gewünschte Organisationseinheit oder das gewünschte Konto zu finden. 4. Wählen Sie Richtlinie anfügen aus.	AWS-Administrator

Zugehörige Ressourcen

- AWS Organizations Dokumentation
- Richtlinien zur Servicekontrolle (SCPs)
- Zentralisierte Inspektionsarchitektur mit AWS Gateway Load Balancer und AWS Transit Gateway (AWS Blogbeitrag)

Beschränken Sie den Zugriff basierend auf IP-Adresse oder Geolokalisierung mithilfe von AWS WAF

Erstellt von Louis Hourcade (AWS)

Übersicht

AWS WAFist eine Firewall für Webanwendungen, die zum Schutz von Webanwendungen und APIs vor gängigen Web-Exploits und Bots beiträgt, die die Verfügbarkeit beeinträchtigen, die Sicherheit gefährden oder übermäßig viele Ressourcen verbrauchen können. Mithilfe von Web-Zugriffskontrolllisten (Web ACLs) AWS WAF können Sie steuern, wie der Datenverkehr Ihre Anwendungen erreicht. In einer Web-ACL fügen Sie Regeln oder Regelgruppen hinzu, die darauf ausgelegt sind, legitimen Datenverkehr zuzulassen, Bot-Verkehr zu kontrollieren und gängige Angriffsmuster zu blockieren. Weitere Informationen finden Sie unter So AWS WAF funktioniert das.

Sie können Ihrem AWS WAF Web die folgenden Regeltypen zuordnen ACLs:

- Verwaltete Regelgruppen — Teams und AWS Marketplace Verkäufer mit AWS verwalteten Regeln bieten vorkonfigurierte Regelgruppen an. Einige verwaltete Regelgruppen wurden entwickelt, um bestimmte Arten von Webanwendungen zu schützen. Andere bieten umfassenden Schutz vor bekannten Bedrohungen oder häufigen Sicherheitslücken.
- Benutzerdefinierte Regeln und benutzerdefinierte Regelgruppen — Sie können auch Regeln und Regelgruppen erstellen, mit denen Sie den Zugriff auf Ihre Webanwendungen anpassen können und APIs. Sie können beispielsweise den Datenverkehr auf der Grundlage einer bestimmten Liste von IP-Adressen oder einer Liste von Ländern einschränken.

Mithilfe dieses Musters und des zugehörigen Code-Repositorys können Sie AWS Cloud Development Kit (AWS CDK)das AWS WAF Web ACLs mit benutzerdefinierten Regeln bereitstellen. Diese Regeln beschränken den Zugriff auf Webanwendungsressourcen auf der Grundlage der IP-Adresse oder des Standorts des Endbenutzers. Sie können optional auch mehrere verwaltete Regelgruppen anhängen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Berechtigungen zum Bereitstellen von AWS WAF Ressourcen

- AWS CDK, in Ihrem Konto installiert und konfiguriert
- Git, installiert

Einschränkungen

- Sie können dieses Muster nur dort verwenden AWS-Regionen , wo AWS WAF es verfügbar ist. Informationen zur Verfügbarkeit in Regionen finden Sie unter AWS-Services Nach Regionen.

Tools

AWS-Services

- AWS Cloud Development Kit (AWS CDK)ist ein Softwareentwicklungs-Framework, das Ihnen hilft, AWS Cloud Infrastruktur im Code zu definieren und bereitzustellen.
- AWS WAFist eine Firewall für Webanwendungen, mit der Sie HTTP- und HTTPS-Anfragen überwachen können, die an Ihre geschützten Webanwendungsressourcen weitergeleitet werden.

Code-Repository

Der Code für dieses Muster ist in der GitHub IP- und Geolocation-Beschränkung mit AWS WAF Repository verfügbar. Der Code stellt zwei Web bereit. AWS WAF ACLs Die erste ist eine regionale Web-ACL, die für Amazon API Gateway Gateway-Ressourcen vorgesehen ist. Die zweite ist die globale Web-ACL für CloudFrontAmazon-Ressourcen. Beide Websites ACLs enthalten die folgenden benutzerdefinierten Regeln:

- `IPMatch`blockiert Anfragen von unzulässigen IP-Adressen.
- `GeoMatch`blockiert Anfragen aus nicht zugelassenen Ländern.

Während der Bereitstellung können Sie optional alle der folgenden verwalteten Regelgruppen an Ihre Website ACLs anhängen:

- Kernregelsatz (CRS) — Diese Regelgruppe enthält Regeln, die allgemein für Webanwendungen gelten. Es trägt zum Schutz vor der Ausnutzung einer Vielzahl von Sicherheitslücken bei, darunter einige der risikoreichen und häufig auftretenden Sicherheitslücken, die in OWASP-Publikationen wie den OWASP Top 10 beschrieben sind.

- Administratorschutz — Diese Regelgruppe enthält Regeln, mit denen Sie den externen Zugriff auf offene Verwaltungsseiten blockieren können.
- Bekannte fehlerhafte Eingaben — Diese Regelgruppe hilft beim Blockieren von Anforderungsmustern, die bekanntermaßen ungültig sind und mit der Ausnutzung oder Entdeckung von Sicherheitslücken in Verbindung stehen.
- IP-Reputationsliste von Amazon — Diese Regelgruppe enthält Regeln, die auf internen Bedrohungsinformationen von Amazon basieren. Sie hilft Ihnen dabei, IP-Adressen zu blockieren, die normalerweise mit Bots oder anderen Bedrohungen in Verbindung gebracht werden.
- Verwaltete Regelgruppe für Linux-Betriebssysteme — Diese Regelgruppe hilft beim Blockieren von Anforderungsmustern, die im Zusammenhang mit der Ausnutzung von Linux-Schwachstellen stehen, einschließlich Linux-spezifischer Local File Inclusion (LFI) -Angriffe.
- Verwaltete Regelgruppe für SQL-Datenbanken — Diese Regelgruppe hilft beim Blockieren von Anforderungsmustern, die mit der Ausnutzung von SQL-Datenbanken in Verbindung stehen, z. B. bei SQL-Injection-Angriffen.

Epen

Konfiguriere das Web AWS WAF ACLs

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Geben Sie den folgenden Befehl ein, um die IP- und Geolocation-Beschränkung mit AWS WAF Repository auf Ihre lokale Workstation zu klonen: `git clone https://github.com/aws-samples/ip-and-geolocation-restriction-with-waf-cdk.git`	Git
Konfigurieren Sie die Regeln.	1. Öffnen Sie im geklonten Repository die Datei app.py.	Allgemein AWS, Python

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	2. Ändern Sie die Werte der folgenden Variablen, um die Regeln anzupassen:
	
	`aws_acccount = "AWS_ACCOUNT"`
	`region = "AWS_REGION"`
	`ip_list = ["CIDR_RANGE_1", "CIDR_RANGE_2"]`
	`geo_list = ["COUNTRY_CODE_1", "COUNTRY_CODE_2"]`
	`aws_managed_rules = True`
	
	Wobei gilt:
	• `aws_account` ist die ID des Ziels AWS-Konto.
	• `region`ist das Ziel AWS-Region für die Web-ACL für API-Gateway-Ressourcen.
	
	Note
	Die Web-ACL für CloudFront Ressourcen ist global und wird in der `us-east-1` Region bereitgestellt.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `ip_list`ist die Liste der CIDR-Bereiche, auf die zugegriffen werden darf. • `geo_list`ist die Liste der Länder, denen der Zugriff gewährt wird. Gültige Werte finden Sie in der AWS WAF Dokumentation. • `aws_manag ed_rules` steuert, ob die verwalteten Regelgruppen der Web-ACL hinzugefügt werden. Wenn dieser Wert ist`True`, werden sie hinzugefügt. Wenn dieser Wert gleich ist`False`, werden sie ausgeschl ossen. 3. Speichern und schließen Sie die Datei app.py.	

Bootstrap und Bereitstellung des Codes

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bootstrap für Ihre AWS Umgebung.	Falls dies noch nicht geschehen ist, müssen Sie Ihre AWS Umgebung booten, bevor Sie die AWS CDK Anwendung bereitstellen können.	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	1. Geben Sie in der AWS CDK CLI den folgenden Befehl ein, um die `us-east-1` Region zu booten:
	`cdk bootstrap aws://<account-id>/us-east-1`
	2. Wenn Sie die Web-ACL für API Gateway in einer anderen Region als bereitstellen`us-east-1` , geben Sie den folgenden Befehl ein, um die Zielregion zu booten:
	`cdk bootstrap aws://<account-id>/<region>`	

Stellen Sie die AWS CDK Anwendung bereit.	1. Geben Sie den folgenden Befehl ein, um die AWS CDK Anwendung bereitzustellen: `cdk deploy --all` 2. Warten Sie, bis die AWS CloudFormation Stack-Bereitstellung abgeschlossen ist.	Allgemeines AWS

Validieren Sie die Bereitstellung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Vergewissern Sie sich, dass das Web ACLs erfolgreich bereitgestellt wurde.	1. Melden Sie sich bei der an AWS Managemen t Console, und öffnen Sie dann die AWS WAF Konsole. 2. Wählen Sie im Navigatio nsbereich Web aus ACLs. 3. Wählen Sie in der Liste von AWS-RegionenGlobal (CloudFront) aus. 4. Vergewissern Sie sich, dass die neue CloudFront Web-ACL bereitgestellt wurde, und stellen Sie sicher, dass sie die von Ihnen definierten IP-Adressen und Geolokali sierungsregeln enthält. Der Standardname dieser Web-ACL lautet. `WebACLClo udfront-<ID>` 5. Wählen Sie in der Liste von die Region aus AWS-Regio nen, in der Sie den Stack bereitgestellt haben. 6. Stellen Sie sicher, dass eine neue Web-ACL für API-Gateway-Ressou rcen bereitgestellt wurde. Vergewissern Sie sich, dass es über die von Ihnen definierten IP-Adressen und Geolocation-Regeln	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	verfügt. Der Standardname dieser Web-ACL lautet. `WebACLApiGW-<ID>`	
(Optional) Ordnen Sie das Internet Ihren Ressourcen ACLs zu.	Ordnen Sie das AWS WAF Internet ACLs Ihren AWS Ressourcen zu, z. B. einem Application Load Balancer, einem API Gateway oder einer CloudFront Distribut ion. Anweisungen finden Sie unter Eine Web-ACL einer Ressource zuordnen oder deren Zuordnung aufheben. AWS Ein Beispiel finden Sie in der Dokumentation unter class CfnWeb ACLAssociation (construct). AWS CDK	Allgemeines AWS

Bereinigen von -Ressourcen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Lösche die Stapel.	1. Trennen Sie die Web-ACL von allen Ressourcen. AWS Anweisungen finden Sie in der AWS WAF Dokumenta tion. 2. Geben Sie in der AWS CDK CLI den folgenden Befehl ein, um die AWS CDK Anwendung zu löschen. `cdk destroy --all`	Allgemeines AWS

Zugehörige Ressourcen

- API-Referenz (AWS CDK Dokumentation)
- aws-cdk-lib.aws_wafv2-Modul (Dokumentation)AWS CDK
- Arbeiten mit dem Web (Dokumentation) ACLs AWS WAF
- Verwaltung Ihrer eigenen Regelgruppen (AWS WAF Dokumentation)
- Regeln (AWS WAF Dokumentation)

Scannen Sie Git-Repositorys mithilfe von Git-Secrets auf vertrauliche Informationen und Sicherheitsprobleme

Erstellt von Saurabh Singh (AWS)

Übersicht

Dieses Muster beschreibt, wie Sie das Open-Source-Tool Git-Secrets von AWS Labs verwenden, um Git-Quell-Repositorys zu scannen und Code zu finden, der möglicherweise vertrauliche Informationen wie Benutzerkennwörter oder AWS Zugriffsschlüssel enthält oder der andere Sicherheitsprobleme aufweist.

`git-secrets`scannt Commits, Commit-Nachrichten und Zusammenführungen, um zu verhindern, dass sensible Informationen wie geheime Informationen zu deinen Git-Repositorys hinzugefügt werden. Wenn beispielsweise ein Commit, eine Commit-Nachricht oder ein Commit in einem Merge-Verlauf mit einem deiner konfigurierten, verbotenen regulären Ausdrucksmuster übereinstimmt, wird der Commit zurückgewiesen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktiver AWS-Konto
- Ein Git-Repository, für das ein Sicherheitsscan erforderlich ist
- Ein Git-Client (Version 2.37.1 und höher) ist installiert

Architektur

Zielarchitektur

- Git
- `git-secrets`

Tools

- git-secrets ist ein Tool, das Sie daran hindert, vertrauliche Informationen in Git-Repositorys zu speichern.
- Git ist ein verteiltes Open-Source-Versionskontrollsystem.

Bewährte Methoden

- Scanne ein Git-Repository immer, indem du alle Revisionen einbeziehst:

```
git secrets --scan-history
```

Epen

Stellen Sie eine Connect zu einer EC2 Instanz her

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie mithilfe von SSH eine Connect zu einer EC2 Instance her.	Stellen Sie mithilfe von SSH und einer Schlüsselpaardatei eine Connect zu einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance her. Sie können diesen Schritt überspringen, wenn Sie ein Repository auf Ihrem lokalen Computer scannen.	Allgemeines AWS

Installieren Sie Git

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Installieren Sie Git.	Installiere Git mit dem folgenden Befehl:	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`yum install git -y` Wenn Sie Ihren lokalen Computer verwenden, können Sie einen Git-Client für eine bestimmte Betriebssystemversion installieren. Weitere Informationen finden Sie auf der Git-Website.	

Klonen Sie das Quell-Repository und installieren Sie Git-Secrets

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Git-Quell-Repository.	Um das Git-Repository zu klonen, das Sie scannen möchten, wählen Sie den Befehl Git clone aus Ihrem Home-Verzeichnis.	Allgemeines AWS

Git-Secrets klonen.	Klonen Sie das `git-secrets` Git-Repository.
	
	`git clone https://github.com/awslabs/git-secrets.git`
	
	`git-secrets` Platziere es irgendwo in deinem, `PATH` sodass Git es aufnimmt, wenn du es ausführst`git-secrets .`
		Allgemeines AWS

Installieren Sie Git-Secrets.	Für Unix und Varianten (Linux/macOS):	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	Sie können das `install` Ziel von `Makefile` (im `git-secrets` Repository bereitgestellt) verwenden, um das Tool zu installieren. Sie können den Installationspfad mithilfe der `MANPREFIX` Variablen `PREFIX` und anpassen.
	`make install`
	Für Windows:
	Führen Sie das im `git-secrets` Repository bereitgestellte PowerShell `install.ps1` Skript aus. Dieses Skript kopiert die Installationsdateien in ein Installationsverzeichnis (`%USERPROFILE%/.git-secrets` standardmäßig) und fügt das Verzeichnis dem aktuellen Benutzer hinzu`PATH`.
	`PS > ./install.ps1`
	Für Homebrew (macOS-Benutzer):
	Führen Sie Folgendes aus:
	`brew install git-secrets`	

Git-Code-Repository scannen

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Gehe zum Quell-Repository.	Wechseln Sie in das Verzeichnis für das Git-Repository, das Sie scannen möchten: `cd my-git-repository`	Allgemeines AWS
Registrieren Sie den AWS-Regelsatz (Git-Hooks).	Um `git-secrets` zu konfigurieren, dass dein Git-Repository bei jedem Commit gescannt wird, führe den folgenden Befehl aus: `git secrets --register-aws`	Allgemeines AWS
Scannen Sie das Repository.	Führen Sie den folgenden Befehl aus, um mit dem Scannen Ihres Repositorys zu beginnen: `git secrets --scan`	Allgemeines AWS
Überprüfen Sie die Ausgabedatei.	Das Tool generiert eine Ausgabedatei, wenn es eine Sicherheitslücke in Ihrem Git-Repository findet. Zum Beispiel: `example.sh:4:AWS_SECRET_ACCESS_KEY = *********`	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`[ERROR] Matched one or more prohibited patterns`
	
	`Possible mitigations:`
	`- Mark false positives as allowed using: git config --add secrets.allowed ...`
	`- Mark false positives as allowed by adding regular expressions to .gitallowed at repository's root directory`
	`- List your configured patterns: git config --get-all secrets.patterns`
	`- List your configured allowed patterns: git config --get-all secrets.allowed`
	`- List your configured allowed patterns in .gitallowed at repository's root directory`
	`- Use --no-verify if this is a one-time false positive`	

Zugehörige Ressourcen

- Tool Git-Secrets

Benachrichtigungen von der AWS-Netzwerk-Firewall an einen Slack-Channel senden

Erstellt von Venki Srivatsav (AWS) und Aromal Raj Jayarajan (AWS)

Übersicht

Dieses Muster beschreibt, wie eine Firewall mithilfe der Amazon Web Services (AWS) Network Firewall mit dem verteilten Bereitstellungsmodell bereitgestellt wird und wie die von der AWS Network Firewall generierten Warnmeldungen an einen konfigurierbaren Slack-Channel weitergegeben werden.

Compliance-Standards wie der Payment Card Industry Data Security Standard (PCI DSS) erfordern die Installation und Wartung einer Firewall zum Schutz von Kundendaten. In der AWS-Cloud wird eine virtuelle private Cloud (VPC) im Zusammenhang mit diesen Compliance-Anforderungen als dasselbe angesehen wie ein physisches Netzwerk. Sie können die Network Firewall verwenden, um den Netzwerkverkehr zwischen Ihren Workloads zu überwachen VPCs und Ihre Workloads zu schützen, die einem Compliance-Standard VPCs unterliegen. Die Network Firewall blockiert den Zugriff oder generiert Warnmeldungen, wenn sie einen unbefugten Zugriff von anderen Personen VPCs im selben Konto erkennt. Die Network Firewall unterstützt jedoch eine begrenzte Anzahl von Zielen für die Übermittlung der Warnmeldungen. Zu diesen Zielen gehören Amazon Simple Storage Service (Amazon S3) -Buckets, CloudWatch Amazon-Protokollgruppen und Amazon Data Firehose-Lieferstreams. Jede weitere Aktion in Bezug auf diese Benachrichtigungen erfordert eine Offline-Analyse mithilfe von Amazon Athena oder Amazon Kinesis.

Dieses Muster bietet eine Methode zur Weitergabe von Warnmeldungen, die von der Network Firewall generiert werden, an einen konfigurierbaren Slack-Kanal, sodass weitere Aktionen nahezu in Echtzeit ausgeführt werden können. Du kannst die Funktionalität auch auf andere Warnmechanismen wie Jira und E-Mail PagerDuty ausweiten. (Diese Anpassungen fallen nicht in den Geltungsbereich dieses Musters.)

