Informationen zum Onboarding erweiterter AMS-Konten

AMS-Onboarding-Leitfaden für Fortgeschrittene

Version September 25, 2025

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

AMS-Onboarding-Leitfaden für Fortgeschrittene: Informationen zum Onboarding erweiterter AMS-Konten

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

Die Marken und Handelsmarken von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, die geeignet ist, die Kunden zu verwirren oder Amazon in einer Weise herabzusetzen oder zu diskreditieren. Alle anderen Marken, die nicht im Besitz von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Einführung in das Onboarding von AWS Managed Services ... 1
Erfahren Sie mehr über AMS ... 2
Wichtige Begriffe ... 2
AMS-Modi ... 9
AMS-Modi und Anwendungen oder Workloads ... 10
Präskriptive AMS-Leitlinien für die Zeit nach der Kontoeröffnung ... 18
Was wir tun, was wir nicht tun ... 18
Verwaltung des Ausgangsverkehrs mit AMS ... 19
IAM-Benutzerrolle ... 21
MALZ: Standard-IAM-Benutzerrollen ... 22
SALZ: Standard-IAM-Benutzerrolle ... 35
Standard-Firewallregeln für den Zugriff ... 42
Ports für Linux-Stack-Instances ... 43
Anschlüsse für Windows-Stack-Instanzen ... 43
Serviceverwaltung ... 45
Kontoverwaltung ... 45
Beginn des Dienstes ... 46
Kundenbeziehungsmanagement (CRM) ... 47
CRM-Prozess ... 47
CRM-Besprechungen ... 48
Vereinbarungen für CRM-Treffen ... 49
Monatliche CRM-Berichte ... 50
Kostenoptimierung ... 51
Framework zur Kostenoptimierung ... 51
Verantwortungsmatrix für die Kostenoptimierung ... 54
Servicezeiten ... 56
Hilfe erhalten ... 57
Verwaltungsmodi ändern ... 58
Übersicht der Modi ... 59
Arten von Modi und Konten in AMS ... 60
AMS-Modi und Anwendungen oder Workloads ... 64
Anwendungsfälle für AMS-Modi in der realen Welt ... 72
RFC-Modus ... 75
Erfahre mehr über RFCs ... 76

Was sind Änderungstypen? ... 118
Behebung von RFC-Fehlern ... 132
Direkter Änderungsmodus ... 143
Erste Schritte mit dem Direct Change-Modus ... 144
Sicherheit und Compliance ... 147
Änderungsmanagement im Direct Change-Modus ... 153
Stapel im Direct Change-Modus erstellen ... 155
Anwendungsfälle für den Direct Change Mode ... 158
Entwicklermodus ... 159
Erste Schritte mit dem Entwicklermodus ... 160
Sicherheits und Compliance ... 163
Änderungsmanagement ... 164
Bereitstellen der Infrastruktur ... 171
Detektivische Kontrollen ... 171
Protokollierung, Überwachung und Ereignisverwaltung ... 171
Vorfallmanagement ... 172
Patch-Management ... 172
Kontinuitätsmanagement ... 172
Sicherheits- und Zugriffsmanagement ... 173
Self-Service-Bereitstellungsmodus in AMS ... 173
Erste Schritte mit dem SSP-Modus in AMS ... 174
Amazon API Gateway ... 175
Alexa for Business ... 176
Amazon AppStream 2.0 ... 177
Amazon Athena ... 180
Amazon Bedrock ... 181
Amazon CloudSearch ... 183
Amazon CloudWatch Synthetics ... 184
Amazon Cognito ... 185
Amazon Comprehend ... 187
Amazon Connect ... 188
Amazon Data Firehose ... 190
DevOpsAmazon-Guru ... 191
Amazon DocumentDB (mit MongoDB-Kompatibilität) ... 192
Amazon-DynamoDB ... 194
Amazon Elastic Container Registry ... 195

EC2 Image Builder 196
Amazon ECS auf AWS Fargate 198
Amazon EKS auf AWS Fargate 201
Amazon EMR 204
Amazon EventBridge 208
Amazon Forecast 210
Amazon FSx 213
Amazon FSx für OpenZFS 215
Amazon FSx für NetApp ONTAP 216
Amazon Inspector Classic 218
Amazon Kendra 219
Amazon Kinesis Data Streams 220
Amazon Kinesis Video Streams 221
Amazon Lex 222
Amazon MQ 223
Amazon Managed Service für Apache Flink 225
Amazon Managed Streaming für Apache Kafka 226
Amazon Managed Service für Prometheus 227
Amazon Personalize 228
Amazon QuickSight 231
Amazon Rekognition 233
Amazon SageMaker KI 234
Amazon Simple Email Service 238
Amazon Simple Workflow Service 239
Amazon Textract 240
Amazon Transcribe 241
Amazon WorkSpaces 242
AMS Code-Dienste 245
AWS Amplify 248
AWS AppSync 249
AWS App Mesh 250
AWS Audit Manager 251
AWS Batch 253
AWS Certificate Manager 254
AWS Private Certificate Authority 255
AWS CloudEndure 258

AWS CloudHSM ... 260
AWS CodeBuild ... 261
AWS CodeCommit ... 263
AWS CodeDeploy ... 265
AWS CodePipeline ... 266
AWS Compute Optimizer ... 268
AWS DataSync ... 269
AWS Device Farm ... 271
AWS Elastic Disaster Recovery ... 272
AWS Elemental MediaConvert ... 273
AWS Elemental MediaLive ... 274
AWS Elemental MediaPackage ... 275
AWS Elemental MediaStore ... 276
AWS Elemental MediaTailor ... 277
AWS Global Accelerator ... 278
AWS Glue ... 279
AWS Lake Formation ... 281
AWS Lambda ... 283
AWS License Manager ... 284
AWS Migration Hub ... 285
AWS Outposts ... 286
AWS Resilience Hub ... 287
AWS Secrets Manager ... 288
AWS Security Hub ... 292
AWS Service Catalog AppRegistry ... 292
AWS Shield ... 293
AWS Snowball Edge ... 295
AWS Step Functions ... 296
AWS Systems Manager Parameter speichern ... 297
AWS Systems Manager -Automatisierung ... 299
AWS Transfer Family ... 303
AWS Transit Gateway ... 304
AWS WAF ... 305
AWS Well-Architected Tool ... 307
AWS X-Ray ... 308
VM Import/Export ... 309

Vom Kunden verwalteter Modus ... 310
Erste Schritte mit dem vom Kunden verwalteten Modus ... 311
AMS- und AWS Service Catalog ... 311
Erste Schritte mit Service Catalog ... 312
Service Catalog in AMS, bevor Sie beginnen ... 312
Onboarding der AMS Multi-Account-Landingzone (MALZ) ... 317
MALZ Netzwerkarchitektur ... 317
Über die Landezone-Netzwerkarchitektur mit mehreren Konten ... 317
Wählen Sie ein MALZ oder mehrere MALZs ... 320
Landing Zone-Konten mit mehreren Konten ... 325
MALZ: Onboarding von Kernkonten ... 362
Erstellen Sie ein AWS Landingzone-Core-Konto mit mehreren Konten ... 362
Erstellen Sie eine IAM-Rolle für AMS, um auf Ihr Konto zuzugreifen ... 364
Sichern Sie das neue Konto mit Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer ... 365
Abonnieren Sie AWS Marketplace EPS ... 365
Netzwerk einrichten ... 366
Zugangsverwaltung einrichten ... 370
MALZ: Onboarding des Bewerbungskontos ... 376
Beantragung eines neuen Anwendungskontos ... 377
Einrichtung von Active Directory für den Verbundzugriff auf AMS IAM-Rollen ... 378
Einrichtung des Netzwerks mit dem neuen Anwendungskonto ... 382
Zusätzliches Konto VPCs im Anwendungskonto einrichten ... 383
Anhang: Liste der Überlegungen zum Onboarding in der Multi-Account-Landezone (MALZ) ... 383
Konfiguration des Kontos ... 384
Warnmeldungen zur Überwachung der AMS-Landezone mit mehreren Konten ... 385
Netzwerkkonfiguration ... 385
Active Directory-Konfiguration ... 387
Trend Micro Endpoint Protection (EPS) ... 387
Zugriff: Bastions, SSH und RDP ... 387
Verbund ... 389
Onboarding der AMS Single-Account-Landingzone (SALZ) ... 390
Der Onboarding-Prozess von AMS SALZ ... 390
SALZ Netzwerkarchitektur ... 391
AMS landing zone Shared Services mit einem Konto ... 392
SALZ: Neues AWS Konto für AMS erstellen ... 393

Erstelle eine AWS-Konto ... 393
Konsolidierte Abrechnung einrichten — neues Konto mit Zahlerkonto verknüpfen ... 396
Konfigurieren Sie Ihren AWS-Konto für AMS-Zugriff ... 397
Abonnieren Sie AWS Marketplace für EPS ... 399
CentOS 7.6 abonnieren AWS Marketplace ... 400
Sichern Sie das neue Konto mit Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer ... 401
SALZ: Netzwerk einrichten ... 401
Weisen Sie IP-Speicherplatz für Ihre AMS-Umgebung zu ... 401
Private Netzwerkkonnektivität zu AWS einrichten ... 402
Richten Sie Ihre Firewall ein ... 404
AMS Bastion-Optionen bei Anwendungsmigrationen/Onboarding ... 404
SALZ: Zugangsmanagement einrichten ... 405
Richten Sie eine Active Directory-Vertrauensstellung (AD) ein ... 406
Verbinden Sie Ihr Active Directory mit den AMS-Rollen AWS Identity and Access Management ... 412
SALZ: Standardeinstellungen ... 418
Endpunktsicherheit (EPS) ... 419
Sicherheitsgruppen ... 424
EC2 IAM-Instanzprofil ... 429
Standardwerte für überwachte Metriken ... 439
Standardeinstellungen für die Aufbewahrung und Rotation von Protokollen ... 457
Standardwerte für das Kontinuitätsmanagement ... 458
Standardeinstellungen patchen ... 459
Den AMS-Service validieren (SALZ) ... 461
Suchen Sie nach Kontoeinstellungen ... 461
Eine Instanz-ID oder IP-Adresse finden ... 465
DNS-freundliche Bastion-Namen ... 468
Suchen nach Bastion-IP-Adressen ... 469
EC2 Instanzen: Erstellen ... 470
Zugriff, anfordern ... 479
Andere | Andere RFC, erstellen (CLI) ... 487
Beliebiger Stapel: Löschen, Neustarten, Starten, Stoppen ... 489
Beispiele aufrufen ... 502
Einen Vorfall melden ... 512
Eine Serviceanfrage erstellen ... 516

Schritte nach dem Onboarding 518
Tutorials 519
Anhang: SALZ-Onboarding-Fragebogen 547
Zusammenfassung der Bereitstellung 548
Überlegungen zur Umgebungsarchitektur 548
Benachrichtigungen zur Überwachung der Landezone mit einem Konto 549
Wartungsfenster 549
Nächste Schritte 550
Anhang: ActiveDirectory Federation Services (ADFS) -Anspruchsregel und SAML-Einstellungen . 551
Konfigurationen von ADFS-Anspruchsregeln 551
Web-Konsole 552
API- und CLI-Zugriff mit SAML 552
Skript-Konfiguration 552
Windows-Konfiguration 552
Linux-Konfiguration 555
Dokumentverlauf 557
..... dlx

Einführung in das Onboarding von AWS Managed Services

Willkommen bei AWS Managed Services (AMS). AMS ist ein Unternehmensservice, der die kontinuierliche Verwaltung Ihrer AWS-Infrastruktur ermöglicht. Dieser Leitfaden soll Ihnen bei den ersten Schritten mit AMS helfen, einschließlich der Einrichtung eines neuen Kontos für AMS, der Einrichtung von Netzwerken und des Zugriffs auf AMS sowie der Validierung Ihres Onboarding-Setups.

Es richtet sich an IT-Administratoren, die mit der Vorbereitung und Durchführung der Aufgaben beauftragt sind, die für die Einbindung des AMS-Service in ein neues AWS-Konto erforderlich sind. Für das Onboarding des AMS-Service sind besondere Rechte erforderlich, um Active Directory-Vertrauensstellungen einzurichten und andere Aufgaben auf Netzwerkebene auszuführen. Hilfe bei der Entscheidung, ob du Landingzone-Konten mit mehreren Konten oder Landingzone-Konten mit einem Konto verwenden möchtest, findest du unter Auswahl eines MALZ oder mehrerer Konten. MALZs

> **Important**
>
> Dieser Leitfaden ist nach dieser Einführung in zwei Teile gegliedert: Einen für Landingzone-Konten mit mehreren Konten und einen für Landingzone-Konten mit einem Konto. Das Onboarding ist für beide sehr unterschiedlich. Bitte gehen Sie weiter zu dem Abschnitt des Leitfadens, der auf Ihre Situation zutrifft.

Themen

- Erfahren Sie mehr über AMS
- Die wichtigsten Begriffe von AMS
- AMS-Modi
- Präskriptive AMS-Leitlinien für die Zeit nach der Kontoeröffnung
- Was wir tun, was wir nicht tun
- Verwaltung des Ausgangsverkehrs mit AMS
- IAM-Benutzerrolle in AMS
- Standard-Firewallregeln für den Zugriff

Erfahren Sie mehr über AMS

Weitere Informationen zu AMS finden Sie in den folgenden Abschnitten des AMS-Benutzerhandbuchs:

- Was ist AWS Managed Services stellt den AMS-Service vor und beschreibt die wichtigsten Funktionen, Abläufe und Schnittstellen sowie eine typische AMS-verwaltete Netzwerkarchitektur. Dieses Kapitel enthält auch Informationen zur Zugriffsverwaltung, einschließlich des Zugriffs auf Ihre von AMS verwalteten Ressourcen und der Verwendung von Bastions.
- Die wichtigsten Begriffe enthalten Definitionen und Erläuterungen zur AMS-Terminologie.
- Understanding AMS Defaults enthält die Standardwerte, die AMS verwendet, einschließlich der Standardwerte für grundlegende Umgebungskomponenten, IAM und, Proxys EC2, überwachte Metriken, Protokollierung, Endpunktsicherheit (EPS), Backups und Patches.
- Change Management bietet detaillierte Informationen zur Funktionsweise von Änderungsanforderungen (RFCs) und Änderungstypen (CTs) sowie Beispiele für die Verwendung von AMS. RFCs
- In mehreren zusätzlichen Kapiteln werden der Zugriff auf die AWS-Konsole, die AMS-CLI, die Verwendung des AMS-Change-Management-Systems, das AMS SKMS, Sicherheit, Serviceanfragen, Vorfälle, Überwachung, Protokolle, EPS, Backups und Patch-Management behandelt.

Weitere Informationen zur AMS-Landingzone-Architektur mit mehreren Konten finden Sie unter Netzwerkarchitektur für mehrere Konten

Weitere Informationen zur Single-Account-Landingzone-Architektur von AMS finden Sie unter Single-Account-Landingzone-Netzwerkarchitektur

Die wichtigsten Begriffe von AMS

- AMS Advanced: Die im Abschnitt „Servicebeschreibung“ der AMS Advanced-Dokumentation beschriebenen Dienste. Siehe Servicebeschreibung.
- AMS Advanced-Konten: AWS Konten, die jederzeit alle Anforderungen der AMS Advanced Onboarding Requirements erfüllen. Informationen zu den Vorteilen von AMS Advanced, Fallstudien und zur Kontaktaufnahme mit einem Vertriebsmitarbeiter finden Sie unter AWS Managed Services.
- AMS Accelerate-Konten: AWS Konten, die jederzeit alle Anforderungen der AMS Accelerate Onboarding-Anforderungen erfüllen. Siehe Erste Schritte mit AMS Accelerate.

- AWS Managed Services: AMS und/oder AMS Accelerate.
- AWS Managed Services Services-Konten: Die AMS-Konten und/oder AMS Accelerate-Konten.
- Kritische Empfehlung: Eine Empfehlung, die im AWS Rahmen einer Serviceanfrage ausgesprochen wurde und Sie darüber informiert, dass Ihre Maßnahmen zum Schutz vor potenziellen Risiken oder Störungen Ihrer Ressourcen oder der AWS-Services Wenn Sie sich entscheiden, einer kritischen Empfehlung bis zum angegebenen Datum nicht zu folgen, tragen Sie die alleinige Verantwortung für alle Schäden, die sich aus Ihrer Entscheidung ergeben.
- Vom Kunden angeforderte Konfiguration: Jede Software, Dienste oder andere Konfigurationen, die nicht identifiziert sind in:
  - Beschleunigen: Unterstützte Konfigurationen oder AMS Accelerate; Servicebeschreibung.
  - AMS Advanced: Unterstützte Konfigurationen oder AMS Advanced; Servicebeschreibung.
- Kommunikation mit einem Vorfall: AMS teilt Ihnen einen Incident mit oder Sie beantragen einen Incident bei AMS über einen Incident, der im Support Center für AMS Accelerate und in der AMS Console for AMS erstellt wurde. Die AMS Accelerate Console bietet eine Zusammenfassung der Vorfälle und Serviceanfragen auf dem Dashboard sowie Links zum Support Center für weitere Informationen.
- Verwaltete Umgebung: Die AMS Advanced-Konten und/oder die AMS Accelerate-Konten, die von AMS betrieben werden.

  Für AMS Advanced gehören dazu Multi-Account-Landingzone-Konten (MALZ) und Single-Account-Landingzone-Konten (SALZ).
- Startdatum der Abrechnung: Der nächste Werktag nach Erhalt AWS der in der AWS Managed Services Onboarding-E-Mail angeforderten Informationen. Die AWS Managed Services Onboarding-E-Mail bezieht sich auf die E-Mail, die von Ihnen gesendet wird AWS , um die Informationen zu sammeln, die für die Aktivierung von AWS Managed Services auf Ihren Konten erforderlich sind.

  Für Konten, die später von Ihnen registriert wurden, ist das Startdatum der Rechnungsstellung der nächste Tag, an dem AWS Managed Services eine Benachrichtigung über die Aktivierung von AWS Managed Services für das registrierte Konto gesendet hat. Eine Benachrichtigung zur Aktivierung von AWS Managed Services erfolgt in folgenden Fällen:

  1. Sie gewähren Zugriff auf ein kompatibles AWS Konto und übergeben es an AWS Managed Services.
  2. AWS Managed Services entwirft und erstellt das AWS Managed Services Services-Konto.

- Kündigung des Dienstes: Sie können die AWS Managed Services für alle AWS Managed Services Services-Konten oder für ein bestimmtes AWS Managed Services Services-Konto aus beliebigem Grund kündigen, indem Sie eine Serviceanfrage mit einer Frist von AWS mindestens 30 Tagen angeben. Am Tag der Kündigung des Service können Sie entweder:
  1. AWS übergibt Ihnen die Kontrolle über alle AWS Managed Services Services-Konten oder gegebenenfalls die angegebenen AWS Managed Services Services-Konten oder
  2. Die Parteien entfernen die AWS Identity and Access Management Rollen, die AWS Zugriff gewähren, von allen AWS Managed Services Services-Konten oder den angegebenen AWS Managed Services Services-Konten, sofern zutreffend.
- Kündigungsdatum des Dienstes: Das Kündigungsdatum des Dienstes ist der letzte Tag des Kalendermonats, der auf das Ende der 30-tägigen Kündigungsfrist folgt. Fällt das Ende der erforderlichen Kündigungsfrist nach dem 20. Tag des Kalendermonats, ist das Kündigungsdatum der letzte Tag des folgenden Kalendermonats. Im Folgenden finden Sie Beispielszenarien für Kündigungstermine.
  - Wenn die Kündigung am 12. April erfolgt, endet die Kündigungsfrist von 30 Tagen am 12. Mai. Das Kündigungsdatum des Dienstes ist der 31. Mai.
  - Wenn am 29. April eine Kündigungsfrist erteilt wird, endet die Kündigungsfrist von 30 Tagen am 29. Mai. Das Kündigungsdatum des Dienstes ist der 30. Juni.
- Bereitstellung von AWS Managed Services: AWS stellt Ihnen die AWS Managed Services zur Verfügung und Sie können ab dem Startdatum des Services für jedes AWS Managed Services-Konto auf AWS Managed Services zugreifen und diese nutzen.
- Kündigung für bestimmte AWS Managed Services-Konten: Sie können die AWS Managed Services für ein bestimmtes AWS Managed Services Services-Konto aus beliebigem Grund kündigen, indem AWS Sie dies durch eine Serviceanfrage („Anfrage zur Kündigung eines AMS-Kontos“) mitteilen.

Bedingungen für das Incident-Management:

- Ereignis: Eine Änderung in Ihrer AMS-Umgebung.
- Warnung: Immer wenn ein unterstütztes Ereignis einen Schwellenwert AWS-Service überschreitet und einen Alarm auslöst, wird eine Warnung erstellt und eine Benachrichtigung an Ihre Kontaktliste gesendet. Darüber hinaus wird ein Vorfall in Ihrer Incident-Liste erstellt.
- Vorfall: Eine ungeplante Unterbrechung oder Leistungsverschlechterung Ihrer AMS-Umgebung oder AWS Managed Services, die zu einer von AWS Managed Services oder Ihnen gemeldeten Beeinträchtigung führt.

- Problem: Eine gemeinsame Grundursache für einen oder mehrere Vorfälle.
- Lösung eines Vorfalls oder Lösung eines Vorfalls:
  - AMS hat alle nicht verfügbaren AMS-Dienste oder -Ressourcen im Zusammenhang mit diesem Vorfall wieder in den verfügbaren Zustand versetzt, oder
  - AMS hat festgestellt, dass nicht verfügbare Stacks oder Ressourcen nicht auf einen verfügbaren Zustand zurückgesetzt werden können, oder
  - AMS hat eine von Ihnen autorisierte Wiederherstellung der Infrastruktur eingeleitet.
- Reaktionszeit bei Vorfällen: Der Zeitunterschied zwischen dem Zeitpunkt, zu dem Sie einen Vorfall erstellen, und dem Zeitpunkt, zu dem AMS eine erste Antwort über die Konsole, E-Mail, das Service Center oder das Telefon bereitstellt.
- Zeit zur Behebung eines Vorfalls: Der Zeitunterschied zwischen dem Zeitpunkt, zu dem entweder AMS oder Sie einen Vorfall auslösen, und dem Zeitpunkt, zu dem der Vorfall behoben wird.
- Priorität des Vorfalls: Wie Vorfälle von AMS oder von Ihnen als „Niedrig“, „Mittel“ oder „Hoch“ priorisiert werden.
  - Niedrig: Ein unkritisches Problem mit Ihrem AMS-Service.
  - Medium: Ein AWS-Service in Ihrer verwalteten Umgebung ist verfügbar, funktioniert aber nicht wie vorgesehen (gemäß der entsprechenden Servicebeschreibung).
  - Hoch: Entweder (1) die AMS-Konsole oder ein oder mehrere AMS APIs in Ihrer verwalteten Umgebung sind nicht verfügbar; oder (2) ein oder mehrere AMS-Stacks oder Ressourcen in Ihrer verwalteten Umgebung sind nicht verfügbar und die Nichtverfügbarkeit verhindert, dass Ihre Anwendung ihre Funktion erfüllt.

  AMS kann Vorfälle gemäß den oben genannten Richtlinien neu kategorisieren.
- Wiederherstellung der Infrastruktur: Erneutes Bereitstellen vorhandener Stacks auf der Grundlage von Vorlagen der betroffenen Stacks und Initiierung einer Datenwiederherstellung auf der Grundlage des letzten bekannten Wiederherstellungspunkts, sofern von Ihnen nicht anders angegeben, wenn eine Behebung des Vorfalls nicht möglich ist.

Bedingungen für die Infrastruktur:

- Verwaltete Produktionsumgebung: Ein Kundenkonto, in dem sich die Produktionsanwendungen des Kunden befinden.
- Verwaltete Nichtproduktionsumgebung: Ein Kundenkonto, das nur Anwendungen enthält, die nicht zur Produktion gehören, z. B. Anwendungen für Entwicklung und Tests.

- AMS-Stack: Eine Gruppe von einer oder mehreren AWS Ressourcen, die von AMS als eine Einheit verwaltet werden.
- Unveränderliche Infrastruktur: Ein für Amazon EC2 Auto Scaling Scaling-Gruppen (ASGs) typisches Infrastrukturwartungsmodell, bei dem aktualisierte Infrastrukturkomponenten (im AWS AMI) bei jeder Bereitstellung ersetzt werden, anstatt direkt aktualisiert zu werden. Die Vorteile einer unveränderlichen Infrastruktur bestehen darin, dass alle Komponenten synchron bleiben, da sie immer auf derselben Basis generiert werden. Die Unveränderlichkeit ist unabhängig von einem Tool oder Workflow zum Erstellen des AMI.
- Veränderbare Infrastruktur: Ein Infrastrukturwartungsmodell, das typisch für Stacks ist, die keine Amazon EC2 Auto Scaling Scaling-Gruppen sind und eine einzelne Instance oder nur wenige Instances enthalten. Dieses Modell entspricht am ehesten der traditionellen, hardwarebasierten Systembereitstellung, bei der ein System zu Beginn seines Lebenszyklus bereitgestellt wird und dann im Laufe der Zeit Updates auf dieses System übertragen werden. Alle Aktualisierungen des Systems werden einzeln auf die Instanzen angewendet und können aufgrund von Anwendungs- oder Systemneustarts zu Systemausfällen führen (abhängig von der Stack-Konfiguration).
- Sicherheitsgruppen: Virtuelle Firewalls für Ihre Instance zur Steuerung des ein- und ausgehenden Datenverkehrs. Sicherheitsgruppen wirken auf der Instance-Ebene und nicht auf der Subnetzebene. Daher kann jeder Instance in einem Subnetz in Ihrer VPC ein anderer Satz von Sicherheitsgruppen zugewiesen werden.
- Service Level Agreements (SLAs): Teil der AMS-Verträge mit Ihnen, die das erwartete Serviceniveau definieren.
- SLA nicht verfügbar und nicht verfügbar:
  - Eine von Ihnen eingereichte API-Anfrage, die zu einem Fehler führt.
  - Eine von Ihnen eingereichte Konsolenanfrage, die zu einer 5xx-HTTP-Antwort führt (der Server ist nicht in der Lage, die Anfrage auszuführen).
  - Alle AWS-Service Angebote, die Stacks oder Ressourcen in Ihrer von AMS verwalteten Infrastruktur bilden, befinden sich im Status „Serviceunterbrechung“, wie im Service Health Dashboard angezeigt.
  - Die Nichtverfügbarkeit, die direkt oder indirekt auf einen AMS-Ausschluss zurückzuführen ist, wird bei der Entscheidung über die Inanspruchnahme von Servicegutschriften nicht berücksichtigt. Dienste gelten als verfügbar, sofern sie nicht die Kriterien für die Nichtverfügbarkeit erfüllen.
- Servicelevel-Ziele (SLOs): Teil der AMS-Verträge mit Ihnen, in denen spezifische Serviceziele für AMS-Services definiert werden.

Bedingungen für das Patchen:

- Obligatorische Patches: Wichtige Sicherheitsupdates zur Behebung von Problemen, die den Sicherheitsstatus Ihrer Umgebung oder Ihres Kontos gefährden könnten. Ein „Kritisches Sicherheitsupdate“ ist ein Sicherheitsupdate, das vom Hersteller eines AMS-unterstützten Betriebssystems als „Kritisch“ eingestuft wird.
- Angekündigte oder veröffentlichte Patches: Patches werden in der Regel nach einem bestimmten Zeitplan angekündigt und veröffentlicht. Neue Patches werden angekündigt, wenn festgestellt wird, dass der Patch benötigt wird. In der Regel wird der Patch bald danach veröffentlicht.
- Patch-Add-on: Tag-basiertes Patchen für AMS-Instances, das die AWS Systems Manager (SSM) -Funktionalität nutzt, sodass Sie Instances taggen und diese Instances mithilfe einer Baseline und eines von Ihnen konfigurierten Fensters patchen lassen können.
- Patch-Methoden:
  - In-Place-Patching: Patchen, das durch Ändern vorhandener Instanzen erfolgt.
  - AMI-Ersatz-Patching: Patching, das durch Ändern des AMI-Referenzparameters einer vorhandenen EC2 Auto Scaling Scaling-Gruppenstartkonfiguration erfolgt.
- Patch-Anbieter (Betriebssystemanbieter, Drittanbieter): Patches werden vom Anbieter oder vom zuständigen Gremium der Anwendung bereitgestellt.
- Patch-Typen:
  - Kritisches Sicherheitsupdate (CSU): Ein Sicherheitsupdate, das vom Hersteller eines unterstützten Betriebssystems als „Kritisch“ eingestuft wurde.
  - Wichtiges Update (IU): Ein Sicherheitsupdate, das vom Hersteller eines unterstützten Betriebssystems als „wichtig“ eingestuft wurde, oder ein nicht sicherheitsrelevantes Update, das vom Hersteller eines unterstützten Betriebssystems als „Kritisch“ eingestuft wurde.
  - Anderes Update (OU): Ein Update des Herstellers eines unterstützten Betriebssystems, bei dem es sich nicht um eine CSU oder eine IU handelt.
- Unterstützte Patches: AMS unterstützt Patches auf Betriebssystemebene. Upgrades werden vom Anbieter veröffentlicht, um Sicherheitslücken oder andere Fehler zu beheben oder die Leistung zu verbessern. Eine Liste der derzeit unterstützten OSs Konfigurationen finden Sie unter Support-Konfigurationen.

Sicherheitsbedingungen:

- Detective Controls: Eine Bibliothek mit von AMS erstellten oder aktivierten Monitoren, die einen kontinuierlichen Überblick über vom Kunden verwaltete Umgebungen und Workloads für

Konfigurationen bieten, die nicht den Sicherheits-, Betriebs- oder Kundenkontrollen entsprechen, und Maßnahmen ergreifen, indem sie Eigentümer benachrichtigen, Ressourcen proaktiv ändern oder beenden.

Bedingungen für Serviceanfragen:

- Serviceanfrage: Eine Anfrage von Ihnen nach einer Maßnahme, die AMS in Ihrem Namen ergreifen soll.
- Warnmeldung: Eine Benachrichtigung, die von AMS auf Ihrer Seite mit der Liste der Serviceanfragen veröffentlicht wird, wenn eine AMS-Warnung ausgelöst wird. Der für Ihr Konto konfigurierte Kontakt wird ebenfalls über die konfigurierte Methode (z. B. E-Mail) benachrichtigt. Wenn Ihre Instanzen/Ressourcen Kontakt-Tags enthalten und Ihrem Cloud Service Delivery Manager (CSDM) Ihre Zustimmung für tagbasierte Benachrichtigungen erteilt haben, werden die Kontaktinformationen (Schlüsselwert) im Tag auch bei automatisierten AMS-Benachrichtigungen benachrichtigt.
- Servicebenachricht: Eine Mitteilung von AMS, die auf Ihrer Seite mit der Liste Ihrer Serviceanfragen veröffentlicht wird.

Verschiedene Bedingungen:

- AWS Managed Services-Schnittstelle: Für AMS: Die AWS Managed Services Advanced Console, AMS CM API und Support API. Für AMS Accelerate: Die Support Konsole und die Support API.
- Kundenzufriedenheit (CSAT): AMS CSAT verfügt über umfassende Analysen, darunter Bewertungen der Fallkorrespondenz zu jedem Fall oder jeder etwaigen Korrespondenz, vierteljährliche Umfragen usw.
- DevOps: DevOps ist eine Entwicklungsmethodik, die sich nachdrücklich für Automatisierung und Überwachung aller Schritte einsetzt. DevOps zielt auf kürzere Entwicklungszyklen, eine höhere Bereitstellungshäufigkeit und zuverlässigere Releases ab, indem die traditionell getrennten Funktionen von Entwicklung und Betrieb auf einer Grundlage der Automatisierung zusammengeführt werden. Wenn Entwickler den Betrieb verwalten können und der Betrieb die Entwicklung beeinflusst, können Probleme und Probleme schneller entdeckt und gelöst werden, und Geschäftsziele lassen sich leichter erreichen.
- ITIL: Die Information Technology Infrastructure Library (ITIL genannt) ist ein ITSM-Framework, mit dem der Lebenszyklus von IT-Services standardisiert werden soll. ITIL ist in fünf Phasen unterteilt,

die den IT-Servicelebenszyklus abdecken: Servicestrategie, Servicedesign, Serviceübergang, Servicebetrieb und Serviceverbesserung.

- IT-Servicemanagement (ITSM): Eine Reihe von Praktiken, die IT-Services auf die Bedürfnisse Ihres Unternehmens abstimmen.
- Managed Monitoring Services (MMS): AMS betreibt sein eigenes Überwachungssystem, den Managed Monitoring Service (MMS), das AWS Gesundheitsereignisse verarbeitet und CloudWatch Amazon-Daten sowie Daten von anderen aggregiert und AMS-Betreiber (rund um die Uhr online) über alle Alarme informiert AWS-Services, die über ein Amazon Simple Notification Service (Amazon SNS) -Thema ausgelöst wurden.
- Namespace: Wenn Sie IAM-Richtlinien erstellen oder mit Amazon Resource Names (ARNs) arbeiten, identifizieren Sie einen AWS-Service mithilfe eines Namespace. Sie verwenden Namespaces bei der Identifikation von Aktionen und Ressourcen.

AMS-Modi

Verwenden Sie diese Option, um den geeigneten AWS Managed Services (AMS) -Modus für das Hosten Ihrer Anwendungen auszuwählen, der auf Ihrer gewünschten Kombination aus Flexibilität und präskriptiver Steuerung basiert, um Ihre Geschäftsergebnisse zu erzielen.

Die Zielgruppe für diese Informationen ist:

- Kundenteams, die für die Strategie und Steuerung ihrer landing zone verantwortlich sind. Diese Informationen helfen dem Team dabei, den Grundstein für eine von AMS verwaltete landing zone mit den AMS-Modi zu legen, die es seinen internen und externen Kunden anbieten möchte.
- Geschäfts- und Anwendungsinhaber, die mit der Migration ihrer Anwendung auf AMS beauftragt sind. Diese Informationen helfen bei der Planung der Anwendungsmigration mit dem passenden AMS-Modus für migrate/host ihre Anwendung. Beachten Sie, dass dieselbe Anwendung in verschiedenen Phasen ihres Software Development Life Cycle (SDLC) -Lebenszyklus in mehr als einem AMS-Modus gehostet werden kann.
- AMS-Partner haben die Aufgabe, Kunden über die verschiedenen Optionen für die Entwicklung und Migration zu AMS zu informieren.

Bei diesen Informationen wird davon ausgegangen, dass Sie bereits die Entscheidung getroffen haben, AMS zu nutzen, um Ihren Weg in die Cloud zu beschleunigen. Lesen Sie dieses paper an zwei Stellen auf Ihrem Weg zur Cloud-Migration: Erstens in der Gründungsphase der Einrichtung der

von AMS verwalteten Plattform. Zweitens, wenn Sie bei Ihrer Cloud-Einführung von der Gründungs- zur Migrationsphase übergehen, kurz nachdem die Einführung in AMS abgeschlossen ist und Sie sich auf die Anwendungs-Governance und den Betrieb konzentrieren.

AMS-Modi und Anwendungen oder Workloads

Berücksichtigen Sie bei der Auswahl des richtigen Modus die Betriebs- und Governance-Anforderungen für Ihre Anwendungen, indem Sie entweder ein neues Anwendungskonto beantragen oder die Anwendung in einem vorhandenen Anwendungskonto hosten. Die Auswahl des geeigneten AMS-Modus für jede Anwendung oder jeden Workload hängt von den folgenden Faktoren ab:

- Die Art der SDLC-Lebenszyklusfunktion, die die Umgebung bereitstellen wird (z. B. Sandbox mit unmoderierten Änderungen, UAT mit einigen häufigen Änderungen, Produktion mit minimalen Änderungen und stark reguliert)
- Die erforderlichen Verwaltungsrichtlinien (die auf OU-Ebene durchgesetzt werden) SCPs
- Betriebsmodell (wenn Sie die operative Verantwortung übernehmen oder diese an AMS auslagern möchten)
- Die gewünschten Geschäftsergebnisse, wie die Zeit für den Betrieb in der Cloud und die Betriebskosten.

> **Note**
>
> Eine Beschreibung der Modustypen pro AMS-Dienst finden Sie unter Modi- und Kontotypen in AMS.
> Praktische Anwendungsfälle der verschiedenen Modi finden Sie unter Anwendungsfälle aus der Praxis für AMS-Modi

In der folgenden Tabelle sind die wichtigsten Überlegungen aufgeführt, die Anwendungsbesitzer bei der Entscheidung für den am besten geeigneten AMS-Modus berücksichtigen sollten. Anwendungsbesitzer sollten vor der Anwendungsmigration eine Bewertungsphase einplanen, um genau zu verstehen, welcher Modus für ihre spezifische Anwendung gilt. Beispiel: Für Anwendungen, die auf Cloud-nativen Diensten oder serverloser Architektur basieren, könnte die beste Option darin bestehen, im Entwicklermodus mit dem Aufbau und der Iteration zu beginnen und die endgültige Infrastruktur als Code mithilfe des AMS Managed — SSP-Modus bereitzustellen. In diesem Fall kann ein geringfügiges Refactoring erforderlich sein, um sicherzustellen, dass alle für die automatisierte Bereitstellung erstellten CloudFormation Vorlagen den von AMS festgelegten Ingest-Richtlinien

entsprechen. Darüber hinaus müssen alle IAM-Berechtigungen von AMS Security genehmigt werden, um sicherzustellen, dass sie dem Modell der geringsten Rechte folgen.

Der AMS-Modus, der für das Hosten der Anwendung ausgewählt wurde, kann Ihnen dabei helfen, Ihr gewünschtes Cloud-Betriebsmodell umzusetzen.

> **Note**
>
> In einer einzigen AMS Managed Landing Zone kann mehr als ein Cloud-Betriebsmodell existieren, basierend auf den verschiedenen AMS-Modi, die für das Hosten der Anwendungen ausgewählt wurden.

Probleme bei der Entscheidung	Standard-CM-Modus/ /OOD *	AWS Service Catalog	Direkter Änderungsmodus	Self-Service-Bereitstellung	Entwicklermodus	Vom Kunden verwaltet
Betriebsbereitschaft						
Protokollierung, Überwachung und Eventmanagement	AMS ist für die gesamte verwaltete Infrastruktur verantwortlich			Der Kunde ist verantwortlich für Self-Service Provisioned Services (SSP)	Kunde, der für Ressourcen verantwortlich ist, die mithilfe der Entwickler-IAM-Rolle außerhalb des AMS CM-Systems bereitgestellt werden	Der Kunde ist verantwortlich
Kontinuitätsmanagement	Verantwortung von AMS für die Ausführung des vom Kunden ausgewählten Backup-Plans			Der Kunde ist verantwortlich für	Kunde, der für Ressourcen verantwor	

Probleme bei der Entscheidung	Standard-CM-Modus/ /OOD *	AWS Service Catalog	Direkter Änderungsmodus	Self-Service-Bereitstellung	Entwicklermodus	Vom Kunden verwaltet
				Self-Service Provisioned Services (SSP)	tlich ist, die mithilfe der Entwickler-IAM-Rolle außerhalb des AMS CM-Systems bereitgestellt werden	
Zugriffsmanagement auf Instanzebene	AMS-Verwaltung über unidirektionales AD-Trust mit lokaler Domäne. Erfordert eine verwaltete Infrastruktur, um der AMS-Domäne beizutreten			Nicht zutreffend	Der Kunde ist verantwortlich für Ressourcen, die mithilfe der Entwickler-IAM-Rolle außerhalb des AMS CM-Systems bereitgestellt werden	

Probleme bei der Entscheidung	Standard-CM-Modus/ /OOD *	AWS Service Catalog	Direkter Änderungsmodus	Self-Service-Bereitstellung	Entwicklermodus	Vom Kunden verwaltet
Sicherheitsmanagement und Zugriffsmanagement auf Kontoebene	AMS-Verantwortung für alle verwalteten Konten			AMS ist für alle verwalteten Konten verantwortlich	Der Kunde ist verantwortlich für Ressourcen, die mithilfe der Entwickler-IAM-Rolle außerhalb des AMS CM-Systems bereitgestellt werden	
Patch-Management	AMS-Verantwortung für alle verwalteten Konten			Der Kunde ist verantwortlich für Self-Service Provisioned Services (SSP)	Kunde, der für Ressourcen verantwortlich ist, die mithilfe der Entwickler-IAM-Rolle außerhalb des AMS CM-Systems bereitgestellt werden	

Probleme bei der Entscheidung	Standard-CM-Modus/ /OOD *	AWS Service Catalog	Direkter Änderungsmodus	Self-Service-Bereitstellung	Entwicklermodus	Vom Kunden verwaltet
Änderungsmanagement	AMS-Verantwortung für alle verwalteten Konten			Der Kunde ist verantwortlich für Self-Service Provisioned Services (SSP)	Kunde, der für Ressourcen verantwortlich ist, die mithilfe der Entwickler-IAM-Rolle außerhalb des AMS CM-Systems bereitgestellt werden	
Verwaltung der Bereitstellung	Präskriptiv und standardisiert für die in AMS angebotenen Bereitstellungsoptionen	Flexibilität bei der direkten Nutzung der AWS-Service-API für den AWS Service Catalog gemäß den vorgeschriebenen AMS-Standards	Flexibilität zur direkten Nutzung der AWS-Service-API gemäß den vorgeschriebenen AMS-Standards	Flexibilität bei der direkten Nutzung des AWS-Service APIs für SSP-Services	Flexibilität bei der direkten Nutzung der AWS-Service-API für die Bereitstellung	

Probleme bei der Entscheidung	Standard-CM-Modus/ /OOD *	AWS Service Catalog	Direkter Änderungsmodus	Self-Service-Bereitstellung	Entwicklermodus	Vom Kunden verwaltet
Verwaltung und Prüfung von Vorfällen	AMS ist für alle verwalteten Konten verantwortlich				Der Kunde ist verantwortlich für Ressourcen, die mithilfe der Entwickler-IAM-Rolle außerhalb des AMS Change Management Systems bereitgestellt werden	
GuardRails und gemeinsam genutzte Infrastruktur (Netzwerk) und Sicherheitsframework	Präskriptive und standardisierte Nutzung von AMS Core Accounts					Flexible und maßgeschneiderte Nutzung von AMS Core Accounts
Bereitschaft zur Anwendung						

Probleme bei der Entscheidung	Standard-CM-Modus/ /OOD *	AWS Service Catalog	Direkter Änderungsmodus	Self-Service-Bereitstellung	Entwicklermodus	Vom Kunden verwaltet
Refactoring von Anwendungen	Ein leichtes Refactoring ist erforderlich				Ein leichtes Refactoring ist erforderlich (falls es mit AMS Standard CM bereitgestellt wurde)	Ein Refactoring ist nicht erforderlich
Support für AWS-Services	Beschränkt auf das, was von AMS unterstützt wird					Nicht begrenzt
Geschäftliche Überlegungen						
Zeit bis zur Betriebsbereitschaft	Drei bis sechs Monate			Mehr als 6 Monate, abhängig von den Kompetenzen des Kunden im Bereich Anwendungsbetrieb		6 bis 18 Monate, abhängig von den Kompetenzen des Kunden in Bezug auf Infrastruktur und Anwendungsbetrieb
Kosten	$$$$			$$$	$$	$

Probleme bei der Entscheidung	Standard-CM-Modus/ /OOD *	AWS Service Catalog	Direkter Änderungsmodus	Self-Service-Bereitstellung	Entwicklermodus	Vom Kunden verwaltet
Anwendungsbeispiele	Webserver mit 3-Tier-Stack, Apps mit Compliance- und regulatorischen Anforderungen			Webserver mit API Gateway, containerisierte Anwendung, die ECS/ EKS nutzt	Iteration/ Optimierung einer Data Lake-Anwendung, die Lambda, Glue, Athena usw. verwendet	Dezentralisiert accounts/ applications wie eine Sandbox, verwaltete Anwendungen von Drittanbietern

* Operations On Demand (OOD) bietet ein Angebot für Kunden, die den Standard-CM-Modus verwenden, um ihre Änderungen mithilfe spezieller Ressourcen zu verwalten. Weitere Informationen finden Sie im Angebotskatalog für Operations on Demand und wenden Sie sich an Ihren Cloud Service Delivery Manager (CSDM).