Voraussetzungen und Einschränkungen

Voraussetzungen

- Slack-Channel (siehe Erste Schritte im Slack-Hilfecenter)
- Erforderliche Rechte, um eine Nachricht an den Channel zu senden

- Die URL des Slack-Endpunkts mit einem API-Token (wähle deine App aus und wähle einen eingehenden Webhook aus, um dessen URL zu sehen; weitere Informationen findest du unter Einen eingehenden Webhook erstellen in der Slack-API-Dokumentation)
- Eine Amazon Elastic Compute Cloud (Amazon EC2) -Testinstanz in den Workload-Subnetzen
- Testregeln in der Network Firewall
- Tatsächlicher oder simulierter Verkehr zum Auslösen der Testregeln
- Ein S3-Bucket für die bereitzustellenden Quelldateien

Einschränkungen

- Derzeit unterstützt diese Lösung nur einen einzigen CIDR-Bereich (Classless Inter-Domain Routing) als Filter für Quelle und Ziel. IPs

Architektur

Zieltechnologie-Stack

- Eine VPC
- Vier Subnetze (zwei für die Firewall und zwei für Workloads)
- Internet-Gateway
- Vier Routing-Tabellen mit Regeln
- Als Warnungsziel verwendeter S3-Bucket, konfiguriert mit einer Bucket-Richtlinie und Ereigniseinstellungen zur Ausführung einer Lambda-Funktion
- Lambda-Funktion mit einer Ausführungsrolle, um Slack-Benachrichtigungen zu senden
- AWS Secrets Manager Manager-Geheimnis zum Speichern der Slack-URL
- Netzwerk-Firewall mit Warnungskonfiguration
- Slack-Kanal

Alle Komponenten mit Ausnahme des Slack-Channels werden durch die CloudFormation Vorlagen und die Lambda-Funktion bereitgestellt, die mit diesem Muster bereitgestellt werden (siehe Abschnitt Code).

Zielarchitektur

Dieses Muster richtet eine dezentrale Netzwerk-Firewall mit Slack-Integration ein. Diese Architektur besteht aus einer VPC mit zwei Availability Zones. Die VPC umfasst zwei geschützte Subnetze und zwei Firewall-Subnetze mit Netzwerk-Firewall-Endpunkten. Der gesamte in und aus den geschützten Subnetzen eingehende und ausgehende Datenverkehr kann durch die Erstellung von Firewall-Richtlinien und -Regeln überwacht werden. Die Netzwerk-Firewall ist so konfiguriert, dass alle Warnmeldungen in einem S3-Bucket platziert werden. Dieser S3-Bucket ist so konfiguriert, dass er eine Lambda-Funktion aufruft, wenn er ein `put` Ereignis empfängt. Die Lambda-Funktion ruft die konfigurierte Slack-URL von Secrets Manager ab und sendet die Benachrichtigung an den Slack-Workspace.

Weitere Informationen zu dieser Architektur finden Sie im AWS-Blogbeitrag Bereitstellungsmodelle für die AWS-Netzwerk-Firewall.

Tools

AWS-Services

- Die AWS Network Firewall ist ein zustandsbehafteter, verwalteter Netzwerk-Firewall sowie Service zur Erkennung und Verhinderung von Eindringlingen VPCs in der AWS-Cloud. Sie können die Network Firewall verwenden, um den Verkehr am Perimeter Ihrer VPC zu filtern und Ihre Workloads auf AWS zu schützen.
- AWS Secrets Manager ist ein Service zum Speichern und Abrufen von Anmeldeinformationen. Mit Secrets Manager können Sie hartcodierte Anmeldeinformationen in Ihrem Code, einschließlich Kennwörtern, durch einen API-Aufruf an Secrets Manager ersetzen, um das Geheimnis programmgesteuert abzurufen. Dieses Muster verwendet Secrets Manager, um die Slack-URL zu speichern.
- Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen. Dieses Muster verwendet Amazon S3, um die CloudFormation Vorlagen und das Python-Skript für die Lambda-Funktion zu speichern. Es verwendet auch einen S3-Bucket als Ziel für Netzwerk-Firewall-Warnmeldungen.
- AWS CloudFormation hilft Ihnen dabei, Ihre AWS-Ressourcen zu modellieren und einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus zu verwalten. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben und sie zusammen als Stapel zu starten und zu konfigurieren, anstatt Ressourcen

einzeln zu verwalten. Dieses Muster verwendet AWS CloudFormation , um automatisch eine verteilte Architektur für Firewall Manager bereitzustellen.

Code

Der Code für dieses Muster ist im Network Firewall Slack Integration Repository verfügbar. GitHub Im `src` Ordner des Repositorys findest du:

- Eine Reihe von CloudFormation Dateien im YAML-Format. Sie verwenden diese Vorlagen, um die Komponenten für dieses Muster bereitzustellen.
- Eine Python-Quelldatei (`slack-lambda.py`) zum Erstellen der Lambda-Funktion.
- Ein .zip-Archiv-Bereitstellungspaket (`slack-lambda.py.zip`) zum Hochladen Ihres Lambda-Funktionscodes.

Folgen Sie den Anweisungen im nächsten Abschnitt, um diese Dateien zu verwenden.

Epen

Richten Sie den S3-Bucket ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie einen S3-Bucket.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/. 2. Wählen oder erstellen Sie einen S3-Bucket, um den Code zu hosten. Ein S3-Bucket-Name ist weltweit eindeutig, und der Namespace wird von allen AWS-Konten gemeinsam genutzt. Der S3-Bucket-Name darf keine führenden	App-Entwickler, App-Besitzer, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Schrägstriche enthalten. Wir empfehlen, dass Sie ein Präfix verwenden, um den Code für dieses Muster zu organisieren. Weitere Informationen finden Sie in der Amazon S3 S3-Dokumentation unter Bucket erstellen.	
Laden Sie die CloudFormation Vorlagen und den Lambda-Code hoch.	1. Laden Sie die folgenden Dateien für dieses Muster aus dem GitHub Repository herunter: • `base.yml` • `igw-ingress-route.yml` • `slack-lambda.py` • `slackLambda.yml` • `decentralized-deployment.yml` • `protected-subnet-route.yml` • `slack-lambda.py.zip` 2. Laden Sie die Dateien in den S3-Bucket hoch, den Sie erstellt haben.	App-Entwickler, App-Besitzer, Cloud-Administrator

Stellen Sie die CloudFormation Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die CloudFormation Vorlage.	Öffnen Sie die CloudFormation AWS-Konsole in derselben AWS-Region wie Ihr S3-Bucket und stellen Sie die Vorlage bereit`base.yml`. Diese Vorlage erstellt die erforderlichen AWS-Ressourcen und Lambda-Funktionen für die Benachrichtigungen, die an den Slack-Channel übertragen werden sollen. Weitere Informationen zum Bereitstellen von CloudFormation Vorlagen finden Sie in der CloudFormation Dokumentation unter Erstellen eines Stacks auf der CloudFormation AWS-Konsole.	App-Entwickler, App-Besitzer, Cloud-Administrator
Vervollständigen Sie die Parameter in der Vorlage.	Geben Sie den Stacknamen an und konfigurieren Sie die Parameterwerte. Eine Liste der Parameter, ihrer Beschreibungen und Standardwerte finden Sie unter CloudFormation Parameter im Abschnitt Zusätzliche Informationen.	App-Entwickler, App-Besitzer, Cloud-Administrator
Erstellen Sie den Stack.	1. Überprüfen Sie die Stack-Details und aktualisieren Sie die Werte auf	App-Entwickler, App-Besitzer, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	der Grundlage Ihrer Umgebungsanforderungen. 2. Wählen Sie Stack erstellen aus, um die Vorlage bereitzustellen.	

Überprüfen Sie die Lösung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Testen Sie die Bereitstellung.	Verwenden Sie die CloudFormation AWS-Konsole oder die AWS-Befehlszeilenschnittstelle (AWS CLI), um zu überprüfen, ob die im Abschnitt Target-Technologie-Stack aufgeführten Ressourcen erstellt wurden. Wenn die CloudFormation Vorlage nicht erfolgreich bereitgestellt werden kann, überprüfen Sie die Werte, die Sie für die `pAvailabilityZone2` Parameter `pAvailabilityZone1` und angegeben haben. Diese sollten für die AWS-Region geeignet sein, in der Sie die Lösung bereitstellen. Eine Liste der Availability Zones für jede Region finden Sie in der EC2 Amazon-Dokumentation unter Regionen und Zonen.	App-Entwickler, App-Besitzer, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Testen Sie die Funktionalität.	1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
	
	2. Erstellen Sie eine EC2 Instance in einem der geschützten Subnetze. Wählen Sie ein Amazon Linux 2 AMI (HVM), das als HTTPS-Server verwendet werden soll. Anweisungen finden Sie in der EC2 Amazon-Dokumentation unter Eine Instance starten.
	
	Note
	Amazon Linux 2 nähert sich dem Ende des Supports. Weitere Informationen finden Sie unter Amazon Linux FAQs 2.
	
	3. Verwenden Sie die folgenden Benutzerdaten, um einen Webserver auf der EC2 Instance zu installieren:
	
	`#!/bin/bash`
	`yum install httpd -y`
	`systemctl start httpd`
	`systemctl stop`
	`firewalld`
	`cd /var/www/html`
		App-Entwickler, App-Besitzer, Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`echo "Hello!! this is a NFW alert test page, 200 OK" > index.html`
	
	4. Erstellen Sie die folgenden Netzwerk-Firewallregeln:
	
	Regel ohne Status:
	
	`Source: 0.0.0.0/0`
	`Destination 10.0.3.65 /32 (private IP of the EC2 instance)`
	`Action: Forward`
	
	Staatliche Regel:
	
	`Protocol: HTTP`
	`Source ip/port: Any / Any`
	`Destination ip/port: Any /Any`
	
	5. Rufen Sie die öffentliche IP des Webservers ab, den Sie in Schritt 3 erstellt haben.
	
	6. Greifen Sie in einem Browser auf die öffentliche IP zu. Sie sollten die folgende Meldung im Browser sehen:
	
	`Hello!! this is a NFW alert test page, 200 OK`
	
	Sie erhalten auch eine Benachrichtigung im Slack-	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Kanal. Die Benachrichtigung kann sich je nach Größe der Nachricht verzögern. Zu Testzwecken sollten Sie in Erwägung ziehen, einen CIDR-Filter bereitzustellen, der nicht zu eng ist (z. B. würde ein CIDR-Wert mit /32 als zu eng und /8 als zu breit angesehen). Weitere Informationen finden Sie im Abschnitt Filterverhalten unter Zusätzliche Informationen.	

Zugehörige Ressourcen

- Bereitstellungsmodelle für die AWS-Netzwerk-Firewall (AWS-Blogbeitrag)
- AWS-Netzwerk-Firewall-Richtlinien (AWS-Dokumentation)
- Network Firewall Slack-Integration (GitHub Repository)
- Erstelle einen Slack-Workspace (Slack-Hilfecenter)

Zusätzliche Informationen

CloudFormation parameters (Parameter

Parameter	Beschreibung	Standard- oder Beispielwert
`pVpcName`	Der Name der zu erstellenden VPC.	Inspektion
`pVpcCidr`	Der CIDR-Bereich, den die VPC erstellen soll.	10.0.0.0/16

`pVpcInstanceTenancy`	Wie EC2 Instances auf die physische Hardware verteilt werden. Es stehen folgende Optionen zur Verfügung: `default` (Shared Tenancy) oder `dedicated` (Single Tenancy).	default
`pAvailabilityZone1`	Die erste Availability Zone für die Infrastruktur.	us-east-2a
`pAvailabilityZone2`	Die zweite Availability Zone für die Infrastruktur.	us-east-2b
`pNetworkFirewallSubnet1Cidr`	Der CIDR-Bereich für das erste Firewall-Subnetz (mindestens /28).	10.0.1.0/24
`pNetworkFirewallSubnet2Cidr`	Der CIDR-Bereich für das zweite Firewall-Subnetz (mindestens /28).	10.0.2.0/24
`pProtectedSubnet1Cidr`	Der CIDR-Bereich für das erste geschützte Subnetz (Workload).	10.0.3.0/24
`pProtectedSubnet2Cidr`	Der CIDR-Bereich für das zweite geschützte Subnetz (Workload).	10.0.4.0/24
`pS3BucketName`	Der Name des vorhandenen S3-Buckets, in den Sie den Lambda-Quellcode hochgeladen haben.	us-w2- yourname-lambda-functions
`pS3KeyPrefix`	Das Präfix des S3-Buckets, in den Sie den Lambda-Quellcode hochgeladen haben.	aod-test

pAWSSecretName4Slack	Der Name des Geheimnisses, das die Slack-URL enthält.	SlackEnpoint-Cfn
pSlackChannelName	Der Name des Slack-Channels, den du erstellt hast.	einige Namensbenachrichtigungen
pSlackUserName	Slack-Benutzername.	Slack-Benutzer
pSecretKey	Das kann ein beliebiger Schlüssel sein. Wir empfehlen, die Standardeinstellung zu verwenden.	Webhook-URL
pWebHookUrl	Der Wert der Slack-URL.	https://hooks.slack.com/services/T??? 9 T?? /A031885 JRM7 /9D4Y??????
pAlertS3Bucket	Der Name des S3-Buckets, der als Ziel für die Netzwerk-Firewall-Warnung verwendet werden soll. Dieser Bucket wird für Sie erstellt.	us-w2- yourname-security-aod-alerts
pSecretTagName	Der Tagname für das Geheimnis.	AppName
pSecretTagValue	Der Tag-Wert für den angegebenen Tag-Namen.	LambdaSlackIntegration
pdestCidr	Der Filter für den CIDR-Zielbereich. Weitere Informationen finden Sie im nächsten Abschnitt, Filterverhalten.	10.0.0.0/16

`pdestCondition`	Eine Markierung, die angibt, ob die Zielübereinstimmung ausgeschlossen oder eingeschlossen werden soll. Weitere Informationen finden Sie im folgenden Abschnitt. Gültige Werte sind `include` und `exclude`.	include
`psrcCidr`	Der Filter für den CIDR-Quellbereich, für den eine Warnung ausgegeben werden soll. Weitere Informationen finden Sie im folgenden Abschnitt.	118.2.0.0/16
`psrcCondition`	Die Markierung, mit der der Quellen-Treffer ausgeschlossen oder aufgenommen werden soll. Weitere Informationen finden Sie im folgenden Abschnitt.	include

Verhalten des Filters

Wenn Sie in AWS Lambda keine Filter konfiguriert haben, werden alle generierten Benachrichtigungen an Ihren Slack-Kanal gesendet. Die Quelle und das Ziel IPs der generierten Benachrichtigungen werden mit den CIDR-Bereichen abgeglichen, die Sie bei der Bereitstellung der Vorlage konfiguriert haben. CloudFormation Wenn eine Übereinstimmung gefunden wird, wird die Bedingung angewendet. Wenn entweder die Quelle oder das Ziel in den konfigurierten CIDR-Bereich fällt und mindestens eines davon mit der Bedingung konfiguriert ist`include`, wird eine Warnung generiert. Die folgenden Tabellen enthalten Beispiele für CIDR-Werte, -Bedingungen und -Ergebnisse.

CIDR wurde konfiguriert	Alarm-IP	Configured	Warnung

Quelle	10.0.0.0/16	10.0.0.25	include	Ja
Zieladresse	100.0.0.0/16	202.0.0.13	include	

	CIDR konfiguriert	Alarm-IP	Configured	Warnung
Quelle	10.0.0.0/16	10.0.0.25	exclude	Nein
Zieladresse	100.0.0.0/16	202.0.0.13	include	

	CIDR konfiguriert	Alarm-IP	Configured	Warnung
Quelle	10.0.0.0/16	10.0.0.25	include	Ja
Zieladresse	100.0.0.0/16	100.0.0.13	include	

	CIDR konfiguriert	Alarm-IP	Configured	Warnung
Quelle	10.0.0.0/16	90.0.0.25	include	Ja
Zieladresse	Null	202.0.0.13	include	

	CIDR konfiguriert	Alarm-IP	Configured	Warnung
Quelle	10.0.0.0/16	90.0.0.25	include	Nein
Zieladresse	100.0.0.0/16	202.0.0.13	include	

Vereinfachen Sie die Verwaltung privater Zertifikate mithilfe von AWS Private CA und AWS RAM

Erstellt von Everett Hinckley (AWS) und Vivek Goyal (AWS)

Übersicht

Sie können die AWS Private Certificate Authority (AWS Private CA) verwenden, um private Zertifikate für die Authentifizierung interner Ressourcen und das Signieren von Computercode auszustellen. Dieses Muster bietet eine CloudFormation AWS-Vorlage für die schnelle Bereitstellung einer mehrstufigen CA-Hierarchie und eine konsistente Bereitstellungserfahrung. Optional können Sie AWS Resource Access Manager (AWS RAM) verwenden, um die CA sicher innerhalb Ihrer Organisationen oder Organisationseinheiten (OUs) in AWS Organizations gemeinsam zu nutzen und die CA zu zentralisieren, während Sie AWS RAM zur Verwaltung von Berechtigungen verwenden. Es ist nicht für jedes Konto eine private CA erforderlich, sodass Sie mit diesem Ansatz Geld sparen. Darüber hinaus können Sie Amazon Simple Storage Service (Amazon S3) verwenden, um die Zertifikatssperrliste (CRL) und die Zugriffsprotokolle zu speichern.

Diese Implementierung bietet die folgenden Funktionen und Vorteile:

- Zentralisiert und vereinfacht die Verwaltung der privaten CA-Hierarchie mithilfe von AWS Private CA.
- Exportiert Zertifikate und Schlüssel auf vom Kunden verwaltete Geräte auf AWS und vor Ort.
- Verwendet eine CloudFormation AWS-Vorlage für eine schnelle Bereitstellung und ein konsistentes Bereitstellungserlebnis.
- Erstellt eine private Stammzertifizierungsstelle zusammen mit einer untergeordneten CA-Hierarchie von 1, 2, 3 oder 4.
- Nutzt optional AWS-RAM, um die untergeordnete Zertifizierungsstelle der Endeinheit mit anderen Konten auf Organisations- oder OU-Ebene zu teilen.
- Spart Geld, da durch die Verwendung von AWS-RAM keine private CA für jedes Konto erforderlich ist.
- Erstellt einen optionalen S3-Bucket für die CRL.
- Erstellt einen optionalen S3-Bucket für CRL-Zugriffsprotokolle.

Voraussetzungen und Einschränkungen

Voraussetzungen

Wenn Sie die CA innerhalb einer AWS-Organisationsstruktur gemeinsam nutzen möchten, identifizieren oder richten Sie Folgendes ein:

- Ein Sicherheitskonto für die Erstellung und gemeinsame Nutzung der CA-Hierarchie.
- Eine separate Organisationseinheit oder ein Konto für Tests.
- Teilen ist innerhalb des Verwaltungskontos von AWS Organizations aktiviert. Weitere Informationen finden Sie unter Aktivieren der gemeinsamen Nutzung von Ressourcen innerhalb von AWS Organizations in der AWS-RAM-Dokumentation.

Einschränkungen

- CAs sind regionale Ressourcen. Alle CAs befinden sich in einem einzigen AWS-Konto und in einer einzigen AWS-Region.
- Benutzergenerierte Zertifikate und Schlüssel werden nicht unterstützt. Für diesen Anwendungsfall empfehlen wir, dass Sie diese Lösung so anpassen, dass sie eine externe Stammzertifizierungsstelle verwendet.
- Ein öffentlicher CRL-Bucket wird nicht unterstützt. Wir empfehlen, dass Sie die CRL privat halten. Wenn ein Internetzugang zur CRL erforderlich ist, lesen Sie den Abschnitt über die Verwendung von Amazon CloudFront als CRLs Server unter Aktivieren der Funktion S3 Block Public Access (BPA) in der Dokumentation zu AWS Private CA.
- Dieses Muster implementiert einen Ansatz für eine einzelne Region. Wenn Sie eine Zertifizierungsstelle mit mehreren Regionen benötigen, können Sie untergeordnete Zertifizierungsstellen in einer zweiten AWS-Region oder vor Ort implementieren. Diese Komplexität würde den Rahmen dieses Musters sprengen, da die Implementierung von Ihrem spezifischen Anwendungsfall, dem Workload-Volumen, den Abhängigkeiten und Anforderungen abhängt.