> **Note**
>
> Beim Preisvergleich zwischen SSP-Modus und Entwicklermodus wird davon ausgegangen, dass dieselben AWS-Services bereitgestellt werden.

Vergleich der AMS-Modi mit Geschäfts- und IT-Zielen

Wie gezeigt, sind die Modi AMS-Managed Standard Change, AWS Service Catalog oder Direct Change am besten geeignet, wenn Sie nach einem stark kontrollierten und standardisierten Governance-Modell für Ihre Anwendungen suchen. Wenn Sie ein maßgeschneidertes Governance-Modell benötigen, bei dem der Schwerpunkt auf Anwendungsinnovationen liegt, ohne dass Sie dafür betriebsbereit sein müssen, wählen Sie den Modus Customer Managed. Im vom Kunden verwalteten Modus kann die Operationalisierung Ihrer Anwendungen länger dauern, da Sie die Verantwortung für

die Einrichtung von Mitarbeitern, Prozessen und Tools zur Unterstützung betrieblicher Funktionen wie Incident Management, Configuration Management, Provisioning Management, Security Management, Patch Management usw. tragen.

Präskriptive AMS-Leitlinien für die Zeit nach der Kontoeröffnung

Da Unternehmen verteilte Abläufe und DevOps Praktiken einführen, gibt es eine Reihe zentraler betrieblicher Funktionen, die vor der Bereitstellung von Workloads auf jedes Konto angewendet werden sollten, um den Grundpfeilern von Well Architected gerecht zu werden.

Über diesen Link werden eine ZIP-Datei mit einem Word-Dokument und eine ZIP-Datei mit Skripten und Beispielen heruntergeladen. Bei der automatisierten Kontoeinrichtung handelt es sich um eine Reihe von Skripten, mit denen die Einrichtung eines neuen Anwendungskontos automatisiert oder als Bootstrap bezeichnet wird.

Sobald ein neues Konto verkauft ist und bevor irgendwelche Workloads bereitgestellt werden, richten Sie Standard-Backup-Pläne, Patch-Fenster und Verschlüsselung (und mehr) ein, um das Konto aus betrieblicher, sicherheitstechnischer und verwaltungstechnischer Sicht einsatzbereit zu machen. Um die Agilität, Konsistenz und Reaktionsfähigkeit bei der Einrichtung von Anwendungskonten zu verbessern, finden Sie die folgende Beispielanleitung als Referenz.

Automatisierte Kontoeinrichtung.

Was wir tun, was wir nicht tun

AMS bietet Ihnen einen standardisierten Ansatz für die Bereitstellung der AWS-Infrastruktur und bietet das erforderliche kontinuierliche Betriebsmanagement. Eine vollständige Beschreibung der Rollen, Verantwortlichkeiten und unterstützten Services finden Sie in der Servicebeschreibung.

> **Note**
>
> Um AMS aufzufordern, einen zusätzlichen AWS-Service bereitzustellen, reichen Sie eine Serviceanfrage ein. Weitere Informationen finden Sie unter Serviceanfragen stellen.

- Was wir tun:

  Nachdem Sie das Onboarding abgeschlossen haben, können Sie in der AMS-Umgebung Änderungsanfragen (RFCs), Incidents und Serviceanfragen entgegennehmen. Ihre Interaktion

mit dem AMS-Service dreht sich um den Lebenszyklus eines Anwendungsstapels. Neue Stacks werden anhand einer vorkonfigurierten Liste von Vorlagen bestellt, in bestimmten Virtual Private Cloud (VPC) -Subnetzen gestartet, während ihrer Betriebsdauer durch Änderungsanforderungen (RFCs) geändert und rund um die Uhr auf Ereignisse und Vorfälle überwacht.

Aktive Anwendungs-Stacks werden von AMS überwacht und verwaltet, einschließlich Patches, und erfordern während der gesamten Lebensdauer des Stacks keine weiteren Maßnahmen, es sei denn, eine Änderung ist erforderlich oder der Stack wird außer Betrieb genommen. Von AMS festgestellte Vorfälle, die den Zustand und die Funktion des Stacks beeinträchtigen, wird eine Benachrichtigung generiert. Möglicherweise müssen Sie Maßnahmen ergreifen, um diese zu beheben oder zu überprüfen. Fragen zu Anleitungen und andere Anfragen können gestellt werden, indem Sie eine Serviceanfrage einreichen.

Darüber hinaus können Sie mit AMS kompatible AWS-Services aktivieren, die nicht von AMS verwaltet werden. Informationen zu AWS-AMS-kompatiblen Diensten finden Sie unter Self-Service-Bereitstellungsmodus.

- Was wir NICHT tun:

  AMS vereinfacht zwar die Anwendungsbereitstellung durch die Bereitstellung einer Reihe manueller und automatisierter Optionen, Sie sind jedoch für die Entwicklung, das Testen, die Aktualisierung und das Management Ihrer Anwendung verantwortlich. AMS bietet Unterstützung bei der Behebung von Infrastrukturproblemen, die sich auf Anwendungen auswirken, AMS kann jedoch nicht auf Ihre Anwendungskonfigurationen zugreifen oder diese validieren.

Verwaltung des Ausgangsverkehrs mit AMS

Standardmäßig hat die Route mit einem Ziel-CIDR von 0.0.0.0/0 für private AMS-Subnetze und Subnetze für Kundenanwendungen ein NAT-Gateway (Network Address Translation) als Ziel. AMS-Dienste TrendMicro und Patching sind Komponenten, die ausgehenden Zugriff auf das Internet haben müssen, damit AMS seinen Dienst bereitstellen kann und Betriebssysteme Updates abrufen können. TrendMicro

AMS unterstützt die Umleitung des ausgehenden Datenverkehrs über ein vom Kunden verwaltetes Ausgangsgerät in das Internet, sofern:

- Es fungiert als impliziter (z. B. transparenter) Proxy.

and

- Es ermöglicht AMS-HTTP- und HTTPS-Abhängigkeiten (in diesem Abschnitt aufgeführt), um das kontinuierliche Patchen und die Wartung der von AMS verwalteten Infrastruktur zu ermöglichen.

Einige Beispiele sind:

- Das Transit Gateway (TGW) hat eine Standardroute, die über die AWS Direct Connect Connect-Verbindung im Multi-Account Landing Zone Networking-Konto auf die vom Kunden verwaltete, lokale Firewall verweist.
- Der TGW hat eine Standardroute, die auf einen AWS-Endpunkt in der ausgehenden Multi-Account-Landingzone-VPC verweist, der AWS nutzt PrivateLink, und auf einen vom Kunden verwalteten Proxy in einem anderen AWS-Konto verweist.
- Der TGW hat eine Standardroute, die auf eine vom Kunden verwaltete Firewall in einem anderen AWS-Konto verweist, mit einer site-to-site VPN-Verbindung als Anhang zur Multi-Account-Landing Zone TGW.

AMS hat die entsprechenden HTTP- und HTTPS-Abhängigkeiten von AMS identifiziert und entwickelt und verfeinert diese Abhängigkeiten kontinuierlich. Weitere Informationen finden Sie unter egressMgmt.zip. Zusammen mit der JSON-Datei enthält die ZIP-Datei eine README-Datei.

> **Note**
>
> - Diese Informationen sind nicht vollständig — einige erforderliche externe Websites sind hier nicht aufgeführt.
> - Verwenden Sie diese Liste nicht im Rahmen einer Ablehnungsliste oder einer Blockierungsstrategie.
> - Diese Liste dient als Ausgangspunkt für einen Regelsatz zur Filterung ausgehender Zugriffe, wobei davon ausgegangen wird, dass mithilfe von Berichtstools genau ermittelt werden kann, wo der tatsächliche Datenverkehr von der Liste abweicht.

Wenn Sie Informationen zur Filterung des ausgehenden Datenverkehrs benötigen, senden Sie eine E-Mail an Ihren CSDM: ams-csdm@amazon.com.

IAM-Benutzerrolle in AMS

Eine IAM-Rolle ähnelt einem IAM-Benutzer insofern, als es sich um eine AWS Identität mit Berechtigungsrichtlinien handelt, die festlegen, was die Identität tun darf und was nicht. AWS Eine Rolle ist jedoch nicht einer einzigen Person zugeordnet, sondern kann von allen Personen angenommen werden, die diese Rolle benötigen.

Derzeit gibt es eine AMS-Standardbenutzerrolle für AMS-Standardkonten und eine zusätzliche Rolle `customer_managed_ad_user_role` für AMS-Konten mit Managed Active Directory. `Customer_ReadOnly_Role`

Die Rollenrichtlinien legen Berechtigungen für CloudWatch Amazon S3 S3-Protokollaktionen, AMS-Konsolenzugriff, Leseeinschränkungen für die meisten AWS-Services, eingeschränkten Zugriff auf die S3-Konsole des Kontos und AMS-Change-Typ-Zugriff fest.

Darüber hinaus `Customer_ReadOnly_Role` verfügt der über mutative Reserved-Instance-Berechtigungen, mit denen Sie Instances reservieren können. Es hat einige Kosteneinsparungsmöglichkeiten. Wenn Sie also wissen, dass Sie über einen längeren Zeitraum eine bestimmte Anzahl von EC2 Amazon-Instances benötigen, können Sie diese APIs aufrufen. Weitere Informationen finden Sie unter Amazon EC2 Reserved Instances.

> **Note**
>
> Das AMS Service Level Objective (SLO) für die Erstellung benutzerdefinierter IAM-Richtlinien für IAM-Benutzer beträgt vier Arbeitstage, es sei denn, eine bestehende Richtlinie wird wiederverwendet. Wenn Sie die bestehende IAM-Benutzerrolle ändern oder eine neue hinzufügen möchten, reichen Sie jeweils einen IAM: Update Entity oder IAM: Create Entity RFC ein.

Wenn Sie mit Amazon IAM-Rollen nicht vertraut sind, finden Sie wichtige Informationen unter IAM-Rollen.

Multi-Account-Landingzone (MALZ): Die standardmäßigen, nicht angepassten Richtlinien für Benutzerrollen für mehrere Konten von AMS finden Sie unter Weiter. MALZ: Standard-IAM-Benutzerrollen

MALZ: Standard-IAM-Benutzerrollen

JSON-Richtlinienerklärungen für die standardmäßigen AMS-Landingzone-Benutzerrollen mit mehreren Konten.

> **Note**
>
> Die Benutzerrollen sind anpassbar und können je nach Konto unterschiedlich sein. Anweisungen zur Suche nach Ihrer Rolle finden Sie hier.

Dies sind Beispiele für die standardmäßigen MALZ-Benutzerrollen. Um sicherzustellen, dass Sie die benötigten Richtlinien festgelegt haben, führen Sie den AWS-Befehl aus `get-role`oder melden Sie sich bei der AWS-Management -> IAM-Konsole an und wählen Sie im Navigationsbereich Rollen aus.

Rollen der wichtigsten OU-Konten

Ein Kernkonto ist ein von Malz verwaltetes Infrastrukturkonto. AMS-Landingzone mit mehreren Konten Zu den Kernkonten gehören ein Verwaltungskonto und ein Netzwerkkonto.

Core-OU-Konto: Allgemeine Rollen und Richtlinien

Rolle	Richtlinie oder Richtlinien
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(Öffentliche verwaltete AWS-Richtlinie).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportZugriff (Öffentliche AWS-verwaltete Richtlinie).
AWSManagedServicesChangeManagementRole (Version des Hauptkontos)	ReadOnlyAccess
	AWSSupportAccess
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy

OU-Hauptkonto: Rollen und Richtlinien für Verwaltungskonten

Rolle	Richtlinie oder Richtlinien
AWSManagedServicesBillingRole	AMSBillingRichtlinie (AMSBillingRichtlinie).
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(Öffentliche verwaltete AWS-Richtlinie).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportZugriff (Öffentliche AWS-verwaltete Richtlinie).
AWSManagedServicesChangeManagementRole (Version des Verwaltungskontos)	ReadOnlyAccess
	AWSSupportAccess
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy
	AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

OU-Hauptkonto: Rollen und Richtlinien für Netzwerkkonten

Rolle	Richtlinie oder Richtlinien
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(Öffentliche verwaltete AWS-Richtlinie).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportZugriff (Öffentliche AWS-verwaltete Richtlinie).
AWSManagedServicesChangeManagementRole (Version des Netzwerkkontos)	ReadOnlyAccess

Rolle	Richtlinie oder Richtlinien
	AWSSupportAccess
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy
	AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

Rollen von Anwendungskonten

Anwendungskontorollen werden auf Ihre anwendungsspezifischen Konten angewendet.

Anwendungskonto: Rollen und Richtlinien

Rolle	Richtlinie oder Richtlinien
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(Öffentliche verwaltete AWS-Richtlinie).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportZugriff (Öffentliche AWS-verwaltete Richtlinie). Diese Richtlinie bietet Zugriff auf alle Support-Aktivitäten und Ressourcen. Weitere Informationen finden Sie unter Erste Schritte mit AWS Support.
AWSManagedServicesSecurityOpsRole	ReadOnlyAccess
	AWSSupportBeispiel für Access Diese Richtlinie bietet Zugriff auf alle Support-Aktivitäten und Ressourcen.

Rolle	Richtlinie oder Richtlinien
	AWSCertificateManagerFullAccess Informationen, (Öffentliche verwaltete AWS-Richtlinie)
	AWSWAFFullAccess Informationen, (Öffentliche AWS-verwaltete Richtlinie). Diese Richtlinie gewährt vollen Zugriff auf AWS-WAF-Ressourcen.
	AMSSecretsManagerSharedPolicy
AWSManagedServicesChangeManagementRole (Version des Anwendungskontos)	ReadOnlyAccess
	AWSSupportZugriff (Öffentliche AWS-verwaltete Richtlinie). Diese Richtlinie bietet Zugriff auf alle Support-Aktivitäten und Ressourcen. Weitere Informationen finden Sie unter Erste Schritte mit AWS Support.
	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AMSReservedInstancesPolicy
	AMSS3Richtlinie
AWSManagedServicesAdminRole	ReadOnlyAccess
	AWSSupportAccess
	AMSChangeManagementInfrastructurePolicy
	AWSMarketplaceManageSubscriptions
	AMSSecretsManagerSharedPolicy

Rolle	Richtlinie oder Richtlinien
	AMSChangeManagementPolicy
	AWSCertificateManagerFullAccess
	AWSWAFFullAccess
	AMSS3Richtlinie
	AMSReservedInstancesPolicy

Beispiele für Richtlinien

Für die meisten verwendeten Richtlinien werden Beispiele bereitgestellt. Um die ReadOnlyAccess Richtlinie einzusehen (die Seiten lang ist, da sie nur Lesezugriff auf alle AWS Services bietet), können Sie diesen Link verwenden, wenn Sie ein aktives AWS-Konto haben:. ReadOnlyAccess Außerdem ist hier eine komprimierte Version enthalten.

AMSBillingRichtlinie

`AMSBillingPolicy`

Die neue Rolle „Abrechnung“ kann von Ihrer Buchhaltungsabteilung verwendet werden, um Rechnungsinformationen oder Kontoeinstellungen im Verwaltungskonto einzusehen und zu ändern. Sie verwenden diese Rolle, um auf Informationen wie alternative Kontakte zuzugreifen, die Nutzung der Kontoressourcen einzusehen, Ihre Abrechnung im Auge zu behalten oder sogar Ihre Zahlungsmethoden zu ändern. Diese neue Rolle umfasst alle Berechtigungen, die auf der Webseite AWS Billing IAM-Aktionen aufgeführt sind.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "aws-portal:ViewBilling",
                "aws-portal:ModifyBilling"
            ],
```

```
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToBilling"
        },
        {
            "Action": [
                "aws-portal:ViewAccount",
                "aws-portal:ModifyAccount"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToAccountSettings"
        },
        {
            "Action": [
                "budgets:ViewBudget",
                "budgets:ModifyBudget"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToAccountBudget"
        },
        {
            "Action": [
                "aws-portal:ViewPaymentMethods",
                "aws-portal:ModifyPaymentMethods"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPaymentMethods"
        },
        {
            "Action": [
                "aws-portal:ViewUsage"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToUsage"
        },
        {
            "Action": [
                "cur:DescribeReportDefinitions",
                "cur:PutReportDefinition",
                "cur:DeleteReportDefinition",
```

```
                "cur:ModifyReportDefinition"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToCostAndUsageReport"
        },
        {
            "Action": [
                "pricing:DescribeServices",
                "pricing:GetAttributeValues",
                "pricing:GetProducts"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPricing"
        },
        {
            "Action": [
                "ce:*",
                "compute-optimizer:*"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToCostExplorerComputeOptimizer"
        },
        {
            "Action": [
                "purchase-orders:ViewPurchaseOrders",
                "purchase-orders:ModifyPurchaseOrders"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPurchaseOrders"
        },
        {
            "Action": [
                "redshift:AcceptReservedNodeExchange",
                "redshift:PurchaseReservedNodeOffering"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToRedshiftAction"
        },
        {
```

```
            "Action": "savingsplans:*",
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AWSSavingsPlansFullAccess"
        }
    ]
}
```

AMSChangeManagementReadOnlyPolicy

`AMSChangeManagementReadOnlyPolicy`

Berechtigungen zum Einsehen aller AMS-Änderungstypen und des Verlaufs der angeforderten Änderungstypen.

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

`AMSMasterAccountSpecificChangeManagementInfrastructurePolicy`

Berechtigungen zum Anfordern des Änderungstyps Deployment | Verwaltete landing zone | Verwaltungskonto | Anwendungskonto erstellen (mit VPC).

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

`AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy`

Berechtigungen zum Anfordern der Bereitstellung | Verwaltete landing zone | Netzwerkkonto | Änderungstyp der Anwendungsroutentabelle erstellen.

AMSChangeManagementInfrastructurePolicy

`AMSChangeManagementInfrastructurePolicy`(für die Verwaltung | Andere | Andere CTs)

Berechtigungen zum Anfordern der Verwaltung | Andere | Andere | Erstellung und Verwaltung | Andere | Andere | Änderungstypen aktualisieren.

AMSSecretsManagerSharedPolicy

`AMSSecretsManagerSharedPolicy`

Berechtigungen zum Einsehen von passwords/hashes Geheimnissen, die von AMS geteilt wurden AWS Secrets Manager (z. B. Passwörter für die Infrastruktur zu Prüfungszwecken).

Berechtigungen zum Erstellen von password/hashes Geheimnissen zur Weitergabe an AMS. (zum Beispiel Lizenzschlüssel für Produkte, die bereitgestellt werden müssen).

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
   "Sid": "AllowAccessToSharedNameSpaces",
   "Effect": "Allow",
   "Action": "secretsmanager:*",
   "Resource": [
    "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
    "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
   ]
  },
  {
   "Sid": "DenyGetSecretOnCustomerNamespace",
   "Effect": "Deny",
   "Action": "secretsmanager:GetSecretValue",
   "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  },
  {
   "Sid": "AllowReadAccessToAMSNameSpace",
   "Effect": "Deny",
   "NotAction": [
    "secretsmanager:Describe*",
    "secretsmanager:Get*",
    "secretsmanager:List*"
   ],
   "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
  }
 ]
}
```

AMSChangeManagementPolicy

`AMSChangeManagementPolicy`

Berechtigungen zum Anfordern und Anzeigen aller AMS-Änderungstypen sowie des Verlaufs der angeforderten Änderungstypen.

AMSReservedInstancesPolicy

`AMSReservedInstancesPolicy`

Berechtigungen zur Verwaltung von Amazon EC2 Reserved Instances; Preisinformationen finden Sie unter Amazon EC2 Reserved Instances.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Sid": "AllowReservedInstancesManagement",
  "Effect": "Allow",
  "Action": [
   "ec2:ModifyReservedInstances",
   "ec2:PurchaseReservedInstancesOffering"
  ],
  "Resource": [
   "*"
  ]
 }]
}
```

AMSS3Richtlinie

`AMSS3Policy`

Berechtigungen zum Erstellen und Löschen von Dateien aus vorhandenen Amazon S3 S3-Buckets.

> **Note**
>
> Diese Berechtigungen gewähren nicht die Möglichkeit, S3-Buckets zu erstellen. Dies muss mit dem Änderungstyp Deployment | Erweiterte Stack-Komponenten | S3-Speicher | Create erfolgen.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:PutObject"
            ],
            "Resource": "*"
        }
    ]
}
```

AWSSupportZugriff

`AWSSupportAccess`

Voller Zugriff auf Support. Weitere Informationen finden Sie unter Erste Schritte mit Support. Informationen zum Premium-Support finden Sie unter Support.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "support:*"
  ],
  "Resource": "*"
 }]
}
```

AWSMarketplaceManageSubscriptions

`AWSMarketplaceManageSubscriptions`(Öffentlich AWS verwaltete Richtlinie)

Berechtigungen zum Abonnieren, Abbestellen und Ansehen von AWS Marketplace Abonnements.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Action": [
   "aws-marketplace:ViewSubscriptions",
   "aws-marketplace:Subscribe",
   "aws-marketplace:Unsubscribe"
  ],
  "Effect": "Allow",
  "Resource": "*"
 }]
}
```

AWSCertificateManagerFullAccess

`AWSCertificateManagerFullAccess`

Voller Zugriff auf AWS Certificate Manager. Weitere Informationen finden Sie unter AWS Certificate Manager.

`AWSCertificateManagerFullAccess`Informationen, (Öffentliche AWS-verwaltete Richtlinie).

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "acm:*"
  ],
  "Resource": "*"
 }]
}
```

AWSWAFFullZugriff

`AWSWAFFullAccess`

Voller Zugriff auf AWS WAF. Weitere Informationen finden Sie unter AWS WAF - Web Application Firewall.

`AWSWAFFullAccess`Informationen, (Öffentlich AWS verwaltete Richtlinie). Diese Richtlinie gewährt vollen Zugriff auf AWS WAF Ressourcen.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Action": [
   "waf:*",
   "waf-regional:*",
   "elasticloadbalancing:SetWebACL"
  ],
  "Effect": "Allow",
  "Resource": "*"
 }]
}
```

ReadOnlyAccess

`ReadOnlyAccess`

Schreibgeschützter Zugriff auf alle AWS Dienste und Ressourcen auf der AWS Konsole. Wenn ein neuer Dienst AWS gestartet wird, aktualisiert AMS die ReadOnlyAccess Richtlinie, um Nur-Lese-Berechtigungen für den neuen Dienst hinzuzufügen. Die aktualisierten Berechtigungen werden auf alle Auftraggeber-Entitäten angewendet, an die die Richtlinie angefügt ist.

Dies gewährt nicht die Möglichkeit, sich bei EC2 Hosts oder Datenbank-Hosts anzumelden.

Wenn Sie eine aktive Richtlinie haben AWS-Konto, können Sie diesen Link verwenden ReadOnlyAccess, um die gesamte ReadOnlyAccess Richtlinie einzusehen. Die gesamte ReadOnlyAccess Richtlinie ist sehr lang, da sie nur Lesezugriff für alle bietet. AWS-Services Das Folgende ist ein teilweiser Auszug der Richtlinie. ReadOnlyAccess

Single-Account-Landingzone (SALZ): Die standardmäßigen, unangepassten Benutzerrollenrichtlinien für Single-Account-Landingzonen von AMS finden Sie unter SALZ: Standard-IAM-Benutzerrolle Weiter.

SALZ: Standard-IAM-Benutzerrolle

JSON-Richtlinienerklärungen für die standardmäßige AMS-Landingzone-Benutzerrolle mit einem Konto.

> **Note**
>
> Die SALZ-Standardbenutzerrolle ist anpassbar und kann je nach Konto unterschiedlich sein. Anweisungen zur Suche nach Ihrer Rolle finden Sie hier.

Im Folgenden finden Sie ein Beispiel für die standardmäßige SALZ-Benutzerrolle. Führen Sie den `get-role`Befehl aus, um sicherzustellen, dass Sie die Richtlinien für Sie festgelegt haben. Oder melden Sie sich bei der AWS Identity and Access Management Konsole unter an https://console.aws.amazon.com/iam/und wählen Sie dann Rollen aus.

Die Rolle „Nur Lesen“ für den Kunden ist eine Kombination aus mehreren Richtlinien. Es folgt eine Aufschlüsselung der Rolle (JSON).

Audit-Richtlinie für Managed Services:

ReadOnly IAM-Richtlinie für Managed Services

Benutzerrichtlinie für Managed Services

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
     "Sid": "AllowCustomerToListTheLogBucketLogs",
     "Effect": "Allow",
     "Action": [
       "s3:ListBucket"
     ],
     "Resource": [
       "arn:aws:s3:::mc-a*-logs-*"
     ],
     "Condition": {
       "StringLike": {
         "s3:prefix": [
           "aws/*",
```

```
            "app/*",
            "encrypted",
            "encrypted/",
            "encrypted/app/*"
          ]
        }
      }
    },
    {
      "Sid": "BasicAccessRequiredByS3Console",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Sid": "AllowCustomerToGetLogs",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/aws/*",
        "arn:aws:s3:::mc-a*-logs-*/encrypted/app/*"
      ]
    },
    {
      "Sid": "AllowAccessToOtherObjects",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject*",
        "s3:Get*",
        "s3:List*",
        "s3:PutObject*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
```

```
      "Sid": "AllowCustomerToListTheLogBucketRoot",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:prefix": [
            "",
            "/"
          ]
        }
      }
    },
    {
      "Sid": "AllowCustomerCWLConsole",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Sid": "AllowCustomerCWLAccessLogs",
      "Effect": "Allow",
      "Action": [
        "logs:FilterLogEvents",
        "logs:GetLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/*",
        "arn:aws:logs:*:*:log-group:/infra/*",
        "arn:aws:logs:*:*:log-group:/app/*",
        "arn:aws:logs:*:*:log-group:RDSOSMetrics:*:*"
      ]
    },
    {
      "Sid": "AWSManagedServicesFullAccess",
```

```
      "Effect": "Allow",
      "Action": [
        "amscm:*",
        "amsskms:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "ModifyAWSBillingPortal",
      "Effect": "Allow",
      "Action": [
        "aws-portal:Modify*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "DenyDeleteCWL",
      "Effect": "Deny",
      "Action": [
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Sid": "DenyMCCWL",
      "Effect": "Deny",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/mc/*"
      ]
```

```
    },
    {
      "Sid": "DenyS3MCNamespace",
      "Effect": "Deny",
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/encrypted/mc/*",
        "arn:aws:s3:::mc-a*-logs-*/mc/*",
        "arn:aws:s3:::mc-a*-logs-*-audit/*",
        "arn:aws:s3:::mc-a*-internal-*/*",
        "arn:aws:s3:::mc-a*-internal-*"
      ]
    },
    {
      "Sid": "ExplicitDenyS3CfnBucket",
      "Effect": "Deny",
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::cf-templates-*"
      ]
    },
    {
      "Sid": "DenyListBucketS3LogsMC",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "auditlog/*",
            "encrypted/mc/*",
            "mc/*"
          ]
        }
      }
    },
```

```
    {
      "Sid": "DenyS3LogsDelete",
      "Effect": "Deny",
      "Action": [
        "s3:Delete*",
        "s3:Put*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/*"
      ]
    },
    {
      "Sid": "DenyAccessToKmsKeysStartingWithMC",
      "Effect": "Deny",
      "Action": [
        "kms:*"
      ],
      "Resource": [
        "arn:aws:kms::*:key/mc-*",
        "arn:aws:kms::*:alias/mc-*"
      ]
    },
    {
      "Sid": "DenyListingOfStacksStartingWithMC",
      "Effect": "Deny",
      "Action": [
        "cloudformation:*"
      ],
      "Resource": [
        "arn:aws:cloudformation:*:*:stack/mc-*"
      ]
    },
    {
      "Sid": "AllowCreateCWMetricsAndManageDashboards",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:PutMetricData"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowCreateandDeleteCWDashboards",
```

```
      "Effect": "Allow",
      "Action": [
        "cloudwatch:DeleteDashboards",
        "cloudwatch:PutDashboard"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Gemeinsame Richtlinie für Customer Secrets Manager

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSecretsManagerListSecrets",
      "Effect": "Allow",
      "Action": "secretsmanager:listSecrets",
      "Resource": "*"
    },
    {
      "Sid": "AllowCustomerAdminAccessToSharedNameSpaces",
      "Effect": "Allow",
      "Action": "secretsmanager:*",
      "Resource": [
        "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
        "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
      ]
    },
   {
      "Sid": "DenyCustomerGetSecretCustomerNamespace",
      "Effect": "Deny",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
    },
    {
      "Sid": "AllowCustomerReadOnlyAccessToAMSNameSpace",
      "Effect": "Deny",
```