Architektur

Zieltechnologie-Stack

- Private AWS-Zertifizierungsstelle
- AWS RAM

- Amazon S3
- AWS Organizations
- AWS CloudFormation

Zielarchitektur

Dieses Muster bietet zwei Optionen für die Weitergabe an AWS Organizations:

Option 1 – Den Share auf Organisationsebene erstellen. Alle Konten in der Organisation können die privaten Zertifikate mithilfe der gemeinsamen Zertifizierungsstelle ausstellen, wie in der folgenden Abbildung dargestellt.

Option 2 – Erstellen Sie den Anteil auf der Ebene der Organisationseinheit (OU). Nur die Konten in der angegebenen Organisationseinheit können die privaten Zertifikate mithilfe der gemeinsamen Zertifizierungsstelle ausstellen. Im folgenden Diagramm können beispielsweise Entwickler 1 und Entwickler 2 private Zertifikate mithilfe der gemeinsamen Zertifizierungsstelle ausstellen, wenn die Freigabe auf der Ebene der Sandbox-Organisationseinheit erstellt wird.

Tools

AWS-Services

- AWS Private CA — AWS Private Certificate Authority (AWS Private CA) ist ein gehosteter privater CA-Dienst für die Ausstellung und den Widerruf privater digitaler Zertifikate. Er hilft Ihnen dabei, private CA-Hierarchien, einschließlich Stamm- und untergeordneter Zertifizierungsstellen, zu erstellen CAs, ohne die Investitions- und Wartungskosten für den Betrieb einer lokalen Zertifizierungsstelle anfallen zu müssen.
- AWS RAM — Mit AWS Resource Access Manager (AWS RAM) können Sie Ihre Ressourcen sicher zwischen AWS-Konten und innerhalb Ihrer Organisation oder OUs in AWS Organizations gemeinsam nutzen. Um den Betriebsaufwand in einer Umgebung mit mehreren Konten zu reduzieren, können Sie eine Ressource erstellen und AWS-RAM verwenden, um diese Ressource für mehrere Konten gemeinsam zu nutzen.
- AWS Organizations — AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten.

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen. Dieses Muster verwendet Amazon S3 zum Speichern der Zertifikatssperrliste (CRL) und der Zugriffsprotokolle.
- AWS CloudFormation — AWS CloudFormation hilft Ihnen dabei, Ihre AWS-Ressourcen zu modellieren und einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus zu verwalten. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben und sie zusammen als Stack zu starten und zu konfigurieren, anstatt Ressourcen einzeln zu verwalten. Dieses Muster verwendet AWS CloudFormation , um automatisch eine mehrstufige CA-Hierarchie bereitzustellen.

Code

Der Quellcode für dieses Muster ist im Hierarchie-Repository von AWS Private CA verfügbar. GitHub Das Repository umfasst:

- Die CloudFormation AWS-Vorlage`ACMPCA-RootCASubCA.yaml`. Sie können diese Vorlage verwenden, um die CA-Hierarchie für diese Implementierung bereitzustellen.
- Testdateien für Anwendungsfälle wie das Anfordern, Exportieren, Beschreiben und Löschen eines Zertifikats.

Folgen Sie den Anweisungen im Abschnitt Epics, um diese Dateien zu verwenden.

Epen

Gestalten Sie die CA-Hierarchie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sammeln Sie Informationen zum Betreff des Zertifikats.	Sammeln Sie Informationen zum Zertifikatsinhaber: Name der Organisation, Organisationseinheit, Land, Bundesland, Ort und allgemeiner Name.	Cloud-Architekt, Sicherheitsarchitekt, PKI-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Sammeln Sie optionale Informationen über AWS Organizations.	Wenn die CA Teil einer AWS-Organisationsstruktur sein soll und Sie die CA-Hierarchie innerhalb dieser Struktur gemeinsam nutzen möchten, erfassen Sie die Verwaltungskontonummer, die Organisations-ID und optional die OU-ID (wenn Sie die CA-Hierarchie nur mit einer bestimmten OU teilen möchten). Ermitteln Sie außerdem die AWS-Organisationskonten oder OUs, falls vorhanden, mit denen Sie die CA teilen möchten.	Cloud-Architekt, Sicherheitsarchitekt, PKI-Ingenieur
Entwerfen Sie die CA-Hierarchie.	Ermitteln Sie, welches Konto das Stammkonto und das untergeordnete CAs Konto beherbergen soll. Ermitteln Sie, wie viele untergeordnete Ebenen für die Hierarchie zwischen den Stamm- und den Endzertifikaten erforderlich sind. Weitere Informationen finden Sie unter Entwerfen einer CA-Hierarchie in der Dokumentation zu AWS Private CA.	Cloud-Architekt, Sicherheitsarchitekt, PKI-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Legen Sie die Benennungs- und Kennzeichnungskonventionen für die CA-Hierarchie fest.	Ermitteln Sie die Namen für die AWS-Ressourcen: die Stammzertifizierungsstelle und jede untergeordnete Zertifizierungsstelle. Ermitteln Sie, welche Tags jeder Zertifizierungsstelle zugewiesen werden sollen.	Cloud-Architekt, Sicherheitsarchitekt, PKI-Ingenieur
Ermitteln Sie die erforderlichen Verschlüsselungs- und Signierungsalgorithmen.	Ermitteln Sie Folgendes: • Die Anforderungen Ihres Unternehmens an den Verschlüsselungsalgorithmus für die öffentlichen Schlüssel, die Ihre Zertifizierungsstelle verwendet, wenn sie ein Zertifikat ausstellt. Die Standardeinstellung ist RSA_2048. • Der Schlüsselalgorithmus, den Ihre CA für das Signieren von Zertifikaten verwendet. Die Standardeinstellung ist SHA256 WITHRSA.	Cloud-Architekt, Sicherheitsarchitekt, PKI-Ingenieur
Ermitteln Sie die Anforderungen für den Widerruf von Zertifikaten für die CA-Hierarchie.	Wenn Funktionen zum Widerruf von Zertifikaten erforderlich sind, richten Sie eine Namenskonvention für den S3-Bucket ein, der die Zertifikatssperrliste (CRL) enthält.	Cloud-Architekt, Sicherheitsarchitekt, PKI-Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ermitteln Sie die Protokollierungsanforderungen für die CA-Hierarchie.	Wenn Funktionen zur Zugriffsprotokollierung erforderlich sind, richten Sie eine Namenskonvention für den S3-Bucket ein, der die Zugriffsprotokolle enthält.	Cloud-Architekt, Sicherheitsarchitekt, PKI-Ingenieur
Legen Sie die Ablaufzeiträume für Zertifikate fest.	Ermitteln Sie das Ablaufdatum für das Stammzertifikat (die Standardeinstellung ist 10 Jahre), die Endzertifikate (die Standardeinstellung ist 13 Monate) und die Zertifikate der untergeordneten Zertifizierungsstellen (die Standardeinstellung ist 3 Jahre). Zertifikate untergeordneter Zertifizierungsstellen sollten früher ablaufen als Zertifikate der Zertifizierungsstellen auf höheren Hierarchieebenen. Weitere Informationen finden Sie unter Verwaltung des privaten CA-Lebenszyklus in der Dokumentation zu AWS Private CA.	Cloud-Architekt, Sicherheitsarchitekt, PKI-Ingenieur

Stellen Sie die CA-Hierarchie bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erfüllen von -Voraussetzungen	Führen Sie die Schritte im Abschnitt Voraussetzungen dieses Musters aus.	Cloud-Administrator, Sicherheitsingenieure, PKI-Ingenieure

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie CA-Rollen für verschiedene Personas.	1. Ermitteln Sie die Typen von AWS Identity and Access Management (IAM) -Rollen oder -Benutzern in AWS IAM Identity Center (Nachfolger von AWS Single Sign-On), die für die Verwaltung der verschied enen Ebenen der CA-Hierar chie erforderlich sind, z. B. RootCAAdmin, Subordina te und. CAAdmin Certifica teConsumer 2. Ermitteln Sie die Granulari tät der Richtlinien, die für die Trennung von Aufgaben erforderlich sind. 3. Erstellen Sie die erforderl ichen IAM-Rollen oder - Benutzer in IAM Identity Center in dem Konto, in dem sich die CA-Hierarchie befindet.	Cloud-Administrator, Sicherhei tsingenieure, PKI-Ingenieure

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie den CloudFormation Stack bereit.	1. Laden Sie die GitHub Vorlage AWSPCA-RootCASubCA .yaml aus dem Repository für dieses Muster herunter. 2. Stellen Sie die Vorlage über die CloudFormation AWS-Konsole oder die AWS-Befehlszeilenschnittstelle (AWS CLI) bereit. Weitere Informationen finden Sie in der CloudFormation Dokumentation unter Arbeiten mit Stacks. 3. Vervollständigen Sie die Parameter in der Vorlage, einschließlich des Organisationsnamens, des Organisationsnamens, des Schlüsselalgorithmus, des Signaturalgorithmus und anderer Optionen.	Cloud-Administrator, Sicherheitsingenieure, PKI-Ingenieure

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Entwickeln Sie eine Lösung für die Aktualisierung von Zertifikaten, die von benutzerv erwalteten Ressourcen verwendet werden.	Ressourcen integrierter AWS-Services wie Elastic Load Balancing aktualisi eren Zertifikate automatis ch vor Ablauf. Benutzerv erwaltete Ressourcen, wie Webserver, die auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances laufen, erfordern jedoch einen anderen Mechanismus. 1. Ermitteln Sie, für welche benutzerverwalteten Ressourcen Endentitä tszertifikate von der privaten Zertifizierungsstelle erforderlich sind. 2. Planen Sie einen Prozess, um über den Ablauf von benutzerverwalteten Ressourcen und Zertifika ten informiert zu werden. -Beispiele finden Sie nachfolgend. • Verwenden einer verwalteten AWS Config-Regel • Amazon CloudWatch und Amazon verwenden EventBridge 3. Schreiben Sie benutzerd efinierte Skripts, um Zertifikate auf benutzerv	Cloud-Administrator, Sicherhei tsingenieure, PKI-Ingenieure

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	erwalteten Ressourcen zu aktualisieren, und integrier en Sie sie in AWS-Servi ces, um die Updates zu automatisieren. Weitere Informationen zu integrier ten AWS-Services finden Sie unter In AWS Certifica te Manager integrierte Services in der ACM-Dokumentation.	

Validieren und dokumentieren Sie die CA-Hierarchie

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Validieren Sie die optionale AWS-RAM-Sharing.	Wenn die CA-Hierarchie mit anderen Konten in AWS Organizations gemeinsam genutzt wird, melden Sie sich über die AWS-Manag ementkonsole bei einem dieser Konten an, navigiere n Sie zur AWS Private CA-Konsole und vergewissern Sie sich, dass die neu erstellte CA für dieses Konto gemeinsam genutzt wird. Nur die Zertifizi erungsstelle auf der untersten Ebene in der Hierarchie wird sichtbar sein, da dies die Zertifizierungsstelle ist, die die Zertifikate der Endeinhei t generiert. Wiederholen Sie	Cloud-Administrator, Sicherhei tsingenieure, PKI-Ingenieure

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	den Vorgang für eine Auswahl der Konten, mit denen die CA gemeinsam genutzt wird.	
Überprüfen Sie die CA-Hierarchie mit Lebenszyklustests für Zertifikate.	Suchen Sie im GitHub Repository für dieses Muster nach den Lebenszyklustests. Führen Sie die Tests über die AWS-CLI aus, um ein Zertifikat anzufordern, ein Zertifikat zu exportieren, ein Zertifikat zu beschreiben und ein Zertifikat zu löschen.	Cloud-Administrator, Sicherheitsingenieure, PKI-Ingenieure
Importieren Sie die Zertifikatskette in Trust Stores.	Damit Browser und andere Anwendungen einem Zertifikat vertrauen können, muss der Aussteller des Zertifikats im Trust Store des Browsers, einer Liste vertrauenswürdiger CAs Zertifikate, enthalten sein. Fügen Sie die Zertifikatskette für die neue CA-Hierarchie zum Trust Store Ihres Browsers und Ihrer Anwendung hinzu. Vergewissern Sie sich, dass die Zertifikate der Endeinheit vertrauenswürdig sind.	Cloud-Administrator, Sicherheitsingenieure, PKI-Ingenieure

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein Runbook, um die CA-Hierarchie zu dokumentieren.	Erstellen Sie ein Runbook-Dokument, um die Architektur der CA-Hierarchie, die Kontostruktur, mit der Endentitätszertifikate angefordert werden können, den Erstellungsprozess und grundlegende Verwaltungsaufgaben wie das Ausstellen von Endentitätszertifikaten (sofern Sie Self-Service durch untergeordnete Konten nicht zulassen möchten), die Nutzung und die Nachverfolgung zu beschreiben.	Cloud-Administrator, Sicherheitsingenieure, PKI-Ingenieure

Zugehörige Ressourcen

- Entwerfen einer CA-Hierarchie (AWS Private CA-Dokumentation)
- Eine private Zertifizierungsstelle erstellen (Dokumentation zu AWS Private CA)
- So verwenden Sie AWS-RAM, um Ihr AWS Private CA-Konto gemeinsam zu nutzen (AWS-Blogbeitrag)
- Bewährte Methoden für AWS Private CA (AWS-Blogbeitrag)
- Aktivieren Sie die gemeinsame Nutzung von Ressourcen innerhalb von AWS Organizations (AWS-RAM-Dokumentation)
- Verwaltung des privaten CA-Lebenszyklus (Dokumentation zu AWS Private CA)
- acm-certificate-expiration-check für AWS Config (AWS Config-Dokumentation)
- AWS Certificate Manager bietet jetzt die Überwachung des Ablaufs von Zertifikaten über Amazon CloudWatch (AWS-Ankündigung)
- In AWS Certificate Manager integrierte Services (ACM-Dokumentation)

Zusätzliche Informationen

Verwenden Sie beim Exportieren von Zertifikaten eine Passphrase, die kryptografisch sicher ist und der Strategie Ihres Unternehmens zur Verhinderung von Datenverlust entspricht.

Deaktivieren Sie die Sicherheitsstandardkontrollen für alle Security Hub Hub-Mitgliedskonten in einer Umgebung mit mehreren Konten

Erstellt von Michael Fuellbier (AWS) und Ahmed Bakry (AWS)

Übersicht

> **Important**
>
> AWS Security Hub unterstützt jetzt die zentrale Konfiguration für Sicherheitsstandards und -kontrollen für alle Konten. Diese neue Funktion adressiert viele der Szenarien, die von der Lösung in diesem AWS Prescriptive Guidance-Muster abgedeckt werden. Bevor Sie die Lösung in diesem Muster bereitstellen, finden Sie weitere Informationen unter Zentrale Konfiguration in Security Hub.

In der Amazon Web Services (AWS) Cloud können AWS Security Hub Standardsteuerungen wie CIS AWS Foundations Benchmark oder AWS Foundational Security Best Practices nur manuell von einer einzigen AWS-Konto aus ausgeschaltet (deaktiviert) werden. In einer Umgebung mit mehreren Konten können Sie die Kontrollen für mehrere Security Hub Hub-Mitgliedskonten nicht mit „einem Klick“ (d. h. einem API-Aufruf) ausschalten. Dieses Muster zeigt, wie Sie mit einem Klick die Standardsteuerungen von Security Hub für alle Security Hub-Mitgliedskonten deaktivieren, die von Ihrem Security Hub-Administratorkonto verwaltet werden.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Eine Umgebung mit mehreren Konten, bestehend aus einem Security Hub-Administratorkonto, das mehrere Mitgliedskonten verwaltet
- AWS Command Line Interface (AWS CLI) Version 2, installiert
- AWS Serverless Application Model Befehlszeilenschnittstelle (AWS SAM CLI), installiert

Einschränkungen

- Dieses Muster funktioniert nur in einer Umgebung mit mehreren Konten, in der ein einzelnes Security Hub-Administratorkonto mehrere Mitgliedskonten verwaltet.

- Die Initiierung des Ereignisses führt zu mehreren parallel Aufrufen, wenn Sie viele Steuerelemente in einem sehr kurzen Zeitraum ändern. Dies kann zu einer Drosselung der API führen und dazu führen, dass die Aufrufe fehlschlagen. Dieses Szenario kann beispielsweise eintreten, wenn Sie viele Steuerelemente mithilfe der Security Hub Controls CLI programmgesteuert ändern.

Architektur

Das folgende Diagramm zeigt ein Beispiel für einen AWS Step Functions Workflow, der die Standardsteuerungen von Security Hub für mehrere Security Hub-Mitgliedskonten deaktiviert (vom Security Hub-Administratorkonto aus betrachtet).

Das Diagramm umfasst den folgenden Arbeitsablauf:

1. Eine EventBridge Amazon-Regel wird täglich initiiert und ruft die Zustandsmaschine auf. Sie können den Zeitpunkt der Regel ändern, indem Sie den `Schedule` Parameter in Ihrer AWS CloudFormation Vorlage aktualisieren.
2. Eine EventBridge Regel wird immer dann initiiert, wenn ein Steuerelement im Security Hub-Administratorkonto ein- oder ausgeschaltet wird.
3. Ein Step Functions Functions-Zustandsmaschine überträgt den Status der Sicherheitsstandardsteuerungen (d. h. Steuerungen, die ein- oder ausgeschaltet sind) vom Security Hub-Administratorkonto an die Mitgliedskonten.
4. In jedem Mitgliedskonto wird eine kontoübergreifende AWS Identity and Access Management (IAM) -Rolle bereitgestellt, die von der Zustandsmaschine übernommen wird. Die Zustandsmaschine schaltet die Steuerungen in jedem Mitgliedskonto ein oder aus.
5. Eine Amazon DynamoDB-Tabelle enthält Ausnahmen und Informationen darüber, welche Kontrollen in einem bestimmten Konto aktiviert oder deaktiviert werden müssen. Diese Informationen überschreiben die Konfigurationen, die vom Security Hub-Administratorkonto für das angegebene Mitgliedskonto abgerufen wurden.

> **Note**
>
> Mit der geplanten EventBridge Regel soll sichergestellt werden, dass neu hinzugefügte Security Hub Hub-Mitgliedskonten denselben Kontrollstatus haben wie bestehende Konten.

Tools

AWS-Services

- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, mit dem Sie Ihre Anwendungen mit Echtzeitdaten aus einer Vielzahl von Quellen verbinden können. Zum Beispiel AWS Lambda Funktionen, HTTP-Aufruf-Endpunkte, die API-Ziele verwenden, oder Event-Busse in anderen. AWS-Konten
- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie AWS-Services über Befehle in Ihrer Befehlszeilen-Shell interagieren können.
- AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Es führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- AWS Serverless Application Model (AWS SAM) ist ein Open-Source-Framework, mit dem Sie serverlose Anwendungen in der erstellen können. AWS Cloud
- AWS Security Hubbietet einen umfassenden Überblick über Ihren Sicherheitsstatus in. AWS Es hilft Ihnen auch dabei, Ihre AWS Umgebung anhand von Industriestandards und Best Practices im Bereich Sicherheit zu überprüfen.
- AWS Step Functionsist ein serverloser Orchestrierungsservice, mit dem Sie AWS Lambda Funktionen und andere Funktionen kombinieren können, um geschäftskritische AWS-Services Anwendungen zu erstellen.