```
      "NotAction": [
        "secretsmanager:Describe*",
        "secretsmanager:Get*",
        "secretsmanager:List*"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
    }
  ]
}
```

Abonnementrichtlinie für Customer Marketplace

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowMarketPlaceSubscriptions",
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Standard-Firewallregeln für den Zugriff

Dies sind die Standard-Firewallregeln, die für den Zugriff auf Ihre Instances erforderlich sind.

> **Note**
>
> Informationen zu Firewallregeln und Ports, die für die Einrichtung einer einseitigen AD-Vertrauensstellung erforderlich sind, finden Sie im AMS-Sicherheitsleitfaden, indem Sie zur

AWS Artifact-Konsole -> Registerkarte Berichte gehen und nach AWS Managed Services suchen.

Ports für Linux-Stack-Instances

Diese Regeln sind für Ihre Authentifizierung bei AMS Linux-Stacks erforderlich.

Die Linux-Instance portiert Regeln VON: Linux-Stack-Instanz ZU: CORP-Domänencontroller

Port	Protokoll	Service	Richtung
389	TCP	LDAP	Ingress
389	UDP	LDAP	Ingress
88	TCP	Kerberos	Ingress
88	UDP	Kerberos	Ingress

Anschlüsse für Windows-Stack-Instanzen

Diese Regeln sind für Ihre Authentifizierung bei AMS Windows Stacks erforderlich.

VON: Windows Stack-Instanz ZU: CORP Domain Controller

Port	Protokoll	Service	Richtung
88	TCP | UDP	Kerberos	Eingang und Ausgang
135	TCP | UDP	DCE/RPC-Locator-Dienst	Eingang und Ausgang
389	TCP | UDP	LDAP	Eingang und Ausgang
3268	TCP | UDP	msft-gc, Microsoft Global Catalog (LDAP-Dienst, der Daten aus Active Directory-Gesamtstrukturen enthält)	Eingang und Ausgang

Port	Protokoll	Service	Richtung
445	TCP	Microsoft-DS Active Directory, Windows-Freigaben	Eingang und Ausgang
49152–65535	TCP	Dynamische oder private Ports, die nicht bei IANA registriert werden können. Dieser Bereich wird für private oder maßgeschneiderte Dienste oder temporäre Zwecke sowie für die automatische Zuweisung kurzlebiger Ports verwendet.	Eintritt und Austritt

Servicemanagement in AWS Managed Services

Themen

- Kontoverwaltung in AWS Managed Services
- Beginn des Dienstes in AWS Managed Services
- Kundenbeziehungsmanagement (CRM)
- Kostenoptimierung in AWS Managed Services
- Servicezeiten in AWS Managed Services
- Hilfe zu AWS Managed Services erhalten

So funktioniert der AMS-Service für Sie.

Kontoverwaltung in AWS Managed Services

In diesem Abschnitt wird die AMS-Kontoverwaltung behandelt.

Ihnen wird ein Cloud Service Delivery Manager (CSDM) zugewiesen, der Ihnen bei AMS beratend zur Seite steht und über ein detailliertes Verständnis Ihres Anwendungsfalls und Ihrer Technologiearchitektur für die verwaltete Umgebung verfügt. CSDMs arbeiten mit Kundenbetreuern, technischen Kundenbetreuern, AWS Managed Services Services-Cloudarchitekten (CAs) und AWS-Lösungsarchitekten (SAs) zusammen, um bei der Einführung neuer Projekte zu helfen und Empfehlungen zu bewährten Methoden während der gesamten Softwareentwicklungs- und Betriebsprozesse zu geben. Das CSDM ist die wichtigste Anlaufstelle für AMS. Die wichtigsten Aufgaben Ihres CSDM sind:

- Organisieren und leiten Sie monatliche Besprechungen zur Servicebewertung mit Kunden.
- Geben Sie Einzelheiten zur Sicherheit, zu Softwareupdates für die Umgebung und zu Optimierungsmöglichkeiten an.
- Machen Sie sich für Ihre Anforderungen, einschließlich Funktionsanfragen für AMS, stark.
- Beantworten und lösen Sie Anfragen zur Abrechnung und Serviceberichterstattung.
- Bieten Sie Einblicke für Empfehlungen zur Finanz- und Kapazitätsoptimierung.

Beginn des Dienstes in AWS Managed Services

Beginn des Service: Das Datum des Servicebeginns für ein AWS Managed Services Services-Konto ist der erste Tag des ersten Kalendermonats, nach dem AWS Sie darüber informiert, dass die in den Onboarding-Anforderungen für dieses AWS Managed Services Services-Konto festgelegten Aktivitäten abgeschlossen wurden. Sofern AWS eine solche Benachrichtigung nach dem 20. Tag eines Kalendermonats sendet, ist das Datum des Servicebeginns der erste Tag des zweiten Kalendermonats nach dem Datum dieser Benachrichtigung.

Beginn des Dienstes

- R steht für verantwortliche Partei, die die Arbeit zur Erfüllung der Aufgabe erledigt.
- I steht für informiert, d. h. eine Partei, die über den Fortschritt informiert wird, oft erst, wenn die Aufgabe oder das Ergebnis abgeschlossen ist.

Beginn der Dienstleistung

Schritt #	Titel des Schritts	Beschreibung	Custome	AMS
1.	Übergabe des AWS-Kontos an Kunden	Der Kunde erstellt ein neues AWS-Konto und übergibt es an AWS Managed Services	R	I
2.	AWS Managed Services Services-Konto — Design	Finalisieren Sie den Entwurf des AWS Managed Services Services-Kontos	I	R
3.	AWS Managed Services Services-Konto — erstellen	Ein AWS Managed Services Services-Konto wird gemäß dem Design in Schritt 2 erstellt	I	R

Kundenbeziehungsmanagement (CRM)

AWS Managed Services (AMS) bietet einen CRM-Prozess (Customer Relationship Management), um sicherzustellen, dass eine klar definierte Beziehung zu Ihnen aufgebaut und aufrechterhalten wird. Die Grundlage dieser Beziehung bildet das Wissen von AMS über Ihre Geschäftsanforderungen. Der CRM-Prozess ermöglicht ein genaues und umfassendes Verständnis von:

- Ihre Geschäftsanforderungen und wie Sie diese Bedürfnisse erfüllen können
- Ihre Fähigkeiten und Einschränkungen
- AMS und Ihre unterschiedlichen Verantwortlichkeiten und Pflichten

Der CRM-Prozess ermöglicht es AMS, einheitliche Methoden zur Erbringung von Dienstleistungen für Sie und zur Steuerung Ihrer Beziehung zu AMS zu verwenden. Der CRM-Prozess umfasst:

- Identifizierung Ihrer wichtigsten Stakeholder
- Aufbau eines Führungsteams
- Durchführung und Dokumentation von Besprechungen zur Leistungsbeurteilung mit Ihnen
- Bereitstellung eines formellen Servicebeschwerdeverfahrens mit einem Eskalationsverfahren
- Implementierung und Überwachung Ihres Zufriedenheits- und Feedback-Prozesses
- Verwaltung Ihres Vertrags

CRM-Prozess

Der CRM-Prozess umfasst die folgenden Aktivitäten:

- Identifizieren und Verstehen Ihrer Geschäftsprozesse und Bedürfnisse. Ihre Vereinbarung mit AMS identifiziert Ihre Stakeholder.
- Definition der Dienstleistungen, die gemäß Ihren Bedürfnissen und Anforderungen erbracht werden sollen.
- Treffen mit Ihnen im Rahmen der Serviceüberprüfung, um alle Änderungen des AMS-Serviceumfangs, der SLA, des Vertrags und Ihrer Geschäftsanforderungen zu besprechen. Es können vorläufige Treffen mit Ihnen abgehalten werden, um Leistungen, Erfolge, Probleme und Aktionspläne zu besprechen.
- Überwachen Sie Ihre Zufriedenheit mithilfe unserer Kundenzufriedenheitsumfrage und des Feedbacks, das Sie bei Besprechungen erhalten.

- Berichterstattung über die Leistung in monatlichen, intern gemessenen Leistungsberichten.
- Wir besprechen den Service gemeinsam mit Ihnen, um Verbesserungsmöglichkeiten zu ermitteln. Dazu gehört auch die regelmäßige Kommunikation mit Ihnen über das Niveau und die Qualität des erbrachten AMS-Dienstes.

CRM-Besprechungen

Die AMS Cloud Service Delivery Manager (CSDMs) führen regelmäßig Treffen mit Ihnen durch, um die einzelnen Servicebereiche (Betrieb, Sicherheit und Produktinnovationen) und die Führungsqualitäten (SLA-Berichte, Zufriedenheitsmaßnahmen und Änderungen Ihrer Geschäftsanforderungen) zu besprechen.

Meeting	Zweck	Mode	Teilnehmer
Wöchentliche Statusüberprüfung (optional)	Ausstehende Probleme oder Vorfälle, Patches, Sicherheitsereignisse, Problemaufzeichnungen Betriebstrend über 12 Wochen (+/- 6) Bedenken des Anwendungsbetreibers Zeitplan für das Wochenende	Kunde vor Ort location/ Telecom/Chime	AMS: CSDM und Cloud-Architekt (CA) Vom Kunden zugewiesene Teammitglieder (z. B.: Cloud-/ Infrastruktur-, Anwendungssupport-, Architekturteams usw.)
Monatlicher Geschäftsbericht	Überprüfen Sie die Leistung auf Serviceniveau (Berichte, Analysen und Trends) Finanzielle Analyse Produkt-Roadmap BESETZUNG	Kunde vor Ort location/ Telecom/Chime	AMS: CSDM, Cloud-Architekt (CA), AMS-Kundenbetreuer, Technischer Produktmanager (TPM) von AMS (optional), AMS

Meeting	Zweck	Mode	Teilnehmer
			OPS-Manager (optional) Sie: Vertreter des Anwendungsbetreibers
Vierteljährlicher Geschäftsbericht	Leistung und Trends der Scorecard und des Service Level Agreements (SLA) (6 Monate) Künftige Pläne/Migrationen für die kommenden 3/6/9/12 Monate Risiko und Risikominderung Wichtige Verbesserungsinitiativen Artikel der Produkt-Roadmap Auf die zukünftige Ausrichtung ausgerichtete Möglichkeiten Finanzdaten Initiativen zur Kosteneinsparung Geschäftsoptimierung	Standort des Kunden vor Ort	AMS: CSDM, Cloud-Architekt, AMS-Kundenbetreuer, AMS-Serviceleiter, AMS-Betriebsleiter Sie: Vertreter des Anwendungsbetreibers, Servicemitarbeiter, Serviceleiter

Vereinbarungen für CRM-Treffen

Das AMS CSDM ist für die Dokumentation des Treffens verantwortlich, einschließlich:

- Erstellung der Tagesordnung, einschließlich Aktionspunkten, Themen und Teilnehmerlisten.
- Erstellung der Liste der Aktionspunkte, die bei jeder Sitzung überprüft werden, um sicherzustellen, dass die Punkte termingerecht abgeschlossen und gelöst werden.

- Verteilung des Sitzungsprotokolls und der Liste der Aktionspunkte per E-Mail an die Besprechungsteilnehmer innerhalb eines Werktages nach der Besprechung.
- Speichern von Besprechungsprotokollen im entsprechenden Dokumentenspeicher.

In Ermangelung des CSDM erstellt und verteilt der AMS-Vertreter, der die Sitzung leitet, das Protokoll.

> **Note**
>
> Ihr CSDM arbeitet mit Ihnen zusammen, um Ihre Kontoverwaltung festzulegen.

Monatliche CRM-Berichte

Ihr AMS CSDM bereitet monatliche Präsentationen zur Serviceleistung vor und versendet sie. Die Präsentationen enthalten Informationen zu folgenden Themen:

- Datum des Berichts
- Zusammenfassung und Einblicke:
  - Wichtige Hinweise: Gesamtzahl und Anzahl der aktiven Stacks, Status der Stack-Patches, Onboarding-Status des Accounts (nur beim Onboarding), Zusammenfassungen der kundenspezifischen Probleme
  - Leistung: Statistiken zur Behebung von Vorfällen, zu Warnmeldungen, Patches, Änderungsanfragen (RFCs), Serviceanfragen sowie zur Verfügbarkeit von Konsole und API
  - Probleme, Herausforderungen, Bedenken und Risiken: Status der kundenspezifischen Probleme
  - Künftige Themen: Kundenspezifische Onboarding- oder Problemlösungspläne
- Verwaltete Ressourcen: Grafiken und Kreisdiagramme von Stapeln
- AMS-Metriken: Überwachungs- und Ereignismetriken, Vorfallkennzahlen, AMS-SLA-Einhaltungskennzahlen, Serviceanforderungskennzahlen, Change-Management-Metriken, Speichermetriken, Kontinuitätskennzahlen, Trusted Advisor Advisor-Metriken und Kostenübersichten (auf verschiedene Arten dargestellt). Anfragen zu Funktionen. Kontaktinformationen.

> **Note**
>
> Zusätzlich zu den beschriebenen Informationen informiert Sie Ihr CSDM auch über jede wesentliche Änderung des Geltungsbereichs oder der Bedingungen, einschließlich der Inanspruchnahme von Subunternehmern durch AMS für betriebliche Aktivitäten.
> AMS generiert Berichte über Patches und Backups, die Ihr CSDM in Ihren monatlichen Bericht aufnimmt. Als Teil des Systems zur Berichtsgenerierung fügt AMS Ihrem Konto einige Infrastrukturen hinzu, auf die Sie nicht zugreifen können:
>
> - Ein S3-Bucket mit den gemeldeten Rohdaten
> - Eine Athena-Instanz mit Abfragedefinitionen zum Abfragen der Daten
> - Ein Glue Crawler zum Lesen der Rohdaten aus dem S3-Bucket

Kostenoptimierung in AWS Managed Services

AWS Managed Services stellt Ihnen im Rahmen Ihrer monatlichen Geschäftsberichte jeden Monat detaillierte Berichte zur Kostenauslastung und zu Einsparungen bereit (MBRs).

AMS folgt einer Reihe von Standardprozessen und -mechanismen, um Möglichkeiten zur Kosteneinsparung in Ihren verwalteten Konten zu ermitteln und Sie bei der Planung und Einführung der Änderungen zur Optimierung Ihrer AWS-Ausgaben zu unterstützen.

> **Note**
>
> AMS entwickelt derzeit ein Video, das Ihnen bei der Kostenoptimierung helfen soll. Der erste Schritt besteht darin, Ihnen ein PDF und eine Excel-Tabelle mit bewährten Methoden zur Kostenoptimierung zur Verfügung zu stellen. Um auf diese Ressourcen zuzugreifen, öffnen Sie die ZIP-Datei mit der Kurzanleitung zur Kostenoptimierung.

Framework zur Kostenoptimierung

AMS verfolgt gemeinsam mit Ihnen einen dreistufigen Ansatz, um Ihre AWS-Kosten zu optimieren:

1. Identifizieren Sie Möglichkeiten zur Kostenoptimierung in Ihrer verwalteten Umgebung
2. Stellen Sie Ihnen einen Plan zur Kostenoptimierung vor
3. Unterstützen Sie uns dabei, die Kostenoptimierung auf messbare Weise zu erreichen

Identifizieren Sie Möglichkeiten zur Kostenoptimierung in der verwalteten Umgebung

AMS verwendet AWS native Tools wie Cost Explorer und Trusted Advisor und nutzt gleichzeitig über 20 Kosteneinsparungsmuster in den Bereichen Architekturoptimierung, EC2 instanzielle und AWS kundenorientierte Optimierung, um maßgeschneiderte Kosteneinsparungsempfehlungen für Sie zu erstellen.

Einige der Optimierungsempfehlungen beinhalten die folgenden.

Empfehlungen zur architektonischen Optimierung:

- Optimale Nutzung der S3-Speicherklasse: Amazon S3 bietet eine Reihe von Speicherklassen, um verschiedene Workload-Anforderungen in Bezug auf Datenzugriff, Ausfallsicherheit und Kosten zu erfüllen. S3 Intelligent-Tiering und S3-Speicherklassenanalysen auf der Grundlage der Workload-Anforderungen ermöglichen es Ihnen, die S3-Kosten effizient zu verwalten.
- Verwendung von Caching-Architekturen: Durch die Nutzung von Cache-Instanzen können Sie gegebenenfalls einige Datenbankinstanzen ersetzen und gleichzeitig Ihre IOPS-Anforderungen erfüllen.
- Einsparungen beim EBS-Upgrade: Die Migration Ihrer EBS-Volumes von gp2 auf gp3 bietet Kosteneinsparungen von bis zu 20% und Sie können unabhängig von der Volume-Größe von einer vorhersehbaren Basisleistung von 3.000 IOPS und 125 MiB/s profitieren.
- Einsatz von Elastizität: Die Funktionen zur auto-scaling AWS ermöglichen eine effektive Ressourcennutzung und Möglichkeiten zur Kostenoptimierung. Durch die regelmäßige Überprüfung und Aktualisierung der Richtlinien zur Instanzskalierung je nach Bedarf können weitere Kosten eingespart werden.

EC2 instanzorientierte Empfehlungen

- Richtige Dimensionierung von Instanzen: Die Empfehlungen konzentrierten sich auf die Dimensionierung der Instanzen und die optimale Konfiguration auf der Grundlage der Nutzung. Zu den Empfehlungen gehören auch die Nutzung der Amazon EC2 Auto Scaling Scaling-Funktion und das Ersetzen von EC2 Instances, sofern zutreffend, durch statische Webinhalte auf Amazon S3 usw. AWS Lambda
- Instance-Planung: Die Verwendung von AMS Resource Scheduler zum automatischen Starten und Stoppen von Instances auf der Grundlage eines Zeitplans trägt dazu bei, die Kosten einzudämmen, insbesondere für Instances, die nicht zur Produktion gehören und außerhalb der Geschäftszeiten nicht genutzt werden.

- Sparpläne abonnieren: Der Sparplan ist die einfachste Möglichkeit, bei der Nutzung zu sparen. AWS Die EC2 Instance-Sparpläne bieten bis zu 72% Einsparungen bei der Nutzung Ihrer Amazon EC2 Instances im Vergleich zu On-Demand-Preisen. Die Amazon SageMaker AI-Sparpläne bieten bis zu 64% Ersparnis bei der Nutzung Ihrer Amazon SageMaker AI-Services. AMS gibt Ihnen auf der Grundlage Ihrer AWS Ressourcennutzung entsprechende Empfehlungen zu Sparplänen.
- Hinweise zur Nutzung und Nutzung von Reserved Instances (RI): Amazon EC2 Reserved Instances (RI) bieten einen erheblichen discount (bis zu 75%) im Vergleich zu On-Demand-Preisen und ermöglichen eine Kapazitätsreservierung, wenn sie in einer bestimmten Availability Zone verwendet werden.
- Nutzung von Spot-Instances: Fehlertolerante Workloads können Spot-Instances nutzen und die Preise um bis zu 90% senken.
- Kündigung von Instances im Leerlauf: Identifizierung und Meldung von Instances, die sich im Leerlauf befinden oder nur eine geringe Auslastung aufweisen und beendet werden können.

Kundenorientierte Empfehlungen

- Kontobereinigung: Auf Kontoebene identifiziert AMS auch nicht genutzte EBS-Volumes, doppelte CloudTrail Pfade, leere Konten mit ungenutzten Ressourcen usw. und gibt Empfehlungen für die Bereinigung.
- SLA-Empfehlungen: Darüber hinaus überprüft AMS Ihre Plus- und Premium-Konten regelmäßig und empfiehlt, die richtige SLA-Stufe für die Konten zu wählen.
- Optimierung der AMS-Automatisierung: AMS optimiert kontinuierlich die AMS-Automatisierung und die Infrastruktur, die für die Bereitstellung von AMS-Diensten verwendet wird.

Präsentieren Sie Kunden und unterstützen Sie sie bei der Planung

AMS führt monatliche Geschäftsüberprüfungen (MBRs) mit den wichtigsten Kundenakteuren durch und stellt die identifizierten Möglichkeiten, Mechanismen und Empfehlungen zur Kosteneinsparung sowie mögliche Kosteneinsparungen vor. Wir arbeiten weiter mit Ihnen zusammen, um die erforderlichen Änderungen zu planen.

Unterstützung bei der Umsetzung der Empfehlungen und Messung der Kostenauswirkungen

AMS hilft bei der Erzielung und Messung von Kostenauswirkungen und Optimierungsänderungen.

Sie bewerten die Auswirkungen, Risiken und Erfolgskriterien der empfohlenen Änderungen auf die Anwendung und stellen über die AMS-Konsole die entsprechenden Änderungsanträge (RFCs). AMS arbeitet mit Ihnen zusammen und implementiert die Änderungen im Zusammenhang mit der Kostenoptimierung in Ihren verwalteten Konten. AMS misst die Auswirkungen auf die Kosten und bezieht die erzielten Einsparungen in die monatlichen Geschäftsberichte ein (MBRs).

Verantwortungsmatrix für die Kostenoptimierung

Verantwortlichkeiten bei der AMS-Kostenoptimierung.

Kostenoptimierung RACI

Aktivität	Customer	AMS
Zusammentellung von Empfehlungen zur Kosteneinsparung und Erstellung des Berichts	I	R
Vorlage des Kosteneinsparungsberichts	C	R
Planungsänderungen im Zusammenang mit Kostenein	R	C

Aktivität	Customer	AMS
sparungen		
Bewertung der Auswirkungen und des Risikos der Änderung	R	C
Erhebung RFCs zur Umsetzung der Änderungen	R	C
Überprüfung RFCs und Umsetzung der Änderungen	C	R
Testen der Anwendung und Validierung der Änderungsimplementierung	R	C

Aktivität	Customer	AMS
Messung der Kostenauswirkungen nach der Änderung und Präsentation beim Kunden	I	R

Servicezeiten in AWS Managed Services

Funktion	AMS für Fortgeschrittene
	Premium-Stufe
Serviceanfrage	24/7
Verwaltung von Zwischenfällen (P2-P3)	Rund um die
Sicherung und Wiederherstellung	24/7
Patch-Management	24/7
Überwachen und Warnen	24/7
Automatisierte Änderungsanforderung (RFC)	24/7
Nicht automatisierter Änderungsantrag (RFC)	24/7
Manager für die Bereitstellung von Cloud-Diensten (CSDM)	Montag bis Freitag: 08:00 — 17:00 Uhr, lokale Geschäftszeiten

Hilfe zu AWS Managed Services erhalten

AMS unterstützt Sie mit Incident Management, Service Request Management und Change Management 24 Stunden am Tag, 7 Tage die Woche, 365 Tage im Jahr (gemäß dem für das Konto geltenden AMS Service Level Agreement).

Um ein Leistungsproblem mit dem AWS- oder AMS-Service zu melden, das sich auf Ihre verwaltete Umgebung auswirkt, verwenden Sie die AMS-Konsole und reichen Sie einen Vorfallbericht ein. Einzelheiten finden Sie unter Einen Vorfall melden. Allgemeine Informationen zum AMS Incident Management finden Sie unter Reaktion auf Vorfälle.

Verwenden Sie die AMS-Konsole und reichen Sie eine Serviceanfrage ein, um Informationen oder Ratschläge zu erhalten oder zusätzliche Services von AMS in Anspruch zu nehmen. Einzelheiten finden Sie unter Serviceanfrage erstellen. Allgemeine Informationen zu AMS-Serviceanfragen finden Sie unter Verwaltung von Serviceanfragen.

Verwaltungsmodi ändern

AWS Managed Services (AMS) verwendet den Änderungsverwaltungsmodus, um Änderungen in AMS Advanced zu überwachen. Die Änderungsverwaltungsmodi helfen Ihnen dabei, hohe Betriebsstandards für die Umwelt aufrechtzuerhalten, Risiken zu kontrollieren und negative Auswirkungen zu vermeiden. AMS Advanced verfügt über verschiedene Modi, die unterschiedliche Kontroll- und Risikostufen bieten. Alle Modi, mit Ausnahme des vom Kunden verwalteten Modus, werden von AMS verwaltet. Im Folgenden sind die verfügbaren Änderungsverwaltungsmodi aufgeführt:

- RFC-Modus (früher Standard-CM-Modus): Stellt ein RFC-System (Request for Change) und benutzerdefinierte AMS-Änderungstypen () bereit CTs
- Direct Change-Modus: Entspricht dem RFC-Modus, plus Verwendung von AWS APIs und Konsolen zur Erstellung von AMS-verwalteten Ressourcen
- AWS Service Catalog auf AMS: Ähnlich dem Direct Change-Modus, aber anstatt das AMS-Change-Management-System (RFCs) zu verwenden, verwenden Sie AWS Service Catalog, um Ressourcen zu erstellen, die AMS dann verwaltet.
- Entwicklermodus: Wie im Direct Change-Modus werden nur die Ressourcen, die Sie mit AWS APIs und Konsolen erstellen, nicht von AMS verwaltet — Sie sind für deren Verwaltung verantwortlich.
- Self Service Provisioning (SSP) -Modus: Entspricht dem Entwicklermodus, außer dass kein Zugriff auf das AMS-Change-Management-System besteht (nein) RFCs
- Kundenverwalteter Modus: AMS bietet Ihnen eine landing zone mit mehreren Konten, aber die gesamte Ressourcenverwaltung liegt in Ihrer Verantwortung

Das Änderungsmanagementsystem AWS Managed Services (AMS), das die Change Management (CM) -API verwendet, bietet Operationen zur Erstellung und Verwaltung von Change (RFCs) -Anfragen sowohl für Multi-Account-Landingzone-Konten (MALZ) als auch für Single-Account-Landingzone-Konten (SALZ).

Eine Änderungsanforderung (RFC) ist eine Anfrage, die entweder von Ihnen oder AMS über die AMS-Schnittstelle erstellt wird, um eine Änderung an Ihrer verwalteten Umgebung vorzunehmen. Sie enthält eine Change Type (CT) -ID für einen bestimmten Vorgang.

Die AMS Change Management (CM) -API bietet Operationen zur Erstellung und Verwaltung von Change (RFCs) -Anfragen. Sie können sie erstellen, aktualisieren, einreichen, genehmigen, ablehnen

und stornieren RFCs. Die AMS-Operatoren können Inhalte erstellen, aktualisieren, einreichen, genehmigen, zurückweisen, stornieren und RFCs als geschlossen markieren.

Eine Liste der reservierten AMS-Präfixe, die nicht in Tags oder anderen Namen verwendet werden dürfen, finden Sie unter Reservierte Präfixe.

Informationen zu den einzelnen Änderungstypen, einschließlich Schemas und Beispielen, finden Sie in der AMS Change Type Reference.

> **Note**
>
> Alle API-Aufrufe für das Änderungsmanagement werden in AWS aufgezeichnet CloudTrail. Weitere Informationen finden Sie unter Zugreifen auf Ihre Protokolle.

Übersicht der Modi

Verwenden Sie diese Informationen, um den geeigneten AWS Managed Services (AMS) -Modus für das Hosten Ihrer Anwendungen auszuwählen, der auf Ihrer gewünschten Kombination aus Flexibilität und präskriptiver Steuerung basiert, um Ihre Geschäftsergebnisse zu erzielen.

Die Zielgruppe für diese Informationen ist:

- Kundenteams, die für die Strategie und Steuerung ihrer landing zone verantwortlich sind. Diese Informationen helfen dem Team dabei, den Grundstein für eine von AMS verwaltete landing zone mit den AMS-Modi zu legen, die es seinen internen und externen Kunden anbieten möchte.
- Geschäfts- und Anwendungsinhaber, die mit der Migration ihrer Anwendung auf AMS beauftragt sind. Diese Informationen helfen bei der Planung der Anwendungsmigration mit dem passenden AMS-Modus für migrate/host ihre Anwendung. Beachten Sie, dass dieselbe Anwendung in verschiedenen Phasen ihres Software Development Life Cycle (SDLC) -Lebenszyklus in mehr als einem AMS-Modus gehostet werden kann.
- AMS-Partner haben die Aufgabe, Kunden über die verschiedenen Optionen für die Entwicklung und Migration zu AMS zu informieren.

Diese Informationen sind in der Gründungsphase der Einrichtung Ihrer AMS-verwalteten Plattform und beim Übergang von der Grundlagen- zur Migrationsphase Ihrer Cloud-Einführung äußerst nützlich, kurz nachdem die Einführung in AMS abgeschlossen ist und Sie sich auf die Anwendungssteuerung und den Betrieb konzentrieren.

Arten von Modi und Konten in AMS

Die Modi von AWS Managed Services (AMS) können als die Art der Interaktion mit dem AMS-Service im Rahmen des spezifischen Governance-Frameworks für jeden Modus definiert werden. Die Unterschiede zwischen der landing zone, der landing zone mit mehreren Konten oder MALZ und der landing zone mit einem Konto oder SALZ, werden notiert.

> **Note**
>
> Einzelheiten zur Anwendungsbereitstellung und zur Auswahl des richtigen AMS-Modus finden Sie unter AMS-Modi und Anwendungen oder Workloads.
> Praxisnahe Anwendungsfälle der verschiedenen Modi finden Sie unter Anwendungsfälle aus der Praxis für AMS-Modi

Die folgende Tabelle enthält Beschreibungen der Modi pro AMS-Dienst.

AMS-Funktion	RFC-Modus (früher Standard-CM-Modus)/ OOD *	Direkter Änderungsmodus	AWS Service Catalog	Self-Service-Bereitstellung //Entwicklermodus	Vom Kunden verwaltet
Konfiguration der Landezone	MALZ und SALZ	MALZ und SALZ		MALZ und SALZ	
Änderungsmanagement	Planung ändern, manuelle Änderungen überprüfen und Datensatz ändern	Entspricht dem RFC-Modus für Änderungen mit hohem Risiko wie IAM oder Sicherheitsgruppen		Keine	

AMS-Funktion	RFC-Modus (früher Standard-CM-Modus)/ OOD *	Direkter Änderungsmodus	AWS Service Catalog	Self-Service-Bereitstellung //Entwicklermodus	Vom Kunden verwaltet
Protokollierung, Überwachung, Guardrails und Eventmanagement	Ja (unterstützte Ressourcen)			Nein	
Kontinuitätsmanagement	Ja (unterstützte Ressourcen)			Nicht zutreffend/ Nein	Nein
Sicherheitsmanagement	Sicherheitskontrollen auf Instanzebene und Kontrollen auf Kontoebene			Kontrollen auf Kontoebene	Kontrollen auf AWS-Organisationsebene
Patch-Management	Ja			Nicht zutreffend//Nein	Nein
Vorfall- und Problemmanagement	SLA für Reaktion und Lösung für Ressourcen, die von AMS unterstützt werden			Antwort-SLA für die daraus resultierenden Ressourcen	Nein
Berichterstellung	Ja			Nein	

AMS-Funktion	RFC-Modus (früher Standard-CM-Modus)/ OOD *	Direkter Änderungsmodus	AWS Service Catalog	Self-Service-Bereitstellung //Entwicklermodus	Vom Kunden verwaltet
Verwaltung von Serviceanfragen	Ja			Nur Support-Anfragen	Nein

* Operations On Demand (OOD) bietet ein Angebot für Kunden, die den RFC-Modus verwenden, um ihre Änderungen mithilfe spezieller Ressourcen zu verwalten. Weitere Informationen finden Sie im Angebotskatalog für Operations on Demand und wenden Sie sich an Ihren Cloud Service Delivery Manager (CSDM).

> **Note**
>
> Self-Service-Bereitstellungsmodus in AMSund beide AMS Advanced-Entwicklermodus scheinen für eine Anwendung geeignet zu sein, deren komplexe Architektur auf nativen AWS-Services basiert. Bei der Architektur von Workloads gehen Sie je nach Ihrem Geschäftskontext Kompromisse zwischen betrieblicher Exzellenz und Agilität ein. Dies ist eine gute Möglichkeit, über die Auswahl des SSP-Modus oder des Entwicklermodus für Ihre Anwendung nachzudenken. Die Auswahl kann sich auch je nach der SDLC-Phase der Anwendung ändern. Beispiel: Wenn die Anwendung produktionsbereit ist, ist der SSP-Modus aufgrund der strengeren AMS-Richtlinien in diesem Modus möglicherweise die geeignetere Option. Die Schutzmaßnahmen werden in Form von präventiven Kontrollen wie der RFC-basierten Änderungssteuerung für IAM-Updates und auf der Ebene der Anwendungs-OU durchgesetzt. SCPs Diese Geschäftsentscheidungen können Ihre technischen Prioritäten beeinflussen. Sie könnten eine Optimierung vornehmen, um die Flexibilität der Anwendungseigentümer in der „Pre-Prod“ -Phase zu erhöhen, auf Kosten der Verwaltung und des betrieblichen Supports.

MALZ-Architektur und zugehörige AMS-Modi

Die AMS Multi-Account-Landing Zone (MALZ) bietet Ihnen die Möglichkeit, Anwendungskonten (oder Ressourcenkonten) automatisch unter den standardmäßigen Organisationseinheiten (OU) bereitzustellen: vom Kunden verwaltete OU, Managed OU oder Development OU. Die Infrastruktur, die in den Anwendungskonten bereitgestellt wird, die unter diesen Konten erstellt wurden, OUs unterliegt dem spezifischen AMS-Modus, der von diesen Basiskonten angeboten wird. OUs Es ist üblich, in demselben Anwendungskonto eine Mischung aus zwei oder mehr Modi vorzufinden. Beispiel: RFC-Modus und SSP-Modus können in einem AMS-verwalteten Konto koexistieren, das eine Pipeline-Architektur hostet, die aus API Gateway und Lambda für Triggerfunktionen und S3 und SQS für EC2 Aufnahme und Orchestrierung besteht. In diesem Fall würde der SSP-Modus für Lambda und API Gateway gelten.

Abbildung 1 zeigt, wie verschiedene Modi in der Grundversion von AMS angeboten werden. OUs Wenn Sie in AMS ein neues Anwendungskonto beantragen, müssen Sie die Organisationseinheit für das Konto auswählen.

MALZ-Architektur und zugehörige AMS-Modi

AMS nutzt die Grundlagen, die auf den bewährten Methoden von AWS OUs basieren, um Konten mithilfe von Service Control Policies () logisch zu verwalten. SCPs Auf diese Weise kann das Governance-Framework in jedem AMS-Modus durchgesetzt werden. Alle Governance- und Sicherheitsvorkehrungen (in Form von SCPs), die auf das Fundament angewendet werden, werden automatisch OUs auch auf das Fundament angewendet. custom/child OUs Zusätzliche SCPs können für das Kind angefordert werden. OUs Es ist wichtig zu verstehen, dass Anwendungskonten nicht dasselbe sind wie Modi. Modi werden auf die innerhalb der Konten bereitgestellte Infrastruktur angewendet und definieren die betrieblichen Verantwortlichkeiten zwischen AMS und den Kunden.

Abbildung 1: MALZ-Architektur und zugehörige AMS-Modi

> **Note**
>
> „Restriktiv“ bedeutet, dass Sie für diese Programme benutzerdefinierte Richtlinien anfordern können. Diese werden von AMS genehmigt OUs, damit sichergestellt ist, dass sie die Fähigkeit von AMS, optimale Betriebsabläufe zu gewährleisten, nicht beeinträchtigen. case-

by-case Eine ausführliche Liste der AMS-Leitplanken finden Sie unter AMS Guardrails im Benutzerhandbuch.

AMS-Modi und Anwendungen oder Workloads

Berücksichtigen Sie bei der Auswahl des richtigen Modus die Betriebs- und Governance-Anforderungen für Ihre Anwendungen, indem Sie entweder ein neues Anwendungskonto beantragen oder die Anwendung in einem vorhandenen Anwendungskonto hosten. Die Auswahl des geeigneten AMS-Modus für jede Anwendung oder jeden Workload hängt von den folgenden Faktoren ab:

- Die Art der SDLC-Lebenszyklusfunktion, die die Umgebung bereitstellen wird (z. B. Sandbox mit unmoderierten Änderungen, UAT mit einigen häufigen Änderungen, Produktion mit minimalen Änderungen und stark reguliert)
- Die erforderlichen Verwaltungsrichtlinien (die auf OU-Ebene durchgesetzt werden) SCPs
- Betriebsmodell (wenn Sie die operative Verantwortung übernehmen oder diese an AMS auslagern möchten)
- Die gewünschten Geschäftsergebnisse, wie die Zeit für den Betrieb in der Cloud und die Betriebskosten.

> **Note**
>
> Eine Beschreibung der Modustypen pro AMS-Dienst finden Sie unter Modi- und Kontotypen in AMS.
> Praktische Anwendungsfälle der verschiedenen Modi finden Sie unter Anwendungsfälle aus der Praxis für AMS-Modi

In der folgenden Tabelle sind die wichtigsten Überlegungen aufgeführt, die Anwendungsbesitzer bei der Entscheidung für den am besten geeigneten AMS-Modus berücksichtigen sollten. Anwendungsbesitzer sollten vor der Anwendungsmigration eine Bewertungsphase einplanen, um genau zu verstehen, welcher Modus für ihre spezifische Anwendung gilt. Beispiel: Für Anwendungen, die auf Cloud-nativen Diensten oder serverloser Architektur basieren, könnte die beste Option darin bestehen, im Entwicklermodus mit dem Aufbau und der Iteration zu beginnen und die endgültige Infrastruktur als Code mithilfe des AMS Managed — SSP-Modus bereitzustellen. In diesem Fall kann ein geringfügiges Refactoring erforderlich sein, um sicherzustellen, dass alle für die automatisierte

Bereitstellung erstellten CloudFormation Vorlagen den von AMS festgelegten Ingest-Richtlinien entsprechen. Darüber hinaus müssen alle IAM-Berechtigungen von AMS Security genehmigt werden, um sicherzustellen, dass sie dem Modell der geringsten Rechte folgen.

Der AMS-Modus, der für das Hosten der Anwendung ausgewählt wurde, kann Ihnen dabei helfen, Ihr gewünschtes Cloud-Betriebsmodell umzusetzen.

> **Note**
>
> In einer einzigen AMS Managed Landing Zone kann mehr als ein Cloud-Betriebsmodell existieren, basierend auf den verschiedenen AMS-Modi, die für das Hosten der Anwendungen ausgewählt wurden.

Probleme bei der Entscheidung	Standard-CM-Modus/ /OOD *	AWS Service Catalog	Direkter Änderungsmodus	Self-Service-Bereitstellung	Entwicklermodus	Vom Kunden verwaltet
Betriebsbereitschaft						
Protokollierung, Überwachung und Eventmanagement	AMS ist für die gesamte verwaltete Infrastruktur verantwortlich			Der Kunde ist verantwortlich für Self-Service Provisioned Services (SSP)	Kunde, der für Ressourcen verantwortlich ist, die mithilfe der Entwickler-IAM-Rolle außerhalb des AMS CM-Systems bereitgestellt werden	Der Kunde ist verantwortlich
Kontinuitätsmanagement	Verantwortung von AMS für die Ausführung des vom Kunden ausgewählten Backup-Plans			Der Kunde ist verantwor	Kunde, der für Ressource	

Probleme bei der Entscheidung	Standard-CM-Modus/ /OOD *	AWS Service Catalog	Direkter Änderungsmodus	Self-Service-Bereitstellung	Entwicklermodus	Vom Kunden verwaltet
				tlich für Self-Service Provisioned Services (SSP)	n verantwortlich ist, die mithilfe der Entwickler-IAM-Rolle außerhalb des AMS CM-Systems bereitgestellt werden	
Zugriffsmanagement auf Instanzebene	AMS-Verwaltung über unidirektionales AD-Trust mit lokaler Domäne. Erfordert eine verwaltete Infrastruktur, um der AMS-Domäne beizutreten			Nicht zutreffend	Der Kunde ist verantwortlich für Ressourcen, die mithilfe der Entwickler-IAM-Rolle außerhalb des AMS CM-Systems bereitgestellt werden	

Probleme bei der Entscheidung	Standard-CM-Modus/ /OOD *	AWS Service Catalog	Direkter Änderungsmodus	Self-Service-Bereitstellung	Entwicklermodus	Vom Kunden verwaltet
Sicherheitsmanagement und Zugriffsmanagement auf Kontoebene	AMS-Verantwortung für alle verwalteten Konten			AMS ist für alle verwalteten Konten verantwortlich	Der Kunde ist verantwortlich für Ressourcen, die mithilfe der Entwickler-IAM-Rolle außerhalb des AMS CM-Systems bereitgestellt werden	
Patch-Management	AMS-Verantwortung für alle verwalteten Konten			Der Kunde ist verantwortlich für Self-Service Provisioned Services (SSP)	Kunde, der für Ressourcen verantwortlich ist, die mithilfe der Entwickler-IAM-Rolle außerhalb des AMS CM-Systems bereitgestellt werden	

Probleme bei der Entscheidung	Standard-CM-Modus/ /OOD *	AWS Service Catalog	Direkter Änderungsmodus	Self-Service-Bereitstellung	Entwicklermodus	Vom Kunden verwaltet
Änderungsmanagement	AMS-Verantwortung für alle verwalteten Konten			Der Kunde ist verantwortlich für Self-Service Provisioned Services (SSP)	Kunde, der für Ressourcen verantwortlich ist, die mithilfe der Entwickler-IAM-Rolle außerhalb des AMS CM-Systems bereitgestellt werden	
Verwaltung der Bereitstellung	Präskriptiv und standardisiert für die in AMS angebotenen Bereitstellungsoptionen	Flexibilität bei der direkten Nutzung der AWS-Service-API für den AWS Service Catalog gemäß den vorgeschriebenen AMS-Standards	Flexibilität zur direkten Nutzung der AWS-Service-API gemäß den vorgeschriebenen AMS-Standards	Flexibilität bei der direkten Nutzung des AWS-Service APIs für SSP-Services	Flexibilität bei der direkten Nutzung der AWS-Service-API für die Bereitstellung	

Probleme bei der Entscheidung	Standard-CM-Modus/ /OOD *	AWS Service Catalog	Direkter Änderungsmodus	Self-Service-Bereitstellung	Entwicklermodus	Vom Kunden verwaltet
Verwaltung und Prüfung von Vorfällen	AMS ist für alle verwalteten Konten verantwortlich				Der Kunde ist verantwortlich für Ressourcen, die mithilfe der Entwickler-IAM-Rolle außerhalb des AMS Change Management Systems bereitgestellt werden	
GuardRails und gemeinsam genutzte Infrastruktur (Netzwerk) und Sicherheitsframework	Präskriptive und standardisierte Nutzung von AMS Core Accounts					Flexible und maßgeschneiderte Nutzung von AMS Core Accounts
Bereitschaft zur Anwendung						

Probleme bei der Entscheidung	Standard-CM-Modus/ /OOD *	AWS Service Catalog	Direkter Änderungsmodus	Self-Service-Bereitstellung	Entwicklermodus	Vom Kunden verwaltet
Refactoring von Anwendungen	Ein leichtes Refactoring ist erforderlich				Ein leichtes Refactoring ist erforderlich (falls es mit AMS Standard CM bereitgestellt wurde)	Ein Refactoring ist nicht erforderlich
Support für AWS-Services	Beschränkt auf das, was von AMS unterstützt wird					Nicht begrenzt
Geschäftliche Überlegungen						
Zeit bis zur Betriebsbereitschaft	Drei bis sechs Monate			Mehr als 6 Monate, abhängig von den Kompetenzen des Kunden im Bereich Anwendungsbetrieb		6 bis 18 Monate, abhängig von den Kompetenzen des Kunden in Bezug auf Infrastruktur und Anwendungsbetrieb
Kosten	$$$$			$$$	$$	$

Probleme bei der Entscheidung	Standard-CM-Modus/ /OOD *	AWS Service Catalog	Direkter Änderungsmodus	Self-Service-Bereitstellung	Entwicklermodus	Vom Kunden verwaltet
Anwendungsbeispiele	Webserver mit 3-Tier-Stack, Apps mit Compliance- und regulatorischen Anforderungen			Webserver mit API Gateway, containerisierte Anwendung, die ECS/ EKS nutzt	Iteration/ Optimierung einer Data Lake-Anwendung, die Lambda, Glue, Athena usw. verwendet	Dezentralisiert accounts/ applications wie eine Sandbox, verwaltete Anwendungen von Drittanbietern

* Operations On Demand (OOD) bietet ein Angebot für Kunden, die den Standard-CM-Modus verwenden, um ihre Änderungen mithilfe spezieller Ressourcen zu verwalten. Weitere Informationen finden Sie im Angebotskatalog für Operations on Demand und wenden Sie sich an Ihren Cloud Service Delivery Manager (CSDM).

> **Note**
>
> Beim Preisvergleich zwischen SSP-Modus und Entwicklermodus wird davon ausgegangen, dass dieselben AWS-Services bereitgestellt werden.

Vergleich der AMS-Modi mit Geschäfts- und IT-Zielen

Wie gezeigt, sind die Modi AMS-Managed Standard Change, AWS Service Catalog oder Direct Change am besten geeignet, wenn Sie nach einem stark kontrollierten und standardisierten Governance-Modell für Ihre Anwendungen suchen. Wenn Sie ein maßgeschneidertes Governance-Modell benötigen, bei dem der Schwerpunkt auf Anwendungsinnovationen liegt, ohne dass Sie dafür betriebsbereit sein müssen, wählen Sie den Modus Customer Managed. Im vom Kunden verwalteten Modus kann die Operationalisierung Ihrer Anwendungen länger dauern, da Sie die Verantwortung für

die Einrichtung von Mitarbeitern, Prozessen und Tools zur Unterstützung betrieblicher Funktionen wie Incident Management, Configuration Management, Provisioning Management, Security Management, Patch Management usw. tragen.

Anwendungsfälle für AMS-Modi in der realen Welt

Untersuchen Sie diese, um herauszufinden, wie AMS-Modi verwendet werden können.

- Anwendungsfall 1: Geschäftliche Notwendigkeit zur Senkung der Kosten durch einen zeitkritischen Ausstieg aus dem Rechenzentrum: Ein Unternehmen mit einem wichtigen Geschäftsereignis, wie einem Ausstieg aus dem Rechenzentrum, ist daran interessiert, seine lokalen Anwendungen in der Cloud neu zu hosten. Der Großteil des lokalen Inventars besteht aus Windows- und Linux-Servern mit einer Mischung aus Betriebssystemversionen. Dabei möchte der Kunde auch die Kosteneinsparungen nutzen, die der Umstieg auf die Cloud mit sich bringt, und die technische und sicherheitstechnische Situation seiner Anwendungen verbessern. Der Kunde möchte schnell handeln, verfügt aber noch nicht über das nötige Fachwissen im Bereich Cloud-Betrieb. Der Kunde muss ein ausgewogenes Verhältnis zwischen Refactoring finden. Zu viel Refactoring kann angesichts eines engen Zeitrahmens riskant sein. Mit einigen Refaktorierungen, wie der Aktualisierung von Betriebssystemversionen und der Optimierung von Datenbanken, können Anwendungen jedoch das nächste Leistungsniveau erreichen. In diesem Beispiel kann der Kunde den AMS-verwalteten RFC-Modus wählen, um die meisten seiner Anwendungen neu zu hosten. AMS bietet den Betrieb der Infrastruktur und berät die Betriebsteams des Kunden gleichzeitig in Bezug auf bewährte Verfahren für den sicheren Betrieb in der Cloud.

  Der von AMS verwaltete AWS Service Catalog und der AMS-verwaltete Direct Change-Modus bieten dem Kunden zusätzliche Flexibilität und erreichen gleichzeitig dieselben Geschäftsergebnisse und Ziele. Darüber hinaus kann der Kunde das Angebot AMS Operations On Demand (OOD) nutzen, um über eigene AMS-Betriebstechniker zu verfügen, die die Ausführung von Änderungsanträgen priorisieren (). RFCs

  Während der Kunde die undifferenzierten betrieblichen Aufgaben der Infrastruktur (Patching, Backups, Kontoverwaltung usw.) an AMS auslagern kann, kann er sich weiterhin auf die Optimierung seiner Anwendung konzentrieren und seine internen Teams auf den Cloud-Betrieb ausweiten. AMS stellt dem Kunden monatliche Berichte über Kosteneinsparungen zur Verfügung und gibt Empfehlungen zur Ressourcenoptimierung. In diesem Anwendungsfall können end-of-life Anwendungen, die auf älteren Betriebssystemversionen wie Windows 2003 und 2008 gehostet wurden und die der Kunde nicht umgestaltet hat, auch zu AMS migriert und in einem Konto gehostet werden, das den vom Kunden verwalteten Modus nutzt.

- Anwendungsfall 2, Aufbau eines Data Lake mit Lambda, Glue, Athena innerhalb der sicheren AMS-Grenzen: Ein Unternehmen möchte einen Data Lake einrichten, um die Berichtsanforderungen für mehrere AMS-Anwendungen zu erfüllen. Der Kunde möchte S3-Buckets für die Speicherung von Datensätzen und AWS Athena verwenden, um den Datensatz für jeden Bericht abzufragen. S3 und AWS Athena werden in separaten AMS Managed Accounts bereitgestellt. Das Konto bei S3 verfügt auch über andere Dienste wie Glue, Lambda und Step Functions zum Aufbau einer Datenerfassungspipeline. Glue, Lambda, Athena und Step Functions gelten in diesem Fall als Self-Service Provisioning (SSP) -Services. Der Kunde hat außerdem eine EC2 Instanz in dem Konto bereitgestellt, die als Ad-hoc-Server fungiert. tooling/scripting Der Kunde fordert AMS zunächst auf, die SSP-Dienste in seinem AMS-verwalteten Konto zu aktivieren. AMS stellt für jeden Service eine IAM-Rolle bereit, die der Kunde übernehmen kann, sobald die Rolle in die Verbundlösung des Kunden integriert ist. Zur Vereinfachung der Verwaltung kann der Kunde auch die Richtlinien für die einzelnen IAM-Rollen in einer benutzerdefinierten Rolle zusammenfassen, sodass beim Arbeiten zwischen den AWS-Services keine Rollen mehr gewechselt werden müssen. Sobald die Rolle im Konto aktiviert ist, kann der Kunde die Services gemäß seinen Anforderungen konfigurieren. Der Kunde muss jedoch mit dem AMS-Change-Management-System zusammenarbeiten, um je nach Anwendungsfall zusätzliche Berechtigungen anzufordern.

  Für den Zugriff auf Glue Crawlers benötigt Glue beispielsweise zusätzliche Berechtigungen. Zusätzliche Berechtigungen sind auch erforderlich, um Ereignisquellen für Lambda zu erstellen. Der Kunde wird mit AMS zusammenarbeiten, um die IAM-Rollen zu aktualisieren, sodass Athena kontenübergreifenden Zugriff hat, um S3-Buckets abzufragen. Aktualisierungen von Servicerollen oder serviceverknüpften Rollen werden ebenfalls über das AMS Change Management benötigt, damit Lambda den Step Functions Functions-Dienst aufruft, und Glue, um in alle S3-Buckets zu lesen und in sie zu schreiben. AMS arbeitet mit Kunden zusammen, um sicherzustellen, dass das Zugriffsmodell mit den geringsten Rechten eingehalten wird und die angeforderten IAM-Änderungen nicht zu freizügig sind und die Umgebung nicht unnötigen Risiken aussetzen. Das Data Lake-Team des Kunden verbringt Zeit damit, alle IAM-Berechtigungen zu planen, die für die spezifische Architektur des Kunden erforderlich sind, und bittet AMS, diese zu aktivieren. Dies liegt daran, dass alle IAM-Änderungen manuell verarbeitet und vom AMS-Sicherheitsteam überprüft werden. Die Zeit für die Bearbeitung dieser Anfragen sollte im Zeitplan für die Anwendungsbereitstellung berücksichtigt werden.

  Da die SSP-Dienste innerhalb des Accounts betriebsbereit sind, kann der Kunde über das AMS Incident Management und die Serviceanfragen Support anfordern und Probleme melden. AMS überwacht jedoch nicht aktiv die Leistungs- und Parallelitätskennzahlen für Lambda oder Job-Metriken für Glue. Es liegt in der Verantwortung des Kunden, sicherzustellen, dass für SSP-Dienste

eine angemessene Protokollierung und Überwachung aktiviert ist. Die EC2 Instance und der S3-Bucket im Konto werden vollständig von AMS verwaltet.

- Anwendungsfall 3, schnelle und flexible Einrichtung einer CICD-Bereitstellungspipeline in AMS: Ein Kunde möchte eine Jenkins-basierte CICD-Pipeline einrichten, um die Code-Pipeline für alle Anwendungskonten in AMS bereitzustellen. Für den Kunden ist es möglicherweise am geeignetsten, diese CICD-Pipeline im AMS-Managed Direct Change Mode (DCM) oder im AMS-Managed Developer-Modus zu hosten, da er so flexibel den Jenkins-Server mit der erforderlichen benutzerdefinierten Konfiguration einrichten kann EC2, mit den gewünschten IAM-Zugriffsberechtigungen CloudFormation und S3-Buckets, die das Artefakt-Repository hosten. Dies ist zwar auch im AMS-verwalteten RFC-Modus möglich, das Kundenteam müsste jedoch mehrere Handbücher RFCs für IAM-Rollen erstellen, um anhand der am wenigsten zulässigen Genehmigungen zu iterieren, die manuell von AMS überprüft werden. DCM ermöglicht es den Kunden, ihre betrieblichen Ziele auf AWS zu erreichen und gleichzeitig die Notwendigkeit zu vermeiden, mehrere Handbücher RFCs für IAM-Rollen zu erstellen, wenn der vom AMS verwaltete RFC-Modus verwendet wird, um die am wenigsten zulässigen Genehmigungen zu verwenden, die manuell von AMS überprüft werden. Dies würde sowohl Zeit als auch Schulung seitens des Kunden erfordern, um die AMS-Prozesse und -Tools auf den neuesten Stand zu bringen. Im Entwicklermodus kann der Kunde mit einer „Entwicklerrolle“ beginnen, um die Infrastruktur mithilfe von nativem AWS bereitzustellen APIs. Der schnellste und flexibelste Weg, diese Pipeline einzurichten, wäre die Verwendung des AMS Managed-Developer-Modus. Der Entwicklermodus bietet den schnellsten und einfachsten Weg, wobei er Kompromisse bei der Betriebsintegration eingeht, während DCM weniger flexibel ist, aber das gleiche Maß an Betriebsunterstützung bietet wie der RFC-Modus.
- Anwendungsfall 4, maßgeschneidertes Betriebsmodell innerhalb der AMS-Stiftung: Ein Kunde steht vor einem terminbedingten Verlassen des Rechenzentrums und eine seiner Unternehmensanwendungen wird vollständig von einem Drittanbieter-MSP verwaltet, einschließlich Anwendungsbetrieb und Infrastrukturbetrieb. Unter der Annahme, dass der Kunde im Zeitplan keine Zeit hat, diese Anwendung so umzugestalten, dass sie von AMS betrieben werden kann, ist der Modus „Kundenverwaltung“ eine geeignete Option. Der Kunde kann die Vorteile der automatisierten und schnellen Einrichtung der von AMS verwalteten Landing Zone nutzen. Sie können die zentralisierte Kontoverwaltung nutzen, die den Verkauf und die Konnektivität der Konten über das zentrale Netzwerkkonto steuert. Es vereinfacht auch ihre Abrechnung, indem die Gebühren für alle vom Kunden verwalteten Konten über das AMS Payer-Konto konsolidiert werden. Der Kunde hat die Flexibilität, sein maßgeschneidertes Zugangsmanagementmodell einzurichten, wobei der MSP von der für AMS Managed Accounts verwendeten Standardzugriffsverwaltung getrennt ist. Auf diese Weise kann der Kunde im Modus

„Kundenverwaltung“ eine von AMS verwaltete Umgebung einrichten und gleichzeitig seine Geschäftsanforderungen erfüllen, die sich aus der lokalen Umgebung ergeben. In diesem Fall ist der Kunde für die Erstellung eines Cloud-Betriebsmodells verantwortlich, wenn der Kunde auch über Windows-basierte Anwendungen verfügt, die er in die Cloud migriert, und diese in ein vom Kunden verwaltetes Konto verschieben möchte. Dies kann komplex, teuer und zeitaufwändig sein, je nachdem, ob der Kunde in der Lage ist, traditionelle IT-Prozesse zu transformieren und Mitarbeiter zu schulen. Der Kunde kann Zeit und Kosten sparen, indem er solche Workloads auf ein von AMS verwaltetes Konto überträgt und den Infrastrukturbetrieb an AMS auslagert.

> **Note**
>
> Kunden haben manchmal das Bedürfnis, Anwendungskonten zwischen dem Governance-Framework des RFC- oder SSP-Modus und dem Entwicklermodus zu verschieben. Beispielsweise können Kunden im Rahmen der ersten Lift-and-Shift-Migration eine Anwendung im AMS-verwalteten Modus hosten, möchten die Anwendung aber im Laufe der Zeit neu schreiben, um sie für Cloud-native AWS-Services zu optimieren. Sie könnten den Modus des Pre-Prod-Kontos von AMS-verwaltetem RFC in den AMS-verwalteten Entwicklermodus ändern, was ihnen die Flexibilität und Agilität für die Bereitstellung der Infrastruktur gibt. Sobald jedoch Änderungen an der Bereitstellung der Infrastruktur mithilfe der „Entwicklerrolle“ vorgenommen wurden, kann dieselbe Infrastruktur nicht mehr in den AMS-verwalteten RFC-Modus zurückversetzt werden. Dies liegt daran, dass AMS den Betrieb der Infrastruktur, die außerhalb des AMS-Change-Management-Systems bereitgestellt wurde, nicht garantieren kann. Kunden müssen möglicherweise ein neues Anwendungskonto erstellen, das den AMS-verwalteten RFC-Modus bietet, und dann die „optimierte“ Infrastrukturkonfiguration mithilfe von CloudFormation Vorlagen oder benutzerdefinierter Daten, die in ein von AMS verwaltetes Konto AMIs aufgenommen wurden, erneut bereitstellen. Dies ist eine saubere Methode, um eine produktionsbereite Konfiguration bereitzustellen. Nach der Bereitstellung unterliegt die Anwendung der vorgeschriebenen AMS-Verwaltung und dem Betrieb. Das Gleiche gilt für den Wechsel zwischen dem vom Kunden verwalteten Modus und dem AMS-verwalteten Modus.

RFC-Modus

Der RFC-Modus ist der Standardmodus für Kunden mit AMS Advanced Operations Plan. Er umfasst ein Change-Management-System mit Änderungsanträgen oder RFCs einen Katalog von Änderungstypen, anhand derer Sie die gewünschten Ergänzungen oder Änderungen an Ihren Konten

beantragen können. Dieses Change-Management-System bietet ein gewisses Maß an Sicherheit, indem es einschränkt, wer Änderungen an Ihren Konten vornehmen kann.

Einzelheiten zu den Änderungstypen von AMS Advanced finden Sie unter Was sind AMS-Änderungstypen? .

Einzelheiten zum Onboarding bei AMS Advanced finden Sie unter Einführung in AWS Managed Services Onboarding.

Exemplarische Anleitungen zum Änderungstyp finden Sie im Abschnitt „Zusätzliche Informationen“ für den entsprechenden Änderungstyp im Abschnitt AMS Advanced Change Type Reference — Änderungstypen nach Klassifizierung.

> **Note**
>
> Der RFC-Modus wurde zuvor als „Change Management-Modus“ oder „Standard-CM-Modus“ bezeichnet.

Themen

- Erfahre mehr über RFCs
- Was sind Änderungstypen?
- Behebung von RFC-Fehlern in AMS

Erfahre mehr über RFCs

Änderungsanträge, oder RFCs, funktionieren auf zweierlei Weise. Erstens sind Parameter für den RFC selbst erforderlich. Dies sind die Optionen in der `CreateRfc` API. Und zweitens gibt es Parameter, die für die Aktion des RFC erforderlich sind (die Ausführungsparameter). Weitere Informationen zu den `CreateRfc` Optionen finden Sie im CreateRfcAbschnitt der AMS-API-Referenz. Diese Optionen werden normalerweise im Bereich Zusätzliche Konfigurationen der Seiten „RFC erstellen“ angezeigt.

Sie können einen RFC mit der `CreateRfc` API, `aws amscm create-rfc` CLI oder mithilfe der AMS-Konsole RFC-Seiten erstellen erstellen und einreichen. Ein Tutorial zur Erstellung eines RFC finden Sie unter. Erstellen Sie einen RFC

Themen

- Was sind RFCs?
- Authentifizieren Sie sich, wenn Sie die AMS API/CLI CLI
- RFC-Sicherheitsüberprüfungen verstehen
- Verstehen Sie die Klassifizierungen von RFC-Änderungstypen
- RFC-Aktionen und Aktivitätsstatus verstehen
- RFC-Statuscodes verstehen
- Verstehen Sie das RFC-Update CTs und die Erkennung von CloudFormation Template-Drift
- Zeitplan RFCs
- Genehmigen oder Ablehnen RFCs
- RFC-eingeschränkte Laufzeiten anfordern
- Erstellen, Klonen, Aktualisieren, Suchen und Stornieren RFCs
- Verwenden Sie die AMS-Konsole mit RFCs
- Erfahren Sie mehr über gängige RFC-Parameter
- Melden Sie sich für die tägliche RFC-E-Mail an

Was sind RFCs?

Mit einem Änderungsantrag (RFC) nehmen Sie eine Änderung in Ihrer von AMS verwalteten Umgebung vor oder bitten AMS, in Ihrem Namen eine Änderung vorzunehmen. Um einen RFC zu erstellen, wählen Sie aus AMS-Änderungstypen, wählen RFC-Parameter (z. B. Zeitplan) und reichen die Anfrage dann entweder über die AMS-Konsole oder die API-Befehle und ein. CreateRfcSubmitRfc

Ein RFC enthält zwei Spezifikationen, eine für den RFC selbst und eine für die Change Type (CT) -Parameter. In der Befehlszeile können Sie einen Inline-RFC-Befehl oder eine CreateRfc Standardvorlage im JSON-Format verwenden, die Sie zusammen mit der CT-JSON-Schemadatei ausfüllen und einreichen, die Sie erstellen (basierend auf den CT-Parametern). Der CT-Name ist eine informelle Beschreibung des CT. Ein CSIO (Kategorie, Unterkategorie, Gegenstand, Operation) ist eine formellere Beschreibung eines CT. Bei der Erstellung eines RFC muss nur die CT-ID angegeben werden.

AMS benachrichtigt Sie, wenn die Änderung erfolgreich (Success) oder erfolglos (Failure) abgeschlossen wurde.

> **Note**
>
> Informationen zur Behebung von RFC-Fehlern finden Sie unter. Behebung von RFC-Fehlern in AMS

Die folgende Grafik zeigt den Arbeitsablauf eines von Ihnen eingereichten RFC.

Authentifizieren Sie sich, wenn Sie die AMS API/CLI CLI

Wenn Sie die AMS-API/CLI verwenden, müssen Sie sich mit temporären Anmeldeinformationen authentifizieren. Um temporäre Sicherheitsanmeldedaten für Verbundbenutzer anzufordern GetFederationToken, rufen Sie AssumeRole, AssumeRoleWithSAML oder AssumeRoleWithWebIdentityAWS Security Token Service (STS) an. APIs

Eine gängige Wahl ist SAML. Nach der Einrichtung fügen Sie jeder Operation, die Sie aufrufen, ein Argument hinzu. Beispiel: `aws --profile saml amscm list-change-type-categories`.

Eine Abkürzung für SAML 2.0-Profile besteht darin, die Profilvariable am Anfang jedes API/CLI mit zu setzen `set AWS_DEFAULT_PROFILE=saml` (für Windows; für Linux wäre das der Fall`export AWS_DEFAULT_PROFILE=saml`). Informationen zur Einstellung von CLI-Umgebungsvariablen finden Sie unter Konfiguration der AWS-Befehlszeilenschnittstelle, Umgebungsvariablen.

RFC-Sicherheitsüberprüfungen verstehen

Das Genehmigungsverfahren für das Änderungsmanagement von AWS Managed Services (AMS) stellt sicher, dass wir eine Sicherheitsüberprüfung der Änderungen durchführen, die wir an Ihren Konten vornehmen.

AMS bewertet alle Änderungsanträge (RFCs) anhand der technischen Standards von AMS. Jede Änderung, die die Sicherheitslage Ihres Kontos aufgrund einer Abweichung von den technischen Standards beeinträchtigen könnte, wird einer Sicherheitsüberprüfung unterzogen. Während der Sicherheitsüberprüfung weist AMS auf relevante Risiken hin, und in Fällen mit hohem oder sehr hohem Sicherheitsrisiko akzeptiert oder lehnt Ihr autorisiertes Sicherheitspersonal den RFC ab. Alle Änderungen werden auch daraufhin bewertet, ob sie sich negativ auf die Betriebsfähigkeit von AMS auswirken. Wenn potenzielle nachteilige Auswirkungen festgestellt werden, sind zusätzliche Prüfungen und Genehmigungen innerhalb von AMS erforderlich.

Technische Standards von AMS

Die technischen Standards von AMS definieren die Mindestsicherheitskriterien, Konfigurationen und Prozesse, um die grundlegende Sicherheit Ihrer Konten zu gewährleisten. Diese Standards müssen sowohl von AMS als auch von Ihnen befolgt werden.

Jede Änderung, die die Sicherheitslage Ihres Kontos aufgrund einer Abweichung von den technischen Standards potenziell beeinträchtigen könnte, wird einem Risikoakzeptanzprozess unterzogen, bei dem das relevante Risiko von AMS hervorgehoben und vom autorisierten Sicherheitspersonal von Ihrer Seite akzeptiert oder abgelehnt wird. All diese Änderungen werden auch bewertet, um zu beurteilen, ob sie sich negativ auf die Fähigkeit von AMS auswirken würden, das Konto zu führen. Falls ja, sind zusätzliche Prüfungen und Genehmigungen innerhalb von AMS erforderlich.

RFC-Prozess für das Kundensicherheitsrisikomanagement (CSRM)

Wenn jemand aus Ihrem Unternehmen eine Änderung an Ihrer verwalteten Umgebung anfordert, überprüft AMS die Änderung, um festzustellen, ob die Anfrage die Sicherheitslage Ihres Kontos verschlechtern könnte, weil sie nicht den technischen Standards entspricht. Wenn die Anfrage die Sicherheitslage des Kontos beeinträchtigt, informiert AMS Ihren Ansprechpartner für das Sicherheitsteam über das entsprechende Risiko und führt die Änderung durch. Oder, wenn die Änderung ein hohes oder sehr hohes Sicherheitsrisiko für die Umgebung mit sich bringt, bittet AMS um die ausdrückliche Zustimmung Ihres Ansprechpartners im Sicherheitsteam in Form einer Risikoakzeptanz (siehe unten). Der AMS-Prozess zur Risikoakzeptanz bei Kunden ist darauf ausgerichtet:

- Stellen Sie sicher, dass Risiken klar identifiziert und den richtigen Eigentümern mitgeteilt werden
- Minimieren Sie die identifizierten Risiken für Ihre Umgebung
- Lassen Sie sich von den zuständigen Sicherheitskontakten, die mit dem Risikoprofil Ihres Unternehmens vertraut sind, die Genehmigung einholen und dokumentieren
- Reduzieren Sie den laufenden Betriebsaufwand für identifizierte Risiken

Wie kann man auf technische Standards und hohe oder sehr hohe Risiken zugreifen

Wir haben die Dokumentation zu den technischen Standards von AMS als Bericht für Sie https://console.aws.amazon.com/artifact/als Referenz zur Verfügung gestellt. Anhand der Dokumentation zu den technischen Standards von AMS können Sie herausfinden, ob für eine Änderung die

Risikobereitschaft Ihres autorisierten Sicherheitskontakts erforderlich ist, bevor Sie einen Änderungsantrag (RFC) einreichen.

Suchen Sie den Bericht über technische Standards, indem Sie in der Suchleiste der Registerkarte AWS Artifact Berichte nach „AWS Managed Services (AMS) Technical Standards“ suchen, nachdem Sie sich mit der Standardeinstellung angemeldet haben AWSManagedServicesChangeManagementRole.

> **Note**
>
> Das technische Standarddokument von AMS ist für die Kunden_ ReadOnly _Rolle in der landing zone mit einem Konto zugänglich. In der landing zone mit mehreren Konten, die AWSManaged ServicesAdminRole von Sicherheitsadministratoren und von Anwendungsteams AWSManaged ServicesChangeManagementRole verwendet wird, kann für den Zugriff auf das Dokument verwendet werden. Wenn Ihr Team eine benutzerdefinierte Rolle verwendet, erstellen Sie einen RFC „Andere“ | „Andere“, um Zugriff zu beantragen. Wir aktualisieren dann die angegebene benutzerdefinierte Rolle.

Verstehen Sie die Klassifizierungen von RFC-Änderungstypen

Die Änderungstypen, die Sie beim Einreichen eines RFC verwenden, sind in zwei große Kategorien unterteilt:

- Bereitstellung: Diese Klassifizierung dient der Erstellung von Ressourcen.
- Verwaltung: Diese Klassifizierung dient zum Aktualisieren oder Löschen von Ressourcen. Die Kategorie Verwaltung enthält auch Änderungstypen für den Zugriff auf Instanzen, das Verschlüsseln oder Teilen sowie das Starten AMIs, Stoppen, Neustarten oder Löschen von Stacks.

RFC-Aktionen und Aktivitätsstatus verstehen

`RfcActionState`(API)/Activity State (Konsole) helfen Ihnen dabei, den Status menschlicher Eingriffe oder Aktionen in einem RFC zu verstehen. Wird hauptsächlich für manuelle Zwecke verwendet und `RfcActionState` hilft Ihnen zu verstehen RFCs, wann entweder Sie oder AMS Operations Maßnahmen ergreifen müssen, und zeigt Ihnen, wann AMS Operations aktiv an Ihrem RFC arbeitet. Dies sorgt für mehr Transparenz in Bezug auf die Aktionen, die während des Lebenszyklus eines RFC ergriffen werden.

`RfcActionState`Definitionen für (API) /Aktivitätsstatus (Konsole):

- AwsOperatorAssigned: Ein AWS-Betreiber arbeitet aktiv an Ihrem RFC.
- AwsActionPending: Eine Antwort oder Aktion von AWS wird erwartet.
- CustomerActionPending: Eine Antwort oder Aktion des Kunden wird erwartet.
- NoActionPending: Weder von AWS noch vom Kunden sind Maßnahmen erforderlich.
- NotApplicable: Dieser Status kann nicht von AWS-Betreibern oder -Kunden festgelegt werden und wird nur für diejenigen verwendet RFCs , die vor der Veröffentlichung dieser Funktion erstellt wurden.

Der Status der RFC-Aktionen hängt davon ab, ob für den eingereichten Änderungstyp eine manuelle Überprüfung erforderlich ist und ob die Planung auf „ASAP“ gesetzt ist oder nicht.

- ActionStateRFC-Änderungen während der Prüfung, Genehmigung und des Starts eines manuellen Änderungstyps mit verzögerter Planung:
  - Nachdem Sie einen manuellen, geplanten RFC eingereicht haben, ändert sich dieser ActionStateautomatisch AwsActionPendingzu dem Hinweis, dass ein Operator den RFC überprüfen und genehmigen muss.
  - Wenn ein Operator beginnt, Ihren RFC aktiv zu überprüfen, ändert sich der ActionStateAwsOperatorAssigned
  - Wenn der Operator Ihren RFC genehmigt, ändert sich der RFC-Status in Geplant und der ActionStateautomatisch in. NoActionPending
  - Wenn die geplante Startzeit des RFC erreicht ist, ändert sich der RFC-Status auf und der ActionStateautomatische Wechsel wird in angezeigt InProgress, dass ein Operator für die Überprüfung des RFC zugewiesen werden muss. AwsActionPending
  - Wenn ein Operator anfängt, den RFC aktiv auszuführen, ändert er den Wert in. ActionStateAwsOperatorAssigned
  - Sobald der Vorgang abgeschlossen ist, schließt der Operator den RFC. Dadurch wird der Wert automatisch ActionStateauf NoActionPendinggeändert.

Important

- Aktionsstatus können nicht von Ihnen festgelegt werden. Sie werden entweder automatisch auf der Grundlage von Änderungen im RFC oder manuell von AMS-Operatoren festgelegt.
- Wenn Sie einem RFC Korrespondenz hinzufügen, ActionStatewird dieser automatisch auf gesetzt. AwsActionPending
- Wenn ein RFC erstellt wird, ActionStatewird der automatisch auf gesetzt. NoActionPending
- Wenn ein RFC gesendet wird, ActionStatewird der automatisch auf gesetzt. AwsActionPending
- Wenn ein RFC abgelehnt, storniert oder mit dem Status Erfolgreich oder Fehlgeschlagen abgeschlossen wird, ActionStatewird er automatisch auf zurückgesetzt. NoActionPending
- Aktionsstatus sind sowohl für automatisierte als auch für manuelle Aktionen aktiviert RFCs, sind jedoch hauptsächlich für manuelle Aktionen von Bedeutung, RFCs da für diese Art von Aktionen RFCs häufig eine Kommunikation erforderlich ist.

Sehen Sie sich die Anwendungsfallbeispiele für RFC-Aktionsstatus an

Anwendungsfall: Sichtbarkeit bei manuellen RFC-Prozessen

- Sobald Sie einen manuellen RFC eingereicht haben, ändert sich der Status der RFC-Aktion automatisch in, `AwsActionPending` um anzuzeigen, dass ein Operator den RFC überprüfen und genehmigen muss. Wenn ein Operator beginnt, Ihren RFC aktiv zu überprüfen, ändert sich der RFC-Aktionsstatus auf. `AwsOperatorAssigned`
- Stellen Sie sich einen manuellen RFC vor, der genehmigt und geplant wurde und bereit ist, mit der Ausführung zu beginnen. Sobald sich der RFC-Status auf ändert`InProgress`, ändert sich der RFC-Aktionsstatus automatisch auf. `AwsActionPending` Er ändert sich wieder auf, `AwsOperatorAssigned` sobald ein Operator den RFC aktiv ausführt.
- Wenn ein manueller RFC abgeschlossen ist (als „Erfolg“ oder „Fehlschlag“ geschlossen), ändert sich der Status der RFC-Aktion in, `NoActionPending` um anzuzeigen, dass weder vom Kunden noch vom Betreiber weitere Aktionen erforderlich sind.

Anwendungsfall: RFC-Korrespondenz

- Wenn es sich um einen manuellen RFC handeltPending Approval, benötigt ein AMS-Operator möglicherweise weitere Informationen von Ihnen. Die Operatoren senden eine Nachricht an den RFC und ändern den RFC-Aktionsstatus auf. CustomerActionPending Wenn Sie antworten, indem Sie eine neue RFC-Korrespondenz hinzufügen, ändert sich der RFC-Aktionsstatus automatisch auf. AwsActionPending
- Wenn ein automatisierter oder manueller RFC ausgefallen ist, können Sie den RFC-Details eine Korrespondenz hinzufügen und den AMS-Operator fragen, warum der RFC fehlgeschlagen ist. Wenn Ihre Korrespondenz hinzugefügt wird, wird der RFC-Aktionsstatus automatisch auf gesetzt. AwsActionPending Wenn der AMS-Operator den RFC abruft, um Ihre Korrespondenz einzusehen, ändert sich der RFC-Aktionsstatus auf. AwsOperatorAssigned Wenn der Operator antwortet, indem er eine neue RFC-Korrespondenz hinzufügt, kann der RFC-Aktionsstatus auf gesetzt werdenCustomerActionPending, was bedeutet, dass eine weitere Antwort vom Kunden erwartet wird, oder auf, was bedeutetNoActionPending, dass keine Antwort vom Kunden erforderlich oder erwartet wird.

RFC-Statuscodes verstehen

RFC-Statuscodes helfen Ihnen dabei, Ihre Anfragen zu verfolgen. Sie können diese Statuscodes während eines RFC-Laufs in der CLI-Ausgabe oder durch Aktualisieren der RFC-Listenseite in der Konsole beobachten.

Sie können die Codes für einen RFC auch auf der Detailseite für diesen RFC sehen, die so aussehen könnte:

Möglicherweise finden Sie in Ihrer Liste einen RFC, den Sie nicht eingereicht haben. Wenn AMS-Operatoren einen CT verwenden, der nur intern verwendet wird, reichen sie ihn in einem RFC ein und er wird in Ihrer RFC-Liste angezeigt. Weitere Informationen finden Sie unter Nur interne Änderungstypen.

> **Important**
>
> Sie können Benachrichtigungen über RFC-Statusänderungen anfordern. Einzelheiten finden Sie unter Benachrichtigungen über RFC-Statusänderungen.

RFC-Statuscodes

Herzlichen Glückwunsch	Fehler
Bearbeitung: Der RFC wurde erstellt, aber nicht eingereicht PendingApproval /Eingereicht: Der RFC wurde eingereicht und das System ermittelt, ob er genehmigt werden muss, und holt diese Genehmigung, falls erforderlich, ein Genehmigt von AWS//Genehmigt vom Kunden: Der RFC wurde genehmigt. Automatisierte Geräte RFCs werden von AWS genehmigt, manuelle RFCs werden von Betreibern und manchmal auch von Kunden genehmigt Geplant: Der RFC hat die Syntax- und Anforderungsprüfungen bestanden und ist für die Ausführung geplant InProgress: Der RFC wird gerade ausgeführt. Beachten Sie, RFCs dass das Bereitstellen mehrerer Ressourcen oder die Ausführung mit langer Laufzeit UserData länger dauert Ausgeführt: Der RFC wurde ausgeführt Erfolgreich//Erfolgreich: Der RFC wurde erfolgreich abgeschlossen	Abgelehnt: RFCs werden in der Regel zurückgewiesen, weil sie nicht validiert werden können. Beispielsweise wurde eine unbrauchbare Ressource, d. h. ein Subnetz, angegeben Storniert: RFCs werden in der Regel storniert, weil sie die Validierung nicht bestehen, bevor die konfigurierte Startzeit abgelaufen ist Fehlgeschlagen: Der RFC ist ausgefallen. Die Gründe für den Fehler finden Sie StatusReason in der Ausgabe, und AMS Operations erstellt automatisch ein Trouble-Ticket und kommuniziert bei Bedarf mit Ihnen

> **Note**
>
> Storniert oder abgelehnt RFCs können Sie erneut einreichen mit UpdateRfc; siehe auch. Aktualisierung RFCs

Wenn der RFC alle erforderlichen Bedingungen erfüllt (z. B. wenn alle erforderlichen Parameter angegeben sind), ändert sich der Status in `PendingApproval` (auch bei automatisierter Ausführung ist CTs eine Genehmigung erforderlich, was automatisch geschieht, wenn Syntax- und Parameterprüfungen erfolgreich sind). Wenn er nicht erfolgreich ist, ändert sich der Status zu`Rejected`. Das `StatusReason` enthält Informationen zu Ablehnungen; die `ExecutionOutput` Felder enthalten Informationen zur Genehmigung und zum Abschluss. Zu den Fehlercodes gehören:

- InvalidRfcStateException: Der RFC befindet sich in einem Status, der die aufgerufene Operation nicht zulässt. Wenn der RFC beispielsweise in den Status Eingereicht übergegangen ist, kann er nicht mehr geändert werden.
- InvalidRfcScheduleException: Die TimeoutInMinutes Parameter StartTime EndTime, oder wurden verletzt.
- InternalServerError: Es ist ein Problem mit dem System aufgetreten.
- InvalidArgumentException: Ein Parameter ist falsch angegeben. Beispielsweise wird ein inakzeptabler Wert verwendet.
- ResourceNotFoundException: Ein Wert, z. B. die Stack-ID, kann nicht gefunden werden.

Wenn die geplanten angeforderten Start- und Endzeiten (auch bekannt als das Änderungslauffenster) vor der Genehmigung der Änderung liegen, ändert sich der RFC-Status auf`Canceled`. Wenn die Änderung genehmigt wurde, ändert sich der RFC-Status auf. `Scheduled` Das Fenster für die Ausführung von Änderungen bei ASAP RFCs besteht aus der Zeit der Übermittlung zuzüglich des `ExpectedExecutionDuration` Werts für den CT.

Eine geplante Änderung (mit einem `RequestedStartTime` in der CLI eingereicht) kann jederzeit vor dem Eintreffen des Fensters für die Ausführung von Änderungen geändert oder storniert werden. Wenn die geplante Änderung geändert wird, muss sie erneut eingereicht werden.

Wenn die Startzeit der Änderung eintrifft (geplant oder so schnell wie möglich) und die Genehmigungen abgeschlossen sind, ändert sich der Status auf `InProgress` und es können keine Änderungen vorgenommen werden. Wenn die Änderung innerhalb des angegebenen Zeitfensters für die Ausführung von Änderungen abgeschlossen ist, ändert sich der Status in. `Success` Schlägt ein Teil der Änderung fehl oder ist die Änderung am Ende des Fensters für den Änderungslauf noch in Bearbeitung, ändert sich der Status in`Failure`.

> **Note**
>
> Während des Status „`InProgressSuccess`," oder „`Failure`Change" kann der RFC nicht geändert oder abgebrochen werden.

Das folgende Diagramm zeigt den RFC-Status vom CreateRFC-Aufruf bis zur Auflösung.

Verstehen Sie das RFC-Update CTs und die Erkennung von CloudFormation Template-Drift

In AMS bereitgestellte Ressourcen verwenden eine modifizierte AWS CloudFormation Vorlage. Wenn bei einer Ressource ein Parameter direkt über die AWS Management Console eines Dienstes geändert wurde, ist der CloudFormation Erstellungsdatensatz dieser Ressource nicht mehr synchron. Wenn dies passiert und Sie versuchen, einen AMS-Aktualisierungsänderungstyp zu verwenden, um die Ressource in AMS zu aktualisieren, verweist AMS auf die ursprüngliche Ressourcenkonfiguration und setzt möglicherweise geänderte Parameter zurück. Dieser Reset kann schädlich sein, weshalb AMS die Verwendung von RFCs Update-Änderungstypen nicht zulässt, wenn zusätzliche AMS-Konfigurationsänderungen erkannt werden.

Verwenden Sie den Konsolenfilter, um eine Liste der Arten von Update-Änderungen zu erhalten.

Behebung von Abweichungen FAQs

Fragen und Antworten zur Behebung von AMS-Abweichungen. Es gibt zwei Arten von Änderungen, mit denen Sie die Behebung von Abweichungen einleiten können: Der eine ist Ausführungsmodus=manuell oder „Überprüfung erforderlich", der andere ist Ausführungsmodus=automatisiert.

Unterstützte Ressourcen zur Drift-Korrektur (ct-3kinq0u4l33zf)

Dies sind die Ressourcen, die vom Änderungstyp „Drift Remediation" (ct-3kinq0u4l33zf) unterstützt werden. Verwenden Sie zur Behebung von Ressourcen stattdessen den Änderungstyp „Überprüfung erforderlich" (ct-34sxfo53yuzah).

```
AWS::EC2::Instance
AWS::EC2::SecurityGroup
AWS::EC2::VPC
AWS::EC2::Subnet
```

```
AWS::EC2::NetworkInterface
AWS::EC2::EIP
AWS::EC2::InternetGateway
AWS::EC2::NatGateway
AWS::EC2::NetworkAcl
AWS::EC2::RouteTable
AWS::EC2::Volume
AWS::AutoScaling::AutoScalingGroup
AWS::AutoScaling::LaunchConfiguration
AWS::AutoScaling::LifecycleHook
AWS::AutoScaling::ScalingPolicy
AWS::AutoScaling::ScheduledAction
AWS::ElasticLoadBalancing::LoadBalancer
AWS::ElasticLoadBalancingV2::Listener
AWS::ElasticLoadBalancingV2::ListenerRule
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::CloudWatch::Alarm
```

Änderungstypen für Drift-Korrektur

Fragen und Antworten zur Verwendung der Änderungstypen für die AMS-Drift-Korrektur

Eine Liste der unterstützten Ressourcen für die Drift-Korrekturfunktion finden Sie unter. Unterstützte Ressourcen zur Drift-Korrektur (ct-3kinq0u4l33zf)

> **Important**
>
> Bei der Drift-Korrektur werden die and/or Parameter der Stack-Vorlagen geändert, und es ist zwingend erforderlich, dass Sie Ihre lokalen Template-Repositorys oder alle Automatisierungen, die diese Stacks aktualisieren, aktualisieren, sodass sie die neuesten Stack-Vorlagen und -Parameter verwenden. Die Verwendung alter and/or Vorlagenparameter ohne Synchronisierung kann zu schädlichen Änderungen an den zugrunde liegenden Ressourcen führen.
> Das automatisierte CT (ct-3kinq0u4l33zf) unterstützt die Korrektur von nur 10 Ressourcen pro RFC. Um die verbleibenden Ressourcen in Stapeln von 10 zu korrigieren, erstellen Sie neue Ressourcen, bis alle Ressourcen behoben sind. RFCs

Welchen Änderungstyp für Drift Remediation sollte ich verwenden?

Wir empfehlen, das automatisierte CT (ct-3kinq0u4l33zf) ohne Überprüfung zu verwenden, wenn:

- Sie versuchen, eine Aktualisierung einer vorhandenen Stack-Ressource mithilfe eines automatisierten CT durchzuführen, und der RFC wird unverändert zurückgewiesen. `DRIFTED`
- Sie haben in der Vergangenheit ein Update CT verwendet und es ist fehlgeschlagen, weil der Stack DRIFTED wurde. Sie müssen nicht erneut versuchen, ein Update durchzuführen, sondern können stattdessen die manuelle Überprüfung durchführen.

Wir empfehlen, das für die Überprüfung erforderliche manuelle CT (ct-34sxfo53yuzah) nur dann zu verwenden, wenn fehlerhafte Ressourcentypen von der Drift-Behebung nicht unterstützt werden (keine Überprüfung erforderlich), automatisiert, CT (ct-3kinq0u4l33zf) oder wenn die Drift-Korrektur (keine Überprüfung erforderlich), automatisiert, CT fehlschlägt.

Welche Änderungen werden während der Problembehebung am Stack vorgenommen?

Für die Wiederherstellung sind Aktualisierungen der and/or Parameter der Stack-Vorlage erforderlich, je nachdem, welche Eigenschaften verändert wurden. Bei der Wiederherstellung wird auch die Stack-Richtlinie des Stacks während der Wiederherstellung aktualisiert und die Stack-Richtlinie nach Abschluss der Wiederherstellung auf ihren vorherigen Wert zurückgesetzt.

Wie können wir sehen, welche Änderungen an den Parametern der Stack-Vorlage vorgenommen wurden? and/or

In der Antwort auf den RFC wird eine Zusammenfassung der Änderungen mit den folgenden Informationen bereitgestellt:

- `ChangeSummaryJson`: Enthält eine Zusammenfassung der Änderungen der and/or Stack-Vorlagenparameter als Teil der Drift-Korrektur. Die Sanierung wird in mehreren Phasen durchgeführt. Diese Änderungsübersicht besteht aus Änderungen für einzelne Phasen. Wenn die Korrektur erfolgreich ist, überprüfen Sie die Änderungen der letzten Phase. ExecutionPlan In der JSON-Datei finden Sie die Phasen, die der Reihe nach ausgeführt wurden. Beispielsweise wird ein RestoreReferences Abschnitt, wenn er vorhanden ist, immer am Ende ausgeführt und enthält JSON für Änderungen nach der Korrektur. Wenn die Wiederherstellung im DryRun Modus ausgeführt würde, wäre keine dieser Änderungen auf den Stack angewendet worden.
- `PreRemediationStackTemplateAndConfigurationJson`: Enthält einen Konfigurations-Snapshot des CloudFormation Stacks, einschließlich Vorlage, Parametern und Ausgaben, StackPolicyBody bevor die Korrektur auf dem Stack ausgelöst wurde.

Was muss ich tun, nachdem die Korrektur durchgeführt wurde?

> ⚠ Important
>
> Sie müssen Ihre lokalen Vorlagen-Repositorys oder jegliche Automatisierung, die den Stack mit den Korrigierungen aktualisieren würde, mit den neuesten Vorlagen und Parametern aktualisieren, die in der RFC-Zusammenfassung enthalten sind. Dies ist sehr wichtig, da die Verwendung der alten and/or Vorlagenparameter zu weiteren zerstörerischen Änderungen an den Stack-Ressourcen führen kann.

Wird meine Anwendung während dieser Sanierung beeinträchtigt?

Die Wiederherstellung ist ein Offline-Prozess, der nur für die CloudFormation Stack-Konfiguration ausgeführt wird. An der zugrunde liegenden Ressource werden keine Aktualisierungen durchgeführt.

Kann ich weiterhin Verwaltung | Andere | Andere verwenden RFCs , um nach der Wiederherstellung Aktualisierungen an Ressourcen durchzuführen?

Wir empfehlen, dass Sie Aktualisierungen der Stack-Ressourcen immer mithilfe des verfügbaren automatisierten Updates CTs durchführen. Wenn das verfügbare Update Ihren Anwendungsfall CTs nicht unterstützt, verwenden Sie Verwaltung | Andere | Andere Anfragen.

Werden durch die Problembehebung neue Ressourcen im Stack erstellt?

Durch die Behebung werden keine neuen Ressourcen im Stack erstellt. Bei der Behebung werden jedoch neue Ausgaben erstellt und der Abschnitt mit den Metadaten der Stack-Vorlage aktualisiert, sodass die Zusammenfassung der Problembehebung als Referenz gespeichert wird.

Wird die Problembehebung immer erfolgreich sein?

Die Behebung erfordert eine sorgfältige Analyse und Validierung der Vorlagenkonfiguration, um festzustellen, ob sie durchgeführt werden kann. In Szenarien, in denen diese Validierungen fehlschlagen, wird der Behebungsprozess gestoppt und es werden keine Änderungen an der Stack-Vorlage oder den Parametern vorgenommen. Außerdem kann die Korrektur nur für unterstützte Ressourcentypen durchgeführt werden.

Wie kann ich Aktualisierungen an Stack-Ressourcen durchführen, wenn die Behebung nicht erfolgreich ist?

Sie können das Update Management | Other | Other | Update CT (ct-0xdawir96cy7k) verwenden, um Änderungen anzufordern. AMS überwacht solche Szenarien und arbeitet an der Verbesserung der Behebungslösung.

Kann ich Stacks korrigieren, die sowohl unterstützte als auch nicht unterstützte Ressourcentypen haben?

Ja. Die Wiederherstellung wird jedoch nur durchgeführt, wenn die unterstützten Ressourcentypen im Stack DRIFTED gefunden werden. Wenn nicht unterstützte Ressourcentypen DRIFTED sind, wird die Behebung nicht fortgesetzt.

Kann ich eine Problembehebung für Stacks beantragen, die durch Ingest außerhalb von CFN erstellt wurden? CTs

Ja. Die Korrektur kann für Stacks unabhängig vom Änderungstyp durchgeführt werden, der für die Erstellung des Stacks verwendet wurde.

Kann ich vor der Behebung wissen, welche Änderungen am Stack vorgenommen werden würden?

Ja. Beide Änderungstypen bieten eine DryRunOption, mit der Sie Änderungen anfordern können, die bei einer Korrektur des Stacks vorgenommen würden. Die endgültigen Korrekturänderungen können jedoch je nach der Abweichung, die zum Zeitpunkt der Korrektur auf dem Stack vorhanden war, unterschiedlich sein.

Zeitplan RFCs

Mit der Planungsfunktion können Sie eine Startzeit für RFCs auswählen. Die folgenden Optionen sind in der Planungsfunktion verfügbar:

- Führen Sie diese Änderung so schnell wie möglich aus: AMS führt den RFC aus, sobald er genehmigt wurde. Die meisten CTs werden automatisch genehmigt. Verwenden Sie diese Option, wenn der RFC nicht zu einem bestimmten Zeitpunkt starten soll.
- Planen Sie diese Änderung: Legen Sie einen Tag, eine Uhrzeit und eine Zeitzone fest, an der der RFC ausgeführt werden soll. Bei automatisierten Änderungstypen empfiehlt es sich, eine Startzeit anzufordern, die mindestens 10 Minuten nach der geplanten Einreichung des RFC liegt. Für die Überprüfung der erforderlichen Änderungstypen ist es erforderlich, dass Sie eine Startzeit beantragen, die mindestens 24 Stunden nach der geplanten Einreichung des RFC liegt. Wenn der RFC bis zur konfigurierten Startzeit nicht genehmigt wird, wird der RFC abgelehnt.

Legen Sie einen RFC-Zeitplan fest

Verwenden Sie eine der folgenden Methoden, um einen RFC zu planen:

Führen Sie diese Änderung so schnell wie möglich aus:

- Konsole: Nichts tun. Dabei wird der standardmäßige RFC-Zeitplan verwendet.
- API oder CLI: Entfernen Sie die `RequestedEndTime` Optionen `RequestedStartTime` und im Vorgang Create RFC.

ASAP „Überprüfung erforderlich“ RFCs werden automatisch abgelehnt, wenn sie nicht innerhalb von dreißig Tagen nach Einreichung genehmigt werden.

Planen Sie diese Änderung ein:

- Konsole: Wählen Sie das Optionsfeld Diese Änderung planen aus. Ein Bereich mit der Startzeit wird geöffnet. Geben Sie manuell einen Tag ein oder verwenden Sie das Kalender-Widget, um einen Tag auszuwählen. Geben Sie eine Uhrzeit in UTC ein, ausgedrückt im Format ISO 8601, und verwenden Sie die Dropdownliste, um einen Ort auszuwählen. Standardmäßig verwendet AMS das ISO 8601-Format YYYYMMDDThhmmss Z YYYY-MM-DDThh oder:MM:SSZ. Beide Formate werden akzeptiert.

  > **Note**
  >
  > Die Standard-Endzeit liegt 4 Stunden nach der von Ihnen eingegebenen Startzeit. Um die Endzeit Ihrer geplanten Änderung auf mehr als 4 Stunden festzulegen, verwenden Sie die API oder CLI, um die Änderung auszuführen.

- API oder CLI: Senden Sie Werte für die `RequestedEndTime` Parameter `RequestedStartTime` und im Vorgang Create RFC. Durch die Übergabe eines konfigurierten Elements wird die Ausführung eines automatisierten Änderungstyps, der bereits gestartet wurde, `RequestedEndTime` nicht gestoppt. Bei einem Änderungstyp „Überprüfung erforderlich“ können Sie eine Verlängerung beantragen oder Sie werden möglicherweise aufgefordert, den RFC erneut einzureichen, wenn der Änderungstyp „Überprüfung erforderlich“ noch nicht abgeschlossen ist und Sie mit AMS in Kontakt stehen. `RequestedEndTime`

> **Tip**
>
> Ein Beispiel für eine Anzeige der UTC-Zeit finden Sie unter UTC auf der Time-IS-Website. Beispiel für ein ISO 8601-Format für den date/time Wert 2016-12-05 um 14:20 Uhr: 2016-12-05T 14:20:00 Z oder 20161205T142000Z.

Wenn Sie angeben...

- nur a`RequestedStartTime`, der RFC gilt als geplant und der `RequestedEndTime` wird mit dem `ExecutionDurationInMinutes` Wert gefüllt.
- nur a`RequestedEndTime`, wir werfen eine InvalidArgumentException.
- `RequestedStartTime`sowohl als auch`RequestedEndTime`, wir überschreiben die `RequestedEndTime` mit der angegebenen Startzeit plus dem `ExecutionDurationInMinutes` Wert.
- `RequestedStartTime`weder noch`RequestedEndTime`, wir behalten diese Werte bei Null und der RFC wird als ASAP-RFC behandelt.

> **Note**
>
> Für alle geplanten Änderungen wird eine nicht spezifizierte Endzeit angegeben RFCs, die aus der Uhrzeit des angegebenen Zeitpunkts `RequestedStartTime` plus dem `ExpectedExecutionDurationInMinutes` Attribut des übermittelten Änderungstyps besteht. Wenn der beispielsweise „60“ (Minuten) `ExpectedExecutionDurationInMinutes` ist und der angegebene Wert `2016-12-05T14:20:00Z` (5. Dezember 2016 um 4:20 Uhr) `RequestedStartTime` ist, würde die tatsächliche Endzeit auf den 5. Dezember 2016 um 5:20 Uhr festgelegt. Um den `ExpectedExecutionDurationInMinutes` für einen bestimmten Änderungstyp zu finden, führen Sie diesen Befehl aus:
>
> ```
> aws amscm --profile saml get-change-type-version --
> change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.
> {ExpectedDuration:ExpectedExecutionDurationInMinutes}"
> ```

Verwenden Sie die Option RFC-Priorität

Verwenden Sie die Option Priorität in `execution mode = manual` Änderungstypen, um AMS Operations auf die Dringlichkeit der Anfrage hinzuweisen.

Option Priorität in`execution mode = manual`:

Geben Sie die Priorität eines manuellen RFC als Hoch, Mittel oder Niedrig an. RFCs Als hoch eingestuft werden, werden geprüft und genehmigt, bevor sie als Mittel RFCs eingestuft werden. Dabei gelten die RFC-Servicelevel-Ziele (SLOs) und deren Einreichungszeiten. RFCs mit niedriger Priorität oder ohne angegebene Priorität werden in der Reihenfolge verarbeitet, in der sie eingereicht wurden.

Genehmigen oder Ablehnen RFCs

RFCs Die Vorlage mit der erforderlichen Genehmigung (manuell) CTs muss von Ihnen oder AMS genehmigt werden. Vorab genehmigte Daten werden automatisch verarbeitet CTs . Weitere Informationen finden Sie unter Anforderungen an die CT-Zulassung.

> **Note**
>
> Wenn Sie „Überprüfung erforderlich“ verwenden CTs, empfiehlt AMS, die ASAP-Scheduling-Option zu verwenden (wählen Sie ASAP in der Konsole, lassen Sie Start- und Endzeit leer in der API/CLI), da diese einen AMS-Operator CTs erfordern, der den RFC überprüft und möglicherweise mit Ihnen kommuniziert, bevor er genehmigt und ausgeführt werden kann. Wenn Sie diese einplanen, achten Sie darauf RFCs, dass Sie mindestens 24 Stunden einplanen. Wenn die Genehmigung nicht vor der geplanten Startzeit erfolgt, wird der RFC automatisch abgelehnt.

Wenn ein für eine Genehmigung erforderlicher RFC erfolgreich von AMS eingereicht wurde, muss er von Ihnen ausdrücklich genehmigt werden. Oder wenn Sie einen RFC einreichen, für den eine Genehmigung erforderlich ist, muss dieser von AMS genehmigt werden. Wenn Sie einen von AMS eingereichten RFC genehmigen müssen, erhalten Sie eine E-Mail oder eine andere vorab festgelegte Mitteilung mit der Bitte um Genehmigung. Die Kommunikation beinhaltet die RFC-ID. Nachdem die Kommunikation gesendet wurde, führen Sie einen der folgenden Schritte aus:

- Konsole Genehmigen oder Ablehnen: Verwenden Sie die RFC-Detailseite für den entsprechenden RFC:

- API//CLI Approve: ApproveRfcmarkiert eine Änderung als genehmigt. Die Maßnahme muss sowohl vom Eigentümer als auch vom Betreiber ergriffen werden, falls beide erforderlich sind. Im Folgenden finden Sie ein Beispiel für einen CLI-Genehmigungsbefehl. Ersetzen Sie im folgenden Beispiel RFC_ID durch die entsprechende RFC-ID.