Code-Repository

Der Code für dieses Muster ist im GitHub AWS Security Hub Cross-Account Controls Disabler-Repository verfügbar. Das Code-Repository enthält die folgenden Dateien und Ordner:

- UpdateMembers/template.yaml — Diese Datei enthält Komponenten, die im Security Hub-Administratorkonto bereitgestellt wurden, einschließlich der Step Functions-Zustandsmaschine und der Regeln. EventBridge
- member-iam-role/template.yaml — Diese Datei enthält den Code für die Bereitstellung der kontoübergreifenden IAM-Rolle in einem Mitgliedskonto.
- StateMachine.json — Diese Datei definiert den Workflow der State Machine.

- GetMembers/index.py — Diese Datei enthält den Code für den State Machine. GetMembers Ein Skript ruft den Status der Sicherheitsstandardkontrollen in allen vorhandenen Security Hub Hub-Mitgliedskonten ab.
- UpdateMember/index.py — Diese Datei enthält ein Skript, das den Kontrollstatus in jedem Mitgliedskonto aktualisiert.
- CheckResult/index.py — Diese Datei enthält ein Skript, das den Status des Workflow-Aufrufs überprüft (akzeptiert oder fehlgeschlagen).

Epen

Stellen Sie eine kontoübergreifende IAM-Rolle in den Security Hub Hub-Mitgliedskonten bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Identifizieren Sie die Konto-ID des Security Hub-Administratorkontos.	Richten Sie ein Security Hub-Administratorkonto ein und notieren Sie sich dann die Konto-ID des Administratorkontos.	Cloud-Architekt
Stellen Sie die CloudFormation Vorlage bereit, die die kontoübergreifende IAM-Rolle in den Mitgliedskonten enthält.	Führen Sie den folgenden member-iam-roleBefehl aus, um die Vorlage /template.yaml in allen Mitgliedskonten bereitzustellen, die vom Security Hub-Administratorkonto verwaltet werden: `aws cloudformation deploy \ --template-file member-iam-role/template.yaml \ --capabilities CAPABILITY_NAMED_IAM \ --stack-name <your-stack-name> \`	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	`--parameter-overrides SecurityHubAdminAccountId=<account-ID>` Der `SecurityHubAdminAccountId` Parameter muss mit der Security Hub-Administratorkonto-ID übereinstimmen, die Sie zuvor notiert haben.	

Stellen Sie eine Zustandsmaschine im Security Hub-Administratorkonto bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Package Sie die CloudFormation Vorlage, die die Zustandsmaschine mit enthält AWS SAM.	Führen Sie den folgenden UpdateMembersBefehl aus, um die Vorlage /template.yaml im Security Hub-Administratorkonto zu packen:
	
	`sam package \`
	`--template-file UpdateMembers/template.yaml \`
	`--output-template-file UpdateMembers/template-out.yaml \`
	`--s3-bucket <amzn-s3-demo-bucket>`
	
	Note
	Ihr Amazon Simple Storage Service (Amazon S3) -
		AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Bucket muss sich in demselben Bucket befinden, in AWS-Region dem Sie die CloudFormation Vorlage bereitstellen.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die verpackte CloudFormation Vorlage im Security Hub-Administratork onto bereit.	Führen Sie den folgenden Befehl aus, um die CloudForm ation Vorlage im Security Hub-Administratorkonto bereitzus tellen: `aws cloudformation deploy \ --template-file UpdateMembers/temp late-out.yaml \ --capabilities CAPABILITY_IAM \ --stack-name <stack-name>` In der Vorlage member-ia m-role/template.yaml muss der Parameter mit dem `MemberIAMRolePath` Parameter übereinstimmen und übereinstimmen. `IAMRolePath MemberIAM RoleName IAMRoleName` **Note** Da es sich bei Security Hub um einen regionalen Dienst handelt, müssen Sie die Vorlage in jedem Dienst einzeln bereitstellen AWS-Region. Stellen Sie sicher, dass Sie die	AWS DevOps

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Lösung zunächst in einem Amazon S3 S3-Bucket in jeder Region verpacken.	

Zugehörige Ressourcen

- Ein Security Hub-Administratorkonto einrichten (Security Hub Hub-Dokumentation)
- Umgang mit Fehlern, Wiederholungsversuchen und Hinzufügen von Warnmeldungen zu AWS Step Functions State Machine-Ausführungen (Blogbeitrag)AWS

Aktualisieren Sie die AWS-CLI-Anmeldeinformationen aus dem AWS IAM Identity Center mithilfe von PowerShell

Erstellt von Tschad Miles (AWS) und Andy Bowen (AWS)

Übersicht

Wenn Sie Anmeldeinformationen für AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) mit AWS Command Line Interface (AWS CLI) SDKs, AWS oder AWS Cloud Development Kit (AWS CDK) verwenden möchten, müssen Sie die Anmeldeinformationen normalerweise von der IAM Identity Center-Konsole kopieren und in die Befehlszeilenschnittstelle einfügen. Dieser Vorgang kann viel Zeit in Anspruch nehmen und muss für jedes Konto wiederholt werden, für das Zugriff erforderlich ist.

Eine gängige Lösung ist die Verwendung des `aws sso configure` AWS-CLI-Befehls. Dieser Befehl fügt Ihrer AWS-CLI oder Ihrem AWS-SDK ein für IAM Identity Center aktiviertes Profil hinzu. Der Nachteil dieser Lösung besteht jedoch darin, dass Sie den Befehl `aws sso login` für jedes AWS-CLI-Profil oder Konto ausführen müssen, das Sie auf diese Weise konfiguriert haben.

Als alternative Lösung beschreibt dieses Muster, wie benannte AWS-CLI-Profile und AWS-Tools verwendet werden, PowerShell um Anmeldeinformationen für mehrere Konten aus einer einzigen IAM Identity Center-Instance gleichzeitig zu speichern und zu aktualisieren. Das Skript speichert außerdem IAM Identity Center-Sitzungsdaten im Speicher, um Anmeldeinformationen zu aktualisieren, ohne sich erneut bei IAM Identity Center anmelden zu müssen.

Voraussetzungen und Einschränkungen

Voraussetzungen

- PowerShell, installiert und konfiguriert. Weitere Informationen finden Sie unter Installation PowerShell (Microsoft-Dokumentation).
- AWS-Tools für PowerShell, installiert und konfiguriert. Aus Leistungsgründen empfehlen wir dringend, die modularisierte Version von AWS Tools for zu installieren PowerShell, genannt`AWS.Tools`. Jeder AWS-Service wird von einem eigenen, kleinen Modul unterstützt. Geben Sie in der PowerShell Eingabeaufforderung die folgenden Befehle ein, um die für dieses Muster benötigten Module zu installieren: `AWS.Tools.InstallerSSO`, und`SSOIDC`.

```
Install-Module AWS.Tools.Installer
```

```
Install-AWSToolsModule SSO, SSOOIDC
```

Weitere Informationen finden Sie unter Installieren von AWS.Tools unter Windows oder Installieren von AWS.Tools unter Linux oder macOS.

- AWS CLI oder das AWS-SDK müssen zuvor mit funktionierenden Anmeldeinformationen konfiguriert werden, indem Sie einen der folgenden Schritte ausführen:
  - Verwenden Sie den `aws configure` AWS-CLI-Befehl. Weitere Informationen finden Sie unter Schnellkonfiguration (AWS-CLI-Dokumentation).
  - Konfigurieren Sie AWS CLI oder AWS CDK, um temporären Zugriff über eine IAM-Rolle zu erhalten. Weitere Informationen finden Sie unter Abrufen von IAM-Rollenanmeldedaten für den CLI-Zugriff (IAM Identity Center-Dokumentation).

Einschränkungen

- Dieses Skript kann nicht in einer Pipeline oder einer vollautomatischen Lösung verwendet werden. Wenn Sie dieses Skript bereitstellen, müssen Sie den Zugriff über das IAM Identity Center manuell autorisieren. Das Skript wird dann automatisch fortgesetzt.

Produktversionen

- Für alle Betriebssysteme wird empfohlen, PowerShell Version 7.0 oder höher zu verwenden.

Architektur

Sie können das Skript in diesem Muster verwenden, um mehrere IAM Identity Center-Anmeldeinformationen gleichzeitig zu aktualisieren, und Sie können eine Anmeldeinformationsdatei für die Verwendung mit AWS CLI, AWS oder AWS SDKs CDK erstellen.

Tools

AWS-Services

- AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit AWS-Services interagieren können.

- Mit AWS IAM Identity Center können Sie den Single Sign-On (SSO) -Zugriff auf all Ihre AWS-Konten und Cloud-Anwendungen zentral verwalten.
- Bei den AWS-Tools für PowerShell handelt es sich um eine Reihe von PowerShell Modulen, die Ihnen helfen, Operationen auf Ihren AWS-Ressourcen von der PowerShell Befehlszeile aus zu skripten.

Andere Tools

- PowerShellist ein Automatisierungs- und Konfigurationsverwaltungsprogramm von Microsoft, das unter Windows, Linux und macOS läuft.

Bewährte Methoden

Bewahren Sie für jede IAM Identity Center-Instanz eine Kopie dieses Skripts auf. Die Verwendung eines Skripts für mehrere Instanzen wird nicht unterstützt.

Epen

Führen Sie das SSO-Skript aus

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Passen Sie das SSO-Skript an.	1. Kopieren Sie das SSO-Skript im Abschnitt Zusätzliche Informationen. 2. Definieren Sie im `Param` Abschnitt für Ihre AWS-Umgebung die Werte für die folgenden Variablen: • `DefaultRoleName` — Die IAM-Rolle oder der standardmäßig zu verwendende Berechtigungssatz. • `Region`— Die AWS-Region, in der IAM	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Identity Center bereitgestellt wird. Eine vollständige Liste der Regionen und ihrer Codes finden Sie unter Regionale Endpunkte. • `StartUrl`— Die URL, die für den Zugriff auf Ihre IAM Identity Center-Anmeldeseite verwendet wurde. Verwenden Sie dasselbe Format wie für den Beispielwert im Skript. • `EnvironmentName` — Ein Kurzname, der auf diese Kopie des Skripts verweist und verwendet wird, wenn Sie mehrere Skriptkopien in derselben Sitzung ausführen. 3. Bearbeiten Sie unter Zeile 10, die wie folgt lautet# `Add your Account Information` , die folgenden Werte in den Hash-Tabellen, um sie an Ihre Umgebung anzupassen: • `Profile`— Der AWS-CLI-Profilname, in dem die temporären Anmeldeinformation	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	en gespeichert werden sollen. • `AccountId` — Die ID des AWS-Kontos, für das Sie Anmeldeinformation en abrufen. • `RoleName`— Der Name der IAM Identity Center-Rolle oder des Berechtigungssatze s, den Sie verwenden möchten. Sie können dies so belassen, als `$DefaultRoleName` ob Sie dieselbe Rolle verwenden möchten, die Sie im `Param` Abschnitt definiert haben. Jede Zeile in der Hashtabel le muss mit einem Komma enden, mit Ausnahme der letzten.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Führen Sie das SSO-Skript aus.	Es wird empfohlen, dass Sie Ihr benutzerdefiniertes Skript in der PowerShell Shell mit dem folgenden Befehl ausführen.
	`./Set-AwsCliSsoCredentials.ps1`
	Sie können das Skript auch von einer anderen Shell aus ausführen, indem Sie den folgenden Befehl eingeben.
	`pwsh Set-AwsCliSsoCredentials.ps1`
		Cloud-Administrator

Fehlerbehebung

Problem	Lösung
`No Access`-Fehler	Die von Ihnen verwendete IAM-Rolle verfügt nicht über Berechtigungen für den Zugriff auf die Rolle oder den Berechtigungssatz, die Sie in einem `RoleName` Parameter definiert haben. Aktualisieren Sie die Berechtigungen für die Rolle, die Sie verwenden, oder definieren Sie eine andere Rolle oder einen anderen Berechtigungssatz im Skript.

Zugehörige Ressourcen

- Wo werden die Konfigurationseinstellungen gespeichert? (AWS-CLI-Dokumentation)

- Konfiguration der AWS-CLI für die Verwendung von AWS IAM Identity Center (AWS-CLI-Dokumentation)
- Benannte Profile verwenden (AWS-CLI-Dokumentation)

Zusätzliche Informationen

SSO-Skript

Ersetzen Sie im folgenden Skript Platzhalter in spitzen Klammern (**<>**) durch Ihre eigenen Informationen und entfernen Sie die spitzen Klammern.

```
Set-AwsCliSsoCredentials.ps1
Param(
    $DefaultRoleName = '<AWSAdministratorAccess>',
    $Region          = '<us-west-2>',
    $StartUrl        = "<https://d-12345abcde.awsapps.com/start/>",
    $EnvironmentName = "<CompanyName>"
)
Try {$SsoAwsAccounts = (Get-Variable -name "$($EnvironmentName)SsoAwsAccounts" -Scope
 Global -ErrorAction 'SilentlyContinue').Value.Clone()}
Catch {$SsoAwsAccounts = $False}
if (-not $SsoAwsAccounts) { $SsoAwsAccounts = @(
# Add your account information in the list of hash tables below, expand as necessary,
 and do not forget the commas
    @{Profile = "<Account1>"      ; AccountId = "<012345678901 >"; RoleName =
 $DefaultRoleName },
    @{Profile = "<Account2>"      ; AccountId = "<123456789012>"; RoleName =
 "<AWSReadOnlyAccess>" }
)}
$ErrorActionPreference = "Stop"
if (-not (Test-Path ~\.aws))      { New-Item ~\.aws -type Directory }
if (-not (Test-Path ~\.aws\credentials)) { New-Item ~\.aws\credentials -type File }
$CredentialFile = Resolve-Path ~\.aws\credentials
$PsuedoCreds    = @{AccessKey =
 'AKAEXAMPLE123ACCESS';SecretKey='PsuedoS3cret4cceSSKey123PsuedoS3cretKey'} # Pseudo
 Creds, do not edit.
Try {$SSOTokenExpire = (Get-Variable -Scope Global -Name
 "$($EnvironmentName)SSOTokenExpire" -ErrorAction 'SilentlyContinue').Value} Catch
 {$SSOTokenExpire = $False}
Try {$SSOToken       = (Get-Variable -Scope Global -Name "$($EnvironmentName)SSOToken"
 -ErrorAction 'SilentlyContinue').Value }      Catch {$SSOToken       = $False}
if ( $SSOTokenExpire -lt (Get-Date) ) {
```

```
    $SSOToken = $Null
    $Client   = Register-SSOOIDCClient -ClientName cli-sso-client -ClientType public -
Region $Region @PsuedoCreds
    $Device   = $Client | Start-SSOOIDCDeviceAuthorization -StartUrl $StartUrl -Region
 $Region @PsuedoCreds
    Write-Host "A Browser window should open. Please login there and click ALLOW." -
NoNewline
    Start-Process $Device.VerificationUriComplete
    While (-Not $SSOToken){
        Try {$SSOToken = $Client | New-SSOOIDCToken -DeviceCode $Device.DeviceCode -
GrantType "urn:ietf:params:oauth:grant-type:device_code" -Region $Region @PsuedoCreds}
        Catch {If ($_.Exception.Message -notlike "*AuthorizationPendingException*")
{Write-Error $_.Exception} ; Start-Sleep 1}
    }
    $SSOTokenExpire = (Get-Date).AddSeconds($SSOToken.ExpiresIn)
    Set-Variable -Name "$($EnvironmentName)SSOToken" -Value $SSOToken -Scope Global
    Set-Variable -Name "$($EnvironmentName)SSOTokenExpire" -Value $SSOTokenExpire -
Scope Global
}
$CredsTime     = $SSOTokenExpire - (Get-Date)
$CredsTimeText = ('{0:D2}:{1:D2}:{2:D2} left on SSO Token' -f $CredsTime.Hours,
 $CredsTime.Minutes, $CredsTime.Seconds).TrimStart("0 :")
for ($i = 0; $i -lt $SsoAwsAccounts.Count; $i++) {
    if (([DateTimeOffset]::FromUnixTimeSeconds($SsoAwsAccounts[$i].CredsExpiration /
 1000)).DateTime -lt (Get-Date).ToUniversalTime()) {
        Write-host "`r
    `rRegistering Profile $($SsoAwsAccounts[$i].Profile)" -NoNewline
        $TempCreds = $SSOToken | Get-SSORoleCredential -AccountId
 $SsoAwsAccounts[$i].AccountId -RoleName $SsoAwsAccounts[$i].RoleName -Region $Region
 @PsuedoCreds
        [PSCustomObject]@{AccessKey = $TempCreds.AccessKeyId; SecretKey =
 $TempCreds.SecretAccessKey; SessionToken = $TempCreds.SessionToken
        } | Set-AWSCredential -StoreAs $SsoAwsAccounts[$i].Profile -ProfileLocation
 $CredentialFile
        $SsoAwsAccounts[$i].CredsExpiration = $TempCreds.Expiration
    }
}
Set-Variable -name "$($EnvironmentName)SsoAwsAccounts" -Value $SsoAwsAccounts.Clone() -
Scope Global
Write-Host "`r$($SsoAwsAccounts.Profile) Profiles registered, $CredsTimeText"
```

Verwenden Sie AWS Config, um die Sicherheitskonfigurationen von Amazon Redshift zu überwachen

Erstellt von Lucas Kauffman (AWS) und Abhishek Sengar (AWS)

Übersicht

Mit AWS Config können Sie die Sicherheitskonfigurationen für Ihre AWS-Ressourcen bewerten. AWS Config kann die Ressourcen überwachen, und wenn die Konfigurationseinstellungen gegen Ihre definierten Regeln verstoßen, kennzeichnet AWS Config die Ressource als nicht konform.

Sie können AWS Config verwenden, um Ihre Amazon Redshift Redshift-Cluster und -Datenbanken zu evaluieren und zu überwachen. Weitere Informationen zu Sicherheitsempfehlungen und Funktionen finden Sie unter Sicherheit in Amazon Redshift. Dieses Muster beinhaltet benutzerdefinierte AWS Lambda Lambda-Regeln für AWS Config. Sie können diese Regeln in Ihrem Konto bereitstellen, um die Sicherheitskonfigurationen Ihrer Amazon Redshift Redshift-Cluster und -Datenbanken zu überwachen. Die Regeln in diesem Muster helfen Ihnen, mithilfe von AWS Config zu bestätigen, dass:

- Die Audit-Protokollierung ist für die Datenbanken im Amazon Redshift Redshift-Cluster aktiviert
- SSL ist erforderlich, um eine Verbindung zum Amazon Redshift Redshift-Cluster herzustellen
- Es werden FIPS-Chiffren (Federal Information Processing Standards) verwendet
- Datenbanken im Amazon Redshift Redshift-Cluster sind verschlüsselt
- Die Überwachung der Benutzeraktivitäten ist aktiviert

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS Config muss in Ihrem AWS-Konto aktiviert sein. Weitere Informationen finden Sie unter Einrichten von AWS Config mit der Konsole oder Einrichten von AWS Config mit der AWS-CLI.
- Python Version 3.9 oder höher muss für den AWS Lambda Lambda-Handler verwendet werden. Weitere Informationen finden Sie unter Arbeiten mit Python (AWS Lambda Lambda-Dokumentation).

Produktversionen

- Python-Version 3.9 oder höher

Architektur

Zieltechnologie-Stack

- AWS Config

Zielarchitektur

1. AWS Config führt die benutzerdefinierte Regel regelmäßig aus.
2. Die benutzerdefinierte Regel ruft die Lambda-Funktion auf.
3. Die Lambda-Funktion überprüft die Amazon Redshift Redshift-Cluster auf nicht konforme Konfigurationen.
4. Die Lambda-Funktion meldet den Konformitätsstatus jedes Amazon Redshift Redshift-Clusters an AWS Config.