```
aws amscm approve-rfc --rfc-id RFC_ID
```

- API//CLI Reject: RejectRfcmarkiert eine Änderung als abgelehnt. Im Folgenden finden Sie ein Beispiel für einen CLI-Ablehnungsbefehl. Ersetzen Sie im folgenden Beispiel RFC_ID durch die entsprechende RFC-ID.

```
aws amscm reject-rfc --rfc-id RFC_ID --reason "no longer relevant"
```

RFC-eingeschränkte Laufzeiten anfordern

Früher als Sperrtage bezeichnet, können Sie die Einschränkung bestimmter Zeiträume beantragen. Während dieser Zeiten können keine Änderungen vorgenommen werden.

Um einen eingeschränkten Ausführungszeitraum festzulegen, verwenden Sie die UpdateRestrictedExecutionTimesAPI-Operation und legen Sie einen bestimmten Zeitraum in UTC fest. Der von Ihnen angegebene Zeitraum hat Vorrang vor allen zuvor angegebenen Zeiträumen. Wenn Sie einen RFC während der angegebenen eingeschränkten Laufzeit einreichen, schlägt die Übermittlung fehl und es wird der Fehler Ungültiger RFC-Zeitplan angezeigt. Sie können bis zu 200 eingeschränkte Zeiträume angeben. Standardmäßig ist kein eingeschränkter Zeitraum festgelegt. Im Folgenden finden Sie ein Beispiel für einen Anforderungsbefehl (mit konfigurierter SAML-Authentifizierung):

```
aws amscm  --profile saml update-restricted-execution-times --restricted-execution-
times="[{\"TimeRange\":{\"StartTime\":\"2018-01-01T12:00:00Z\",\"EndTime\":
\"2018-01-01T12:00:01Z\"}}]"
```

Sie können Ihre aktuelle RestrictedExecutionTimes Einstellung auch anzeigen, indem Sie den ListRestrictedExecutionTimesAPI-Vorgang ausführen. Beispiel:

```
aws amscm  --profile saml list-restricted-execution-times
```

Wenn Sie einen RFC während einer bestimmten eingeschränkten Ausführungszeit einreichen möchten, fügen Sie den RestrictedExecutionTimesOverrideIdmit dem Wert von

OverrideRestrictedTimeRangeshinzu und senden Sie den RFC dann wie gewohnt weiter. Es hat sich bewährt, diese Methode nur für kritische RFCs oder Notfall-RFCs zu verwenden. Weitere Informationen finden Sie in der API-Referenz für SubmitRfc.

Erstellen, Klonen, Aktualisieren, Suchen und Stornieren RFCs

Die folgenden Beispiele führen Sie durch verschiedene RFC-Operationen.

Themen

- Erstellen Sie einen RFC
- Mit der AMS-Konsole klonen RFCs (neu erstellen)
- Aktualisierung RFCs
- Finden RFCs
- Stornieren RFCs

Erstellen Sie einen RFC

Einen RFC mit der Konsole erstellen

Im Folgenden finden Sie die erste Seite des RFC-Erstellungsprozesses in der AMS-Konsole, auf der Quick Cards geöffnet und Browse-Änderungstypen aktiv sind:

Im Folgenden finden Sie die erste Seite des RFC-Erstellungsprozesses in der AMS-Konsole, auf der die Option Nach Kategorie auswählen aktiviert ist:

So funktioniert es:

1. Navigieren Sie zur Seite RFC erstellen: Klicken Sie im linken Navigationsbereich der AMS-Konsole, um die RFCs Listenseite RFCszu öffnen, und klicken Sie dann auf RFC erstellen.
2. Wählen Sie in der Standardansicht „Änderungstypen durchsuchen“ einen beliebten Änderungstyp (CT) oder wählen Sie in der Ansicht „Nach Kategorie auswählen“ einen CT aus.
   - Nach Änderungstyp suchen: Sie können im Bereich Schnellerstellung auf ein beliebtes CT klicken, um sofort die Seite RFC ausführen zu öffnen. Beachten Sie, dass Sie mit Quick Create keine ältere CT-Version auswählen können.

Verwenden Sie zum Sortieren CTs den Bereich Alle Änderungstypen in der Karten - oder Tabellenansicht. Wählen Sie in einer der Ansichten einen CT aus und klicken Sie dann auf RFC erstellen, um die Seite RFC ausführen zu öffnen. Falls zutreffend, wird neben der Schaltfläche „RFC erstellen“ die Option Mit älterer Version erstellen angezeigt.

- Nach Kategorie auswählen: Wählen Sie eine Kategorie, eine Unterkategorie, einen Artikel und einen Vorgang aus. Daraufhin wird das Feld mit den CT-Details geöffnet. Dort können Sie gegebenenfalls die Option „Mit älterer Version erstellen“ auswählen. Klicken Sie auf RFC erstellen, um die Seite RFC ausführen zu öffnen.

3. Öffnen Sie auf der Seite RFC ausführen den Bereich CT-Name, um das Feld mit den CT-Details zu sehen. Ein Betreff ist erforderlich (dieser wird für Sie ausgefüllt, wenn Sie Ihr CT in der Ansicht „Änderungstypen durchsuchen“ auswählen). Öffnen Sie den Bereich Zusätzliche Konfiguration, um Informationen zum RFC hinzuzufügen.

   Verwenden Sie im Bereich Ausführungskonfiguration die verfügbaren Dropdownlisten oder geben Sie Werte für die erforderlichen Parameter ein. Um optionale Ausführungsparameter zu konfigurieren, öffnen Sie den Bereich Zusätzliche Konfiguration.
4. Wenn Sie fertig sind, klicken Sie auf Ausführen. Wenn keine Fehler vorliegen, wird die Seite mit dem RFC erfolgreich erstellt mit den übermittelten RFC-Details und der ersten Run-Ausgabe angezeigt.
5. Öffnen Sie den Bereich Run-Parameter, um die von Ihnen eingereichten Konfigurationen zu sehen. Aktualisieren Sie die Seite, um den RFC-Ausführungsstatus zu aktualisieren. Optional können Sie den RFC abbrechen oder eine Kopie davon mit den Optionen oben auf der Seite erstellen.

Einen RFC mit der CLI erstellen

So funktioniert es:

1. Verwenden Sie entweder Inline Create (Sie geben einen `create-rfc` Befehl mit allen RFC- und Ausführungsparametern aus) oder Template Create (Sie erstellen zwei JSON-Dateien, eine für die RFC-Parameter und eine für die Ausführungsparameter) und geben Sie den `create-rfc` Befehl mit den beiden Dateien als Eingabe aus. Beide Methoden werden hier beschrieben.
2. Reichen Sie den `aws amscm submit-rfc --rfc-id` *`ID`* Befehl RFC: mit der zurückgegebenen RFC-ID ein.

   Überwachen Sie den RFC: -Befehl. `aws amscm get-rfc --rfc-id` *`ID`*

Verwenden Sie diesen Befehl, um die Version des Änderungstyps zu überprüfen:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Sie können alle `CreateRfc` Parameter mit jedem RFC verwenden, unabhängig davon, ob sie Teil des Schemas für den Änderungstyp sind oder nicht. Um beispielsweise Benachrichtigungen zu erhalten, wenn sich der RFC-Status ändert, fügen Sie diese Zeile dem RFC-Parameter-Teil der Anfrage hinzu (nicht den Ausführungsparametern). `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` Eine Liste aller CreateRfc Parameter finden Sie in der AMS Change Management API-Referenz.

INLINE-ERSTELLUNG:

Geben Sie den Befehl create RFC mit den direkt angegebenen Ausführungsparametern aus (vermeiden Sie Anführungszeichen, wenn Sie die Ausführungsparameter inline angeben), und senden Sie dann die zurückgegebene RFC-ID. Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:

```
aws amscm create-rfc --change-type-id "CT_ID" --change-type-version "VERSION" --title
 "TITLE" --execution-parameters "{\"Description\": \"example\"}"
```

VORLAGE ERSTELLEN:

> **Note**
>
> In diesem Beispiel für die Erstellung eines RFC wird der Stack-Änderungstyp Load Balancer (ELB) verwendet.

1. Suchen Sie das entsprechende CT. Der folgende Befehl durchsucht CT-Klassifikationszusammenfassungen nach solchen, die „ELB“ im Artikelnamen enthalten, und erstellt eine Ausgabe der Kategorie, des Artikels, der Operation und der ChangeType ID in Tabellenform (Unterkategorie für beide ist`Advanced stack components`).

```
aws amscm list-change-type-classification-summaries --query
 "ChangeTypeClassificationSummaries[?contains(Item,'ELB')].
[Category,Item,Operation,ChangeTypeId]" --output table
```

```
-------------------------------------------------------------------
|                            CtSummaries                          |
+-----------+--------------------------+--------------------------+
| Deployment| Load balancer (ELB) stack | Create | ct-123h45t6uz7jl |
| Management| Load balancer (ELB) stack | Update | ct-0ltm873rsebx9 |
+-----------+--------------------------+--------------------------+
```

2. Finden Sie die aktuellste Version des CT:

   `ChangeTypeId`und`ChangeTypeVersion`: Die Änderungstyp-ID für diese exemplarische Vorgehensweise lautet `ct-123h45t6uz7jl` (create ELB). Um die neueste Version herauszufinden, führen Sie diesen Befehl aus:

   ```
   aws amscm list-change-type-version-summaries --filter
    Attribute=ChangeTypeId,Value=ct-123h45t6uz7jl
   ```

3. Informieren Sie sich über die Optionen und Anforderungen. Der folgende Befehl gibt das Schema in eine JSON-Datei namens CreateElbParams .json aus.

   ```
   aws amscm get-change-type-version --change-type-id "ct-123h45t6uz7jl" --query
    "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateElbParams.json
   ```

4. Ändern und speichern Sie die JSON-Datei mit den Ausführungsparametern. In diesem Beispiel wird die Datei „ CreateElbParams.json“ genannt.

   Bei einem Bereitstellungs-CT StackTemplateId ist das im Schema enthalten und muss in den Ausführungsparametern eingereicht werden.

   Für die Angabe TimeoutInMinutes, wie viele Minuten für die Erstellung des Stacks vorgesehen sind, bevor der RFC fehlschlägt, verzögert diese Einstellung die RFC-Ausführung nicht, aber Sie müssen genügend Zeit einplanen (geben Sie beispielsweise nicht „5" an). Gültige Werte sind „60" bis „360", für CTs Langzeitanwendungen UserData: Create und Create EC2 ASG. Wir empfehlen für alle anderen Bereitstellungen den zulässigen Höchstwert von „60“. CTs

Geben Sie die ID der VPC an, in der der Stack erstellt werden soll. Sie können die VPC-ID mit dem CLI-Befehl abrufen. `aws amsskms list-vpc-summaries`

```
{
"Description":      "ELB-Create-RFC",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-sdhopv00000000000",
"Name":             "MyElbInstance",
"TimeoutInMinutes": 60,
"Parameters":   {
    "ELBSubnetIds":                     ["SUBNET_ID"],
    "ELBHealthCheckHealthyThreshold":   4,
    "ELBHealthCheckInterval":           5,
    "ELBHealthCheckTarget":             "HTTP:80/",
    "ELBHealthCheckTimeout":            60,
    "ELBHealthCheckUnhealthyThreshold": 5,
    "ELBScheme":                        false
    }
}
```

5. Geben Sie die RFC-JSON-Vorlage in eine Datei in Ihrem aktuellen Ordner namens .json aus: CreateElbRfc

```
aws amscm create-rfc --generate-cli-skeleton > CreateElbRfc.json
```

6. Ändern und speichern Sie die CreateElbRfc JSON-Datei. Da Sie die Ausführungsparameter in einer separaten Datei erstellt haben, entfernen Sie die `ExecutionParameters` Zeile. Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:

```
{
"ChangeTypeVersion":    "2.0",
"ChangeTypeId":         "ct-123h45t6uz7jl",
"Title":                "Create ELB"
}
```

7. Erstellen Sie den RFC. Der folgende Befehl spezifiziert die Ausführungsparameterdatei und die RFC-Vorlagendatei:

```
aws amscm create-rfc --cli-input-json file://CreateElbRfc.json --execution-
parameters file://CreateElbParams.json
```

Sie erhalten die ID des neuen RFC in der Antwort und können sie verwenden, um den RFC zu senden und zu überwachen. Bis Sie ihn abschicken, verbleibt der RFC im Bearbeitungszustand und startet nicht.

Tipps

> **Note**
>
> Sie können das AMS verwenden, um einen RFC API/CLI zu erstellen, ohne eine RFC-JSON-Datei oder eine JSON-Datei mit CT-Ausführungsparametern zu erstellen. Dazu verwenden Sie den `create-rfc` Befehl und fügen dem Befehl die erforderlichen RFC- und Ausführungsparameter hinzu. Dies wird „Inline Create“ genannt. Beachten Sie, dass alle Bereitstellungen CTs innerhalb des `execution-parameters` Blocks ein `Parameters` Array mit den Parametern für die Ressource enthielten. Die Parameter müssen Anführungszeichen enthalten, die mit einem umgekehrten Schrägstrich (\) maskiert werden. Die andere dokumentierte Methode zur Erstellung eines RFC heißt „Template Create“. Hier erstellen Sie eine JSON-Datei für die RFC-Parameter und eine weitere JSON-Datei für die Ausführungsparameter und senden die beiden Dateien mit dem `create-rfc` Befehl ab. Diese Dateien können als Vorlagen dienen und für die future wiederverwendet werden. RFCs Bei der Erstellung RFCs mit Vorlagen können Sie einen Befehl verwenden, um die JSON-Datei mit dem gewünschten Inhalt zu erstellen, indem Sie einen Befehl wie in der Abbildung gezeigt ausführen. Die Befehle erstellen eine Datei mit dem Namen „parameters.json“ mit dem angezeigten Inhalt. Sie können diese Befehle auch verwenden, um die RFC-JSON-Datei zu erstellen.

Mit der AMS-Konsole klonen RFCs (neu erstellen)

Sie können die AMS-Konsole verwenden, um einen vorhandenen RFC zu klonen.

Gehen Sie folgendermaßen vor, um einen RFC mithilfe der AMS-Konsole zu klonen oder neu zu erstellen:

1. Suchen Sie den entsprechenden RFC. Klicken Sie in der linken Navigationsleiste auf RFCs.

   Das RFCs Dashboard wird geöffnet.

2. Scrollen Sie durch die Seiten, bis Sie den RFC gefunden haben, den Sie klonen möchten. Verwenden Sie die Option Filter, um die Liste einzugrenzen. Wählen Sie den RFC aus, den Sie klonen möchten.

   Die RFC-Detailseite wird geöffnet.

3. Klicken Sie auf Kopie erstellen.

   Die Seite „Änderungsantrag erstellen“ wird geöffnet, auf der alle Optionen wie im ursprünglichen RFC festgelegt sind.

4. Nehmen Sie die gewünschten Änderungen vor. Um zusätzliche Optionen festzulegen, ändern Sie die Option Basic in Advanced. Nachdem Sie alle Optionen festgelegt haben, wählen Sie Absenden.

   Die aktive RFC-Detailseite wird mit einer neuen RFC-ID für den geklonten RFC geöffnet, und der geklonte RFC wird im RFC-Dashboard angezeigt.

Aktualisierung RFCs

Sie können einen zurückgewiesenen oder noch nicht eingereichten RFC erneut einreichen, indem Sie den RFC aktualisieren und ihn dann einreichen oder erneut einreichen. Beachten Sie, dass die meisten abgelehnt RFCs werden, weil der angegebene Wert vor der Einreichung bestanden `RequestedStartTime` wurde oder der angegebene Wert für die Ausführung des RFC nicht TimeoutInMinutes ausreicht (da ein erfolgreicher RFC TimeoutInMinutes nicht verlängert wird, empfehlen wir, diesen Wert immer auf mindestens „60" und bis zu „360" für eine Amazon- EC2 oder Amazon EC2 Auto Scaling Scaling-Gruppe mit langer Laufzeit zu setzen). UserData In diesem Abschnitt wird beschrieben, wie Sie die CLI-Version des `UpdateRfc` Befehls verwenden, um einen RFC mit einem neuen RFC-Parameter oder mit neuen Parametern zu aktualisieren, die entweder stringifiziertes JSON oder eine aktualisierte Parameterdatei verwenden.

Dieses Beispiel beschreibt die Verwendung der CLI-Version der UpdateRfc AMS-API (siehe Update RFC). Es gibt zwar Änderungstypen für die Aktualisierung einiger Ressourcen (DNS privat und öffentlich, Load Balancer-Stacks und Stack-Patching-Konfiguration), aber es gibt kein CT zur Aktualisierung eines RFC.

Wir empfehlen, dass Sie jeweils einen UpdateRfc Vorgang einreichen. Wenn Sie mehrere Updates einreichen, z. B. für einen DNS-Stack, schlagen die Aktualisierungen möglicherweise fehl, wenn versucht wird, den DNS gleichzeitig zu aktualisieren.

ERFORDERLICHE DATEN`RfcId`: Der RFC, den Sie aktualisieren.

OPTIONALE DATEN`ExecutionParameters`: Sofern Sie kein nicht erforderliches Feld aktualisieren, würden Sie beispielsweise geänderte Ausführungsparameter angeben`Description`, um die Probleme zu beheben, die dazu geführt haben, dass der RFC abgelehnt oder storniert wurde. Alle übermittelten Werte, die nicht Null sind, überschreiben diese Werte im ursprünglichen RFC.

1. Suchen Sie den entsprechenden abgelehnten oder stornierten RFC. Sie können diesen Befehl verwenden (Sie können den Wert durch ersetzen): `Canceled`

   ```
   aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Rejected
   ```

2. Sie können jeden der folgenden RFC-Parameter ändern:

   ```
   {
       "Description": "string",
       "ExecutionParameters": "string",
       "ExpectedOutcome": "string",
       "ImplementationPlan": "string",
       "RequestedEndTime": "string",
       "RequestedStartTime": "string",
       "RfcId": "string",
       "RollbackPlan": "string",
       "Title": "string",
       "WorstCaseScenario": "string"}
   ```

   Beispielbefehl zur Aktualisierung des Felds Beschreibung:

   ```
   aws amscm update-rfc --description "AMSTestNoOpsActionRequired" --rfc-id "RFC_ID"
    --region us-east-1
   ```

   Beispielbefehl zur Aktualisierung des ExecutionParameters VpcId Felds:

   ```
   aws amscm update-rfc  --execution-parameters "{\"VpcId\":\"VPC_ID\"}" --rfc-id
    "RFC_ID" --region us-east-1
   ```

   Beispielbefehl, der den RFC mit einer Ausführungsparameterdatei aktualisiert, die die Aktualisierungen enthält; siehe Beispiel für eine Ausführungsparameterdatei in Schritt 2 von: EC2 stack | Create:

```
aws amscm update-rfc --execution-parameters file://CreateEc2ParamsUpdate.json --
rfc-id "RFC_ID" --region us-east-1
```

3. Reichen Sie den RFC erneut ein `submit-rfc` und verwenden Sie dabei dieselbe RFC-ID, die Sie bei der ersten Erstellung des RFC haben:

   ```
   aws amscm submit-rfc --rfc-id RFC_ID
   ```

   Wenn der RFC erfolgreich ist, erhalten Sie in der Befehlszeile keine Bestätigungs- oder Fehlermeldungen.

4. Führen Sie den folgenden Befehl aus, um den Status der Anforderung zu überwachen und die Ausführungsausgabe anzuzeigen.

   ```
   aws amscm get-rfc --rfc-id RFC_ID
   ```

Finden RFCs

Suchen Sie mit der Konsole nach einer Änderungsanforderung (RFC)

Gehen Sie folgendermaßen vor, um mithilfe der AMS-Konsole nach einem RFC zu suchen.

> **Note**
>
> Dieses Verfahren gilt nur für geplante RFCs Benutzer, die RFCs die ASAP-Option nicht verwendet haben.

1. Klicken Sie in der linken Navigationsleiste auf RFCs.

   Das RFCs Dashboard wird geöffnet.

2. Scrollen Sie durch die Liste oder verwenden Sie die Option Filter, um die Liste zu verfeinern.

   Die RFC-Liste ändert sich je nach Filterkriterium.

3. Wählen Sie den Betreff-Link für den gewünschten RFC.

   Die RFC-Detailseite für diesen RFC wird mit Informationen wie der RFC-ID geöffnet.

4. Wenn das Dashboard viele enthält RFCs , können Sie die Option Filter verwenden, um nach RFC zu suchen:

   - Betreff: Die Betreffzeile oder der Titel (in der API/CLI), der dem RFC bei seiner Erstellung gegeben wurde.
   - RFC-ID: Die Kennung für den RFC.
   - Aktivitätsstatus: Wenn Sie den RFC-Status kennen, können Sie wählen, ob ein Operator gerade den RFC betrachtet, AwsOperatorAssignedwas AwsActionPendingbedeutet, dass ein AMS-Operator etwas ausführen muss, bevor die RFC-Ausführung fortgesetzt werden kann, oder CustomerActionPendingob Sie eine Aktion ausführen müssen, bevor die RFC-Ausführung fortgesetzt werden kann.
   - Status: Wenn Sie den RFC-Status kennen, können Sie wählen zwischen:
     - Geplant: RFCs die geplant waren.
     - Abgesagt: RFCs die wurden storniert.
     - In Bearbeitung: RFCs In Bearbeitung.
     - Erfolgreich: RFCs Das wurde erfolgreich ausgeführt.
     - Abgelehnt: RFCs die wurden abgelehnt.
     - Bearbeitung: RFCs die gerade bearbeitet werden.
     - Fehlschlag: RFCs das ist fehlgeschlagen.
     - Ausstehende Genehmigung: RFCs Dies kann erst fortgesetzt werden, wenn AMS oder Sie die Genehmigung erteilt haben. In der Regel bedeutet dies, dass Sie den RFC genehmigen müssen. Sie werden in Ihrer Liste der Serviceanfragen eine entsprechende Servicebenachrichtigung erhalten haben.
   - Typ ändern: Wählen Sie die Kategorie, Unterkategorie, Artikel und Vorgang aus, und die ID des Änderungstyps wird für Sie abgerufen.
   - Angeforderte Startzeit oder Angeforderte Endzeit: Mit dieser Filteroption können Sie „Vorher“ oder „Nachher“ wählen und dann ein Datum und optional eine Uhrzeit (hh:mm und Zeitzone) eingeben. Dieser Filter funktioniert nur nach Zeitplan erfolgreich RFCs (nicht so schnell wie RFCs möglich).
   - Status: Entweder geplant, Storniert, In Bearbeitung, Erfolgreich, Abgelehnt, Bearbeitung oder Fehlgeschlagen.
   - Betreff: Der Betreff (oder Titel, wenn der RFC mit der API/CLI erstellt wurde), den Sie dem RFC gegeben haben.
   - Typ-ID ändern: Verwenden Sie die Kennung für den mit dem RFC übermittelten Änderungstyp.

Mit der Suche können Sie die Filter hinzufügen, wie im folgenden Screenshot gezeigt.

5. Klicken Sie auf den Betreff-Link für den gewünschten RFC.

   Die RFC-Detailseite für diesen RFC mit Informationen, einschließlich der RFC-ID, wird geöffnet.

Einen Änderungsantrag (RFC) mit der CLI finden

Sie können mehrere Filter verwenden, um einen RFC zu finden.

Verwenden Sie diesen Befehl, um die Version des Änderungstyps zu überprüfen:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Sie können alle `CreateRfc` Parameter mit jedem RFC verwenden, unabhängig davon, ob sie Teil des Schemas für den Änderungstyp sind oder nicht. Um beispielsweise Benachrichtigungen zu erhalten, wenn sich der RFC-Status ändert, fügen Sie diese Zeile dem RFC-Parameter-Teil der Anfrage hinzu (nicht den Ausführungsparametern). `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` Eine Liste aller CreateRfc Parameter finden Sie in der AMS Change Management API-Referenz.

Wenn Sie sich die RFC-ID nicht notieren und sie später finden müssen, können Sie das AMS Change Management (CM) -System verwenden, um danach zu suchen und die Ergebnisse mit einem Filter oder einer Abfrage einzugrenzen.

1. Der ListRfcSummariesCM-API-Vorgang verfügt über Filter. Sie können Ergebnisse auf der Grundlage einer `Value` Kombination aus `Attribute` und in einer logischen UND-Operation oder basierend auf einem `AttributeCondition`, einem und filtern`Values`.

RFC-Filterung

Attribut	Zulässige Werte	Gültige Bedingungen	Standardbedingung	Hinweise
ActualEndTime	Eine beliebige Zeichenfolge, die eine ISO86 01-Datetime darstellt (z. B. „20170101 T000000Z“)	Vorher, Nachher, Dazwischen	Keine	Die Bedingung Vorher oder Nachher akzeptiert nur einen Wert im Feld Werte. Die Between-Bedingung muss genau zwei Werte im Wertefeld haben, wobei der erste Wert für ein Datum stehen sollte, das vor dem zweiten Wert liegt
ActualStartTime	Jede Zeichenfolge, die eine Datetime von ISO86 01 darstellt (z. B. „20170101 T000000Z“)	Vorher, Nachher, Dazwischen	Keine	Die Bedingung Vorher oder Nachher akzeptiert nur einen Wert im Feld Werte. Die Between-Bedingung muss genau zwei Werte im Wertefeld haben, wobei der erste Wert für ein Datum stehen sollte, das vor dem zweiten Wert liegt
AutomationStatusId	Manuell, Automatisiert	Gleichheitszeichen	Gleichheitszeichen	Es gibt nur zwei Automatisierungsstatus

Attribut	Zulässige Werte	Gültige Bedingungen	Standardbedingung	Hinweise
ChangeTypeId	Jede gültige Änderungstyp-ID, z. B. ct-123h45t6uz7jl	Gleichheitszeichen	Gleichheitszeichen	Suchen Sie nach einem Änderungstyp oder CSIO
ChangeTypeVersion	Jede gültige Änderungstyp-ID, zum Beispiel 1.0	Gleichheitszeichen	Gleichheitszeichen	Einen Änderungstyp oder CSIO finden
CreatedBy	Beliebige Zeichenfolge (die maximal zulässige Länge beträgt 2048 Zeichen)	Enthält	Enthält	Das CreatedBy Feld des RFC enthält den ARN des Benutzers, der ihn erstellt hat
CreatedTime	Jede Zeichenfolge, die eine ISO86 01 Datetime darstellt (zum Beispiel „20170101 T000000Z“)	Vorher, Nachher, Dazwischen	Keine	Die Bedingung Vorher oder Nachher akzeptiert nur einen Wert im Feld Werte. Die Between-Bedingung muss genau zwei Werte im Wertefeld haben, wobei der erste Wert für ein Datum stehen sollte, das vor dem zweiten Wert liegt

Attribut	Zulässige Werte	Gültige Bedingungen	Standardbedingung	Hinweise
LastModifiedTime	Jede Zeichenfolge, die eine Datetime von ISO86 01 darstellt (z. B. „20170101T000000Z“)	Vorher, Nachher, Dazwischen	Keine	Die Bedingung Vorher oder Nachher akzeptiert nur einen Wert im Feld Werte. Die Between-Bedingung muss genau zwei Werte im Wertefeld haben, wobei der erste Wert für ein Datum stehen sollte, das vor dem zweiten Wert liegt
LastSubmittedTime	Jede Zeichenfolge, die eine Datetime von ISO86 01 darstellt (z. B. „20170101T000000Z“)	Vorher, Nachher, Dazwischen	Keine	Die Bedingung Vorher oder Nachher akzeptiert nur einen Wert im Feld Werte. Die Between-Bedingung muss genau zwei Werte im Wertefeld haben, wobei der erste Wert für ein Datum stehen sollte, das vor dem zweiten Wert liegt

Attribut	Zulässige Werte	Gültige Bedingungen	Standardbedingung	Hinweise
RequestedEndTime	Jede Zeichenfolge, die eine Datetime von ISO86 01 darstellt (z. B. „20170101T000000Z“)	Vorher, Nachher, Dazwischen	Keine	Die Bedingung Vorher oder Nachher akzeptiert nur einen Wert im Feld Werte. Die Between-Bedingung muss genau zwei Werte im Wertefeld haben, wobei der erste Wert für ein Datum stehen sollte, das vor dem zweiten Wert liegt
RequestedStartTime	Jede Zeichenfolge, die eine Datetime von ISO86 01 darstellt (z. B. „20170101T000000Z“)	Vorher, Nachher, Dazwischen	Keine	Die Bedingung Vorher oder Nachher akzeptiert nur einen Wert im Feld Werte. Die Between-Bedingung muss genau zwei Werte im Wertefeld haben, wobei der erste Wert für ein Datum stehen sollte, das vor dem zweiten Wert liegt
RfcStatusId	Abgebrochen, Bearbeitung, Fehlgeschlagen,, InProgress PendingApproval, Abgelehnt, Geplant, Erfolgreich	Gleichheitszeichen	Gleichheitszeichen	Aktualisieren Sie die RFC-Liste in der AMS-Konsole oder führen Sie den Befehl aus GetRfc

Attribut	Zulässige Werte	Gültige Bedingungen	Standardbedingung	Hinweise
Titel	Jeder gültige RFC-Titel	Enthält	Enthält	Reguläre Ausdrücke in jedem einzelnen Feld werden nicht unterstützt. Suche ohne Berücksichtigung von Groß- und Kleinschreibung

Beispiele:

Um alle Informationen IDs zu finden, die sich auf SQS RFCs beziehen (wobei SQS im Artikelbereich des CT enthalten ist), können Sie diesen Befehl verwenden:

```
list-rfc-summaries --query 'RfcSummaries[?contains(Item.Name,`SQS`)].
[Category.Id,Subcategory.Id,Type.Id,Item.Id,RfcId]' --output table
```

Was ungefähr das Folgende zurückgibt:

```
--------------------------------------------------------------------------
|                          ListRfcSummaries                              |
+----------+---------------------------------+-------+-------+----------------+
|Deployment| Advanced Stack Components      |SQS    |Create |ct-123h45t6uz7jl|
|Management| Monitoring & Notification  |SQS    |Update |ct-123h45t6uz7jl|
+----------+---------------------------------+-------+-------+----------------+
```

Ein weiterer verfügbarer Filter `list-rfc-summaries` ist`AutomationStatusId`, um nach RFCs automatisierten oder manuellen Filtern zu suchen:

```
aws amscm list-rfc-summaries --filter Attribute=AutomationStatusId,Value=Automated
```

Ein weiterer verfügbarer Filter für `list-rfc-summaries` ist `Title` (Betreff in der Konsole):

```
 Attribute=Title,Value=RFC-TITLE
```

Beispiel für die neue Anforderungsstruktur in JSON, die Folgendes zurückgibt RFCs :

- (Der Titel ENTHÄLT den Ausdruck „Windows 2012" ODER „Amazon Linux“) UND
- (RfcStatusId ENTSPRICHT „Erfolg“ ODER "InProgress„) UND
- (20170101T000000Z <= <= 20170103T000000Z) UND (<= RequestedStartTime 20170103T000000Z) ActualEndTime

```
{
  "Filters": [
    {
      "Attribute": "Title",
      "Values": ["Windows 2012", "Amazon Linux"],
      "Condition": "Contains"
    },
    {
      "Attribute": "RfcStatusId",
      "Values": ["Success", "InProgress"],
      "Condition": "Equals"
    },
    {
      "Attribute": "RequestedStartTime",
      "Values": ["20170101T000000Z", "20170103T000000Z"],
      "Condition": "Between"
    },
    {
      "Attribute": "ActualEndTime",
      "Values": ["20170103T000000Z"],
      "Condition": "Before"
    }
  ]
}
```

> **Note**
>
> Mit der Weiterentwicklung beabsichtigt AMS, `Filters` die folgenden Felder in einer kommenden Version nicht mehr zu unterstützen:
>
> - Wert: Das Feld Wert ist Teil des Felds Filter. Verwenden Sie das Wertefeld, das erweiterte Funktionen unterstützt.

- RequestedEndTimeRange: Verwenden Sie das Feld RequestedEndTime innerhalb des Filters, das erweiterte Funktionen unterstützt
- RequestedStartTimeRange: Verwenden Sie das Feld RequestedStartTime innerhalb des Filters, das erweiterte Funktionen unterstützt.

Informationen zur Verwendung von CLI-Abfragen finden Sie unter So filtern Sie die Ausgabe mit der Option --query und in der Referenz zur Abfragesprache, JMESPath Spezifikation.

2. Wenn Sie die AMS-Konsole verwenden:

   Gehen Sie zur RFCsListenseite. Bei Bedarf können Sie nach dem RFC-Betreff filtern, den Sie `Title` bei der Erstellung als RFC eingegeben haben.

Tipps

> **Note**
>
> Dieses Verfahren gilt nur für geplante RFCs Benutzer, die die RFCs ASAP-Option nicht verwendet haben.

Stornieren RFCs

Sie können einen RFC mit der Konsole oder der AMS API/CLI stornieren.

Um einen RFC mit der Konsole zu stornieren, suchen Sie den RFC in Ihrer RFC-Liste, öffnen Sie ihn und klicken Sie auf Abbrechen.

Erforderliche Daten:

- `Reason`: Warum kündigen Sie den RFC.
- `RfcId`: Der RFC, den Sie stornieren.

1. Normalerweise würden Sie einen RFC direkt nach dem Absenden stornieren (daher sollte die RFC-ID griffbereit sein). Andernfalls können Sie ihn nur stornieren, wenn Sie ihn geplant haben und er vor der angegebenen Startzeit liegt. Wenn Sie die RFC-ID suchen müssen, können Sie

diesen Befehl verwenden (Sie können den durch einen manuell `Value PendingApproval` genehmigten RFC ersetzen):

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Scheduled
```

2. Beispielbefehl zum Stornieren eines RFC:

```
aws amscm cancel-rfc --reason "Bad Stack ID" --rfc-id "RFC_ID" --profile saml --
region us-east-1
```

Verwenden Sie die AMS-Konsole mit RFCs

Die AMS-Konsole bietet Funktionen, die Ihnen beim erfolgreichen Erstellen und Einreichen helfen RFCs.

Verwenden Sie die RFC-Listenseite (Konsole)

Die RFCsListenseite der AMS-Konsole bietet Ihnen die folgenden Optionen:

- Erweiterte RFC-Suche mithilfe eines Filters. Weitere Informationen finden Sie unter Finden RFCs.
- Finden Sie heraus, wann der RFC das letzte Mal geändert wurde. Dieser Wert steht für das letzte Mal, als der RFC-Status geändert wurde.
- RFC-Details mit dem RFC-Betreff anzeigen. Wenn Sie diesen Link wählen, wird die Detailseite für diesen RFC geöffnet.
- RFC-Status anzeigen. Weitere Informationen finden Sie unter RFC-Statuscodes verstehen

Verwenden Sie RFC Quick Create (Konsole)

Verwenden Sie die RFC-Schnellerstellungskarten oder die Listentabelle oder wählen Sie die Änderungstypen RFCs nach Klassifizierung aus.

Weitere Informationen hierzu finden Sie unter Erstellen Sie einen RFC.

Fügen Sie RFC-Korrespondenz und Anlagen hinzu (Konsole)

Sie können einem RFC Korrespondenz hinzufügen, nachdem er eingereicht wurde und bevor er genehmigt wurde, z. B. solange er sich im Status "" PendingApproval befindet. Nachdem

ein RFC genehmigt wurde (im Status „Geplant“ oder "InProgress„), kann keine Korrespondenz hinzugefügt werden, da dies als Änderung der Anfrage interpretiert werden könnte. Nachdem ein RFC abgeschlossen ist (im Status „Storniert“, „Abgelehnt“, „Erfolgreich“ oder „Fehlgeschlagen“), wird die Korrespondenz wieder aktiviert, obwohl die Korrespondenz deaktiviert wird, sobald ein RFC für mehr als 30 Tage geschlossen ist.

> **Note**
>
> Jede Korrespondenz ist auf 5.000 Zeichen begrenzt.

Einschränkungen für Anlagen:

- Nur drei Anlagen pro Korrespondenz.
- Beschränken Sie sich auf fünfzig Anhänge pro RFC.
- Jeder Anhang muss weniger als 5 MB groß sein.
- Es werden nur Textdateien wie Klartext (`.txt`), kommagetrennte Werte (`.csv`), JSON () oder YAML (`.json`) akzeptiert. `.yaml` Im Fall des YAML-Formats muss die Datei mit der Dateierweiterung angehängt werden. `.yaml`

  > **Note**
  >
  > Textdateien mit XML-Inhalt sind verboten. Wenn Sie XML-Inhalte mit AMS teilen möchten, verwenden Sie eine Serviceanfrage.

- Dateinamen sind auf 255 Zeichen begrenzt und enthalten nur Zahlen, Buchstaben, Leerzeichen, Bindestriche (-), Unterstriche (_) und Punkte (.).
- Das Aktualisieren und Löschen von Anhängen in einem RFC wird derzeit nicht unterstützt.

Gehen Sie folgendermaßen vor, um einem RFC Korrespondenz und Anlagen hinzuzufügen:

1. Suchen Sie in der AMS-Konsole auf der RFC-Detailseite für einen RFC unten auf der Seite nach dem Abschnitt Korrespondenz.

   Vor jeder Korrespondenz:

   Nach einiger Korrespondenz:

2. Um eine neue Korrespondenz hinzuzufügen, geben Sie Ihre Nachricht in das Textfeld Antwort ein. Um Dateien anzuhängen, die sich auf die Korrespondenz beziehen, wählen Sie Anlage hinzufügen und wählen Sie dann die gewünschten Dateien aus.

3. Wenn Sie fertig sind, wählen Sie Senden.

   Die neue Korrespondenz wird zusammen mit den Links zu den angehängten Dateien in der Korrespondenzliste auf der RFC-Detailseite angezeigt.

RFC-E-Mail-Benachrichtigungen konfigurieren (Konsole)

Auf der Seite zum Erstellen von Änderungsanträgen in der AMS-Konsole haben Sie die Möglichkeit, E-Mail-Adressen hinzuzufügen, um Benachrichtigungen über RFC-Statusänderungen zu erhalten:

Darüber hinaus können Sie E-Mail-Adressen für Benachrichtigungen zu beliebigen Änderungstypen hinzufügen, zum Beispiel:

```
aws amscm create-rfc --change-type-id <Change type ID>
                    --change-type-version 1.0 --title "TITLE"
                    --notification "{\"Email\": {\"EmailRecipients\" :
 [\"email@example.com\"]}}"
```

Fügen Sie jeder Inline- oder Template-Anfrage vom Typ Change eine ähnliche Zeile (`--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"`) im RFC-Parameter-Teil der Anfrage hinzu, nicht im Parameter-Teil.

Erfahren Sie mehr über gängige RFC-Parameter

Im Folgenden sind die RFC-Parameter aufgeführt, die Sie einreichen müssen, sowie die Parameter, die häufig in folgenden Bereichen verwendet werden: RFCs

- Typinformationen ändern: ChangeTypeId und ChangeTypeVersion. Eine Liste der Änderungstypen IDs und Versionsnummern finden Sie unter Referenz zum Änderungstyp.

Führen Sie `list-change-type-classification-summaries` in der CLI mit dem `query` Argument aus, um die Ergebnisse einzugrenzen. Grenzen Sie beispielsweise die Ergebnisse ein, um Typen zu ändern, die „Access“ im `Item` Namen enthalten.

```
aws amscm list-change-type-classification-summaries --query
 "ChangeTypeClassificationSummaries [?contains (Item, 'access')].
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

Führen Sie den `get-change-type-version` Befehl aus und geben Sie die ID des Änderungstyps an. Der folgende Befehl ruft die CT-Version für ct-2tylseo8rxfsc ab.

```
aws amscm get-change-type-version --change-type-id ct-2tylseo8rxfsc
```

- Titel: Ein Name für den RFC; dieser wird zum Betreff des RFC in der RFC-Liste der AMS-Konsole, und Sie können danach suchen, indem Sie den Befehl und einen Filter auf `GetRfc Title`
- Planung: Wenn Sie einen geplanten RFC wünschen, müssen Sie die `RequestedEndTime` Parameter `RequestedStartTime` und angeben oder die Konsolenoption „Diese Änderung planen“ verwenden. Bei einem ASAP-RFC (der ausgeführt wird, sobald er genehmigt wurde), wenn Sie die CLI verwenden, lassen Sie den Wert leer `RequestedStartTime` und `RequestedEndTime` null. Wenn Sie die Konsole verwenden, akzeptieren Sie die ASAP-Option.

  Wenn das `RequestedStartTime` fehlt, wird der RFC zurückgewiesen.
- Bereitstellung CTs: Die Ausführungsparameter oder `Parameters` die spezifischen Einstellungen, die für die Bereitstellung der Ressource erforderlich sind. Sie sind je nach CT sehr unterschiedlich.
- Nichtbereitstellung CTs: Ressourcen CTs , die keine Ressource bereitstellen, z. B. Zugriff CTs oder Andere | Andere, oder Stapel löschen, haben nur minimale Ausführungsparameter und keinen `Parameters` Block.
- Manche verlangen RFCs auch, dass Sie angeben`TimeoutInMinutes`, wie viele Minuten für die Erstellung des Stacks vorgesehen sind, bevor der RFC fehlschlägt. Gültige Werte liegen zwischen 60 (Minuten) und 360 (bei langer UserData Laufzeit). Wenn die Ausführung nicht abgeschlossen werden kann, bevor der Wert überschritten `TimeoutInMinutes` wird, schlägt der RFC fehl. Diese Einstellung verzögert jedoch nicht die Ausführung des RFC.
- RFCs die Instanzen erstellen, wie z. B. einen S3-Bucket oder einen ELB, stellen im Allgemeinen ein Schema bereit, mit dem Sie bis zu sieben Tags (Schlüssel/Wert-Paare) hinzufügen können. Sie können Ihrem S3-Bucket weitere Tags hinzufügen, indem Sie über Deployment | Advanced stack components | Tag | Create change type (ct-3cx7we852p3af) einen RFC einreichen. EC2,

EFS, RDS und die mehrstufigen Schemas (HA Two-Tiered und HA One-Tiered) ermöglichen bis zu fünfzig Tags. Tags werden im Teil des Schemas angegeben. `ExecutionParameters` Die Bereitstellung von Tags kann von großem Wert sein. Weitere Informationen finden Sie unter Tagging Your Amazon EC2 Resources.

Wenn Sie die AMS-Konsole verwenden, müssen Sie den Bereich Zusätzliche Konfiguration öffnen, um Tags hinzuzufügen.

> **Tip**
>
> Viele CT-Schemas haben ein `Description` `Name` UND-Feld am oberen Rand des Schemas. Diese Felder werden verwendet, um den Stack oder die Stack-Komponente zu benennen, sie benennen nicht die Ressource, die Sie erstellen. Einige Schemas bieten einen Parameter zum Benennen der Ressource, die Sie erstellen, andere nicht. Das CT-Schema für Create EC2 Stack bietet beispielsweise keinen Parameter zum Benennen der EC2 Instanz. Dazu müssen Sie ein Tag mit dem Schlüssel „Name“ und dem Wert, den der Name haben soll, erstellen. Wenn Sie kein solches Tag erstellen, wird Ihre EC2 Instanz in der EC2 Konsole ohne ein Namensattribut angezeigt.

Verwenden Sie die Option AWS RFC-Region

Die AMS-API und die CLI-Endpunkte (`amscmundamsskms`) sind da. `us-east-1` Wenn Sie sich mit Security Assertion Markup Language (SAML) verbünden, werden Ihnen beim Onboarding Skripte zur Verfügung gestellt, die Ihre Region auf us-east-1 setzen. AWS Wenn Sie SAML verwenden, müssen Sie die Option nicht angeben, wenn Sie einen Befehl ausgeben. `--region` Wenn Ihre SAML für die Verwendung von us-east-1 konfiguriert ist, sich Ihr Konto jedoch nicht in dieser AWS Region befindet, müssen Sie Ihre kontointegrierte Region angeben, wenn Sie andere AWS Befehle ausführen (z. B.). `aws s3`

> **Note**
>
> Die meisten Befehlsbeispiele in diesem Handbuch enthalten diese Option nicht. `--region`

Melden Sie sich für die tägliche RFC-E-Mail an

Mit der RFC-Digest-Funktion können Sie sich für eine tägliche E-Mail anmelden, in der die RFC-Aktivitäten in Ihrem Konto in den letzten 24 Stunden zusammengefasst werden. Die RFC-Digest-Funktion ist ein optimierter Prozess, der die Anzahl der E-Mail-Benachrichtigungen reduziert, die Sie zu Ihrem Konto erhalten. RFCs Der RFC-Digest kann die Wahrscheinlichkeit verringern, dass Sie Aktionen verpassen, für die Ihre Antwort noch aussteht.

Um die RFC-Digest-Funktion zu aktivieren, wenden Sie sich an Ihren AMS Cloud Service Delivery Manager (CSDM). Der CSDM abonniert Sie. Sie können bis zu 20 E-Mail-Adressen (oder Aliase) anfordern, die in Ihre RFC-Digest-E-Mail-Liste aufgenommen werden sollen. Der aktuelle E-Mail-Zeitplan ist auf 09:00 Uhr UTC-8 festgelegt.

Um die RFC-Digest-Funktion zu deaktivieren, wenden Sie sich mit Ihrer Anfrage an Ihren CSDM.

Wenn Sie den RFC-Digest nicht einrichten und Benachrichtigungen zu Ihrem wünschen RFCs, oder wenn Sie detailliertere Informationen zu Ihrem wünschen, RFCs als der RFC-Digest bietet, verwenden Sie das Change Management System, um CloudWatch Ereignisbenachrichtigungen oder E-Mail-Benachrichtigungen für jeden einzelnen RFC einzurichten, zu dem Sie Informationen wünschen. Informationen zum Einrichten von RFC-Benachrichtigungen finden Sie unter Benachrichtigungen über RFC-Statusänderungen.

Der RFC-Digest enthält unter anderem folgende Themen:

- Ausstehende Genehmigung durch den Kunden: Listen RFCs , die sich im PendingApprovalStatus befinden und auf Ihre Genehmigung warten
- Ausstehende Kundenantwort: Listen RFCs , die auf Ihre Antwort zur RFC-Korrespondenz warten
- Ausstehende AWS-Genehmigung oder -Antwort: Listen RFCs , die bei AMS auf eine Antwort oder Genehmigung warten
- Abgeschlossen: Listen mit Status „ RFCs Erfolgreich“, „Fehlgeschlagen“, „Storniert“ und „Abgelehnt

Im Folgenden finden Sie ein Beispiel für einen RFC-Digest:

Was sind Änderungstypen?

Der Änderungstyp bezieht sich auf die Aktion, die eine Änderungsanforderung (RFC) von AWS Managed Services (AMS) ausführt, und umfasst die Änderungsaktion selbst sowie die

Art der Änderung — manuell oder automatisiert. AMS verfügt über eine große Sammlung von Änderungstypen, die von anderen Amazon-Webservices nicht verwendet werden. Sie verwenden diese Änderungstypen, wenn Sie einen Änderungsantrag (RFC) einreichen, um Ressourcen bereitzustellen oder zu verwalten oder Zugriff darauf zu erhalten.

Themen

- Automatisiert und manuell CTs
- Anforderungen an die CT-Zulassung
- Typversionen ändern
- Änderungstypen erstellen
- Änderungstypen aktualisieren
- Nur interne Änderungstypen
- Typschemas ändern
- Verwaltung von Berechtigungen für Änderungstypen
- Sensible Informationen aus Änderungstypen redigieren
- Finden eines Änderungstyps mithilfe der Abfrageoption

Automatisiert und manuell CTs

Eine Einschränkung für Änderungstypen besteht darin, ob sie automatisiert oder manuell sind. Dies ist das `AutomationStatusId` Änderungstypattribut, das in der AMS-Konsole als Ausführungsmodus bezeichnet wird.

Automatisierte Änderungstypen haben erwartete Ergebnisse und Ausführungszeiten und durchlaufen das automatisierte AMS-System, in der Regel innerhalb einer Stunde oder weniger (dies hängt weitgehend davon ab, welche Ressourcen der CT bereitstellt). Manuelle Änderungstypen sind ungewöhnlich, werden aber unterschiedlich behandelt, da sie erfordern, dass ein AMS-Operator auf den RFC reagiert, bevor er ausgeführt werden kann. Das bedeutet manchmal, dass Sie mit dem RFC-Absender kommunizieren müssen, sodass manuelle Änderungstypen unterschiedlich lange dauern, bis sie abgeschlossen sind.

Für alle geplanten Änderungen RFCs wird eine nicht spezifizierte Endzeit als Uhrzeit des angegebenen Änderungstyps `RequestedStartTime` plus das `ExpectedExecutionDurationInMinutes` Attribut des übermittelten Änderungstyps angegeben. Wenn der beispielsweise „60“ (Minuten) `ExpectedExecutionDurationInMinutes` ist und der angegebene Wert `2016-12-05T14:20:00Z` (5. Dezember 2016 um 4:20 Uhr)

`RequestedStartTime` ist, würde die tatsächliche Endzeit auf den 5. Dezember 2016 um 5:20 Uhr festgelegt. Um den `ExpectedExecutionDurationInMinutes` für einen bestimmten Änderungstyp zu finden, führen Sie diesen Befehl aus:

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

> **Note**
>
> Geplant RFCs mit Ausführungsmodus = Manuell muss in der Konsole so eingestellt sein, dass sie mindestens 24 Stunden in der future ausgeführt wird. Dieser Vorbehalt gilt nicht für die AMS-API/CLI, aber es ist dennoch wichtig, die manuelle Planung RFCs mindestens 8 Stunden im Voraus vorzunehmen.

> **Note**
>
> Wenn Sie „Überprüfung erforderlich“ verwenden CTs, empfiehlt AMS, die ASAP-Scheduling-Option zu verwenden (wählen Sie ASAP in der Konsole, lassen Sie Start- und Endzeit leer in der API/CLI), da diese einen AMS-Operator CTs erfordern, der den RFC überprüft und möglicherweise mit Ihnen kommuniziert, bevor er genehmigt und ausgeführt werden kann. Wenn Sie diese einplanen, achten Sie darauf RFCs, dass Sie mindestens 24 Stunden einplanen. Wenn die Genehmigung nicht vor der geplanten Startzeit erfolgt, wird der RFC automatisch abgelehnt.

AMS ist bestrebt, auf ein manuelles CT innerhalb von vier Stunden zu antworten und wird sich so schnell wie möglich mit Ihnen in Verbindung setzen. Es könnte jedoch viel länger dauern, bis der RFC tatsächlich ausgeführt wird.

Eine Liste der Dateien CTs , die manuell sind und eine Überprüfung durch AMS erfordern, finden Sie in der CSV-Datei „Change Type“, die auf der Seite „Entwicklerressourcen“ der Konsole verfügbar ist.

YouTube Video: Wie finde ich automatisierte Änderungstypen für AMS RFCs?

Um den Ausführungsmodus für einen CT in der AMS-Konsole zu finden, müssen Sie die Suchoption Änderungstypen durchsuchen verwenden. Die Ergebnisse zeigen den Ausführungsmodus des entsprechenden Änderungstyps oder der entsprechenden Änderungstypen.

Führen Sie diesen Befehl aus, um die `AutomationStatus` für einen bestimmten Änderungstyp mithilfe der AMS-CLI zu finden:

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

Sie können die Änderungstypen auch in der AMS Change Type Reference nachschlagen, die Informationen zu allen AMS-Änderungstypen enthält.

> **Note**
>
> Die AMS API/CLI sind derzeit nicht Teil von AWSAPI/CLI. To access the AMS API/CLI. Sie laden das AMS-SDK über die AMS-Konsole herunter.

Anforderungen an die CT-Zulassung

Für AMS gelten CTs immer zwei Genehmigungsbedingungen, AwsApprovalIdCustomerApprovalIddie angeben, ob der RFC von AMS oder von Ihnen oder einer anderen Person verlangt, die Ausführung zu genehmigen.

Die Genehmigungsbedingung hängt in gewisser Weise mit dem Ausführungsmodus zusammen. Einzelheiten finden Sie unterAutomatisiert und manuell CTs.

Um die Genehmigungsbedingung für ein CT herauszufinden, können Sie in der AMS Change Type Reference nachschauen oder den Befehl ausführen GetChangeTypeVersion. In beiden Fällen erhalten Sie auch den CT `AutomationStatusId` - oder Ausführungsmodus.

Sie können die RFCs Genehmigung über die AMS-Konsole oder mit dem folgenden Befehl genehmigen:

```
aws amscm approve-rfc --rfc-id RFC_ID
```

Bedingung für die CT-Zulassung

Wenn die Bedingung für die CT-Zulassung	Es bedarf der Genehmigung von	And
`AwsApprovalId: Required`	Das AMS-System vom Typ Change,	Es ist keine Aktion erforderlich. Dieser Zustand ist typisch für automatisierte Systeme CTs.
`AwsApprovalId: NotRequiredIfSubmitter`	Das AMS-System ändert den Typ und sonst niemand, wenn der eingereichte RFC für das Konto gilt, für das er eingereicht wurde,	Es ist keine Aktion erforderlich. Dieser Zustand ist typisch für manuelle Geräte CTs , da sie stets von den AMS-Mitarbeitern überprüft werden.
`CustomerApprovalId: NotRequired`	Das AMS-System zur Änderung des Typs,	Wenn der RFC Syntax- und Parameterprüfungen besteht, wird er auto genehmigt.
`CustomerApprovalId: Required`	Das AMS-Change-Typsystem und Sie	Sie erhalten eine Benachrichtigung, und Sie müssen den RFC ausdrücklich genehmigen, indem Sie entweder auf die Benachrichtigung antworten oder den ApproveRfcVorgang ausführen.
`CustomerApprovalId: NotRequiredIfSubmitter`	Das AMS-System ändert den Typ und sonst niemand, wenn Sie den RFC eingereicht haben.	Wenn der RFC Syntax- und Parameterprüfungen besteht, wird er auto genehmigt.

Wenn die Bedingung für die CT-Zulassung	Es bedarf der Genehmigung von	And
Dringender Sicherheitsvorfall oder Patch	AMS	Wird auto genehmigt und implementiert.

Typversionen ändern

Die Änderungstypen werden versioniert und die Version ändert sich, wenn eine größere Aktualisierung des Änderungstyps vorgenommen wird.

Nachdem Sie in der AMS-Konsole einen Änderungstyp ausgewählt haben, haben Sie die Möglichkeit, den Bereich Zusätzliche Konfiguration zu öffnen und eine Version des Änderungstyps auszuwählen. Sie können auch in der API/CLI Befehlszeile eine Version vom Typ „Change Type“ angeben. Möglicherweise möchten Sie dies aus verschiedenen Gründen tun, darunter:

- Sie wissen, dass die Version des Änderungstyps Update, die Sie möchten, mit der Version des Änderungstyps Erstellen übereinstimmen muss, mit der Sie die Ressource erstellt haben, die Sie jetzt aktualisieren möchten. Angenommen, Sie haben eine Elastic Load Balancer (ELB) -Instance, die Sie mit ELB Create Change Type Version 1 erstellt haben. Um sie zu aktualisieren, wählen Sie ELB Update Version 1.
- Sie möchten eine Version des Änderungstyps verwenden, die andere Optionen enthält als der letzte Änderungstyp. Wir empfehlen dies nicht, da AMS-Updates ihre Typen hauptsächlich aus Sicherheitsgründen ändern und wir empfehlen, dass Sie immer die neueste Version wählen.

Änderungstypen erstellen

Die Änderungstypen von Create werden version-to-version den Änderungstypen vom Typ Update zugeordnet. Das heißt, die Version des Änderungstyps, die Sie für die Bereitstellung einer Ressource verwenden, muss mit der Version des Änderungstyps Update übereinstimmen, den Sie später zum Ändern dieser Ressource verwenden würden. Wenn Sie beispielsweise einen S3-Bucket mit dem Änderungstyp Create S3 Bucket, Version 2.0, erstellen und später einen RFC zur Änderung dieses S3-Buckets einreichen möchten, müssen Sie auch den Änderungstyp Update S3-Bucket, Version 2.0, verwenden, auch wenn es einen Änderungstyp Update S3-Bucket mit Version 3.0 gibt.

Wir empfehlen, die Änderungstyp-ID und die Version aufzuzeichnen, die Sie verwenden, wenn Sie eine Ressource mit dem Änderungstyp Create bereitstellen, falls Sie später den Änderungstyp Update verwenden möchten, um sie zu ändern.

Änderungstypen aktualisieren

AMS bietet Änderungstypen aktualisieren, um Ressourcen zu aktualisieren, die mit Create Change Types erstellt wurden. Die Änderungstypen aktualisieren müssen version-to-version mit dem Änderungstyp Create übereinstimmen, der ursprünglich für die Bereitstellung der Ressource verwendet wurde.

Es wird empfohlen, die ID und Version des Änderungstyps, die Sie bei der Bereitstellung einer Ressource verwenden, aufzuzeichnen, um deren Aktualisierung zu vereinfachen.

YouTube Video: Wie verwende ich Update CTs , um Ressourcen in einem AWS Managed Services (AMS) -Konto zu ändern?

Nur interne Änderungstypen

Sie können Änderungstypen sehen, die nur für den internen Gebrauch bestimmt sind. Auf diese Weise wissen Sie, welche Maßnahmen AMS ergreifen kann oder tut. Wenn es einen ausschließlich internen Änderungstyp gibt, den Sie für Ihre Nutzung zur Verfügung haben möchten, reichen Sie eine Serviceanfrage ein.

Beispielsweise gibt es ein CT-System für Verwaltung | Überwachung und Benachrichtigung | CloudWatch Alarmunterdrückung | Update, das nur intern ist. AMS verwendet es, um Infrastruktur-Updates (wie Patches) bereitzustellen, um Alarmbenachrichtigungen zu deaktivieren, die durch die Updates fälschlicherweise ausgelöst werden könnten. Wenn dieses CT eingereicht wird, werden Sie den RFC für das CT in Ihrer RFC-Liste finden. Alle rein internen CTs, die in einem RFC bereitgestellt werden, werden in Ihrer RFC-Liste angezeigt.

Typschemas ändern

Alle Änderungstypen stellen ein JSON-Schema für Ihre Eingaben bei der Erstellung, Änderung oder dem Zugriff auf Ressourcen bereit. Das Schema stellt die Parameter und ihre Beschreibungen bereit, mit denen Sie einen Änderungsantrag (RFC) erstellen können.

Die erfolgreiche Ausführung eines RFC führt zu einer Ausführungsausgabe. Für die Bereitstellung RFCs enthält die Ausführungsausgabe eine „stack_id“, die den Stack darstellt CloudFormation und in der Konsole gesucht werden kann. CloudFormation Die Ausführungsausgabe beinhaltet manchmal die Ausgabe der ID der erstellten Instance, und diese ID kann verwendet werden, um in

der entsprechenden AWS-Konsole nach der Instance zu suchen. Die Ausführungsausgabe „Create ELB CT“ enthält beispielsweise eine „stack_id“, in der gesucht werden kann, CloudFormation und gibt einen Key=ELB-Wert= aus, der in der Amazon-Konsole für Elastic Load <stack-xxxx>Balancing durchsucht werden kann. EC2

Lassen Sie uns ein CT-Schema untersuchen. Dies ist das Schema für CodeDeploy Application Create, ein ziemlich kleines Schema. Einige Schemas haben sehr große `Parameter` Bereiche.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "name": "Create CodeDeploy application",
  "description": "Use to create an AWS CodeDeploy applicati
on
  resource with the specified name.",
  "type": "object",
  "properties": {
    "Description": {
      "description": "The reason for the request.",
      "type": "string",
      "minLength": 1,
      "maxLength": 500
    },
    "VpcId": {
      "description": "ID of the vpc to use, in the form
 vpc-0123abcd or vpc-01234567890abcdef.",
      "type": "string",
      "pattern": "^vpc-[a-z0-9]{8}$"
    },
    "StackTemplateId": {
      "description": "Must be stm-sft6rv00000000000",
      "type": "string",
      "enum": ["stm-sft6rv00000000000"]
    },
    "Name":{
      "description": "A name for the stack or stack component
;
      this becomes the Stack Name.",
      "type": "string",
      "minLength": 1,
      "maxLength": 255
    },
    "Tags": {
```

Der erste Teil des Schemas liefert AMS Informationen über den angeforderten Änderungstyp.

```
      "description": "Up to seven tags (key/value pairs) to
      categorize the resource.",
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "Key": {
            "type": "string",
            "minLength": 1,
            "maxLength": 127
          },
          "Value": {
            "type": "string",
            "minLength": 1,
            "maxLength": 255
          }
        },
        "additionalProperties": false,
        "required": [
          "Key",
          "Value"
        ]
      },
      "minItems": 1,
      "maxItems": 7
    },
    "TimeoutInMinutes": {
      "description": "The maximum amount of time, in minutes,
to
      allow for execution of the change. This will not prolong
execution,
      but the RFC fails if the change is not completed in the
specified time.
      Valid values are 60 up to 360, for long-running
UserData.",
      "type": "number",
      "minimum": 0,
      "maximum": 60
    },
    "Parameters": {
      "description": "Specifications for the stack.",
      "type": "object",
      "properties": {
        "CodeDeployApplicationName": {
```

Mit dem TimeoutIn Minutes Parameter können Sie eine Grenzzeit für die Ausführung des Änderungstyps angeben. Gültige Werte liegen zwischen 60 und 360 für eine lange Laufzeit UserData.

Im Abschnitt Parameter geben Sie Einstellungen für die Ressource an, die Sie erstellen, oder für die Aktion, die Sie anfordern.

In den Abschnitt en „Zusätzliche

```
          "description": "The name of an AWS CodeDeploy
 application.",
          "type": "string",
          "minLength": 1,
          "maxLength": 100,
          "pattern": "^[a-zA-Z0-9._+=,@-]{1,100}$"
        }
      },
      "additionalProperties": false,
      "required": [
        "CodeDeployApplicationName"
      ]
    }
  },
  "additionalProperties": false,
  "required": [
    "Description",
    "VpcId",
    "StackTemplateId",
    "Name",
    "TimeoutInMinutes",
    "Parameters"
  ]
}
```

Eigenschaften“ erfahren Sie, welche Parameter erforderlich und welche optional sind.

> **Note**
>
> Dieses Schema erlaubt bis zu sieben Tags; EFS EC2, RDS und die mehrstufigen Erstellungsschemas erlauben jedoch bis zu 50 Tags.

Verwaltung von Berechtigungen für Änderungstypen

Sie können eine benutzerdefinierte Richtlinie verwenden, um einzuschränken, welche Änderungstypen (CTs) für verschiedene Gruppen oder Benutzer verfügbar sind.

Weitere Informationen dazu finden Sie im AMS-Benutzerhandbuch im Abschnitt Berechtigungen einrichten.

Sensible Informationen aus Änderungstypen redigieren

AMS-Schemas für den Änderungstyp bieten ein Parameterattribut, `"metadata":"ams:sensitive":"true"` das für Parameter verwendet wird, die vertrauliche Informationen enthalten würden, z. B. ein Passwort. Wenn dieses Attribut gesetzt ist, ist die bereitgestellte Eingabe verdeckt. Beachten Sie, dass Sie dieses Parameterattribut nicht festlegen können. Wenn Sie jedoch mit AMS arbeiten, um einen Änderungstyp zu erstellen und einen Parameter haben, den Sie bei der Eingabe verdecken möchten, können Sie dies anfordern.

Finden eines Änderungstyps mithilfe der Abfrageoption

Dieses Beispiel zeigt, wie Sie mithilfe der AMS-Konsole den geeigneten Änderungstyp für den RFC finden, den Sie einreichen möchten.

Sie können die Konsole oder die verwenden API/CLI , um nach einer Änderungstyp-ID (CT) oder Version zu suchen. Es gibt zwei Methoden: entweder eine Suche oder die Auswahl der Klassifizierung. Für beide Auswahltypen können Sie die Suche sortieren, indem Sie entweder „Am häufigsten verwendet“, „Zuletzt verwendet“ oder „Alphabetisch“ auswählen.

YouTube Video: Wie erstelle ich einen RFC mit der AWS Managed Services CLI und wo finde ich das CT-Schema?

Gehen Sie in der AMS-Konsole auf der Seite RFCs-> RFC erstellen wie folgt vor:

- Wenn „Nach Änderungstyp suchen“ ausgewählt ist (Standardeinstellung), können Sie entweder:
  - Verwenden Sie den Bereich Schnellerstellung, um aus den beliebtesten AMS-Programmen auszuwählen CTs. Klicken Sie auf ein Label und die Seite RFC ausführen wird geöffnet, auf der die Option Betreff automatisch für Sie ausgefüllt wird. Füllen Sie die verbleibenden Optionen nach Bedarf aus und klicken Sie auf Ausführen, um den RFC einzureichen.
  - Oder scrollen Sie nach unten zum Bereich Alle Änderungstypen und beginnen Sie, einen CT-Namen in das Optionsfeld einzugeben. Sie müssen nicht den genauen oder vollständigen Namen des Änderungstyps haben. Sie können auch anhand der ID des Änderungstyps, der Klassifizierung oder des Ausführungsmodus (automatisiert oder manuell) nach einem CT suchen, indem Sie die entsprechenden Wörter eingeben.

    Wenn die standardmäßige Kartenansicht ausgewählt ist, werden während der Eingabe passende CT-Karten angezeigt. Wählen Sie eine Karte aus und klicken Sie auf RFC erstellen. Wählen Sie bei ausgewählter Tabellenansicht das entsprechende CT aus und klicken Sie auf RFC erstellen. Bei beiden Methoden wird die Seite RFC ausführen geöffnet.

- Klicken Sie alternativ oben auf der Seite auf Nach Kategorie auswählen, um eine Reihe von Drop-down-Optionsfeldern zu öffnen, um eine Reihe von Auswahlmöglichkeiten für den Änderungstyp zu öffnen.
- Wählen Sie eine Kategorie, eine Unterkategorie, einen Artikel und einen Vorgang aus. Das Informationsfeld für diesen Änderungstyp wird angezeigt. Unten auf der Seite wird ein Bereich angezeigt.
- Wenn Sie bereit sind, drücken Sie die EINGABETASTE. Daraufhin wird eine Liste der passenden Änderungstypen angezeigt.
- Wählen Sie einen Änderungstyp aus der Liste aus. Das Informationsfeld für diesen Änderungstyp wird unten auf der Seite angezeigt.
- Wenn Sie den richtigen Änderungstyp gefunden haben, wählen Sie Create RFC.

> **Note**
>
> Die AMS-CLI muss installiert sein, damit diese Befehle funktionieren. Um die AMS-API oder CLI zu installieren, rufen Sie die Seite Entwicklerressourcen der AMS-Konsole auf. Referenzmaterial zur AMS CM API oder AMS SKMS API finden Sie im Abschnitt AMS-Informationsressourcen im Benutzerhandbuch. Möglicherweise müssen Sie eine `--profile` Option für die Authentifizierung hinzufügen, `aws amsskms` *`ams-cli-command`* `--profile SAML` z. B. Möglicherweise müssen Sie die `--region` Option auch hinzufügen, da allen AMS-Befehlen beispielsweise us-east-1 ausgeht. `aws amscm` *`ams-cli-command`* `--region=us-east-1`

> **Note**
>
> Die AMS-Endpunkte API/CLI (amscm und amsskms) befinden sich in der AWS-Region Nord-Virginia,. `us-east-1` Je nachdem, wie Ihre Authentifizierung eingerichtet ist und in welcher AWS-Region sich Ihr Konto und Ihre Ressourcen befinden, müssen Sie `--region us-east-1` bei der Ausgabe von Befehlen möglicherweise zusätzliche Informationen hinzufügen. Möglicherweise müssen Sie auch angeben`--profile saml`, ob dies Ihre Authentifizierungsmethode ist.

So suchen Sie mit der AMS CM API (siehe ListChangeTypeClassificationSummaries) oder CLI nach einem Änderungstyp:

Sie können einen Filter oder eine Abfrage für die Suche verwenden. Der ListChangeTypeClassificationSummaries Vorgang verfügt über Filteroptionen für `CategorySubcategory`,`Item`, und`Operation`, aber die Werte müssen exakt mit den vorhandenen Werten übereinstimmen. Für flexiblere Ergebnisse bei der Verwendung der CLI können Sie die `--query` Option verwenden.

Ändern Sie die Typfilterung mit der AMS CM API/CLI

Attribut	Zulässige Werte	Gültige/Standardbedingung	Hinweise
ChangeTypeId	Jede Zeichenfolge, die a darstellt ChangeTypeId (Zum Beispiel: ct-abc123xyz7890)	Gleichheitszeichen	Informationen zum Änderungstyp finden Sie in der Referenz zum Änderungstyp. IDs Informationen zum Änderungstyp IDs finden Sie unter Suche nach einem Änderungstyp oder CSIO.
Kategorie	Beliebiger Text in freier Form	Enthält	Reguläre Ausdrücke in jedem einzelnen Feld werden nicht unterstützt. Suche ohne Berücksichtigung von Groß- und Kleinschreibung
Unterkategorie			
Item			
Operation			

1. Hier sind einige Beispiele für Klassifizierungen nach der Art der Angebotsänderung:

   Der folgende Befehl listet alle Kategorien von Änderungstypen auf.

   ```
   aws amscm list-change-type-categories
   ```

Der folgende Befehl listet die Unterkategorien auf, die zu einer bestimmten Kategorie gehören.

```
aws amscm list-change-type-subcategories --category CATEGORY
```

Der folgende Befehl listet die Elemente auf, die zu einer bestimmten Kategorie und Unterkategorie gehören.

```
aws amscm list-change-type-items --category CATEGORY --subcategory SUBCATEGORY
```

2. Hier sind einige Beispiele für die Suche nach Änderungstypen mit CLI-Abfragen:

   Der folgende Befehl durchsucht CT-Klassifikationszusammenfassungen nach solchen, die „S3" im Elementnamen enthalten, und erstellt eine Ausgabe der Kategorie-, Unterkategorie-, Element-, Vorgangs- und Änderungstyp-ID in Tabellenform.

   ```
   aws amscm list-change-type-classification-summaries --query
    "ChangeTypeClassificationSummaries [?contains(Item, 'S3')].
   [Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
   ```

   ```
   +-------------------------------------------------------------+
   |               ListChangeTypeClassificationSummaries         |
   +----------+-------------------------+--+------+--------------+
   |Deployment|Advanced Stack Components|S3|Create|ct-1a68ck03fn98r|
   +----------+-------------------------+--+------+--------------+
   ```

3. Anschließend können Sie die Änderungstyp-ID verwenden, um das CT-Schema abzurufen und die Parameter zu untersuchen. Mit dem folgenden Befehl wird das Schema in eine JSON-Datei mit dem Namen CreateS3Params.schema.json ausgegeben.

   ```
   aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    CreateS3Params.schema.json
   ```

   Informationen zur Verwendung von CLI-Abfragen finden Sie unter So filtern Sie die Ausgabe mit der Option --query und in der Referenz zur Abfragesprache, JMESPath Spezifikation.

4. Nachdem Sie die Änderungstyp-ID erhalten haben, empfehlen wir, die Version für den Änderungstyp zu überprüfen, um sicherzustellen, dass es sich um die neueste Version handelt. Verwenden Sie diesen Befehl, um die Version für einen bestimmten Änderungstyp zu finden:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CHANGE_TYPE_ID
```

Um die `AutomationStatus` für einen bestimmten Änderungstyp zu finden, führen Sie diesen Befehl aus:

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

Führen Sie diesen Befehl aus, um `ExpectedExecutionDurationInMinutes` nach dem für einen bestimmten Änderungstyp zu suchen:

```
aws amscm --profile saml get-change-type-version --change-type-id ct-14027q0sjyt1h
 --query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

Behebung von RFC-Fehlern in AMS

Viele RFC-Fehler bei der AMS-Bereitstellung können anhand der Dokumentation untersucht werden. CloudFormation Weitere Informationen finden Sie unter AWS-Fehlerbehebung CloudFormation: Fehlerbehebung

In den folgenden Abschnitten finden Sie weitere Vorschläge zur Fehlerbehebung.

RFC-Fehler im Bereich „Verwaltung“ in AMS

Mit den AMS-Kategorieänderungstypen (CTs) können Sie Zugriff auf Ressourcen beantragen und vorhandene Ressourcen verwalten. In diesem Abschnitt werden einige häufig auftretende Probleme beschrieben.

RFC-Zugriffsfehler

- Stellen Sie sicher, dass der Benutzername und der FQDN, die Sie im RFC angegeben haben, korrekt sind und in der Domäne vorhanden sind. Hilfe bei der Suche nach Ihrem FQDN finden Sie unter Finden Ihres FQDN.
- Stellen Sie sicher, dass es sich bei der Stack-ID, die Sie für den Zugriff angegeben haben, um einen verwandten Stack handelt EC2. Stacks wie ELB und Amazon Simple Storage Service (S3) sind keine RFCs Zugriffskandidaten. Verwenden Sie stattdessen Ihre Nur-Lese-Zugriffsrolle, um

auf diese Stack-Ressourcen zuzugreifen. Hilfe bei der Suche nach einer Stack-ID finden Sie unter Stack suchen IDs

- Stellen Sie sicher, dass die von Ihnen angegebene Stack-ID korrekt ist und zum entsprechenden Konto gehört.

Hilfe bei anderen RFC-Zugriffsausfällen finden Sie unter Zugriffsverwaltung.

YouTube Video: Wie stelle ich einen Request for Change (RFC) richtig ein, um Ablehnungen und Ausfälle zu vermeiden?

RFC (manuell) CT-Planungsfehler

Die meisten Änderungstypen sind ExecutionMode =Automatisiert, aber einige sind ExecutionMode =Manuell, was sich darauf auswirkt, wie Sie sie planen sollten, um RFC-Fehler zu vermeiden.

Geplant RFCs mit ExecutionMode =Manual, muss so eingestellt sein, dass es mindestens 24 Stunden in der future ausgeführt wird, wenn Sie die AMS-Konsole verwenden, um den RFC zu erstellen. Dieser Vorbehalt gilt nicht für die AMS API/CLI, aber es ist dennoch wichtig, Manual RFCs mindestens 8 Stunden im Voraus zu planen.

AMS ist bestrebt, auf ein manuelles CT innerhalb von vier Stunden zu antworten und wird so schnell wie möglich antworten, aber es könnte viel länger dauern, bis der RFC tatsächlich ausgeführt wird.

Verwendung RFCs mit manuellem Update CTs

AMS Operations lehnt Management | Andere | Andere RFCs für Aktualisierungen von Stacks ab, wenn es für den Stacktyp, den Sie aktualisieren möchten, einen Aktualisierungstyp gibt.