Automatisierung und Skalierung

Die benutzerdefinierten Regeln von AWS Config werden skaliert, um alle Amazon Redshift Redshift-Cluster in Ihrem Konto zu bewerten. Es sind keine zusätzlichen Maßnahmen erforderlich, um diese Lösung zu skalieren.

Tools

AWS-Services

- AWS Config bietet eine detaillierte Ansicht der Ressourcen in Ihrem AWS-Konto und deren Konfiguration. Es hilft Ihnen zu erkennen, wie Ressourcen miteinander zusammenhängen und wie sich ihre Konfigurationen im Laufe der Zeit geändert haben.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.

- AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Er führt Ihren Code nur bei Bedarf aus und skaliert automatisch, sodass Sie nur für die tatsächlich genutzte Rechenzeit zahlen.
- Amazon Redshift ist ein verwalteter Data-Warehouse-Service im Petabyte-Bereich in der AWS-Cloud.

Code-Repository

Der Code für dieses Muster ist im GitHub aws-config-rulesRepository verfügbar. Die benutzerdefinierten Regeln in diesem Repository sind Lambda-Regeln in der Programmiersprache Python. Dieses Repository enthält viele benutzerdefinierte Regeln für AWS Config. In diesem Muster werden nur die folgenden Regeln verwendet:

- `REDSHIFT_AUDIT_ENABLED`— Vergewissern Sie sich, dass die Audit-Protokollierung auf dem Amazon Redshift Redshift-Cluster aktiviert ist. Wenn Sie auch sicherstellen möchten, dass die Überwachung der Benutzeraktivitäten aktiviert ist, stellen Sie stattdessen die `REDSHIFT_USER_ACTIVITY_MONITORING_ENABLED` Regel bereit.
- `REDSHIFT_SSL_REQUIRED`— Vergewissern Sie sich, dass SSL für die Verbindung zum Amazon Redshift Redshift-Cluster erforderlich ist. Wenn Sie auch sicherstellen möchten, dass FIPS-Chiffren (Federal Information Processing Standards) verwendet werden, stellen Sie stattdessen die Regel bereit. `REDSHIFT_FIPS_REQUIRED`
- `REDSHIFT_FIPS_REQUIRED`— Stellen Sie sicher, dass SSL erforderlich ist und FIPS-Chiffren verwendet werden.
- `REDSHIFT_DB_ENCRYPTED`— Vergewissern Sie sich, dass die Datenbanken im Amazon Redshift Redshift-Cluster verschlüsselt sind.
- `REDSHIFT_USER_ACTIVITY_MONITORING_ENABLED`— Vergewissern Sie sich, dass die Auditprotokollierung und die Überwachung der Benutzeraktivitäten aktiviert sind.

Epen

Bereite dich auf die Implementierung der Regeln vor

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Konfigurieren Sie IAM-Richtlinien.	1. Erstellen Sie eine benutzerdefinierte identitätsbasierte	AWS-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	IAM-Richtlinie, die es der Lambda-Ausführungsrolle ermöglicht, die Amazon Redshift Redshift-Clusterkonfigurationen zu lesen. Weitere Informationen finden Sie unter Verwalten des Zugriffs auf Ressourcen (Amazon Redshift Redshift-Dokumentation) und Erstellen von IAM-Richtlinien (IAM-Dokumentation). `{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["redshift:DescribeClusterParameterGroups", "redshift:DescribeClusterParameters", "redshift:DescribeClusters", "redshift:DescribeClusterSecurityGroups", "redshift:DescribeClusterSnapshots", "redshift:DescribeClusterSubnetGroups",`	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"redshift
	:DescribeEventSubs
	criptions",
	"redshift
	:DescribeLoggingSt
	atus"
	],
	"Resource":
	"*"
	}
	]
	}</pre>
	2. Weisen Sie die AWSLambdaAusführungsrichtlinien und die AWSConfigRulesExecutionRoleverwalteten Richtlinien als Berechtigungsrichtlinie für die Lambda-Ausführungsrolle zu. Anweisungen finden Sie unter Hinzufügen von IAM-Identitätsberechtigungen (IAM-Dokumentation).	

Klonen Sie das Repository	Führen Sie in einer Bash-Shell den folgenden Befehl aus. Dadurch wird das aws-config-rulesRepository von geklont. GitHub <pre>git clone https://github.com/awslabs/aws-config-rules.git</pre>	Allgemeines AWS

Stellen Sie die Regeln in AWS Config bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie die Regeln in AWS Config bereit.	Folgen Sie den Anweisungen unter Benutzerdefinierte Lambda-Regeln erstellen (AWS Config-Dokumentation) und stellen Sie eine oder mehrere der folgenden Regeln in Ihrem Konto bereit: • `REDSHIFT_AUDIT_ENABLED` • `REDSHIFT_SSL_REQUIRED` • `REDSHIFT_FIPS_REQUIRED` • `REDSHIFT_DB_ENCRYPTED` • `REDSHIFT_USER_ACTIVITY_MONITORING_ENABLED`	AWS-Administrator
Stellen Sie sicher, dass die Regeln funktionieren.	Folgen Sie nach der Bereitstellung der Regeln den Anweisungen unter Evaluieren Ihrer Ressourcen (AWS Config-Dokumentation), um sicherzustellen, dass AWS Config Ihre Amazon Redshift Redshift-Ressourcen korrekt auswertet.	Allgemeines AWS

Zugehörige Ressourcen

AWS-Servicedokumentation

- Sicherheit in Amazon Redshift (Amazon Redshift Redshift-Dokumentation)
- Verwaltung der Datenbanksicherheit (Amazon Redshift Redshift-Dokumentation)
- Benutzerdefinierte Regeln für AWS Config (AWS Config-Dokumentation)

AWS Prescriptive Guidance

- Stellen Sie sicher, dass für neue Amazon Redshift Redshift-Cluster SSL-Endpunkte erforderlich sind
- Stellen Sie sicher, dass ein Amazon Redshift Redshift-Cluster bei der Erstellung verschlüsselt ist

Zusätzliche Informationen

Sie können die folgenden AWS-verwalteten Regeln in AWS Config verwenden, um die folgenden Sicherheitskonfigurationen für Amazon Redshift zu bestätigen:

- redshift-cluster-configuration-check— Verwenden Sie diese Regel, um zu bestätigen, dass die Audit-Protokollierung für die Datenbanken im Amazon Redshift Redshift-Cluster aktiviert ist, und um zu bestätigen, dass die Datenbanken verschlüsselt sind.
- redshift-require-tls-ssl— Verwenden Sie diese Regel, um zu bestätigen, dass SSL für die Verbindung zum Amazon Redshift Redshift-Cluster erforderlich ist.

Verwenden Sie die Network Firewall, um die DNS-Domänennamen aus der Servernamenanzeige für ausgehenden Datenverkehr zu erfassen

Erstellt von Kirankumar Chandrashekar (AWS)

Übersicht

Dieses Muster zeigt Ihnen, wie Sie die AWS Network Firewall verwenden, um die DNS-Domainnamen zu sammeln, die von der Server Name Indication (SNI) im HTTPS-Header Ihres ausgehenden Netzwerkverkehrs bereitgestellt werden. Network Firewall ist ein verwalteter Service, der es einfach macht, wichtige Netzwerkschutzmaßnahmen für Amazon Virtual Private Cloud (Amazon VPC) bereitzustellen, einschließlich der Fähigkeit, ausgehenden Datenverkehr mit einer Firewall zu sichern, die Pakete blockiert, die bestimmte Sicherheitsanforderungen nicht erfüllen. Die Sicherung des ausgehenden Datenverkehrs zu bestimmten DNS-Domainnamen wird als Ausgangsfilterung bezeichnet. Dabei handelt es sich um eine Methode, bei der der Fluss ausgehender Informationen von einem Netzwerk in ein anderes überwacht und möglicherweise eingeschränkt wird.

Nachdem Sie die SNI-Daten erfasst haben, die die Network Firewall passieren, können Sie Amazon CloudWatch Logs und AWS Lambda verwenden, um die Daten in einem Amazon Simple Notification Service (Amazon SNS) -Thema zu veröffentlichen, das E-Mail-Benachrichtigungen generiert. Die E-Mail-Benachrichtigungen enthalten den Servernamen und andere relevante SNI-Informationen. Darüber hinaus können Sie die Ausgabe dieses Musters verwenden, um ausgehenden Datenverkehr anhand des Domainnamens im SNI mithilfe von Firewallregeln zuzulassen oder einzuschränken. Weitere Informationen finden Sie unter Arbeiten mit statusbehafteten Regelgruppen in der AWS-Netzwerk-Firewall in der Dokumentation zur Network Firewall.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- AWS-Befehlszeilenschnittstelle (AWS CLI) Version 2, installiert und konfiguriert unter Linux, macOS oder Windows.

- Network Firewall, eingerichtet und konfiguriert in Amazon VPC und wird zur Überprüfung des ausgehenden Datenverkehrs verwendet. Sie können die Network Firewall so konfigurieren, dass sie eine der folgenden VPC-Konfigurationen verwendet:
  - Einfache Einzelzonenarchitektur mit einem Internet-Gateway
  - Mehrzonenarchitektur mit einem Internet-Gateway
  - Architektur mit einem Internet-Gateway und einem NAT-Gateway

Architektur

Das folgende Diagramm zeigt, wie die Network Firewall verwendet wird, um SNI-Daten aus ausgehendem Netzwerkverkehr zu sammeln und diese Daten dann mithilfe von CloudWatch Logs und Lambda in einem SNS-Thema zu veröffentlichen.

Das Diagramm zeigt den folgenden Workflow:

1. Die Network Firewall erfasst Domainnamen aus den SNI-Daten im HTTPS-Header Ihres ausgehenden Netzwerkverkehrs.
2. CloudWatch Logs überwacht die SNI-Daten und ruft eine Lambda-Funktion auf, wenn der ausgehende Netzwerkverkehr die Network Firewall passiert.
3. Die Lambda-Funktion liest die von CloudWatch Logs erfassten SNI-Daten und veröffentlicht diese Daten dann in einem SNS-Thema.
4. Das SNS-Thema sendet Ihnen eine E-Mail-Benachrichtigung, die die SNI-Daten enthält.

Automatisierung und Skalierung

- Sie können AWS verwenden CloudFormation, um dieses Muster zu erstellen, indem Sie Infrastruktur als Code verwenden.

Technologie-Stack

- CloudWatch Amazon-Protokolle
- Amazon SNS
- Amazon VPC
- AWS Lambda

- AWS Network Firewall

Tools

AWS-Services

- Amazon CloudWatch Logs — Sie können Amazon CloudWatch Logs verwenden, um Ihre Protokolldateien von Amazon Elastic Compute Cloud (Amazon EC2) -Instances, AWS CloudTrail, Amazon Route 53 und anderen Quellen zu überwachen, zu speichern und darauf zuzugreifen.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) ist ein verwalteter Service, der die Nachrichtenzustellung von Verlagen an Abonnenten (auch bekannt als Produzenten und Verbraucher) ermöglicht.
- Amazon VPC — Amazon Virtual Private Cloud (Amazon VPC) stellt einen logisch isolierten Bereich der AWS-Cloud bereit, in dem Sie AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können. Dieses virtuelle Netzwerk entspricht weitgehend einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben, kann jedoch die Vorzüge der skalierbaren Infrastruktur von AWS nutzen.
- AWS Lambda — AWS Lambda ist ein Rechenservice, mit dem Sie Code ausführen können, ohne Server bereitzustellen oder zu verwalten.
- AWS-Netzwerk-Firewall — Die AWS-Netzwerk-Firewall ist ein verwalteter Service, mit dem Sie auf einfache Weise wichtige Netzwerkschutzmaßnahmen für Ihr gesamtes Amazon VPCs bereitstellen können.

Epen

Erstellen Sie eine CloudWatch Protokollgruppe für die Network Firewall

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine CloudWatch Protokollgruppe.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die CloudWatch -Konsole. 2. Wählen Sie im Navigationsbereich Protokollgruppen aus.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie Actions (Aktionen) und anschließend Create log group (Protokollgruppe erstellen) aus. 4. Geben Sie einen Namen für die Protokollgruppe ein. Wählen Sie anschließend Create log group (Protokollgruppe erstellen) aus. Weitere Informationen finden Sie in der CloudWatch Dokumentation unter Arbeiten mit Protokollgruppen und Protokollströmen.	

Erstellen Sie ein SNS-Thema und ein Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie ein SNS-Thema.	Um ein SNS-Thema zu erstellen, folgen Sie den Anweisungen in der Amazon SNS SNS-Dokumentation.	Cloud-Administrator
Abonnieren Sie einen Endpunkt für das SNS-Thema.	Um eine E-Mail-Adresse als Endpunkt für das von Ihnen erstellte SNS-Thema zu abonnieren, folgen Sie den Anweisungen in der Amazon SNS SNS-Dokumentation. Wählen Sie unter Protokoll die Option Email/Email-JSON aus.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Sie können auch einen anderen Endpunkt wählen, der Ihren Anforderungen entspricht.	

Logging in der Network Firewall einrichten

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Aktivieren Sie die Firewall-Protokollierung.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon VPC-Konsole. 2. Wählen Sie im Navigationsbereich unter NETWORK FIREWALL die Option Firewalls aus. 3. Wählen Sie im Abschnitt Firewalls die Firewall aus, für die Sie den Servernamen vom SNI für ausgehenden Datenverkehr erfassen möchten. 4. Wählen Sie die Registerkarte Firewall-Details und dann im Abschnitt Protokollierung die Option Bearbeiten aus. 5. Wählen Sie als Protokolltyp die Option Warnung	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	aus. Wählen Sie unter Protokollziel für Warnungen die Option CloudWatch Protokollgruppe aus. 6. Suchen Sie unter CloudWatch Protokoll gruppe nach der Protokoll gruppe, die Sie zuvor erstellt haben, wählen Sie sie aus, und klicken Sie dann auf Speichern. Weitere Informationen zur Verwendung von CloudWatc h Logs als Protokollziel für die Network Firewall finden Sie unter Amazon CloudWatch Logs in der Dokumentation zur Network Firewall.	

Richten Sie eine statusbehaftete Regel in der Network Firewall ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie eine Stateful-Regel.	1. Melden Sie sich bei der AWS-Managementkons ole an und öffnen Sie die Amazon VPC-Konsole. 2. Wählen Sie im Navigatio nsbereich unter Network Firewall die Option Netzwerkfirewall-R egelgruppen aus.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	3. Wählen Sie „Netzwerk-Firewall-Regelgruppe erstellen“. 4. Wählen Sie auf der Seite „Netzwerk-Firewall-Regelgruppe erstellen“ als Regelgruppentyp die Option Stateful-Regelgruppe aus. Hinweis: Weitere Informationen finden Sie unter Arbeiten mit statusbehafteten Regelgruppen in der AWS-Netzwerk-Firewall. 5. Geben Sie im Abschnitt Stateful-Regelgruppe einen Namen und eine Beschreibung für die Regelgruppe ein. 6. Geben Sie unter Kapazität die maximale Kapazität an, die Sie für die statusbehaftete Regelgruppe zulassen möchten (bis zum Maximum von 30.000). Hinweis: Sie können diese Einstellung nicht ändern, nachdem Sie die Regelgruppe erstellt haben. Informationen zur Berechnung der Kapazität finden Sie unter Einstellung der Regelgruppenkapazität in der AWS-Netzwerk-Firewall. Informationen zur	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Maximaleinstellung finden Sie unter AWS-Netzwerk-Firewall-Kontingente. 7. Wählen Sie für Stateful-Regelgruppenoptionen die Option 5-Tuple aus. 8. Wählen Sie im Abschnitt Reihenfolge der Stateful-Regeln die Option Standard aus. 9. Behalten Sie im Abschnitt Regelvariablen die Standardwerte bei. 10. Wählen Sie im Abschnitt Regel hinzufügen die Option TLS als Protokoll aus. Wählen Sie als Quelle die Option Beliebig aus. Wählen Sie für Quellport die Option Beliebiger Port aus. Wählen Sie als Ziel die Option Beliebig aus. Wählen Sie für Zielport die Option Beliebiger Port aus. Wählen Sie für Verkehrsrichtung die Option Forward aus. Wählen Sie für Aktion die Option Warnung aus. Wählen Sie Regel hinzufügen aus. 11. Wählen Sie Stateful-Regelgruppe erstellen aus.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Ordnen Sie die statusbehaftete Regel der Network Firewall zu.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon VPC-Konsole. 2. Wählen Sie im Navigationsbereich unter NETWORK FIREWALL die Option Firewalls aus. 3. Wählen Sie die Firewall aus, in der Sie den Servernamen vom SNI für ausgehenden Datenverkehr erfassen möchten. 4. Wählen Sie im Abschnitt Stateful-Regelgruppen die Option Aktionen und dann Unverwaltete statusbehaftete Regelgruppen hinzufügen aus. 5. Wählen Sie auf der Seite Nicht verwaltete statusbehaftete Regelgruppen hinzufügen die statusbehaftete Regelgruppe aus, die Sie zuvor erstellt haben, und klicken Sie dann auf Stateful-Regelgruppe hinzufügen.	Cloud-Administrator

Erstellen Sie eine Lambda-Funktion zum Lesen der Protokolle

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Erstellen Sie den Code für die Lambda-Funktion.	Fügen Sie in einer integrierten Entwicklungsumgebung (IDE), die das CloudWatch Logs-Ereignis von der Network Firewall für ausgehenden Datenverkehr lesen kann, den folgenden Python-3-Code ein und `<SNS-topic-ARN>` ersetzen Sie ihn durch Ihren Wert:
	`import json`
	`import gzip`
	`import base64`
	`import boto3`
	`sns_client = boto3.client('sns')`
	`def lambda_handler(event, context):`
	`  decoded_event = json.loads(gzip.decompress(base64.b64decode(event['awslogs']['data'])))`
	`  body = '''`
	`  {filtermatch}`
	`  '''.format(`
	`  loggroup=decoded_event['logGroup'],`
	`  logstream=decoded_event['logStream'],`
	`  filtermatch=decoded_event['logEvents'][0]['message'],`
	`  )`
		App-Developer

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	print(body)
	filterMatch = json.loads(body)
	data = []
	if 'http' in filterMatch['event']:
	data.append(filterMatch['event']['http']['hostname'])
	elif 'tls' in filterMatch['event']:
	data.append(filterMatch['event']['tls']['sni'])
	result = 'Domain accessed ' + 1*' ' + (data[0]) + 1*' ' 'via AWS Network Firewall ' + 1*' ' + (filterMatch['firewall_name'])
	print(result)
	message = {'ServerName': result}
	send_to_sns = sns_client.publish(
	TargetArn=<SNS-topic-ARN>,
	#Replace with the SNS topic ARN
	Message=json.dumps({'default': json.dumps(message),
	
	'sms': json.dumps(message),
	
	'email': json.dumps(message)}),
	Subject='Server Name passed through the Network Firewall',	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	`MessageStructure='json'`
	`)`
	
	In diesem Codebeispiel wird der Inhalt der CloudWatch Protokolle analysiert und der vom SNI im HTTPS-Header angegebene Servername erfasst.	