RFC-Fehler beim Löschen des Stacks

RFC-Fehler beim Löschen von Stacks: Wenn Sie das CT Management | Standard Stacks | Stack | Delete verwenden, werden Ihnen in der AWS CloudFormation Konsole die detaillierten Ereignisse für den Stack mit dem AMS-Stack-Namen angezeigt. Sie können Ihren Stack identifizieren, indem Sie ihn mit dem Namen vergleichen, den er in der AMS-Konsole hat. Die AWS CloudFormation Konsole bietet weitere Informationen zu den Fehlerursachen.

Bevor Sie einen Stapel löschen, sollten Sie sich überlegen, wie der Stack erstellt wurde. Wenn Sie den Stack mit einem AMS-CT erstellt und die Stack-Ressourcen nicht hinzugefügt oder bearbeitet haben, können Sie davon ausgehen, dass Sie ihn problemlos löschen können. Es ist jedoch eine gute Idee, alle manuell hinzugefügten Ressourcen aus einem Stack zu entfernen, bevor Sie einen Löschstapel-RFC für diesen Stack einreichen. Wenn Sie beispielsweise einen Stack mit

dem Full-Stack-CT (HA Two Tier) erstellen, enthält er eine Sicherheitsgruppe -. SG1 Wenn Sie dann AMS verwenden, um eine weitere Sicherheitsgruppe zu erstellen - und auf die neue SG2 Sicherheitsgruppe verweisen SG2, die als Teil des vollständigen Stacks SG1 erstellt wurde, und dann den Löschstapel-CT verwenden, um den Stack zu löschen, SG1 wird der nicht gelöscht, da er von referenziert wird SG2.

Important

Das Löschen von Stacks kann unerwünschte und unerwartete Folgen haben. Aus diesem Grund zieht es AMS vor, Stacks oder Stack-Ressourcen nicht im Namen von Kunden zu löschen. Beachten Sie, dass AMS in Ihrem Namen nur Ressourcen löscht (durch einen eingereichten Änderungstyp Verwaltung | Andere | Andere | Aktualisierung), die nicht mit dem entsprechenden, automatisierten Änderungstyp gelöscht werden können. Weitere Überlegungen:

- Wenn die Ressourcen für den Löschschutz aktiviert sind, kann AMS helfen, diesen zu entsperren, indem Sie den Änderungstyp Verwaltung | Andere | Andere | Aktualisierung einreichen. Nachdem der Löschschutz aufgehoben wurde, können Sie diese Ressource mit dem automatisierten CT löschen.
- Wenn ein Stack mehrere Ressourcen enthält und Sie nur eine Teilmenge der Stack-Ressourcen löschen möchten, verwenden Sie den Änderungstyp CloudFormation Update (siehe CloudFormation Ingest Stack: Aktualisierung). Sie können auch den Änderungstyp Verwaltung | Andere | Andere | Aktualisierung angeben. Die AMS-Techniker können Ihnen bei Bedarf bei der Erstellung des Changesets helfen.
- Falls aufgrund von Abweichungen Probleme bei der Verwendung des CloudFormation Update CT auftreten, kann AMS helfen, indem Sie ein Management | Other | Other | Other | Update zur Behebung des Fehlers einreichen (sofern vom CloudFormation AWS-Service unterstützt) und ein Update bereitstellen ChangeSet , das Sie dann mit den automatisierten CT, Management/Custom Stack/Stack From CloudFormation Template/ Approve Changeset und Update validieren und ausführen können.

AMS hält sich an die oben genannten Einschränkungen, um sicherzustellen, dass es nicht zu unerwarteten oder unerwarteten Löschungen von Ressourcen kommt.

Weitere Informationen finden Sie unter Fehlerbehebung bei AWS CloudFormation: Stack löschen schlägt fehl.

DNS-Fehler beim RFC-Update

Es kann RFCs vorkommen, dass mehrere Aktualisierungen einer DNS-Hosting-Zone fehlschlagen, manchmal auch ohne Grund. Das RFCs gleichzeitige Erstellen mehrerer Zonen zur Aktualisierung von DNS-Hosting-Zonen (privat oder öffentlich) kann dazu führen RFCs , dass einige fehlschlagen, weil sie versuchen, denselben Stack gleichzeitig zu aktualisieren. AMS Change Management lehnt ab oder schlägt fehl RFCs , wenn ein Stack nicht aktualisiert werden kann, weil der Stack bereits von einem anderen RFC aktualisiert wird. AMS empfiehlt, dass Sie jeweils einen RFC erstellen und warten, bis der RFC erfolgreich ist, bevor Sie einen neuen für denselben Stack starten.

Fehler bei RFC-IAM-Entitäten

AMS stellt eine Reihe von Standard-IAM-Rollen und -Profilen für AMS-Konten bereit, die auf Ihre Bedürfnisse zugeschnitten sind. Möglicherweise müssen Sie jedoch gelegentlich zusätzliche IAM-Ressourcen anfordern.

Das Verfahren zur Einreichung von RFCs Anfragen für benutzerdefinierte IAM-Ressourcen folgt dem Standardablauf für manuelle Anwendungen. Der Genehmigungsprozess umfasst jedoch auch eine Sicherheitsüberprüfung RFCs, um sicherzustellen, dass angemessene Sicherheitskontrollen vorhanden sind. Daher dauert der Vorgang in der Regel länger als bei anderen manuellen RFCs Vorgängen. Um die Zykluszeit bei diesen zu reduzieren RFCs, befolgen Sie bitte die folgenden Richtlinien.

Informationen darüber, was wir unter einer IAM-Überprüfung verstehen und wie sie unseren technischen Standards und unserem Prozess zur Risikoakzeptanz entspricht, finden Sie unterRFC-Sicherheitsüberprüfungen verstehen.

Häufig gestellte Anfragen zu IAM-Ressourcen:

- Wenn Sie nach einer Richtlinie für eine wichtige Cloud-kompatible Anwendung fragen, wie z. B. CloudEndure, schauen Sie sich die vorab genehmigte CloudEndure IAM-Richtlinie von AMS an: Entpacken Sie die WIGs Cloud Endure Landing Zone-Beispieldatei und öffnen Sie die `customer_cloud_endure_policy.json`

> **Note**
>
> Wenn Sie eine restriktivere Richtlinie wünschen, besprechen Sie Ihre Bedürfnisse mit Ihrem Unternehmen und lassen Sie sich, falls erforderlich, von einem AMS Security Review

CloudArchitect/CSDM und Signoff überzeugen, bevor Sie einen RFC zur Umsetzung der Richtlinie einreichen.

- Wenn Sie eine von AMS standardmäßig in Ihrem Konto bereitgestellte Ressource ändern möchten, empfehlen wir Ihnen, anstelle von Änderungen an der vorhandenen eine modifizierte Kopie dieser Ressource anzufordern.
- Wenn Sie Berechtigungen für einen menschlichen Benutzer anfordern (anstatt die Berechtigungen dem Benutzer zuzuweisen), ordnen Sie die Berechtigungen einer Rolle zu und gewähren Sie dem Benutzer dann die Erlaubnis, diese Rolle anzunehmen. Einzelheiten dazu finden Sie unter Temporärer Zugriff auf die AMS Advanced-Konsole.
- Wenn Sie außergewöhnliche Berechtigungen für eine temporäre Migration oder einen temporären Workflow benötigen, geben Sie in Ihrer Anfrage ein Enddatum für diese Berechtigungen an.
- Wenn Sie den Gegenstand Ihrer Anfrage bereits mit Ihrem Sicherheitsteam besprochen haben, legen Sie Ihrem CSDM so detailliert wie möglich einen Nachweis über deren Genehmigung vor.

Wenn AMS einen IAM-RFC ablehnt, geben wir einen klaren Grund für die Ablehnung an. Beispielsweise könnten wir eine Anfrage zur Erstellung einer IAM-Richtlinie ablehnen und erklären, was an der Richtlinie unangemessen ist. In diesem Fall können Sie die identifizierten Änderungen vornehmen und die Anfrage erneut einreichen. Wenn weitere Informationen zum Status einer Anfrage erforderlich sind, reichen Sie eine Serviceanfrage ein oder wenden Sie sich an Ihren CSDM.

In der folgenden Liste werden die typischen Risiken beschrieben, die AMS bei der Überprüfung Ihres IAM zu minimieren versucht. RFCs Wenn Ihr IAM-RFC eines dieser Risiken birgt, kann dies zur Ablehnung des RFC führen. In Fällen, in denen Sie eine Ausnahme benötigen, bittet AMS Ihr Sicherheitsteam um die Genehmigung. Um eine solche Ausnahme zu beantragen, stimmen Sie sich mit Ihrem CSDM ab.

Note

AMS kann aus beliebigem Grund jegliche Änderung der IAM-Ressourcen innerhalb eines Kontos ablehnen. Wenn Sie Bedenken bezüglich einer RFC-Ablehnung haben, wenden Sie sich über eine Serviceanfrage an AMS Operations oder wenden Sie sich an Ihren CSDM.

- Eskalation von Rechten, z. B. Berechtigungen, die es Ihnen ermöglichen, Ihre eigenen Berechtigungen oder die Berechtigungen anderer Ressourcen innerhalb des Kontos zu ändern. Beispiele:

  - Die Verwendung `iam:PassRole` mit einer anderen, privilegierteren Rolle.
  - Zugriff auf attach/detach IAM-Richtlinien durch eine Rolle oder einen Benutzer.
  - Die Änderung der IAM-Richtlinien im Konto.
  - Die Fähigkeit, API-Aufrufe im Kontext der Verwaltungsinfrastruktur zu tätigen.
- Berechtigungen zum Ändern von Ressourcen oder Anwendungen, die für die Bereitstellung von AMS-Diensten für Sie erforderlich sind. Beispiele:
  - Änderung der AMS-Infrastruktur wie der Bastions-, Management-Host- oder EPS-Infrastruktur.
  - Löschen von Protokollverwaltungsfunktionen, AWS Lambda Lambda-Funktionen oder Protokollstreams.
  - Das Löschen oder Ändern der CloudTrail Standard-Überwachungsanwendung.
  - Die Änderung des Active Directory (AD) der Verzeichnisdienste.
  - Deaktivierung CloudWatch (CW) von Alarmen.
  - Die Änderung der Principals, Richtlinien und Namespaces, die im Konto als Teil der landing zone bereitgestellt werden.
- Bereitstellung von Infrastruktur außerhalb von bewährten Verfahren, wie z. B. Genehmigungen, die den Aufbau einer Infrastruktur in einem Zustand ermöglichen, der Ihre Informationssicherheit gefährdet. Beispiele:
  - Die Erstellung von öffentlichen oder unverschlüsselten S3-Buckets oder die öffentliche gemeinsame Nutzung von EBS-Volumes.
  - Die Bereitstellung öffentlicher IP-Adressen.
  - Die Änderung von Sicherheitsgruppen, um einen breiten Zugriff zu ermöglichen.
- Zu weit gefasste Berechtigungen können Auswirkungen auf Anwendungen haben, z. B. Berechtigungen, die zu Datenverlust, Integritätsverlust, unangemessener Konfiguration oder Betriebsunterbrechungen für Ihre Infrastruktur und die Anwendungen innerhalb des Kontos führen können. Beispiele:
  - Deaktivierung oder Umleitung von Netzwerkverkehr über ähnliche oder. APIs `ModifyNetworkInterfaceAttribute` `UpdateRouteTable`
  - Deaktivierung der verwalteten Infrastruktur durch Trennen von Volumes von verwalteten Hosts.
- Berechtigungen für Dienste, die nicht Teil der AMS-Servicebeschreibung sind und von AMS nicht unterstützt werden.

Dienste, die nicht in der AMS-Servicebeschreibung aufgeführt sind, können nicht in AMS-Konten verwendet werden. Wenn Sie Support für eine Funktion oder einen Dienst anfordern möchten, wenden Sie sich bitte an Ihren CSDM.

- Genehmigungen, die Ihr erklärtes Ziel nicht erfüllen, da sie entweder zu großzügig oder zu konservativ sind oder auf die falschen Ressourcen angewendet werden. Beispiele:
  - Eine Anfrage nach `s3:PutObject` Berechtigungen für einen S3-Bucket mit obligatorischer KMS-Verschlüsselung ohne `KMS:Encrypt` Berechtigungen für den entsprechenden Schlüssel.
  - Berechtigungen, die sich auf Ressourcen beziehen, die im Konto nicht vorhanden sind.
  - IAM RFCs , bei dem die Beschreibung des RFC nicht mit der Anfrage zu übereinstimmen scheint.

RFC-Fehler bei der „Bereitstellung“

Mit den Änderungstypen für die Kategorie „Einsatz“ (CTs) von AMS können Sie beantragen, dass Ihrem Konto verschiedene AMS-unterstützte Ressourcen hinzugefügt werden.

Die meisten AMS CTs , die eine Ressource erstellen, basieren auf AWS CloudFormation Vorlagen. Als Kunde haben Sie Lesezugriff auf alle AWS-Services AWS CloudFormation, einschließlich, Sie können anhand der AWS CloudFormation Stack-Beschreibung mithilfe der Konsole schnell den Stack identifizieren, der Ihren Stack darstellt. AWS CloudFormation Der ausgefallene Stack wird sich wahrscheinlich im Status DELETE_COMPLETE befinden. Sobald Sie den AWS CloudFormation Stack identifiziert haben, zeigen Ihnen die Ereignisse, welche spezifische Ressource nicht erstellt werden konnte und warum.

Verwenden Sie die CloudFormation Dokumentation zur Fehlerbehebung

Die meisten AMS-Bereitstellungen RFCs verwenden eine CloudFormation Vorlage, und diese Dokumentation kann bei der Fehlerbehebung hilfreich sein. Die Dokumentation zu dieser AWS CloudFormation Vorlage finden Sie in der Dokumentation:

- Fehler beim Erstellen des Application Load Balancers: AWS::ElasticLoadBalancingV2::LoadBalancer (Application Load Balancer)
- Auto Scaling Scaling-Gruppe erstellen: AWS::AutoScaling::AutoScalingGroup (Auto Scaling-Gruppe)
- Memcache-Cache erstellen: AWS::ElastiCache::CacheCluster (Cache-Cluster)
- Redis-Cache erstellen: AWS::ElastiCache::CacheCluster (Cache-Cluster)

- DNS-Hosted Zone erstellen (wird zusammen mit Create DNS private/public verwendet): AWS::Route53::HostedZone (R53 Hosted Zone)
- DNS-Datensatzsatz erstellen (wird zusammen mit Create DNS private/public verwendet): (Ressourcendatensätze) AWS::Route53::RecordSet
- EC2 Stack erstellen: AWS::EC2::Instance (Elastic Compute Cloud)
- Elastisches Dateisystem (EFS) erstellen: AWS::EFS::FileSystem (Elastisches Dateisystem)
- Load Balancer erstellen: AWS::ElasticLoadBalancing::LoadBalancer (Elastic Load Balancer)
- RDS-Datenbank erstellen: AWS::RDS::DBInstance (Relationale Datenbank)
- Erstellen Sie Amazon S3: AWS::S3::Bucket (Simple Storage Service)
- Warteschlange erstellen: AWS::SQS::Queue (Einfacher Warteschlangendienst)

Fehler beim Erstellen von AMIs RFC

Ein Amazon Machine Image (AMI) ist eine Vorlage, die eine Softwarekonfiguration enthält (z. B. ein Betriebssystem, einen Anwendungsserver und Anwendungen). Von einem AMI aus starten Sie eine Instance, bei der es sich um eine Kopie des AMI handelt, die als virtueller Server in der Cloud ausgeführt wird. AMIs sind sehr nützlich und werden benötigt, um EC2 Instanzen oder Auto Scaling Scaling-Gruppen zu erstellen. Sie müssen jedoch einige Anforderungen beachten:

- Die Instanz, für die Sie angeben, `Ec2InstanceId` muss sich in einem gestoppten Zustand befinden, damit der RFC erfolgreich ist. Verwenden Sie für diesen Parameter keine Auto Scaling Scaling-Gruppeninstanzen (ASG), da die ASG eine gestoppte Instance beendet.
- Um ein AMS Amazon Machine Image (AMI) zu erstellen, müssen Sie mit einer AMS-Instance beginnen. Bevor Sie die Instance zum Erstellen des AMI verwenden können, müssen Sie sie vorbereiten, indem Sie sicherstellen, dass sie gestoppt und von ihrer Domäne getrennt ist. Einzelheiten finden Sie unter Erstellen eines standardmäßigen Amazon-Computerabbilds mithilfe von Sysprep
- Der Name, den Sie für das neue AMI angeben, muss innerhalb des Kontos eindeutig sein, sonst schlägt der RFC fehl. Wie das geht, ist unter AMI | Create beschrieben. Weitere Informationen finden Sie unter AWS AMI Design.

> **Note**
>
> Weitere Informationen zur Vorbereitung der AMI-Erstellung finden Sie unter AMI | Create.

RFCs Erstellen EC2s oder Fehler ASGs

Bei EC2 oder ASG-Ausfällen mit Timeouts empfiehlt AMS, zu überprüfen, ob das verwendete AMI angepasst ist. Falls ja, lesen Sie bitte die Schritte zur AMI-Erstellung in diesem Handbuch (siehe AMI | Create), um sicherzustellen, dass das AMI korrekt erstellt wurde. Ein häufiger Fehler beim Erstellen eines benutzerdefinierten AMI besteht darin, die Schritte im Handbuch zum Umbenennen oder Aufrufen von Sysprep nicht zu befolgen.

RFCs Erstellen von RDS-Fehlern

Fehler im Amazon Relational Database Service (RDS) können aus vielen verschiedenen Gründen auftreten, da Sie bei der Erstellung des RDS viele verschiedene Engines verwenden können und jede Engine ihre eigenen Anforderungen und Einschränkungen hat. Bevor Sie versuchen, einen AMS-RDS-Stack zu erstellen, überprüfen Sie die AWS-RDS-Parameterwerte sorgfältig, siehe Erstellen DBInstance.

Weitere Informationen zu Amazon RDS im Allgemeinen, einschließlich Größenempfehlungen, finden Sie in der Dokumentation zu Amazon Relational Database Service.

RFCs Amazon S3-Fehler erstellen

Ein häufiger Fehler beim Erstellen eines S3-Speicher-Buckets besteht darin, dass kein eindeutiger Name für den Bucket verwendet wird. Wenn Sie einen S3-Bucket Create CT mit demselben Namen wie einen zuvor eingereichten eingereicht haben, würde dies fehlschlagen, da bereits ein S3-Bucket mit diesem Bucket vorhanden wäre BucketName. Dies wird in der AWS CloudFormation Konsole detailliert beschrieben, wo Sie sehen werden, dass das Stack-Ereignis anzeigt, dass der Bucket-Name bereits verwendet wird.

RFC-Validierung versus Ausführungsfehler

RFC-Fehler und zugehörige Meldungen unterscheiden sich in den Ausgabemeldungen auf der RFC-Detailseite der AMS-Konsole für einen ausgewählten RFC:

- Die Gründe für Validierungsfehler sind nur im Statusfeld verfügbar
- Die Gründe für Ausführungsfehler sind sowohl in den Feldern Ausführungsausgabe als auch in den Statusfeldern verfügbar.

RFC-Fehlermeldungen

Wenn Sie bei den aufgelisteten Änderungstypen (CTs) auf den folgenden Fehler stoßen, können Sie diese Lösungen verwenden, um die Ursache der Probleme zu finden und sie zu beheben.

```
{"errorMessage":"An error has occurred during RFC execution. We are
investigating the issue.","errorType":"InternalError"}
```

Wenn Sie weitere Unterstützung benötigen, nachdem Sie sich auf die folgenden Optionen zur Fehlerbehebung bezogen haben, wenden Sie sich per RFC-Korrespondenz an AMS oder stellen Sie eine Serviceanfrage. Weitere Informationen finden Sie unter RFC-Korrespondenz und Anhang (Konsole) und Erstellen einer Serviceanfrage in AMS.

Fehler bei der Workload Ingestion (WIGS)

> **Note**
>
> Validierungstools für Windows und Linux können heruntergeladen und direkt auf Ihren lokalen Servern sowie auf EC2 Instanzen in AWS ausgeführt werden. Diese finden Sie im AMS Advanced Application Developer's Guide Migrating workloads: Linux pre-ingestion validation und Migrating workloads: Windows pre-ingestion validation.

- EC2 Stellen Sie sicher, dass die Instanz im AMS-Zielkonto vorhanden ist. Wenn Sie beispielsweise Ihr AMI von einem Nicht-AMS-Konto für ein AMS-Konto freigegeben haben, müssen Sie in Ihrem AMS-Konto eine EC2 Instance mit dem gemeinsam genutzten AMI erstellen, bevor Sie einen Workload Ingest RFC einreichen können.
- Prüfen Sie, ob für die mit der Instance verbundenen Sicherheitsgruppen ausgehender Datenverkehr zulässig ist. Der SSM-Agent muss in der Lage sein, eine Verbindung zu seinem öffentlichen Endpunkt herzustellen.
- Überprüfen Sie, ob die Instanz über die richtigen Berechtigungen verfügt, um eine Verbindung mit dem SSM-Agenten herzustellen. Diese Berechtigungen sind im Lieferumfang `customer-mc-ec2-instance-profile` enthalten. Sie können dies in der EC2 Konsole überprüfen:

EC2 Fehler beim Stopp des Instance-Stacks

- Prüfen Sie, ob sich die Instance bereits in einem gestoppten oder beendeten Zustand befindet.

- Wenn die EC2 Instance online ist und Ihnen der `InternalError` Fehler angezeigt wird, senden Sie eine Serviceanfrage an AMS zur Untersuchung.
- Beachten Sie, dass Sie den Änderungstyp Management | Advanced stack components | EC2 instance stack | Stop ct-3mvvt2zkyveqj nicht verwenden können, um eine Auto Scaling Scaling-Gruppeninstanz (ASG) zu stoppen. Wenn Sie eine ASG-Instance beenden müssen, reichen Sie eine Serviceanfrage ein.

EC2 Fehler beim Erstellen des Instanzstapels

Die `InternalError` Nachricht stammt von CloudFormation; ein Grund für den Status CREATION_FAILED. Einzelheiten zum Stack-Fehler finden Sie in CloudWatch Stack-Ereignissen, indem Sie die folgenden Schritte ausführen:

- In der AWS-Managementkonsole können Sie eine Liste von Stack-Ereignissen anzeigen, während Ihr Stack erstellt, aktualisiert oder gelöscht wird. Finden Sie das Fehlerereignis in dieser Liste und sehen dann den Statusgrund für dieses Ereignis an.

  Der Statusgrund kann eine Fehlermeldung von AWS CloudFormation oder von einem bestimmten Service enthalten, die Ihnen helfen kann, das Problem zu verstehen.
- Weitere Informationen zum Anzeigen von Stack-Ereignissen finden Sie unter CloudFormation AWS-Stack-Daten und -Ressourcen in der AWS-Managementkonsole anzeigen.

EC2 Fehler bei der Wiederherstellung des Instance-Volumes

AMS erstellt einen internen RFC zur Fehlerbehebung, wenn die Wiederherstellung des EC2 Instance-Volumes fehlschlägt. Dies geschieht, weil die Wiederherstellung des EC2 Instance-Volumes ein wichtiger Bestandteil der Notfallwiederherstellung (DR) ist und AMS diesen internen RFC zur Fehlerbehebung automatisch für Sie erstellt.

Wenn der interne RFC zur Fehlerbehebung erstellt wurde, wird ein Banner mit Links zum RFC angezeigt. Dieser interne RFC zur Fehlerbehebung bietet Ihnen mehr Einblick in RFC-Fehler. Anstatt Wiederholungsversuche zu senden, die zu denselben Fehlern RFCs führen, oder Sie müssen sich wegen dieses Fehlers manuell an AMS wenden, können Sie Ihre Änderungen verfolgen und wissen, dass AMS an dem Fehler arbeitet. Dadurch wird auch die time-to-recovery (TTR) -Metrik für ihre Änderung reduziert, da AMS-Operatoren proaktiv an dem RFC-Fehler arbeiten, anstatt auf Ihre Anfrage zu warten.

Wie erhalte ich Hilfe bei einem RFC

Sie können sich an AMS wenden, um die Ursache Ihres Fehlers zu ermitteln. Die AMS-Geschäftszeiten sind 24 Stunden am Tag, 7 Tage die Woche, 365 Tage im Jahr.

AMS bietet Ihnen verschiedene Möglichkeiten, um Hilfe zu bitten oder Serviceanfragen zu stellen.

- Verwenden Sie die AMS-Konsole und senden Sie eine Serviceanfrage, um Informationen oder Beratung oder um Zugriff auf einen von AMS verwalteten IT-Service zu erhalten oder um einen zusätzlichen Service von AMS anzufordern. Einzelheiten finden Sie unter Serviceanfrage erstellen. Allgemeine Informationen zu AMS-Serviceanfragen finden Sie unter Verwaltung von Serviceanfragen.
- Um ein Leistungsproblem mit dem AWS- oder AMS-Service zu melden, das sich auf Ihre verwaltete Umgebung auswirkt, verwenden Sie die AMS-Konsole und reichen Sie einen Vorfallbericht ein. Einzelheiten finden Sie unter Einen Vorfall melden. Allgemeine Informationen zum AMS Incident Management finden Sie unter Reaktion auf Vorfälle.
- Wenn Sie spezielle Fragen dazu haben, wie Sie oder Ihre Ressourcen oder Anwendungen mit AMS zusammenarbeiten, oder um einen Vorfall zu eskalieren, senden Sie eine E-Mail an eine oder mehrere der folgenden Adressen:
  1. Wenn Sie mit der Serviceanfrage oder der Antwort auf den Vorfallbericht nicht zufrieden sind, senden Sie zunächst eine E-Mail an Ihren CSDM: ams-csdm@amazon.com
  2. Als Nächstes können Sie, falls eine Eskalation erforderlich ist, eine E-Mail an den AMS Operations Manager senden (aber Ihr CSDM wird das wahrscheinlich tun): ams-opsmanager@amazon.com
  3. Eine weitere Eskalation erfolgt an den AMS-Direktor: ams-director@amazon.com
  4. Schließlich sind Sie immer in der Lage, den AMS VP zu erreichen: ams-vp@amazon.com

Direkter Änderungsmodus in AMS

Themen

- Erste Schritte mit dem Direct Change-Modus
- Sicherheit und Compliance
- Änderungsmanagement im Direct Change-Modus
- Stapel im Direct Change-Modus erstellen
- Anwendungsfälle für den Direct Change Mode

Der Direct Change Mode (DCM) von AWS Managed Services (AMS) erweitert das AMS Advanced Change Management um systemeigenen AWS Zugriff auf AMS Advanced Plus- und Premium-Konten zur Bereitstellung und Aktualisierung von AWS Ressourcen. Mit DCM haben Sie die Möglichkeit, native AWS API (Konsole oder CLI/SDK) oder AMS Advanced Change Management Requests for change (RFCs) zu verwenden. In beiden Fällen werden die Ressourcen und Änderungen daran vollständig von AMS unterstützt, einschließlich Überwachung, Patch, Backup und Incident Response Management. Über DCM bereitgestellte Ressourcen werden im AMS Service Knowledge Management System (SKMS) registriert, der von AMS verwalteten Active Directory-Domäne (falls zutreffend) hinzugefügt und führen AMS-Management-Agenten aus. Verwenden Sie vorhandene Tools (z. B. AWS SDK und CDK) CloudFormation, um AMS-verwaltete Stacks zu entwickeln und bereitzustellen. CloudFormation

> **Note**
>
> Durch den Direct Change-Modus wird das AMS-Änderungsmanagement nicht entfernt. RFCs RFCs Mit DCM haben Sie vollen Zugriff auf AMS.

Sehen Sie sich das Video von Akash an, um mehr zu erfahren (6:30)

Erste Schritte mit dem Direct Change-Modus

Überprüfen Sie zunächst die Voraussetzungen und reichen Sie dann einen Änderungsantrag (RFC) in Ihrem berechtigten AMS Advanced-Konto ein.

1. Vergewissern Sie sich, dass das Konto, das Sie mit DCM verwenden möchten, die Anforderungen erfüllt:

   - Das Konto ist AMS Advanced Plus oder Premium.
   - Für das Konto ist Service Catalog nicht aktiviert. Wir unterstützen derzeit nicht das gleichzeitige Onboarding von Konten für DCM und Service Catalog. Wenn Sie bereits bei Service Catalog angemeldet sind, aber an DCM interessiert sind, besprechen Sie Ihre Anforderungen mit Ihrem Cloud Service Delivery Manager (CSDM). Wenn Sie sich dazu entschließen, von Service Catalog zu DCM, Offboard Service Catalog, zu wechseln, fügen Sie die Anfrage in die unten stehende Änderungsanfrage ein. Einzelheiten zum Service Catalog in AMS finden Sie unter AMS und Service Catalog.

2. Senden Sie eine Änderungsanforderung (RFC) über die Optionen Verwaltung | Verwaltetes Konto | Direkter Änderungsmodus | Änderungstyp aktivieren (ct-3rd4781c2nnhp). Ein Beispiel für eine exemplarische Vorgehensweise finden Sie unter Direkter Änderungsmodus | Aktivieren.

   Nach der Verarbeitung des CT werden die vordefinierten IAM-Rollen `AWSManagedServicesCloudFormationAdminRole` und `AWSManagedServicesUpdateRole` E im angegebenen Konto bereitgestellt.
3. Weisen Sie den Benutzern, die DCM-Zugriff benötigen, mithilfe Ihres internen Verbundprozesses die entsprechende Rolle zu.

> **Note**
>
> Sie können eine beliebige Anzahl von SAMLIdentity Anbietern, AWS Diensten und IAM-Entitäten (Rollen, Benutzer usw.) angeben, um die Rollen zu übernehmen. Sie müssen mindestens ein: `SAMLIdentityProviderARNsIAMEntityARNs`, oder `AWSServicePrincipals` angeben. Weitere Informationen erhalten Sie von der IAM-Abteilung Ihres Unternehmens oder von Ihrem AMS Cloud Architect (CA).

IAM-Rollen und -Richtlinien im Direktänderungsmodus

Wenn der Direct Change-Modus in einem Konto aktiviert ist, werden diese neuen IAM-Entitäten bereitgestellt:

`AWSManagedServicesCloudFormationAdminRole`: Diese Rolle gewährt Zugriff auf die CloudFormation Konsole, das Erstellen und Aktualisieren von CloudFormation Stacks, das Anzeigen von Drift-Berichten sowie das Erstellen und Ausführen. CloudFormation ChangeSets Der Zugriff auf diese Rolle wird über Ihren SAML-Anbieter verwaltet.

Folgende verwaltete Richtlinien werden bereitgestellt und der Rolle `AWSManagedServicesCloudFormationAdminRole` zugewiesen:

- AMS Advanced-Anwendungskonto für mehrere Konten (MALZ)
  - AWSManagedServices_CloudFormationAdminPolicy1
  - AWSManagedServices_CloudFormationAdminPolicy2
    - Diese Richtlinie stellt die Berechtigungen dar, die dem gewährt wurden. `AWSManagedServicesCloudFormationAdminRole` Sie und Ihre Partner verwenden diese

Richtlinie, um Zugriff auf eine bestehende Rolle im Konto zu gewähren und dieser Rolle das Starten und Aktualisieren von CloudFormation Stacks im Konto zu ermöglichen. Dies kann zusätzliche Aktualisierungen der AMS Service Control Policy (SCP) erfordern, damit andere IAM-Entitäten Stacks starten können. CloudFormation

- AMS Advanced-Landingzone-Konto (SALZ) mit einem Konto
  - AWSManagedServices_CloudFormationAdminPolicy1
  - AWSManagedServices_CloudFormationAdminPolicy2
  - cdk-legacy-mode-s[Inline-Richtlinie] mit 3 Zugriffen
  - AWS ReadOnlyAccess Richtlinie

`AWSManagedServicesUpdateRole`: Diese Rolle gewährt eingeschränkten Zugriff auf nachgelagerte AWS Dienste APIs. Die Rolle wird mit verwalteten Richtlinien bereitgestellt, die mutierende und nicht mutierende API-Operationen bereitstellen, aber im Allgemeinen mutierende Operationen (wieCreate/Delete/PUT) für bestimmte Dienste wie IAM, KMS, VPC, AMS-Infrastrukturressourcen und -konfiguration usw. einschränken. GuardDuty Der Zugriff auf diese Rolle wird über Ihren SAML-Anbieter verwaltet.

Folgende verwaltete Richtlinien werden bereitgestellt und der Rolle `AWSManagedServicesUpdateRole` zugewiesen:

- AMS Advanced landing zone Anwendungskonto für mehrere Konten
  - AWSManagedServicesUpdateBasePolicy
  - AWSManagedServicesUpdateDenyPolicy
  - AWSManagedServicesUpdateDenyProvisioningPolicy
  - AWSManagedServicesUpdateEC2Und RDSPolicy
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolitik
- AMS Advanced-Landingzone-Konto mit einem Konto
  - AWSManagedServicesUpdateBasePolicy
  - AWSManagedServicesUpdateDenyProvisioningPolicy
  - AWSManagedServicesUpdateEC2Und RDSPolicy
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraRichtlinie 1
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraRichtlinie 2

Darüber hinaus ist der `AWSManagedServicesUpdateRole` Rolle „Verwaltete Richtlinie“ auch die AWS verwaltete Richtlinie `ViewOnlyAccess` zugeordnet.

Sicherheit und Compliance

Für Sicherheit und Compliance sind AMS Advanced und Sie als unser Kunde gemeinsam verantwortlich. Der AMS Advanced Direct Change-Modus ändert nichts an dieser gemeinsamen Verantwortung.

Sicherheit im Direct Change-Modus

AMS Advanced bietet zusätzlichen Mehrwert mit einer präskriptiven landing zone, einem Change-Management-System und einer Zugriffsverwaltung. Bei Verwendung des Direct Change-Modus ändert sich dieses Verantwortungsmodell nicht. Sie sollten sich jedoch zusätzlicher Risiken bewusst sein.

Die Rolle „Update“ im Direktänderungsmodus (siehe IAM-Rollen und -Richtlinien im Direktänderungsmodus) bietet erweiterte Berechtigungen, sodass die Entität, die Zugriff darauf hat, Änderungen an den Infrastrukturressourcen der von AMS unterstützten Dienste in Ihrem Konto vornehmen kann. Bei erhöhten Berechtigungen bestehen je nach Ressource, Service und Aktion unterschiedliche Risiken, insbesondere in Situationen, in denen aufgrund eines Versehens, eines Fehlers oder der mangelnden Einhaltung Ihres internen Prozess- und Kontrollrahmens eine falsche Änderung vorgenommen wird.

Gemäß den technischen Standards von AMS wurden die folgenden Risiken identifiziert, und es werden folgende Empfehlungen ausgesprochen. Detaillierte Informationen zu den technischen Standards von AMS finden Sie unter AWS Artifact. Um darauf zuzugreifen AWS Artifact, wenden Sie sich an Ihren CSDM, um Anweisungen zu erhalten, oder gehen Sie zu Erste Schritte mit AWS Artifact.

AMS-STD-001: Taggen

Normen	Geht es kaputt	Risiken	Empfehlungen
Alle AMS-eigenen Ressourcen müssen das folgende Schlüssel-Wert-Paar haben	Ja. Unterbrechungen für CloudFormation,CloudTrail, EFS, OpenSearch, CloudWatch	Eine falsche Kennzeichnung von AMS-Ressourcen kann sich nachteilig auf die Berichts-	Der Zugriff muss eingeschränkt werden, um Änderungen an den standardmäßigen

Normen	Geht es kaputt	Risiken	Empfehlungen
Alle AMS-eigenen Tags, mit Ausnahme der oben aufgeführten, müssen Präfixe wie oder in case haben. `AMS*` `MC*` upper/lower/mix	Logs, SQS, SSM, Tagging-API — da diese Dienste die `aws:TagsKey` Bedingung, das Tagging für den AMS-Namespace einzuschränken, nicht unterstützen. Der in der folgenden Tabelle AMS-STD-003 angegebene Standard besagt, dass Sie die Umgebung und ändern AppId können, aber nicht für AMS-eigene Ressourcen. AppName Mit IAM-Berechtigungen nicht erreichbar.	, Warnungs- und Patching-Vorgänge Ihrer Ressourcen auf AMS-Seite auswirken.	AMS-Tagging-Anforderungen für andere Personen als AMS-Teams vorzunehmen.
Alle Tags in AMS-eigenen Stacks dürfen aufgrund Ihrer Änderungsanforderungen nicht gelöscht werden.	Ja. CloudFormation unterstützt nicht die `aws:TagsKey` Bedingung, Tags für den AMS-Namespace einzuschränken.		

Normen	Geht es kaputt	Risiken	Empfehlungen
Es ist Ihnen nicht gestattet, die AMS-Tag-Namenskonvention in Ihrer Infrastruktur zu verwenden, wie in Tabelle AMS-STD-002, weiter unten beschrieben.	Ja. Unterbrechungen für CloudFormation, CloudTrail, Amazon Elastic File System (EFS), OpenSearch, CloudWatch Logs, Amazon Simple Queue Service (SQS), Amazon EC2 Systems Manager (SSM), Tagging API; diese Dienste unterstützen nicht die `aws:TagsKey` Bedingung, das Tagging für den AMS-Namespace einzuschränken.		

AMS-STD-002: Identity and Access Management (IAM)

Normen	Geht es kaputt	Risiken	Empfehlungen
4.7 Aktionen, die den Change Management Process (RFC) umgehen, dürfen nicht erlaubt sein, wie z. B. das Starten oder Stoppen einer Instance, das Erstellen von S3-Buckets oder RDS-Instances	Ja. Der Zweck von Self-Service-Aktionen ermöglicht es Ihnen, Aktionen unter Umgehung des AMS-RFC-Systems durchzuführen.	Das Modell des sicheren Zugriffs ist ein zentraler technischer Aspekt von AMS, und ein IAM-Benutzer für Konsolen- oder programmatischen Zugriff umgeht diese Zugriffskontrolle. Der Zugriff der	Der IAM-Benutzer sollte zeitlich begrenzt sein und ihm sollten Berechtigungen auf der Grundlage der geringsten Rechte und erteilt werden. need-to-know

Normen	Geht es kaputt	Risiken	Empfehlungen
usw. Konten im Entwicklermodus und Dienste im Self-Service Provision ed Mode (SSPS) sind ausgenommen, solange die Aktionen innerhalb der Grenzen der zugewiesenen Rolle ausgeführt werden.		IAM-Benutzer wird nicht vom AMS Change Management überwacht. Der Zugriff ist CloudTrail nur angemeldet.	

AMS-STD-003: Netzwerksicherheit

Standards	Geht es kaputt	Risiken	Empfehlungen
S2. Elastic IP auf EC2 Instances darf nur mit einer formellen Risikoakzeptanzver einbarung oder mit einem gültigen Anwendungsfall durch interne Teams verwendet werden.	Ja. Self-Service-Aktionen ermöglich en es Ihnen, Elastic IP-Adressen (EIP) zuzuordnen und die Zuordnung aufzuhebe n.	Durch das Hinzufüge n einer Elastic IP zu einer Instance wird sie dem Internet zugänglich gemacht. Dies erhöht das Risiko der Offenlegu ng von Informationen und unberechtigter Aktivitäten.	Blockieren Sie jeglichen unnötigen Datenverkehr zu dieser Instance über Sicherheitsgruppen und stellen Sie sicher, dass Ihre Sicherhei tsgruppen mit der Instance verknüpft sind, um sicherzus tellen, dass der Datenverkehr nur dann zugelassen wird, wenn er aus geschäftl ichen Gründen benötigt wird.
S14. VPC-Peeri ng und Endpunktv	Ja. Dies ist im Rahmen der IAM-	Der Datenverkehr, der Ihr AMS-Konto	Wir empfehlen, nur mit AMS-Konten

Standards	Geht es kaputt	Risiken	Empfehlungen
erbindungen zwischen Konten, die demselben Kunden gehören, können zugelassen werden.	Richtlinie nicht möglich.	verlässt, wird nicht überwacht, sobald er die Kontogrenze überschreitet.	zu peeren, die Sie besitzen. Wenn Ihr Anwendungsfall dies erfordert, verwenden Sie Sicherhei tsgruppen und Routingtabellen, um zu begrenzen, welche Datenverkehrsberei che, Ressource n und Typen über die entsprechende Verbindung abfließen können.
Die AMS-Basis AMIs kann von AMS-verwalteten und nicht verwalteten Konten gemeinsam genutzt werden, sofern wir überprüfen können, ob sie derselben Organisation gehören. AWS		AMIs kann sensible Daten enthalten und unbeabsichtigten Konten ausgesetzt sein.	Teilen Sie die Daten nur AMIs mit dem Konto, das Ihrer Organisation gehört, oder überprüfen Sie den Anwendungsfall und die Kontoinfo rmationen, bevor Sie sie an Dritte weitergeb en.