So erstellen Sie die Lambda-Funktion:	Um die Lambda-Funktion zu erstellen, folgen Sie den Anweisungen in der Lambda-Dokumentation und wählen Sie Python 3.9 für Runtime.	Cloud-Administrator
Fügen Sie den Code zur Lambda-Funktion hinzu.	Folgen Sie den Anweisungen in der Lambda-Dokumentation, um Ihren Python-Code zu der zuvor erstellten Lambda-Funktion hinzuzufügen.	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie CloudWatch Logs als Trigger zur Lambda-Funktion hinzu.	1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Lambda-Konsole. 2. Wählen Sie im Navigationsbereich Funktionen und dann die Funktion aus, die Sie zuvor erstellt haben. 3. Wählen Sie im Abschnitt Funktionsübersicht die Option Auslöser hinzufügen aus. 4. Wählen Sie auf der Seite Trigger hinzufügen im Abschnitt Trigger-Konfiguration die Option CloudWatch Logs und dann Add aus. 5. Wählen Sie unter Protokollgruppe die CloudWatch Protokollgruppe aus, die Sie zuvor erstellt haben. 6. Geben Sie unter Filtername einen Namen für Ihren Filter ein. 7. Wählen Sie Hinzufügen aus. 8. Wählen Sie auf der Seite Ihrer Funktion auf der Registerkarte Konfiguration im Abschnitt Trigger den Trigger aus, den Sie gerade hinzugefügt haben, und	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	wählen Sie dann Aktivieren aus. Weitere Informationen finden Sie unter Using Lambda with CloudWatch Logs in der Lambda-Dokumentation.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Fügen Sie SNS-Veröffentlichungsberechtigungen hinzu.	Fügen Sie der Lambda-Ausführungsrolle die Berechtigung sns:publish hinzu, sodass Lambda API-Aufrufe zum Veröffentlichen von Nachrichten in SNS tätigen kann. 1. Suchen Sie die Ausführungsrolle der Lambda-Funktion, die Sie zuvor erstellt haben. 2. Fügen Sie Ihrer AWS Identity and Access Management (IAM) -Rolle die folgende Richtlinie hinzu: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "AllowSNSPublish", "Effect": "Allow", "Action": [ "sns:GetTopicAttributes", "sns:Subscribe", "sns:Unsubscribe", "sns:Publish" ],`	Cloud-Administrator

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	<pre>"Resource": "*"
	}
	]
	}</pre>	

Testen Sie die Funktionalität Ihrer SNS-Benachrichtigung

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

Senden Sie den Datenverkehr über die Network Firewall.	1. Senden oder warten Sie, bis der HTTPS-Verkehr die Network Firewall passiert.
	2. Überprüfen Sie die SNS-Benachrichtigungs-E-Mail, die Sie von AWS erhalten, wenn der Datenverkehr die Network Firewall passiert. Die E-Mail enthält die SNI-Details für ausgehenden Datenverkehr. Die aus dem obigen Lambda-Code generierte E-Mail hat beispielsweise den folgenden Inhalt, wenn der aufgerufene Domainname https://aws.amazon.comund das Abonnementprotokoll EMAIL-JSON lautet:
	<pre>{
	"Type": "Notification",</pre>
		Testingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"MessageId": "<messageID>", "TopicArn": "arn:aws:sns:us-west-2:123456789:testSNSTopic", "Subject": "Server Name passed through the Network Firewall", "Message": "{\"ServerName\": \"Domain 'aws.amazon.com' accessed via AWS Network Firewall 'AWS-Network-Firewall-Multi-AZ-firewall\"}", "Timestamp": "2022-03-22T04:10:04.217Z", "SignatureVersion": "1", "Signature": "<Signature>", "SigningCertURL": "<SigningCertUrl>", "UnsubscribeURL": "<UnsubscribeURL>" } Überprüfen Sie dann das Warnprotokoll der Network Firewall bei Amazon, CloudWatch indem Sie den Anweisungen in der CloudWatch Amazon-Dokumentation folgen. Das Warnungsprotokoll zeigt die folgende Ausgabe:	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten

	{
	"firewall_name": "AWS-Network-Firewall-Multi-AZ-firewall",
	"availability_zone": "us-east-2b",
	"event_timestamp": "<event timestamp>",
	"event": {
	"timestamp": "2021-03-22T04:10:04.214222+0000",
	"flow_id": <flow ID>,
	"event_type": "alert",
	"src_ip": "10.1.3.76",
	"src_port": 22761,
	"dest_ip": "99.86.59.73",
	"dest_port": 443,
	"proto": "TCP",
	"alert": {
	"action": "allowed",
	"signature_id": 2,
	"rev": 0,
	"signature": "",
	"category": "",
	"severity": 3
	},
	"tls": {	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	"subject": "CN=aws.amazon.com", "issuerdn": "C=US, O=Amazon, OU=Server CA 1B, CN=Amazon", "serial": "<serial number>", "fingerprint": "<fingerprint ID>", "sni": "aws.amazon.com", "version": "TLS 1.2", "notbefore": "2020-09-30T00:00:00", "notafter": "2021-09-23T12:00:00", "ja3": {}, "ja3s": {} }, "app_proto": "tls" } }	

Verwenden Sie Terraform, um Amazon automatisch GuardDuty für eine Organisation zu aktivieren

Erstellt von Aarthi Kannan (AWS)

Übersicht

Amazon überwacht GuardDuty kontinuierlich Ihre Amazon Web Services (AWS) -Konten und verwendet Bedrohungsinformationen, um unerwartete und potenziell schädliche Aktivitäten in Ihrer AWS-Umgebung zu identifizieren. Die manuelle Aktivierung GuardDuty für mehrere Konten oder Organisationen, in mehreren AWS-Regionen oder über die AWS-Managementkonsole kann umständlich sein. Sie können den Prozess automatisieren, indem Sie ein IaC-Tool (Infrastructure as Code) wie Terraform verwenden, das Dienste und Ressourcen für mehrere Konten und Regionen in der Cloud bereitstellen und verwalten kann.

AWS empfiehlt die Verwendung von AWS Organizations zum Einrichten und Verwalten mehrerer Konten in GuardDuty. Dieses Muster entspricht dieser Empfehlung. Ein Vorteil dieses Ansatzes besteht darin, dass, wenn neue Konten erstellt oder der Organisation hinzugefügt GuardDuty werden, diese Konten für alle unterstützten Regionen automatisch aktiviert werden, ohne dass manuelles Eingreifen erforderlich ist.

Dieses Muster zeigt, wie HashiCorp Terraform verwendet wird, um Amazon GuardDuty für drei oder mehr Amazon Web Services (AWS) -Konten in einer Organisation zu aktivieren. Der mit diesem Muster bereitgestellte Beispielcode bewirkt Folgendes:

- Aktiviert GuardDuty für alle AWS-Konten, die aktuelle Mitglieder der Zielorganisation in AWS Organizations sind
- Aktiviert die Funktion Automatische Aktivierung in GuardDuty, mit der alle Konten, die der Zielorganisation in future hinzugefügt werden, automatisch aktiviert GuardDuty werden
- Ermöglicht die Auswahl der Regionen, in denen Sie sie aktivieren möchten GuardDuty
- Verwendet das Sicherheitskonto der Organisation als GuardDuty delegierter Administrator
- Erstellt einen Amazon Simple Storage Service (Amazon S3) -Bucket im Logging-Konto und konfiguriert ihn so GuardDuty , dass die aggregierten Ergebnisse aller Konten in diesem Bucket veröffentlicht werden
- Weist eine Lebenszyklusrichtlinie zu, die Ergebnisse standardmäßig nach 365 Tagen aus dem S3-Bucket in den Amazon S3 Glacier Flexible Retrieval Storage überträgt

Sie können diesen Beispielcode manuell ausführen oder ihn in Ihre CI/CD-Pipeline (Continuous Integration and Continuous Delivery) integrieren.

Zielpublikum

Dieses Muster wird Benutzern empfohlen, die Erfahrung mit Terraform GuardDuty, Python und AWS Organizations haben.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine Organisation ist in AWS Organizations eingerichtet und umfasst mindestens die folgenden drei Konten:
  - Ein Verwaltungskonto — Dies ist das Konto, von dem aus Sie den Terraform-Code bereitstellen, entweder eigenständig oder als Teil der CI/CD-Pipeline. Der Terraform-Status wird ebenfalls in diesem Konto gespeichert.
  - Ein Sicherheitskonto — Dieses Konto wird als GuardDuty delegierter Administrator verwendet. Weitere Informationen finden Sie unter Wichtige Überlegungen für GuardDuty delegierte Administratoren (GuardDuty Dokumentation).
  - Ein Logging-Konto — Dieses Konto enthält den S3-Bucket, in dem die aggregierten Ergebnisse aller Mitgliedskonten GuardDuty veröffentlicht werden.

  Weitere Informationen zum Einrichten der Organisation mit der erforderlichen Konfiguration finden Sie unter Erstellen einer Kontostruktur (AWS Well-Architected Labs).
- Ein Amazon S3 S3-Bucket und eine Amazon DynamoDB-Tabelle, die als Remote-Backend dienen, um den Status von Terraform im Verwaltungskonto zu speichern. Weitere Informationen zur Verwendung von Remote-Backends für den Terraform-Status finden Sie unter S3-Backends (Terraform-Dokumentation). Ein Codebeispiel, das die Remote-State-Verwaltung mit einem S3-Backend einrichtet, finden Sie unter 3-backend (Terraform Registry). remote-state-s Beachten Sie die folgenden Voraussetzungen:
  - Der S3-Bucket und die DynamoDB-Tabelle müssen sich in derselben Region befinden.
  - Beim Erstellen der DynamoDB-Tabelle muss der Partitionsschlüssel **`LockID`** (Groß- und Kleinschreibung beachten) und der Partitionsschlüsseltyp muss String sein. Für alle anderen Tabelleneinstellungen müssen die Standardwerte verwendet werden. Weitere Informationen finden Sie unter Über Primärschlüssel und Erstellen einer Tabelle (DynamoDB-Dokumentation).

- Ein S3-Bucket, der zum Speichern von Zugriffsprotokollen für den S3-Bucket verwendet GuardDuty wird, in dem die Ergebnisse veröffentlicht werden. Weitere Informationen finden Sie unter Aktivieren der Amazon S3 S3-Serverzugriffsprotokollierung (Amazon S3-Dokumentation). Wenn Sie die Bereitstellung in einer AWS Control Tower Tower-Landezone durchführen, können Sie den S3-Bucket im Protokollarchiv-Konto für diesen Zweck wiederverwenden.
- Terraform Version 0.14.6 oder höher ist installiert und konfiguriert. Weitere Informationen finden Sie unter Erste Schritte — AWS (Terraform-Dokumentation).
- Python-Version 3.9.6 oder höher ist installiert und konfiguriert. Weitere Informationen finden Sie unter Quellversionen (Python-Website).
- Das AWS-SDK für Python (Boto3) ist installiert. Weitere Informationen finden Sie unter Installation (Boto3-Dokumentation).
- jq ist installiert und konfiguriert. Weitere Informationen finden Sie unter jq herunterladen (jq-Dokumentation).

Einschränkungen

- Dieses Muster unterstützt die Betriebssysteme macOS und Amazon Linux 2. Dieses Muster wurde nicht für die Verwendung in Windows-Betriebssystemen getestet.

> **Note**
>
> Amazon Linux 2 nähert sich dem Ende des Supports. Weitere Informationen finden Sie unter Amazon Linux FAQs 2.

- GuardDuty darf in keinem der Konten oder in einer der Zielregionen bereits aktiviert sein.
- Die IaC-Lösung in diesem Muster stellt die Voraussetzungen nicht bereit.
- Dieses Muster wurde für eine AWS-Landezone entwickelt, die den folgenden bewährten Methoden entspricht:
  - Die landing zone wurde mithilfe von AWS Control Tower erstellt.
  - Separate AWS-Konten werden für Sicherheit und Protokollierung verwendet.

Produktversionen

- Terraform-Version 0.14.6 oder höher. Der Beispielcode wurde für Version 1.2.8 getestet.
- Python-Version 3.9.6 oder höher.

Architektur

Dieser Abschnitt gibt einen allgemeinen Überblick über diese Lösung und die Architektur, die durch den Beispielcode festgelegt wurde. Das folgende Diagramm zeigt die Ressourcen, die über die verschiedenen Konten in der Organisation innerhalb einer einzigen AWS-Region bereitgestellt werden.

1. Terraform erstellt die Rolle GuardDutyTerraformOrgRoleAWS Identity and Access Management (IAM) im Sicherheitskonto und im Protokollierungskonto.
2. Terraform erstellt einen S3-Bucket in der AWS-Standardregion im Logging-Konto. Dieser Bucket wird als Veröffentlichungsziel verwendet, um alle GuardDuty Ergebnisse in allen Regionen und aus allen Konten in der Organisation zu aggregieren. Terraform erstellt außerdem einen AWS Key Management Service (AWS KMS) -Schlüssel im Sicherheitskonto, der zur Verschlüsselung der Ergebnisse im S3-Bucket verwendet wird, und konfiguriert die automatische Archivierung von Ergebnissen aus dem S3-Bucket im S3 Glacier Flexible Retrieval Storage.
3. Vom Verwaltungskonto aus benennt Terraform das Sicherheitskonto als delegierten Administrator für. GuardDuty Das bedeutet, dass das Sicherheitskonto nun den GuardDuty Dienst für alle Mitgliedskonten verwaltet, einschließlich des Verwaltungskontos. Einzelne Mitgliedskonten können nicht eigenständig gesperrt oder deaktiviert GuardDuty werden.
4. Terraform erstellt den GuardDuty Detektor im Sicherheitskonto für den GuardDuty delegierten Administrator.
5. Falls es noch nicht aktiviert ist, aktiviert Terraform den S3-Schutz in. GuardDuty Weitere Informationen finden Sie unter Amazon S3 S3-Schutz in Amazon GuardDuty (GuardDuty Dokumentation).
6. Terraform registriert alle aktuellen, aktiven Mitgliedskonten in der Organisation als Mitglieder. GuardDuty
7. Terraform konfiguriert den GuardDuty delegierten Administrator so, dass er die aggregierten Ergebnisse aller Mitgliedskonten im S3-Bucket im Logging-Konto veröffentlicht.
8. Terraform wiederholt die Schritte 3 bis 7 für jede AWS-Region, die Sie auswählen.

Automatisierung und Skalierung

Der bereitgestellte Beispielcode ist modularisiert, sodass Sie ihn für eine automatisierte Bereitstellung in Ihre CI/CD-Pipeline integrieren können.

Tools

AWS-Services

- Amazon DynamoDB ist ein vollständig verwalteter NoSQL-Datenbank-Service, der schnelle und planbare Leistung mit nahtloser Skalierbarkeit bereitstellt.
- Amazon GuardDuty ist ein Dienst zur kontinuierlichen Sicherheitsüberwachung, der Protokolle analysiert und verarbeitet, um unerwartete und potenziell nicht autorisierte Aktivitäten in Ihrer AWS-Umgebung zu identifizieren.
- AWS Identity and Access Management (IAM) hilft Ihnen dabei, den Zugriff auf Ihre AWS-Ressourcen sicher zu verwalten, indem kontrolliert wird, wer authentifiziert und autorisiert ist, diese zu verwenden.
- AWS Key Management Service (AWS KMS) unterstützt Sie bei der Erstellung und Kontrolle kryptografischer Schlüssel zum Schutz Ihrer Daten.
- AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer Organisation konsolidieren können, die Sie erstellen und zentral verwalten.
- Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.
- Das AWS-SDK für Python (Boto3) ist ein Software-Entwicklungskit, mit dem Sie Ihre Python-Anwendung, -Bibliothek oder Ihr Skript in AWS-Services integrieren können.

Andere Tools und Dienste

- HashiCorp Terraform ist eine Befehlszeilenschnittstellenanwendung, mit der Sie mithilfe von Code Cloud-Infrastruktur und -Ressourcen bereitstellen und verwalten können.
- Python ist eine Allzweck-Programmiersprache.
- jq ist ein Befehlszeilenprozessor, der Sie bei der Arbeit mit JSON-Dateien unterstützt.

Code-Repository

Der Code für dieses Muster ist im amazon-guardduty-for-awsorganizations-with-terraform-Repository verfügbar. GitHub

Epen

GuardDuty In der Organisation aktivieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Klonen Sie das Repository	Führen Sie in einer Bash-Shell den folgenden Befehl aus. Unter Das Repository klonen im Abschnitt Zusätzliche Informationen können Sie den vollständigen Befehl kopieren, der die URL des GitHub Repositorys enthält. Dadurch wird das organizations-with-terraform Repository von amazon-guardduty-for-aws- von GitHub geklont. `git clone <github-repository-url>`	DevOps Ingenieur
Bearbeiten Sie die Terraform-Konfigurationsdatei.	1. Replizieren `root` Sie im Ordner des geklonten Repositorys die Datei configuration.json.sample, indem Sie den folgenden Befehl ausführen. `cp configuration.json.sample configuration.json` 2. Bearbeiten Sie die neue Datei configuration.json und definieren Sie die Werte für jede der folgenden Variablen:	DevOps Ingenieur, General AWS, Terraform, Python

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• `managemen t_acc_id` — Konto-ID des Verwaltungskontos. • `delegated_admin_ac c_id` — Konto-ID des Sicherheitskontos. • `logging_acc_id` — Konto-ID des Logging-K ontos. • `target_regions` — Durch Kommas getrennte Liste der AWS-Regio nen, die Sie aktivieren möchten. GuardDuty • `organization_id` — AWS-Organisations- ID der Organisation, in der Sie die Aktivierung durchführen GuardDuty. • `default_region` — Die Region, in der Ihr Terraform-Status im Verwaltungskonto gespeichert ist. Dies ist dieselbe Region, in der Sie den S3-Bucket und die DynamoDB-Tabelle für das Terraform -Backend bereitgestellt haben. • `role_to_assume_for _role_creation` — Name, den Sie einer	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	neuen IAM-Rolle in den Sicherheits- und Protokollierungskonten zuweisen möchten. Sie erstellen diese neue Rolle in der nächsten Geschichte. Terraform übernimmt diese Rolle, um die `GuardDutyTerraformOrgRole` IAM-Rolle in den Sicherheits- und Protokollierungskonten zu erstellen. • `finding_publishing_frequency` — Häufigkeit, mit der Ergebnisse im GuardDuty S3-Bucket veröffentlicht werden. • `guardduty_findings_bucket_region` — Bevorzugte Region, in der Sie den S3-Bucket für veröffentlichte Ergebnisse erstellen möchten. • `logging_acc_s3_bucket_name` — Bevorzugter Name für den S3-Bucket für veröffentlichte Ergebnisse. • `security_acc_kms_key_alias` — AWS-KMS-Alias für den Schlüssel, der zur	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Verschlüsselung der GuardDuty Ergebnisse verwendet wird. • `s3_access_log_bucket_name` — Name eines bereits vorhandenen S3-Buckets, in dem Sie Zugriffsprotokolle für den S3-Bucket sammeln möchten, der für die Ergebnisse verwendet wurde. GuardDuty Dieser Bucket sollte sich in derselben AWS-Region wie der GuardDuty Ergebnis-Bucket befinden. • `tfm_state_backend_s3_bucket` — Name des bereits vorhandenen S3-Buckets, in dem der Terraform-Remote-Backend-Status gespeichert werden soll. • `tfm_state_backend_dynamodb_table` — Name der bereits vorhandenen DynamoDB-Tabelle zum Sperren des Terraform-Status. 3. Speichern und schließen Sie die -Konfigurationsdatei.	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Generieren Sie CloudFormation Vorlagen für neue IAM-Rollen.	Dieses Muster beinhaltet eine IaC-Lösung zum Erstellen von zwei CloudFormation Vorlagen. Diese Vorlagen erstellen zwei IAM-Rollen, die Terraform während des Einrichtungsvorgangs verwendet. Diese Vorlagen entsprechen den bewährten Sicherheitsverfahren für Berechtigungen mit den geringsten Rechten. 1. Navigieren Sie in einer Bash-Shell im `root` Repository-Ordner zu. `cfn-templates/` Dieser Ordner enthält CloudFormation Vorlagendateien mit Stubs. 2. Führen Sie den folgenden Befehl aus. Dadurch werden die Stubs durch die Werte ersetzt, die Sie in der Datei configuration.json angegeben haben. `bash scripts/replace_config_stubs.sh` 3. Vergewissern Sie sich, dass die folgenden CloudFormation Vorlagen in dem	DevOps Ingenieur, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Ordner erstellt wurden: `cfn-templates/` • management-account-role.yaml — Diese Datei enthält die Rollendef inition und die zugehörig en Berechtigungen für die IAM-Rolle im Verwaltun gskonto, das über die Mindestberechtigungen verfügt, die zum Vervollst ändigen dieses Musters erforderlich sind. • role-to-assume-for-role-creation.yaml — Diese Datei enthält die Rollendefinition und die zugehörigen Berechtig ungen für die IAM-Rolle in den Sicherheits- und Protokollierungskonten. Terraform übernimmt diese Rolle, um die Rolle in diesen Konten zu erstellen. GuardDuty TerraformOrgRole	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Erstellen Sie die IAM-Rollen.	Folgen Sie den Anweisungen unter Einen Stack erstellen (CloudFormation Dokumentation) und gehen Sie wie folgt vor: 1. Stellen Sie den Stack role-to-assume-for-role-creation.yaml sowohl im Sicherheits- als auch im Logging-Konto bereit. 2. Stellen Sie den management-account-role.yaml-Stack im Verwaltungskonto bereit. Wenn Sie den Stack erfolgreich erstellt haben und den `CREATE_COMPLETE` Stack-Status in der Ausgabe sehen, notieren Sie sich den Amazon-Ressourcennamen (ARN) dieser neuen Rolle.	DevOps Ingenieur, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Nehmen Sie die IAM-Rolle im Verwaltungskonto an.	Aus Sicherheitsgründen empfehlen wir, dass Sie die neue management-account-roleIAM-Rolle übernehmen, bevor Sie fortfahren. Geben Sie in der AWS-Befehlszeilenschnittstelle Command Line Interface (AWS CLI) den Befehl unter Übernehmen Sie die IAM-Rolle des Verwaltungskontos im Abschnitt Zusätzliche Informationen ein.	DevOps Ingenieur, General AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das Setup-Skript aus.	Führen Sie im `root` Repository-Ordner den folgenden Befehl aus, um das Setup-Skript zu starten. `bash scripts/full-setup.sh` Das Skript full-setup.sh führt die folgenden Aktionen aus: • Exportiert alle Konfigurationswerte als Umgebungsvariablen • Generiert die Codedateien backend.tf und terraform.tfvars für jedes Terraform-Modul • Ermöglicht vertrauenswürdigen Zugriff innerhalb GuardDuty der Organisation über die AWS-CLI. • Importiert den Organisationsstatus in den Terraform-Status • Erstellt den S3-Bucket für die Veröffentlichung von Ergebnissen im Logging-Konto • Erstellt den AWS-KMS-Schlüssel für die Verschlüsselung von Ergebnissen im Sicherheitskonto	DevOps Ingenieur, Python

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	• Wird GuardDuty unternehmensweit in allen ausgewählten Regionen aktiviert, wie im Abschnitt Architektur beschrieben	

(Optional) GuardDuty In der Organisation deaktivieren

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Führen Sie das Bereinigungsskript aus.	Wenn Sie dieses Muster zur Aktivierung GuardDuty für die Organisation verwendet haben und deaktivieren möchten GuardDuty, führen Sie im `root` Repository-Ordner den folgenden Befehl aus, um das Skript cleanup-gd.sh zu starten. `bash scripts/cleanup-gd.sh` Dieses Skript wird GuardDuty in der Zielorganisation deaktiviert, entfernt alle bereitgestellten Ressourcen und setzt die Organisation auf ihren vorherigen Status zurück, bevor Terraform zur Aktivierung verwendet wird. GuardDuty	DevOps Ingenieur, General AWS, Terraform, Python

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Note Dieses Skript entfernt weder die Terraform-Statusdateien noch die Sperrdateien aus den lokalen und Remote-Backends. Wenn Sie dies tun müssen, müssen Sie diese Aktionen manuell ausführen. Außerdem löscht dieses Skript weder die importier te Organisation noch die von ihr verwalteten Konten. Der vertrauen swürdige Zugriff für GuardDuty ist im Rahmen des Bereinigu ngsskripts nicht deaktiviert.	
Entfernen Sie IAM-Rollen.	Löschen Sie die Stacks, die mit den Vorlagen role-to-a ssume-for-role-creation.yam l und .yaml erstellt wurden. management-account-role CloudFormation Weitere Informationen finden Sie unter Löschen eines Stacks (Dokumentation). CloudForm ation	DevOps Ingenieur, General AWS

Zugehörige Ressourcen

AWS-Dokumentation

- Verwaltung mehrerer Konten (GuardDuty Dokumentation)
- Gewährung der geringsten Rechte (IAM-Dokumentation)

AWS-Marketing

- Amazon GuardDuty
- AWS Organizations

Sonstige Ressourcen

- Terraform
- Terraform CLI-Dokumentation

Zusätzliche Informationen

Klonen Sie das Repository

Führen Sie den folgenden Befehl aus, um das GitHub Repository zu klonen.

```
git clone https://github.com/aws-samples/amazon-guardduty-for-aws-organizations-with-terraform
```

Nehmen Sie die IAM-Rolle des Verwaltungskontos an

Führen Sie den folgenden Befehl aus, um die IAM-Rolle im Verwaltungskonto anzunehmen. `<IAM role ARN>`Ersetzen Sie es durch den ARN der IAM-Rolle.

```
export ROLE_CREDENTIALS=$(aws sts assume-role --role-arn <IAM role ARN> --role-session-name AWSCLI-Session --output json)
export AWS_ACCESS_KEY_ID=$(echo $ROLE_CREDENTIALS | jq .Credentials.AccessKeyId | sed 's/"//g')
export AWS_SECRET_ACCESS_KEY=$(echo $ROLE_CREDENTIALS | jq .Credentials.SecretAccessKey | sed 's/"//g')
```

```
export AWS_SESSION_TOKEN=$(echo $ROLE_CREDENTIALS | jq .Credentials.SessionToken | sed
 's/"//g')
```

Überprüfen Sie betriebliche Best Practices für PCI DSS 4.0 mithilfe von AWS Config

Erstellt von Tala Qraitem (AWS) und Alex Goff (AWS)

Übersicht

Der Payment Card Industry Data Security Standard (PCI DSS) beschreibt wichtige technische und betriebliche Protokolle zum Schutz von Zahlungsdaten. PCI DSS wurde entwickelt, um die Datensicherheit für Zahlungskartenkonten zu fördern und zu verbessern. Es erleichtert auch die weltweite Einführung einheitlicher Sicherheitsmaßnahmen. Obwohl es speziell für Umgebungen mit Zahlungskartenkontodaten entwickelt wurde, können Sie PCI DSS verwenden, um sich vor Bedrohungen zu schützen und andere Elemente im Zahlungsökosystem zu schützen.

PCI DSS Version 4.0 wurde veröffentlicht, um den sich wandelnden Anforderungen gerecht zu werden, Klarstellungen oder zusätzliche Hinweise zu geben und die Struktur und das Format des Standards zu verbessern. Weitere Informationen zu den Änderungen finden Sie unter Zusammenfassung der Änderungen von PCI DSS Version 3.2.1 auf 4.0.

Bei einem AWS Config Konformitätspaket handelt es sich um eine Sammlung von AWS Config Regeln und Abhilfemaßnahmen, die Sie bei der Durchführung von Governance-Prüfungen in Bezug auf Sicherheit, Betrieb oder Kostenoptimierung unterstützen. Sie können ein Conformance Pack als einzelne Einheit in einem AWS-Konto und AWS-Region oder unternehmensweit in einer Organisation bereitstellen. AWS Organizations

Die Conformance Packs für PCI DSS Version 4.0 ergänzen das Conformance Pack für Version 3.2.1 und bauen darauf auf. Die Regeln im Conformance Pack entsprechen den Regeln im Standard. Weitere Informationen finden Sie in der Zuordnung im Abschnitt Anlagen. Sie können zwischen zwei Versionen dieses Conformance Packs wählen: eine, die globale Ressourcentypen enthält, und eine, die sie ausschließt.

> **Important**
>
> Conformance Packs sind nicht darauf ausgelegt, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob die Nutzung den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Habe ein aktives AWS-Konto.
- Richten Sie ein AWS Config.
- Erfüllen Sie die Voraussetzungen für Konformitätspakete.
- Stellen Sie das PCI DSS-Konformitätspaket Version 3.2.1 bereit.
- Verfügen Sie über Berechtigungen für den Zugriff auf AWS Config und die Verwaltung von Conformance Packs. Ein Beispiel für eine Richtlinie finden Sie im Abschnitt Zusätzliche Informationen dieses Musters.

Einschränkungen

- In Ihrem AWS-Konto Fall gelten Standardkontingente, die früher als Limits bezeichnet wurden AWS-Service. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Sie können für einige Kontingente eine Erhöhung beantragen, aber nicht alle Kontingente können erhöht werden. Stellen Sie sicher, dass Sie mit den AWS Config Servicebeschränkungen vertraut sind, einschließlich der Grenzwerte für Conformance Packs für einzelne Konten und Conformance Packs für Organisationen.
- Die Version dieses Conformance Packs, die globale Ressourcentypen enthält, ist nur für die Bereitstellung in der Region vorgesehen. `us-east-1`
- Die Version dieses Conformance Packs, die globale Ressourcentypen ausschließt, ist nur für die Bereitstellung in den folgenden Regionen vorgesehen:
  - `ap-east-1`
  - `ap-south-1`
  - `ap-northeast-2`
  - `ap-southeast-1`
  - `ap-southeast-2`
  - `ap-northeast-1`
  - `ca-central-1`
  - `eu-central-1`
  - `eu-west-1`
  - `eu-west-2`

- `eu-west-3`
- `eu-north-1`
- `sa-east-1`
- `us-east-2`
- `us-west-1`
- `us-west-2`

Tools

AWS-Services

- AWS Configbietet einen detaillierten Überblick über die Ressourcen in Ihrem System AWS-Konto und deren Konfiguration. Es hilft Ihnen zu erkennen, wie Ressourcen miteinander zusammenhängen und wie sich ihre Konfigurationen im Laufe der Zeit geändert haben.
- AWS Systems Managerhilft Ihnen bei der Verwaltung Ihrer Anwendungen und Infrastruktur, die in der ausgeführt AWS Cloud werden. Es vereinfacht das Anwendungs- und Ressourcenmanagement, verkürzt die Zeit für die Erkennung und Lösung betrieblicher Probleme und hilft Ihnen, Ihre AWS Ressourcen sicher und in großem Umfang zu verwalten.

Code-Repository

Die Conformance Packs befinden sich im AWS Config Conformance GitHub Packs-Repository. Dieses Repository enthält die folgenden Vorlagen für PCI DSS Version 4.0:

- Bewährte Methoden für den Betrieb von PCI-DSS-v4.0- .yaml including-global-resourcetypes
- Bewährte Methoden für den Betrieb von PCI-DSS-v4.0- .yaml excluding-global-resourcetypes

Epen

Stellen Sie das Conformance Pack bereit und verwalten Sie es

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Laden Sie das Konformit ätspaket herunter.	Wenn Sie das Conforman ce Pack in der `us-east-1`	DevOps Ingenieur

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Region bereitstellen, laden Sie die Vorlage Operational-Best-Practices-for-PCI-DSS-v4.0 - .yaml herunter. including -global-resourcetypes Wenn Sie das Conformance Pack in einer anderen Region bereitstellen, laden Sie die Vorlage Operational-Best-Practices-for-PCI-DSS-v4.0- .yaml herunter. excluding -global-resourcetypes	
(Optional) Ändern Sie das Conformance Pack.	Sie können die Vorlage für das Conformance Pack an die individuellen Bedürfnisse Ihrer Organisation anpassen. Sie können beispielsweise benutzerdefinierte Behebungsmaßnahmen erstellen. Weitere Informationen zum Erstellen und Ändern von Vorlagen finden Sie in der Dokumentation unter Vorlagen für benutzerdefinierte Konformitätspakete erstellen. AWS Config	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Stellen Sie das Conformance Pack bereit.	Wenn Sie die Bereitstellung in einem Ziel AWS-Konto oder durchführen AWS-Region, folgen Sie den Anweisungen unter Bereitstellen von Konformitätspaketen in der AWS Config Dokumentation. Sie können das AWS Management Console oder das AWS Command Line Interface (AWS CLI) verwenden. Wenn Sie das Conformance Pack unternehmensweit in bereitstellen AWS Organizations, folgen Sie den Anweisungen in der Dokumentation unter Bereitstellen des AWS Config Conformance Packs mithilfe von Quick Setup. AWS Systems Manager	Allgemeines AWS
(Optional) Bearbeiten Sie das Conformance Pack.	Wenn Sie das Conformance Pack bearbeiten möchten, folgen Sie den Anweisungen unter Conformance Packs bearbeiten in der Dokumentation. AWS Config Sie können das AWS Management Console oder das verwenden. AWS CLI	Allgemeines AWS

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
(Optional) Löschen Sie das Conformance Pack.	Wenn Sie das Conformance Pack löschen möchten, folgen Sie den Anweisungen unter Löschen von Conformance Packs in der Dokumentation. AWS Config Sie können das AWS Management Console oder das verwenden. AWS CLI	Allgemeines AWS

Zugehörige Ressourcen

AWS Ressourcen

- Konformitätspakete für AWS Config (AWS Config Dokumentation)
- Bereitstellen AWS Config des Conformance Packs mithilfe von Quick Setup (Systems Manager Manager-Dokumentation)
- PCI-DSS-Konformität auf AWS(Website)AWS
- PCI DSS Version 4.0 aktiviert AWS(Leitfaden zur Einhaltung der Vorschriften)

PCI DSS-Ressourcen

- PCI DSS-Ressourcen-Hub, Version 4.0
- Dokumentenbibliothek des PCI Security Standards Council
- Zusammenfassung der Änderungen von PCI DSS Version 3.2.1 auf 4.0

Zusätzliche Informationen

Im Folgenden finden Sie ein Beispiel für eine Richtlinie AWS Identity and Access Management (IAM), die es dem Benutzer ermöglicht, auf Conformance Packs zuzugreifen AWS Config und diese zu verwalten:

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "config:PutConfigRule",
                "config:PutConformancePack",
                "config:DeleteConfigRule",
                "config:DeleteRemediationConfiguration",
                "config:DeleteConformancePack",
                "config:PutRemediationConfigurations",
                "config:BatchGetAggregateResourceConfig",
                "config:BatchGetResourceConfig",
                "config:Get*",
                "config:Describe*",
                "config:Deliver*",
                "config:List*",
                "config:Select*"
            ],
            "Resource": "*"
        }
    ]
}
```

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Stellen Sie sicher, dass für neue Amazon Redshift Redshift-Cluster SSL-Endpunkte erforderlich sind

Erstellt von Priyanka Chaudhary (AWS)

Übersicht

Dieses Muster stellt eine Amazon Web Services (AWS) CloudFormation -Vorlage bereit, die Sie automatisch benachrichtigt, wenn ein neuer Amazon Redshift Redshift-Cluster ohne Secure Sockets Layer (SSL) -Endpunkte gestartet wird.

Amazon Redshift ist ein vollständig verwalteter, cloudbasierter Data-Warehouse-Service im Petabyte-Bereich. Er ist für die Speicherung und Analyse großer Datenmengen konzipiert. Es wird auch zur Durchführung umfangreicher Datenbankmigrationen verwendet. Aus Sicherheitsgründen unterstützt Amazon Redshift SSL zur Verschlüsselung der Verbindung zwischen der SQL Server-Client-Anwendung des Benutzers und dem Amazon Redshift Redshift-Cluster. Um Ihren Cluster so zu konfigurieren, dass er eine SSL-Verbindung erfordert, setzen Sie den `require_SSL` Parameter `true` in der Parametergruppe, die dem Cluster beim Start zugeordnet ist, auf.

Die mit diesem Muster bereitgestellte Sicherheitskontrolle überwacht Amazon Redshift Redshift-API-Aufrufe in CloudTrail AWS-Protokollen und initiiert ein Amazon CloudWatch Events-Ereignis für CreateCluster, ModifyCluster, RestoreFromClusterSnapshotCreateClusterParameterGroup, und. ModifyClusterParameterGroup APIs Wenn das Ereignis eines davon erkennt APIs, ruft es AWS Lambda auf, das ein Python-Skript ausführt. Die Python-Funktion analysiert das CloudWatch Ereignis auf die aufgelisteten CloudTrail Ereignisse. Wenn ein Amazon Redshift Redshift-Cluster aus einem vorhandenen Snapshot erstellt, geändert oder wiederhergestellt wird, eine neue Parametergruppe für den Cluster erstellt oder eine bestehende Parametergruppe geändert wird, überprüft die Funktion den `require_SSL` Parameter für den Cluster. Wenn der Parameterwert ist`false`, sendet die Funktion eine Amazon Simple Notification Service (Amazon SNS) -Benachrichtigung mit den relevanten Informationen an den Benutzer: den Namen des Amazon Redshift Redshift-Clusters, die AWS-Region, das AWS-Konto und den Amazon Resource Name (ARN) für Lambda, von dem diese Benachrichtigung stammt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.

- Eine Virtual Private Cloud (VPC) mit einer Cluster-Subnetzgruppe und einer zugehörigen Sicherheitsgruppe.

Einschränkungen

- Diese Sicherheitskontrolle ist regional. Sie müssen es in jeder AWS-Region bereitstellen, die Sie überwachen möchten.

Architektur

Zielarchitektur

Automatisierung und Skalierung

- Wenn Sie AWS Organizations verwenden, können Sie AWS Cloudformation verwenden, StackSets um diese Vorlage in mehreren Konten bereitzustellen, die Sie überwachen möchten.

Tools

AWS-Services

- AWS CloudFormation — AWS CloudFormation hilft Ihnen dabei, Ihre AWS-Ressourcen zu modellieren und einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus zu verwalten. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben und sie zusammen als Stack zu starten und zu konfigurieren, anstatt Ressourcen einzeln zu verwalten.
- Amazon CloudWatch Events — Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit.
- AWS Lambda — AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten.
- Amazon Redshift — Amazon Redshift ist ein vollständig verwalteter Data-Warehouse-Service im Petabyte-Bereich in der Cloud.

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice. Mit Amazon S3 können Sie jederzeit beliebige Mengen von Daten von überall aus im Internet speichern und aufrufen.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen. Abonnenten erhalten die veröffentlichten Mitteilungen zu den Themen, die sie abonniert haben. Alle Abonnenten eines Themas erhalten dieselben Mitteilungen.

Code

Dieses Muster umfasst die folgenden Anlagen:

- `RedshiftSSLEndpointsRequired.zip`— Der Lambda-Code für die Sicherheitskontrolle.
- `RedshiftSSLEndpointsRequired.yml`— Die CloudFormation Vorlage, die das Ereignis und die Lambda-Funktion einrichtet.

Epen

Richten Sie den S3-Bucket ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Wählen oder erstellen Sie in der Amazon S3 S3-Konsole einen S3-Bucket, um die Lambda-Code-ZIP-Datei zu hosten. Dieser S3-Bucket muss sich in derselben AWS-Region befinden wie der Amazon Redshift Redshift-Cluster, den Sie überwachen möchten. Ein S3-Bucket-Name ist weltweit eindeutig, und der Namespace wird von allen AWS-Konten gemeinsam genutzt. Der S3-Bucket-	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Name darf keine führenden Schrägstriche enthalten.	
Laden Sie den Lambda-Code hoch.	Laden Sie die Lambda-Code-ZIP-Datei, die im Abschnitt Anlagen bereitgestellt wird, in den S3-Bucket hoch.	Cloud-Architekt

Stellen Sie die CloudFormation Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die CloudFormation AWS-Vorlage.	Öffnen Sie die CloudFormation AWS-Konsole in derselben AWS-Region wie Ihr S3-Bucket und stellen Sie die angehängte Vorlage bereit`RedshiftSSLEndpointsRequired.yml` . Weitere Informationen zur Bereitstellung von CloudFormation AWS-Vorlagen finden Sie in der CloudFormation Dokumentation unter Erstellen eines Stacks auf der CloudFormation AWS-Konsole.	Cloud-Architekt
Vervollständigen Sie die Parameter in der Vorlage.	Wenn Sie die Vorlage starten, werden Sie zur Eingabe der folgenden Informationen aufgefordert: • S3-Bucket: Geben Sie den Bucket an, den Sie im	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ersten Epic erstellt oder ausgewählt haben. Hier haben Sie den angehängten Lambda-Code (.zip-Datei) hochgeladen. • S3-Schlüssel: Geben Sie den Speicherort der Lambda-ZIP-Datei in Ihrem S3-Bucket an (z. B. Dateiname .zip oder controls/ filename .zip). Fügen Sie keine führenden Schrägstriche ein. • Benachrichtigungs-E-Mail: Geben Sie eine aktive E-Mail-Adresse an, unter der Sie Amazon SNS SNS-Benachrichtigungen erhalten möchten. • Lamba-Protokollierungsebene: Geben Sie die Protokollierungsebene und die Häufigkeit für die Lambda-Funktion an. Verwenden Sie Info, um detaillierte Informationsmeldungen über den Fortschritt, Fehler für Fehlerereignisse, die die Fortsetzung der Bereitstellung dennoch ermöglichen würden, und Warnmeldungen für potenziell schädlich	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	e Situationen zu protokoll ieren.	

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die CloudFormation Vorlage erfolgreich bereitges tellt wurde, sendet sie eine Abonnement-E-Mail an die von Ihnen angegebene E-Mail-Adresse. Sie müssen dieses E-Mail-Abonnement bestätige n, um Benachrichtigungen über Verstöße zu erhalten.	Cloud-Architekt

Zugehörige Ressourcen

- Einen S3-Bucket erstellen (Amazon S3 S3-Dokumentation)
- Dateien in einen S3-Bucket hochladen (Amazon S3 S3-Dokumentation)
- Einen Stack auf der CloudFormation AWS-Konsole erstellen (CloudFormation AWS-Dokumentation)
- Erstellen einer CloudWatch Ereignisregel, die bei einem AWS-API-Aufruf mithilfe von AWS ausgelöst wird CloudTrail (CloudTrail AWS-Dokumentation)
- Erstellen eines Amazon Redshift Redshift-Clusters (Amazon Redshift Redshift-Dokumentation)
- Konfiguration von Sicherheitsoptionen für Verbindungen (Amazon Redshift Redshift-Dokumentation)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Stellen Sie sicher, dass neue Amazon Redshift Redshift-Cluster in einer VPC gestartet werden

Erstellt von Priyanka Chaudhary (AWS)

Übersicht

Dieses Muster stellt eine Amazon Web Services (AWS) CloudFormation -Vorlage bereit, die Sie automatisch benachrichtigt, wenn ein Amazon Redshift Redshift-Cluster außerhalb einer Virtual Private Cloud (VPC) gestartet wird.

Amazon Redshift ist ein vollständig verwaltetes, cloudbasiertes Data-Warehouse-Produkt im Petabyte-Bereich. Es ist für die Speicherung und Analyse großer Datenmengen konzipiert. Es wird auch zur Durchführung umfangreicher Datenbankmigrationen verwendet. Mit Amazon Virtual Private Cloud (Amazon VPC) können Sie einen logisch isolierten Bereich der AWS-Cloud bereitstellen, in dem Sie AWS-Ressourcen wie Amazon Redshift Redshift-Cluster in einem von Ihnen definierten virtuellen Netzwerk starten können.

Die mit diesem Muster bereitgestellte Sicherheitskontrolle überwacht Amazon Redshift Redshift-API-Aufrufe in CloudTrail AWS-Protokollen und initiiert ein Amazon CloudWatch Events-Ereignis für und. CreateClusterRestoreFromClusterSnapshot APIs Wenn das Ereignis eines davon erkennt APIs, ruft es AWS Lambda auf, das ein Python-Skript ausführt. Die Python-Funktion analysiert das CloudWatch Ereignis. Wenn ein Amazon Redshift Redshift-Cluster anhand eines Snapshots erstellt oder wiederhergestellt wird und außerhalb des Amazon VPC-Netzwerks angezeigt wird, sendet die Funktion eine Amazon Simple Notification Service (Amazon SNS) -Benachrichtigung mit den entsprechenden Informationen an den Benutzer: den Namen des Amazon Redshift Redshift-Clusters, die AWS-Region, das AWS-Konto und den Amazon Resource Name (ARN) für Lambda, von dem diese Benachrichtigung stammt.

Voraussetzungen und Einschränkungen

Voraussetzungen

- Ein aktives AWS-Konto.
- Eine VPC mit einer Cluster-Subnetzgruppe und einer zugehörigen Sicherheitsgruppe.

Einschränkungen

- Die CloudFormation AWS-Vorlage unterstützt nur die RestoreFromClusterSnapshotAktionen CreateClusterund (neue Cluster). Es erkennt keine vorhandenen Amazon Redshift Redshift-Cluster, die außerhalb einer VPC erstellt wurden.
- Diese Sicherheitskontrolle ist regional. Sie müssen es in jeder AWS-Region bereitstellen, die Sie überwachen möchten.

Architektur

Zielarchitektur

Automatisierung und Skalierung

Wenn Sie AWS Organizations verwenden, können Sie AWS Cloudformation verwenden, StackSets um diese Vorlage in mehreren Konten bereitzustellen, die Sie überwachen möchten.

Tools

AWS-Services

- AWS CloudFormation — AWS CloudFormation hilft Ihnen dabei, Ihre AWS-Ressourcen zu modellieren und einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus zu verwalten. Sie können eine Vorlage verwenden, um Ihre Ressourcen und ihre Abhängigkeiten zu beschreiben und sie zusammen als Stapel zu starten und zu konfigurieren, anstatt Ressourcen einzeln zu verwalten.
- AWS CloudTrail — AWS CloudTrail unterstützt Sie bei der Implementierung von Unternehmensführung, Compliance sowie Betriebs- und Risikoprüfungen Ihres AWS-Kontos. Aktionen, die von einem Benutzer, einer Rolle oder einem AWS-Service ausgeführt werden, werden als Ereignisse in aufgezeichnet CloudTrail.
- Amazon CloudWatch Events — Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben, nahezu in Echtzeit.
- AWS Lambda — AWS Lambda ist ein Rechenservice, der die Ausführung von Code unterstützt, ohne Server bereitzustellen oder zu verwalten. AWS Lambda führt Ihren Code nur bei Bedarf aus und skaliert automatisch – von einigen Anforderungen pro Tag bis zu Tausenden pro Sekunde.
- Amazon Redshift — Amazon Redshift ist ein vollständig verwalteter Data-Warehouse-Service im Petabyte-Bereich in der Cloud. Amazon Redshift ist in Ihren Data Lake integriert, sodass Sie Ihre Daten nutzen können, um neue Erkenntnisse für Ihr Unternehmen und Ihre Kunden zu gewinnen.

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) ist ein hoch skalierbarer Objektspeicherservice, den Sie für eine Vielzahl von Speicherlösungen verwenden können, darunter Websites, mobile Anwendungen, Backups und Data Lakes.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) koordiniert und verwaltet die Zustellung oder den Versand von Nachrichten zwischen Herausgebern und Kunden, einschließlich Webservern und E-Mail-Adressen.

Code

Dieses Muster umfasst die folgenden Anlagen:

- `RedshiftMustBeInVPC.zip`— Der Lambda-Code für die Sicherheitskontrolle.
- `RedshiftMustBeInVPC.yml`— Die CloudFormation Vorlage, die das Ereignis und die Lambda-Funktion einrichtet.

Folgen Sie den Anweisungen im nächsten Abschnitt, um diese Dateien zu verwenden.

Epen

Richten Sie den S3-Bucket ein

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Definieren Sie den S3-Bucket.	Wählen oder erstellen Sie in der Amazon S3 S3-Konsole einen S3-Bucket, um die Lambda-Code-ZIP-Datei zu hosten. Dieser S3-Bucket muss sich in derselben AWS-Region befinden wie der Amazon Redshift Redshift-Cluster, den Sie überwachen möchten. Ein S3-Bucket-Name ist weltweit eindeutig, und der Namespace wird von allen AWS-Konten gemeinsam genutzt. Der S3-Bucket-	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	Name darf keine führenden Schrägstriche enthalten.	
Laden Sie den Lambda-Code hoch.	Laden Sie den im Abschnitt Anlagen bereitgestellten Lambda-Code (`RedshiftMustBeInVPC.zip` Datei) in den S3-Bucket hoch.	Cloud-Architekt

Stellen Sie die CloudFormation Vorlage bereit

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Starten Sie die CloudFormation Vorlage.	Öffnen Sie die CloudFormation AWS-Konsole in derselben AWS-Region wie Ihr S3-Bucket und stellen Sie die angehängte Vorlage bereit (`RedshiftMustBeInVPC.yml`). Weitere Informationen zur Bereitstellung von CloudFormation AWS-Vorlagen finden Sie in der CloudFormation Dokumentation unter Erstellen eines Stacks auf der CloudFormation AWS-Konsole.	Cloud-Architekt
Vervollständigen Sie die Parameter in der Vorlage.	Wenn Sie die Vorlage starten, werden Sie zur Eingabe der folgenden Informationen aufgefordert: • S3-Bucket: Geben Sie den Bucket an, den Sie im	Cloud-Architekt

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	ersten Epic erstellt oder ausgewählt haben. Hier haben Sie den angehängten Lambda-Code (.zip-Datei) hochgeladen. • S3-Schlüssel: Geben Sie den Speicherort der Lambda-ZIP-Datei in Ihrem S3-Bucket an (z. B. Dateiname .zip oder controls/ filename .zip). Fügen Sie keine führenden Schrägstriche ein. • Benachrichtigungs-E-Mail: Geben Sie eine aktive E-Mail-Adresse an, unter der Sie Amazon SNS SNS-Benachrichtigungen erhalten möchten. • Lamba-Protokollierungsebene: Geben Sie die Protokollierungsebene und die Häufigkeit für die Lambda-Funktion an. Verwenden Sie Info, um detaillierte Informationsmeldungen über den Fortschritt, Fehler für Fehlerereignisse, die die Fortsetzung der Bereitstellung dennoch ermöglichen würden, und Warnmeldungen für potenziell schädlich	

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
	e Situationen zu protokoll ieren.	

Bestätigen Sie das Abonnement

Aufgabe	Beschreibung	Erforderliche Fähigkeiten
Bestätigen Sie das Abonnement.	Wenn die CloudFormation Vorlage erfolgreich bereitges tellt wurde, sendet sie eine Abonnement-E-Mail an die von Ihnen angegebene E-Mail-Adresse. Sie müssen dieses E-Mail-Abonnement bestätige n, um Benachrichtigungen über Verstöße zu erhalten.	Cloud-Architekt

Zugehörige Ressourcen

- Einen S3-Bucket erstellen (Amazon S3 S3-Dokumentation)
- Dateien in einen S3-Bucket hochladen (Amazon S3 S3-Dokumentation)
- Einen Stack auf der CloudFormation AWS-Konsole erstellen (CloudFormation AWS-Dokumentation)
- Erstellen einer CloudWatch Ereignisregel, die bei einem AWS-API-Aufruf mithilfe von AWS ausgelöst wird CloudTrail (CloudTrail AWS-Dokumentation)
- Erstellen eines Amazon Redshift Redshift-Clusters (Amazon Redshift Redshift-Dokumentation)

Anlagen

Um auf zusätzliche Inhalte zuzugreifen, die mit diesem Dokument verknüpft sind, entpacken Sie die folgende Datei: attachment.zip

Mehr Muster

- Greifen Sie mithilfe von Session Manager und Amazon EC2 Instance Connect auf einen Bastion-Host zu
- Greifen Sie privat auf Container-Anwendungen auf Amazon ECS zu, indem Sie AWS Fargate PrivateLink, AWS und einen Network Load Balancer verwenden
- Greifen Sie mithilfe von AWS PrivateLink und einem Network Load Balancer privat auf Container-Anwendungen auf Amazon ECS zu
- Greifen Sie mit AWS PrivateLink und einem Network Load Balancer privat auf Container-Anwendungen auf Amazon EKS zu
- Erlauben Sie EC2 Instances den Schreibzugriff auf S3-Buckets in AMS-Konten
- Verknüpfen Sie ein AWS CodeCommit Repository in einem AWS-Konto mit Amazon SageMaker AI Studio Classic in einem anderen Konto
- Authentifizieren Sie bestehende Benutzer von React-Anwendungen mithilfe von Amazon Cognito und AWS Amplify UI
- Automatisieren Sie das Hinzufügen oder Aktualisieren von Windows-Registrierungseinträgen mit AWS Systems Manager
- Automatisieren Sie die Durchsetzung von Verschlüsselungen in AWS Glue mithilfe einer CloudFormation AWS-Vorlage
- Automatisches Hinzufügen einer von AWS verwalteten Richtlinie für Systems Manager zu EC2 Instanzprofilen mithilfe von Cloud Custodian und AWS CDK
- Automatisches Verschlüsseln vorhandener und neuer Amazon EBS-Volumes
- Blockieren Sie den öffentlichen Zugriff auf Amazon RDS mithilfe von Cloud Custodian
- Zentralisieren Sie die DNS-Auflösung mithilfe von AWS Managed Microsoft AD und vor Ort von Microsoft Active Directory
- Implementieren Sie zentralisiertes benutzerdefiniertes Checkov-Scanning, um Richtlinien vor der Bereitstellung AWS der Infrastruktur durchzusetzen
- Suchen Sie in den AWS-CDK-Anwendungen oder CloudFormation -Vorlagen nach bewährten Methoden mithilfe von cdk-nag-Regelpaketen
- EC2 Instances beim Start auf obligatorische Tags überprüfen
- Kontenübergreifenden Zugriff auf Amazon DynamoDB konfigurieren
- Konfigurieren Sie die HTTPS-Verschlüsselung für Oracle JD Edwards EnterpriseOne auf Oracle WebLogic mithilfe eines Application Load Balancer

- Konfigurieren Sie die Protokollierung und Überwachung von Sicherheitsereignissen in Ihrer AWS IoT Umgebung
- Konfigurieren Sie die gegenseitige TLS-Authentifizierung für Anwendungen, die auf Amazon EKS ausgeführt werden
- Stellen Sie eine Connect über einen SSH-Tunnel in pgAdmin her
- Erstellen Sie eine React-App mithilfe von AWS Amplify und fügen Sie die Authentifizierung mit Amazon Cognito hinzu
- Erstellen Sie einen Bericht mit den Ergebnissen von Network Access Analyzer für eingehenden Internetzugang in mehreren AWS-Konten
- Passen Sie CloudWatch Amazon-Benachrichtigungen an für AWS Network Firewall
- Stellen Sie eine Firewall mit AWS Network Firewall und AWS Transit Gateway bereit
- Stellen Sie eine ChatOps Lösung zur Verwaltung von SAST-Scanergebnissen bereit, indem Sie Amazon Q Developer in Chat-Anwendungen verwenden, benutzerdefinierte Aktionen und AWS CloudFormation
- Dokumentieren Sie Ihr AWS-Landingzone-Design
- Verschlüsselte Verbindungen für PostgreSQL-DB-Instances in Amazon RDS aktivieren
- Verschlüsseln Sie eine bestehende Amazon RDS for PostgreSQL PostgreSQL-DB-Instance
- Automatisches Tagging von Amazon RDS-Datenbanken beim Start erzwingen
- Erzwingen Sie die Kennzeichnung von Amazon EMR-Clustern beim Start
- Stellen Sie sicher, dass die Amazon EMR-Protokollierung bei Amazon S3 beim Start aktiviert ist
- Generieren Sie mithilfe von Troposphere eine CloudFormation AWS-Vorlage, die von AWS Config verwaltete Regeln enthält
- Erhalten Sie Amazon SNS SNS-Benachrichtigungen, wenn sich der Schlüsselstatus eines AWS KMS KMS-Schlüssels ändert
- Helfen Sie mit, DynamoDB-Tagging durchzusetzen
- Identifizieren und benachrichtigen Sie, wenn Amazon Data Firehose-Ressourcen nicht mit einem AWS KMS Schlüssel verschlüsselt sind
- Implementieren Sie SHA1 Hashing für PII-Daten bei der Migration von SQL Server zu PostgreSQL
- Verbessern Sie die Betriebsleistung, indem Sie Amazon DevOps Guru in mehreren AWS-Regionen, Konten und OUs mit dem AWS CDK aktivieren
- EC2 Windows-Instances in ein AWS Managed Services Services-Konto aufnehmen und migrieren

- Migrieren Sie Amazon RDS for Oracle zu Amazon RDS for PostgreSQL im SSL-Modus mithilfe von AWS DMS
- Migrieren Sie einen ELK-Stack zu Elastic Cloud auf AWS
- Migrieren Sie einen F5 BIG-IP-Workload zu F5 BIG-IP VE in der AWS-Cloud
- Überwachen Sie Amazon Aurora auf Instances ohne Verschlüsselung
- Stellen Sie IAM-Rollen mit den geringsten Rechten bereit, indem Sie eine Rollenautomatenlösung bereitstellen
- Datenbankanmeldedaten rotieren, ohne Container neu zu starten
- Sicherer und optimierter Benutzerzugriff in einer Db2-Verbunddatenbank auf AWS mithilfe vertrauenswürdiger Kontexte
- AWS WAF Logs mithilfe AWS Firewall Manager von Amazon Data Firehose an Splunk senden
- Statische Inhalte in einem Amazon S3 S3-Bucket über eine VPC mithilfe von Amazon bereitstellen CloudFront
- Richten Sie die end-to-end Verschlüsselung für Anwendungen auf Amazon EKS mithilfe von cert-manager und Let's Encrypt ein
- Verwenden Sie Benutzer IDs in IAM-Richtlinien für Zugriffskontrolle und Automatisierung
- Stellen Sie sicher, dass ELB-Load Balancer eine TLS-Terminierung erfordern
- AWS-Netzwerk-Firewall-Protokolle und -Metriken mithilfe von Splunk anzeigen
- Visualisieren Sie IAM-Anmeldedaten für alle AWS-Konten mithilfe von Amazon QuickSight

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.