AMS-STD-007: Protokollierung

Normen	Geht es kaputt	Risiken	Empfehlungen
19. Jedes Protokoll kann von einem AMS-Konto an ein anderes AMS-Konto desselben	Ja. Mögliche Unsicherheiten in Bezug auf Kundenpro tokolle, da die Überprüfung, ob sich	Protokolle können vertrauliche Daten enthalten und sie können unbefugten	Teilen Sie Protokoll e nur mit Konten, die von Ihrer AWS Organisation verwaltet werden, oder

Normen	Geht es kaputt	Risiken	Empfehlungen
Kunden weitergeleitet werden.			
20. Jedes Protokoll kann nur dann von AMS an ein Nicht-AMS-Konto weitergeleitet werden, wenn das Nicht-AMS-Konto demselben AMS-Kunden gehört (indem bestätigt wird, dass sie sich unter demselben AWS Organizations Konto befinden, oder indem die E-Mail-Domain mit dem Firmennamen des Kunden und dem mit PAYER verknüpften Konto abgeglichen wird). Dabei werden interne Tools verwendet.	die Kundenkonten in derselben Organisation befinden, nicht durch die IAM-Richtlinie erreicht werden kann.	Konten zugänglich gemacht werden.	überprüfen Sie den Anwendungsfall und die Kontoinformationen, bevor Sie sie an Dritte weitergeben. Wir können dies auf verschiedene Weise überprüfen. Erkundigen Sie sich bei Ihrem Cloud Service Delivery Manager (CSDM).

Arbeiten Sie mit Ihrem internen Autorisierungs- und Authentifizierungsteam zusammen, um die Berechtigungen für die Rollen im Direct Change-Modus entsprechend zu kontrollieren.

Einhaltung der Vorschriften im Modus „Direkter Wandel“

Der Direct Change-Modus ist sowohl mit produktiven als auch mit produktionsfremden Workloads kompatibel. Es liegt in Ihrer Verantwortung, die Einhaltung aller Compliance-Standards (z. B. PHI, HIPAA, PCI) sicherzustellen und sicherzustellen, dass die Verwendung des Direct Change-Modus Ihren internen Kontrollrahmen und Standards entspricht.

Änderungsmanagement im Direct Change-Modus

Änderungsmanagement ist der Prozess, den AMS Advanced verwendet, um Änderungsanträge zu implementieren. Eine Änderungsanforderung (RFC) ist eine Anfrage, die entweder von Ihnen oder AMS Advanced über die AMS Advanced-Schnittstelle erstellt wird, um eine Änderung an Ihrer verwalteten Umgebung vorzunehmen. Sie enthält eine AMS Advanced-Änderungstyp-ID (CT) für einen bestimmten Vorgang. Weitere Informationen finden Sie unter Change Management.

> **Note**
>
> Durch den Direct Change-Modus wird das AMS-Änderungsmanagement RFCs nicht entfernt. RFCs Mit DCM haben Sie weiterhin vollen Zugriff auf AMS.

Der AMS Direct Change-Modus (DCM) erweitert das AMS Advanced Change Management, indem er systemeigenen AWS Zugriff auf AMS Advanced Plus- und Premium-Konten ermöglicht, um Ressourcen bereitzustellen und zu aktualisieren AWS . Benutzer, denen über die IAM-Rollen die Berechtigung zum Direct Change-Modus erteilt wurde, können den systemeigenen AWS API-Zugriff verwenden, um Ressourcen in ihren AMS Advanced-Konten bereitzustellen und zu ändern. Die Benutzer können AMS Advanced Change Management weiterhin RFCs mit denselben IAM-Rollen verwenden. In beiden Fällen werden die Ressourcen und deren Änderungen vollständig von AMS unterstützt, einschließlich Überwachung, Patch, Backup und Incident Response Management. Benutzer, die nicht über die entsprechende Rolle in diesen Konten verfügen, müssen den RFC-Prozess AMS Advanced Change Management verwenden, um Änderungen vorzunehmen.

Anwendungsfälle des Change-Managements

Aus Sicherheitsgründen können einige Änderungen in AMS Advanced nur über den RFC-Prozess (Change Management Request for Change) vorgenommen werden. Der `AWSManagedServicesCloudFormationAdminRole` ist auf Aktionen beschränkt, die durch CloudFormation (CFN) ergriffen wurden. Weitere Informationen zum Erstellen von Stacks mit DCM finden Sie unter Erstellen von Stacks im Direct Change-Modus. Der `AWSManagedServicesUpdateRole` ist auf die folgenden Aktionen beschränkt.

Exemplarische Vorgehensweisen für jeden Änderungstyp, einschließlich des Änderungstyps Verwaltung | Verwaltetes Konto | Direkter Änderungsmodus | Aktivieren (ct-3rd4781c2nnhp), finden Sie im Abschnitt „Zusätzliche Informationen“ für den entsprechenden Änderungstyp im Abschnitt AMS Advanced Change Type Reference — Änderungstypen nach Klassifizierung.

Service	Aktion
AWS Key Management Service (AWS KMS)	Aktualisierung
AWS Certificate Manager	Erstellen
AWS Identity and Access Management (IAM)	Any
AWS VPN	Any
AMS-Ressourcenplaner	
AWS Backup	Backup-Plan erstellen
Aufnahme von AMS-Workloads () WIGs	Any
AMS-Ausgangsfilterung (verwaltetes Palo Alto)	
Änderungen am AMS Advanced MALZ-Konto	
Amazon GuardDuty	
Erweiterter AMS-Stack-Zugriff	Any
Volumen von Amazon Elastic Block Store (EBS)	Löschen
Standardverschlüsselung für Amazon Elastic Block Store (EBS)	Aktivieren Sie die Standardverschlüsselung
Amazon Elastic Compute Cloud (Amazon EC2)	Hostnamen ändern
Amazon Machine Images (AMI)	Löschen, teilen
EC2 Amazon-Sicherheitsgruppe	Any
AMS Advanced SSPS	
AWS Verwaltetes Microsoft AD	
AMS Advanced-Entwicklermodus	

Service	Aktion
Amazon Simple Storage Service (Amazon-S3)	Erstellen Sie S3-Bucket-Richtlinien
AWS Systems Manager	Erstellen

Stapel im Direct Change-Modus erstellen

Beim Starten von Stacks CloudFormation mit dem müssen zwei Voraussetzungen erfüllt sein`AWSManagedServicesCloudFormationAdminRole`, damit der Stack von AMS verwaltet werden kann:

- Die Vorlage muss eine `AmsStackTransform` enthalten.
- Der Stackname muss mit dem Präfix beginnen, `stack-` gefolgt von einer 17-stelligen alphanumerischen Zeichenfolge.

> **Note**
>
> Um den erfolgreich verwenden zu können`AmsStackTransform`, müssen Sie bestätigen, dass Ihre Stack-Vorlage die `CAPABILITY_AUTO_EXPAND` Fähigkeit enthält, mit der AWS CloudFormation (CFN) den Stack erstellen oder aktualisieren kann. Sie tun dies, indem Sie das `CAPABILITY_AUTO_EXPAND` als Teil Ihrer Create-Stack-Anfrage übergeben. CFN lehnt die Anfrage ab, wenn diese Funktion nicht bestätigt wird, wenn sie in der Vorlage enthalten `AmsStackTransform` ist. Die CFN-Konsole stellt sicher, dass Sie diese Funktion übergeben, wenn Sie die Transformation in Ihrer Vorlage haben. Dies kann jedoch übersehen werden, wenn Sie über deren Funktion mit CFN interagieren. APIs
> Sie müssen diese Funktion immer dann weitergeben, wenn Sie die folgenden CFN-API-Aufrufe verwenden:
>
> - CreateChangeSet
> - CreateStack
> - UpdateStack

Beim Erstellen oder Aktualisieren eines Stacks mit DCM werden dieselben Validierungen und Erweiterungen von CFN Ingest und Stack Update CTs auf dem Stack durchgeführt. Weitere

Informationen finden Sie unter AWS CloudFormation Ingest-Richtlinien, bewährte Methoden und Einschränkungen. Die Ausnahme besteht darin, dass die AMS-Standardsicherheitsgruppen (SGs) nicht an eigenständige EC2 Instances oder EC2 Instances in Auto Scaling Scaling-Gruppen (ASGs) angehängt werden. Wenn Sie Ihre CloudFormation Vorlage mit eigenständigen EC2 Instances oder erstellen ASGs, können Sie die Standardinstanz anhängen. SGs

> **Note**
>
> IAM-Rollen können jetzt mit dem erstellt und verwaltet werden. `AWSManagedServicesCloudFormationAdminRole`

Die AMS-Standardeinstellungen SGs verfügen über Eingangs- und Ausgangsregeln, die es ermöglichen, dass die Instances erfolgreich gestartet werden und dass AMS-Operationen und Sie später über SSH oder RDP darauf zugreifen können. Wenn Sie der Meinung sind, dass die AMS-Standardsicherheitsgruppen zu freizügig sind, können Sie Ihre eigenen Regeln SGs mit restriktiveren Regeln erstellen und diese an Ihre Instance anhängen, sofern Sie und AMS-Operationen dadurch weiterhin bei Vorfällen auf die Instance zugreifen können.

Die AMS-Standardsicherheitsgruppen sind die folgenden:

- SentinelDefaultSecurityGroupPrivateOnly: Kann in der CFN-Vorlage über diesen SSM-Parameter aufgerufen werden `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnly`
- SentinelDefaultSecurityGroupPrivateOnlyEgressAll: Kann in der CFN-Vorlage über diesen SSM-Parameter aufgerufen werden `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnlyEgressAll`

AMS-Transformation

Fügen Sie Ihrer CloudFormation Vorlage eine `Transform` Erklärung hinzu. Dadurch wird ein CloudFormation Makro hinzugefügt, das den Stack beim Start validiert und bei AMS registriert.

JSON-Beispiel

```
"Transform": {
    "Name": "AmsStackTransform",
    "Parameters": {
      "StackId": {"Ref" : "AWS::StackId"}
    }
```

```
  }
```

YAML-Beispiel

```
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
```

Fügen Sie die `Transform` Anweisung auch hinzu, wenn Sie die Vorlage eines vorhandenen Stacks aktualisieren.

JSON-Beispiel

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description" : "Create an SNS Topic",
    "Transform": {
      "Name": "AmsStackTransform",
      "Parameters": {
        "StackId": {"Ref" : "AWS::StackId"}
     }
  },
  "Parameters": {
    "TopicName": {
      "Type": "String",
      "Default": "HelloWorldTopic"
    }
  },
  "Resources": {
    "SnsTopic": {
      "Type": "AWS::SNS::Topic",
      "Properties": {
        "TopicName": {"Ref": "TopicName"}
      }
    }
  }
}
```

YAML-Beispiel

```
AWSTemplateFormatVersion: '2010-09-09'
```

```
Description: Create an SNS Topic
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
Parameters:
  TopicName:
    Type: String
    Default: HelloWorldTopic
Resources:
  SnsTopic:
    Type: AWS::SNS::Topic
    Properties:
      TopicName: !Ref TopicName
```

Stack name

Der Stackname muss mit dem Präfix beginnen, `stack-` gefolgt von einer 17-stelligen alphanumerischen Zeichenfolge. Dies dient der Aufrechterhaltung der Kompatibilität mit anderen AMS-Systemen, die auf dem AMS-Stack IDs arbeiten.

Im Folgenden finden Sie Beispiele für Möglichkeiten, einen kompatiblen Stack zu generieren IDs:

Bash:

```
echo "stack-$(env LC_CTYPE=C tr -dc 'a-z0-9' < /dev/urandom | head -c 17)"
```

Python:

```
import string
import random

'stack-' + ''.join(random.choices(string.ascii_lowercase + string.digits, k=17))
```

Powershell:

```
"stack-" + ( -join ((0x30..0x39) + ( 0x61..0x7A) | Get-Random -Count 17  | %
 {[char]$_}) )
```

Anwendungsfälle für den Direct Change Mode

Im Folgenden sind Anwendungsfälle für den Direct Change Mode aufgeführt:

Bereitstellung und Verwaltung von Ressourcen durch AWS CloudFormation

- Integrieren CloudFormation Sie bestehende Tools und Prozesse.

Kontinuierliches Ressourcenmanagement und Updates

- Kleine atomare Veränderungen mit geringem Risiko.
- Änderungen, die sonst über einen manuellen oder automatisierten RFC laufen würden.
- Tools, für die systemeigener AWS API-Zugriff erforderlich ist.
- Die DCM-Rolle kann verwendet werden, wenn Sie sich in der Migrationsphase befinden. Migrationsteams nutzen die Berechtigungen auf dem DCM, um Stacks zu erstellen oder zu ändern.
- DCM-Rollen können in der CI/CD Pipeline verwendet werden, um neue Aufgaben zu erstellen AMIs, Amazon ECS-Aufgaben zu erstellen usw.

AMS Advanced-Entwicklermodus

Themen

- Erste Schritte mit dem AMS Advanced Developer Mode
- Sicherheit und Compliance im Entwicklermodus
- Änderungsmanagement im Entwicklermodus
- Infrastruktur im AMS-Entwicklermodus bereitstellen
- Detective Controls im AMS-Entwicklermodus
- Protokollierung, Überwachung und Ereignisverwaltung im AMS-Entwicklermodus
- Vorfallmanagement im AMS-Entwicklermodus
- Patch-Management im AMS-Entwicklermodus
- Kontinuitätsmanagement im AMS-Entwicklermodus
- Sicherheits- und Zugriffsmanagement im AMS-Entwicklermodus

Der Entwicklermodus von AWS Managed Services (AMS) verwendet erhöhte Berechtigungen in AMS Advanced Plus- und Premium-Konten, um AWS-Ressourcen außerhalb des AMS Advanced-Change-Management-Prozesses bereitzustellen und zu aktualisieren. Im AMS Advanced Developer-Modus werden dazu native AWS-API-Aufrufe innerhalb der AMS Advanced Virtual Private Cloud (VPC)

genutzt, sodass Sie Infrastruktur und Anwendungen in Ihrer verwalteten Umgebung entwerfen und implementieren können.

Wenn Sie ein Konto verwenden, für das der Entwicklermodus aktiviert ist, werden Continuity Management, Patch Management und Change Management für Ressourcen bereitgestellt, die über den AMS Advanced Change Management-Prozess oder mithilfe eines AMS Amazon Machine Image (AMI) bereitgestellt wurden. Diese AMS-Verwaltungsfunktionen werden jedoch nicht für Ressourcen angeboten, die über native Ressourcen bereitgestellt werden. AWS APIs

Sie sind für die Überwachung der Infrastrukturressourcen verantwortlich, die außerhalb des AMS Advanced Change Management-Prozesses bereitgestellt werden. Der Entwicklermodus ist sowohl mit Produktionsworkloads als auch mit Workloads außerhalb der Produktion kompatibel. Mit erweiterten Berechtigungen tragen Sie eine größere Verantwortung dafür, dass die internen Kontrollen eingehalten werden.

> **Important**
>
> Ressourcen, die Sie im Entwicklermodus erstellen, können nur dann von AMS Advanced verwaltet werden, wenn sie mithilfe von AMS Advanced-Change-Management-Prozessen erstellt wurden.

Der Entwicklermodus ist einer der AMS-Advanced-Modi, die Sie verwenden können. Weitere Informationen finden Sie unter Übersicht der Modi.

Erste Schritte mit dem AMS Advanced Developer Mode

Lernen Sie die verschiedenen AMS Advanced-Konten im AMS Advanced-Entwicklermodus kennen und erfahren Sie, wie Sie den Entwicklermodus erfolgreich implementieren.

Themen

- Bevor Sie mit dem AMS-Entwicklermodus beginnen
- Voraussetzungen für den AMS-Entwicklermodus
- Wie implementiert man den AMS Advanced Developer-Modus
- Berechtigungen für den AMS Advanced-Entwicklermodus

Bevor Sie mit dem AMS-Entwicklermodus beginnen

Bevor Sie den Entwicklermodus implementieren, sollten Sie einige Dinge wissen.

AMS Advanced kann keine vorhandenen Stacks oder Ressourcen in einem DevMode Konto verwalten, die außerhalb des AMS Advanced-Änderungsverwaltungsprozesses durch Änderungsanforderungen (RFCs) erstellt wurden. Solange das Konto aktiv ist, verwaltet AMS Advanced jedoch weiterhin die Ressourcen DevMode, die im Rahmen des AMS Advanced-Change-Management-Prozesses mit bereitgestellt wurden. RFCs

Sie können nicht mit einem DevMode Konto beginnen und es später in ein von AMS Advanced verwaltetes Anwendungskonto umwandeln.

Voraussetzungen für den AMS-Entwicklermodus

Im Folgenden sind die Voraussetzungen für die Implementierung des Entwicklermodus aufgeführt:

- Sie müssen ein AMS Advanced-Kunde mit mindestens einem integrierten AMS Advanced Plus- oder Premium-Konto sein.
- Jedes Konto, das Sie verwenden, muss ein AMS Advanced Plus- oder Premium-Konto sein.
- Multi-Account Landing Zone (MALZ): Sie müssen die `AWSManagedServicesDevelopmentRole` vordefinierte Rolle AWS Identity and Access Management (IAM) verwenden. Sie fordern diese Rolle an. Im nächsten Abschnitt wird beschrieben, wie Sie Berechtigungen für den Entwicklermodus erwerben.
- Single-Account Landing Zone (SALZ): Sie müssen die `customer_developer_role` vordefinierte Rolle AWS Identity and Access Management (IAM) verwenden. Sie fordern diese Rolle an. Im nächsten Abschnitt wird beschrieben, wie Sie Berechtigungen für den Entwicklermodus erwerben.

Wie implementiert man den AMS Advanced Developer-Modus

Sie implementieren den Entwicklermodus, indem Sie beantragen, dass Ihrem berechtigten AMS Advanced-Konto die vordefinierte IAM-Rolle zugewiesen wird:

- MALZ: `AWSManagedServicesDevelopmentRole`
- SALZ: `customer_developer_role`

Anschließend weisen Sie die Rolle den entsprechenden Benutzern in Ihrem Verbundnetzwerk zu.

AMS Advanced empfiehlt, dass Sie sicherstellen, dass Ihre Verwendung des Entwicklermodus Ihren internen Kontrollrahmen und Standards entspricht, da der Entwicklermodus zwei Arten von Änderungen bewirkt: AMS Advanced Change Management für von AMS Advanced verwaltete Ressourcen und kundenverwalteter Rollenverbund für Ressourcen, die Sie als unser Kunde verwalten. Die Prozesse von AMS Advanced entsprechen zwar weiterhin unseren Erklärungen, aber die Kundenprozesse und Kontrollrahmen müssen möglicherweise aktualisiert werden.

Um den Entwicklermodus in Ihrem AMS Advanced-Konto zu implementieren

1. Vergewissern Sie sich, dass das Konto, das Sie im Entwicklermodus verwenden möchten, die unter aufgeführten Anforderungen erfülltVoraussetzungen für den AMS-Entwicklermodus.
2. Reichen Sie eine Änderungsanforderung (RFC) ein, indem Sie den Änderungstyp (CT) Management | Verwaltetes Konto | Entwicklermodus | Aktivieren (Überprüfung erforderlich) verwenden. Ein Beispiel für die Verwendung dieses CT finden Sie unter Entwicklermodus | Aktivieren (Überprüfung erforderlich).

   Nach der Verarbeitung des CT wird die vordefinierte IAM-Rolle (`AWSManagedServicesDevelopmentRole`für MALZ, `customer_developer_role` für SALZ) im angeforderten Konto bereitgestellt.
3. Weisen Sie den Benutzern, die Zugriff auf den Entwicklermodus benötigen, mithilfe Ihres internen Verbundprozesses die entsprechende Rolle zu.

   AMS Advanced empfiehlt, den Zugriff einzuschränken, um eine ungewollte oder nicht genehmigte Bereitstellung oder Änderung von Ressourcen zu verhindern.

Berechtigungen für den AMS Advanced-Entwicklermodus

Die vordefinierte Rolle (`AWSManagedServicesDevelopmentRole`für MALZ, `customer_developer_role` für SALZ) gewährt die Berechtigung zur Erstellung von Anwendungsinfrastrukturressourcen innerhalb der AMS Advanced VPC, einschließlich IAM-Rollen, und schränkt gleichzeitig den Zugriff auf Shared Service-Komponenten ein, die von AMS Advanced betrieben werden (z. B. Management-Hosts, Domain-Controller, Trend Micro EPS, Bastions und nicht unterstützte AWS-Services). Die Rolle schränkt auch den Zugriff auf Folgendes ein AWS-Services: Amazon- GuardDuty, AWS Organizations AWS Directory Service APIs, und AMS Advanced-Protokolle.

Mit der Rolle können Sie zwar zusätzliche IAM-Rollen erstellen, aber die gleichen Berechtigungsgrenzen, die im Zugriff im Entwicklermodus enthalten sind, gelten auch für alle IAM-Rollen, die von der erstellt wurden. `AWSManagedServicesDevelopmentRole`

Sicherheit und Compliance im Entwicklermodus

Für Sicherheit und Compliance sind AMS Advanced und Sie als Kunde gemeinsam verantwortlich. Im erweiterten Entwicklermodus von AMS wird Ihnen die gemeinsame Verantwortung für Ressourcen übertragen, die außerhalb des Change-Management-Prozesses oder im Rahmen des Change-Managements bereitgestellt, aber mit den Berechtigungen im Entwicklermodus aktualisiert wurden. Weitere Informationen zur gemeinsamen Verantwortung finden Sie unter AWS Managed Services.

Vorsichtsmaßnahmen:

- DevMode ermöglicht es Ihnen und Ihrem autorisierten Team, die deny-by-default Prinzipien zu umgehen, die den Kern der AMS-Sicherheit bilden. Die Vorteile, Self-Service und weniger Wartezeit auf AMS, müssen gegen die Nachteile abgewogen werden. Jeder kann unerwartete und zerstörerische Aktionen durchführen, ohne das Wissen seines Sicherheitsteams zu haben. Automatisierte Änderungstypen zur Aktivierung des Dev-Modus und des Direct Change-Modus sind verfügbar, und jede autorisierte Person in Ihrer Organisation kann diese Änderungen ausführen CTs und diese Modi aktivieren.
- Sie sind dafür verantwortlich, die Berechtigungen für die CT-Ausführung von Ihrer Benutzerbasis aus zu verwalten.
- AMS verwaltet keine CT-Ausführungsberechtigungen

Empfehlungen:

- Schützen
  - Kunden können den Zugriff auf dieses CT mithilfe von Zugriffsberechtigungen verhindern. Weitere Informationen finden Sie unter Einschränken von Berechtigungen mithilfe von IAM-Rollenrichtlinienerklärungen
  - Verhindern Sie den Zugriff auf dieses CT, indem Sie einen Proxy, z. B. ein ITSM-System, implementieren
  - Verwenden Sie Richtlinien zur Servicesteuerung (SCPs), die bei Bedarf Richtlinien und Verhaltensweisen verhindern, siehe AMS Preventative and Detective Controls Library
- Erkennen

  - Überwachen Sie Ihre RFCs darauf, dass diese ausgeführt werden CTs (Entwicklermodus aktivieren ct-1opjmhuddw194 und Direktänderungsmodus, Aktivieren Sie ct-3rd4781c2nnhp) und reagieren Sie entsprechend
  - Prüfen Sie, überprüfen Sie Ihre Konten auf das Vorhandensein der and/or IAM-Ressourcen, um die Konten zu identifizieren, für die der Entwicklermodus oder der Direktänderungsmodus bereitgestellt wurden
- Reagieren Sie
  - Entfernen Sie nach Bedarf Konten im Entwicklermodus

Sicherheit im Entwicklermodus

AMS Advanced bietet zusätzlichen Mehrwert mit einer präskriptiven landing zone, einem Change-Management-System und einer Zugriffsverwaltung. Bei Verwendung des Entwicklermodus wird der Sicherheitswert von AMS Advanced beibehalten, indem dieselbe Kontokonfiguration wie die standardmäßigen AMS Advanced-Konten verwendet wird, mit der das standardmäßige, sicherheitsverstärkte AMS Advanced-Netzwerk eingerichtet wird. Das Netzwerk ist durch die in der Rolle festgelegten Berechtigungsgrenzen geschützt (`AWSManagedServicesDevelopmentRole`für MALZ, `customer_developer_role` für SALZ). Dadurch wird verhindert, dass der Benutzer den bei der Einrichtung des Kontos festgelegten Parameterschutz aufhebt.

Benutzer mit dieser Rolle können beispielsweise auf Amazon Route 53 zugreifen, aber die interne Hosting-Zone von AMS Advanced ist eingeschränkt. Dieselben Berechtigungsgrenzen werden für eine IAM-Rolle durchgesetzt`AWSManagedServicesDevelopmentRole`, die von der erstellt wurde. Dadurch wird verhindert, `AWSManagedServicesDevelopmentRole` dass der Benutzer den Parameterschutz aufhebt, der beim Onboarding des Kontos in AMS Advanced eingerichtet wurde.

Einhaltung von Vorschriften im Entwicklermodus

Der Entwicklermodus ist sowohl mit Produktionsworkloads als auch mit Workloads außerhalb der Produktion kompatibel. Es liegt in Ihrer Verantwortung, die Einhaltung aller Compliance-Standards (z. B. PHI, HIPAA, PCI) sicherzustellen und sicherzustellen, dass die Verwendung des Entwicklermodus Ihren internen Kontrollrahmen und Standards entspricht.

Änderungsmanagement im Entwicklermodus

Change Management ist der Prozess, den der AMS Advanced-Service verwendet, um Änderungsanforderungen zu implementieren. Eine Änderungsanforderung (RFC) ist eine Anfrage, die

entweder von Ihnen oder AMS Advanced über die AMS Advanced-Schnittstelle erstellt wird, um eine Änderung an Ihrer verwalteten Umgebung vorzunehmen. Sie enthält eine Change Type (CT) -ID für einen bestimmten Vorgang. Weitere Informationen finden Sie unter Verwaltungsmodi ändern.

Die Änderungsverwaltung wird bei AMS Advanced-Konten, für die Berechtigungen im Entwicklermodus gewährt werden, nicht durchgesetzt. Benutzer, denen die Berechtigung für den Entwicklermodus mit der IAM-Rolle (`AWSManagedServicesDevelopmentRole`für MALZ, `customer_developer_role` für SALZ) erteilt wurde, können den systemeigenen AWS API-Zugriff verwenden, um Ressourcen in ihren AMS Advanced-Konten bereitzustellen und zu ändern. Benutzer, die nicht über die entsprechende Rolle in diesen Konten verfügen, müssen den AMS-Advanced-Change-Management-Prozess verwenden, um Änderungen vorzunehmen.

> **Important**
>
> Ressourcen, die Sie im Entwicklermodus erstellen, können nur dann von AMS Advanced verwaltet werden, wenn sie mithilfe von AMS Advanced-Change-Management-Prozessen erstellt wurden. An AMS Advanced eingereichte Änderungsanträge für Ressourcen, die außerhalb des AMS Advanced-Change-Management-Prozesses erstellt wurden, werden von AMS Advanced abgelehnt, da sie von Ihnen bearbeitet werden müssen.

API-Einschränkungen für Self-Service-Bereitstellungsdienste

Alle selbst bereitgestellten AMS Advanced-Dienste werden im Entwicklermodus unterstützt. Der Zugriff auf selbst bereitgestellte Dienste unterliegt den Einschränkungen, die in den jeweiligen Abschnitten des Benutzerhandbuchs beschrieben sind. Wenn ein selbst bereitgestellter Dienst mit Ihrer Rolle im Entwicklermodus nicht verfügbar ist, können Sie über den Änderungstyp Entwicklermodus eine aktualisierte Rolle anfordern.

Die folgenden Dienste bieten keinen vollen Zugriff auf den Dienst: APIs

Self-Provisioned Services: Eingeschränkt im Entwicklermodus

Service	Hinweise
Amazon API Gateway	Alle APIs Gateway-Aufrufe sind zulässig, außer `SetWebACL`

Service	Hinweise
Application Auto Scaling	Es können nur skalierbare Ziele registriert oder deregistriert und eine Skalierungsrichtlinie hinzugefügt oder gelöscht werden.
AWS CloudFormation	Es kann nicht auf CloudFormation Stacks zugegriffen oder diese geändert werden, denen ein Name als Präfix vorangestellt ist. `mc-`
AWS CloudTrail	Es kann nicht auf CloudTrail Ressourcen zugegriffen oder diese geändert werden, denen ein Name als Präfix vorangestellt ist. `ams-` and/or `mc-`
Amazon Cognito (Benutzerpools)	Softwaretoken können nicht verknüpft werden. Benutzerpools, Benutzerimportaufträge, Ressourcenserver oder Identitätsanbieter können nicht erstellt werden.

Service	Hinweise
AWS Directory Service	Nur die folgenden AWS Directory Service Aktionen sind für die `Connect` `WorkSpaces` Dienste erforderlich. Alle anderen Verzeichn isdienst-Aktionen werden durch die Berechtig ungsgrenzrichtlinie für den Entwicklermodus verweigert: • `ds:AuthorizeApplication` • `ds:CreateAlias` • `ds:CreateIdentityPoolDirectory` • `ds:DeleteDirectory` • `ds:DescribeDirectories` • `ds:GetAuthorizedApplication Details` • `ds:ListAuthorizedApplications` • `ds:UnauthorizeApplication` Bei landing zone Zone-Konten mit einem Konto verweigert die Boundary-Policy ausdrücklich den Zugriff auf das verwaltete AMS Advanced-Verzeichnis, das von AMS Advanced zur Aufrechterhaltung des Zugriffs auf Konten mit aktiviertem Dev-Modus verwendet wird.
Amazon Elastic Compute Cloud	Es kann nicht auf Amazon EC2 APIs zugegriff en werden, die die Zeichenfolge: `DhcpOptio ns Gateway`,`Subnet`,`VPC`, und enthalten`VPN`. Es kann nicht auf EC2 Amazon-Ressourcen zugegriffen oder diese geändert werden, denen ein Tag mit dem Präfix`AMS`,, `mcManagemen tHostASG` , and/or `sentinel` vorangestellt ist.

Service	Hinweise
Amazon EC2 (Berichte)	Es wird nur Lesezugriff gewährt (kann nicht geändert werden). Hinweis: Amazon EC2 Reports zieht um. Der Menüpunkt Berichte wird aus dem Navigationsmenü der EC2 Amazon-Konsole entfernt. Um Ihre EC2 Amazon-Nutzungsberichte nach der Entfernung einzusehen, verwenden Sie die AWS Billing und Cost Management-Konsole.
AWS Identity and Access Management (IAM)	Bestehende Berechtigungsgrenzen können nicht gelöscht oder die Kennwortrichtlinien für IAM-Benutzer geändert werden. IAM-Ressourcen können nur erstellt oder geändert werden, wenn Sie die richtige IAM-Rolle (**`AWSManagedServicesDevelopmentRole`** für MALZ, **`customer_developer_role`** für SALZ) verwenden. IAM-Ressourcen mit dem Präfix:,,, können nicht geändert werden. `ams mc customer_deny_policy` and/or `sentinel` Beim Erstellen einer neuen IAM-Ressource (Rolle, Benutzer oder Gruppe) muss die Berechtigungsgrenze (MALZ:`AWSManagedServicesDevelopmentRolePermissionsBoundary`, SALZ:`ams-app-infra-permissions-boundary`) angehängt werden.
AWS Key Management Service (AWS KMS)	Auf von AMS Advanced verwaltete KMS-Schlüssel kann nicht zugegriffen oder diese geändert werden.

Service	Hinweise
AWS Lambda	Es kann nicht auf AWS Lambda Funktionen zugegriffen oder diese geändert werden, denen das Präfix vorangestellt ist. `AMS`
CloudWatch Logs	Auf CloudWatch Protokollstreams mit dem Präfix:,`mc`, `awslambda`, and/or `AMS` kann nicht zugegriffen werden.
Amazon Relational Database Service (Amazon RDS)	Auf Amazon Relational Database Service (Amazon RDS) -Datenbanken (DBs) mit dem Präfix: kann nicht zugegriffen oder diese geändert werden. `mc-`
AWS Resource Groups	Kann nur auf `Get` API-Aktionen `List` und `Search` Resource Group zugreifen.
Amazon Route 53	Auf die von Route53 AMS Advanced verwaltet en Ressourcen kann nicht zugegriffen oder diese geändert werden.
Amazon S3	Es kann nicht auf Amazon S3 S3-Buckets zugegriffen werden, denen ein Name mit dem Präfix:`ams-*`, `amsms-a`, oder vorangestellt ist. `mc-a`
AWS Security Token Service	Die einzige zulässige Sicherheitstoken-Dienst-API ist. `DecodeAuthorizationMessage`
Amazon SNS	Es kann nicht auf SNS-Themen zugegriff en werden, denen ein Name mit dem Präfix: `AMS-Energon-Topic` , oder vorangestellt ist. `MMS-Topic`

Service	Hinweise
AWS Systems Manager Manager (SSM)	SSM-Parameter mit `ams` dem Präfix, oder können nicht geändert werden. `mc` `svc` Die SSM-API `SendCommand` kann nicht für EC2 Amazon-Instances verwendet werden, denen ein Tag mit `ams` dem Präfix oder vorangestellt ist. `mc`
AWS Taggen	Sie haben nur Zugriff auf AWS Tagging-API-Aktionen, denen das Präfix vorangestellt ist. `Get`
AWS Lake Formation	Die folgenden AWS Lake Formation API-Aktionen werden verweigert: • `lakeformation:DescribeResource` • `lakeformation:GetDataLakeSettings` • `lakeformation:DeregisterResource` • `lakeformation:RegisterResource` • `lakeformation:UpdateResource` • `lakeformation:PutDataLakeSettings`
Amazon Elastic Inference	Sie können nur die Elastic Inference API-Aktion `elastic-inference:Connect` aufrufen. Diese Berechtigung ist in der Datei enthalten `customer_sagemaker_admin_policy` , die dem `customer_sagemaker_admin_role` beigefügt ist. Mit dieser Aktion erhalten Sie Zugriff auf den Elastic Inference Accelerator.

Service	Hinweise
AWS Shield	Kein Zugriff auf einen dieser Dienste APIs oder Konsolen.
Amazon Simple Workflow Service	Kein Zugriff auf diese Dienste APIs oder Konsolen.

Infrastruktur im AMS-Entwicklermodus bereitstellen

Benutzer, die nicht über die IAM-Rolle im Entwicklermodus verfügen, müssen in Konten`AWSManagedServicesDevelopmentRole`, in denen der Entwicklermodus aktiviert ist, den AMS-Advanced-Change-Management-Prozess befolgen, der AMS Advanced nutzt. AMIs Benutzer mit der richtigen Rolle (MALZ:`AWSManagedServicesDevelopmentRole`, SALZ:`customer_developer_role`) können das AMS Advanced Change Management System und AMS Advanced verwenden, sind AMIs aber nicht dazu verpflichtet.

> **Note**
>
> Ein AWS AMI, das nicht über AMS Advanced Workload Ingestion verarbeitet oder in einem AMS Advanced-Konto erstellt wurde, enthält keine für AMS Advanced erforderlichen Konfigurationen.

Detective Controls im AMS-Entwicklermodus

Dieser Abschnitt wurde redigiert, da er sensible sicherheitsrelevante AMS-Informationen enthält. Diese Informationen sind in der AMS-Konsolendokumentation verfügbar. Um auf AWS Artifact zuzugreifen, können Sie sich an Ihren CSDM wenden, um Anweisungen zu erhalten, oder gehen Sie zu Erste Schritte mit AWS Artifact.

Protokollierung, Überwachung und Ereignisverwaltung im AMS-Entwicklermodus

Protokollierung, Überwachung und Ereignisverwaltung sind nicht für Ressourcen verfügbar, die außerhalb des AMS Advanced Change Management-Prozesses bereitgestellt wurden, oder für

Ressourcen, die über das Änderungsmanagement bereitgestellt und dann von einem Konto mit Berechtigungen im Entwicklermodus geändert wurden.

Vorfallmanagement im AMS-Entwicklermodus

Keine Änderung der Reaktionszeiten bei Vorfällen. Für Ressourcen, die außerhalb des Change-Management-Prozesses bereitgestellt wurden, oder für Ressourcen, die über das Änderungsmanagement bereitgestellt und dann von einem Konto mit den Berechtigungen im Entwicklermodus geändert wurden, ist die Lösung eines Vorfalls nach bestem Wissen möglich.

> **Note**
>
> Das AMS Service Level Agreement (SLA) gilt nicht für Ressourcen, die außerhalb des AMS-Change-Management-Systems erstellt oder aktualisiert wurden (Änderungsanforderungen oder RFCs), einschließlich des Entwicklermodus. Daher werden Ressourcen, die im Entwicklermodus aktualisiert oder erstellt wurden, automatisch auf P3 heruntergestuft, und AMS-Support ist nach bestem Bemühen möglich.

Patch-Management im AMS-Entwicklermodus

Patch-Management ist nicht für Ressourcen verfügbar, die außerhalb des AMS Advanced-Change-Management-Prozesses bereitgestellt wurden, oder für Ressourcen, die über das Änderungsmanagement bereitgestellt und dann von einem Konto mit Berechtigungen im Entwicklermodus geändert wurden. Zeiten für Patches:

- Für ein wichtiges Sicherheitsupdate: Innerhalb von 10 Werktagen nach der Veröffentlichung durch den Anbieter für Ressourcen, die über das Änderungsmanagement bereitgestellt und dann von einem Konto mit Berechtigungen im Entwicklermodus geändert wurden.
- Für ein wichtiges Update: Innerhalb von 2 Monaten nach der Veröffentlichung durch den Anbieter für Ressourcen, die über das Änderungsmanagement bereitgestellt und dann über ein Konto mit Berechtigungen im Entwicklermodus geändert wurden.

Kontinuitätsmanagement im AMS-Entwicklermodus

Continuity Management ist nicht für Ressourcen verfügbar, die außerhalb des AMS Advanced-Change-Management-Prozesses bereitgestellt wurden, oder für Ressourcen, die über das

Änderungsmanagement bereitgestellt und dann von einem Konto mit Berechtigungen im Entwicklermodus geändert wurden.

Bei Ressourcen, die außerhalb des AMS Advanced-Change-Management-Prozesses bereitgestellt wurden, oder bei Ressourcen, die über das Änderungsmanagement bereitgestellt und dann von einem Konto mit Berechtigungen im Entwicklermodus geändert wurden, kann die Initiierungszeit für die Wiederherstellung der Umgebung bis zu 12 Stunden in Anspruch nehmen.

Sicherheits- und Zugriffsmanagement im AMS-Entwicklermodus

Für den Schutz vor Schadsoftware sind Sie für Ressourcen verantwortlich, die außerhalb des AMS Advanced-Change-Management-Prozesses bereitgestellt wurden, oder für Ressourcen, die über das Änderungsmanagement bereitgestellt und dann von einem Konto mit Berechtigungen im Entwicklermodus geändert wurden. Der Zugriff auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances, die nicht über AMS Advanced Change Management bereitgestellt werden, kann durch Schlüsselpaare gesteuert werden, anstatt einen Verbundzugriff bereitzustellen.

Self-Service-Bereitstellungsmodus in AMS

Der Self-Service Provisioning (SSP) -Modus von AWS Managed Services (AMS) bietet vollen Zugriff auf native AWS Service- und API-Funktionen in AMS-verwalteten Konten. Sie greifen über standardisierte, auf bestimmte Bereiche zugeschnittene Rollen auf Services zu. AWS Identity and Access Management AMS bietet Serviceanfragen und das Management von Vorfällen. Warnmeldungen, Überwachung, Protokollierung, Patches, Backups und Änderungsmanagement liegen in Ihrer Verantwortung. In vielen Fällen werden Self-Service Provisioning Services (SSPS) selbst oder serverlos verwaltet und erfordern keine Verwaltung bestimmter betrieblicher Aufgaben wie das Patchen. Sie profitieren von der Nutzung dieser Services innerhalb der durch AMS-Guardrails definierten Umgebungsgrenzen. Alle IAM-Änderungen (einschließlich serviceverknüpfter Rollen, Servicerollen, kontoübergreifender Rollen oder Richtlinienaktualisierungen) müssen von AMS Operations genehmigt werden, um die grundlegende Sicherheit der Plattform aufrechtzuerhalten. Sie können AWS CloudFormation Vorlagen verwenden, um die Bereitstellung dieser Dienste zu automatisieren. Dies wird jedoch nicht für alle SSP-Dienste unterstützt.

> **Important**
>
> Verwenden Sie den SSP-Modus in Ihren AWS Managed Services (AMS) -Konten, um auf AWS Services zuzugreifen und diese zu nutzen, mit den angegebenen Einschränkungen.

Es gibt einige AWS-Services , die Sie ohne AMS-Verwaltung in Ihrem AMS-Konto verwenden können. Die Dienste im Self-Service Provisioning-Modus, kurz SSPS, werden im Abschnitt beschrieben, wie Sie sie zu Ihrem AMS-Konto hinzufügen können und FAQs für welche Dienste.

Self-Service Provisioning Services werden so angeboten, wie sie sind, und Sie sind für deren Verwaltung verantwortlich. AMS bietet keine Benachrichtigungen, Überwachungs-, Protokollierungs- oder Patching-Funktionen für die Ressourcen, die mit diesen Diensten verknüpft sind. AMS bietet IAM-Rollen, mit denen Sie den Dienst in Ihrem AMS-Konto sicher nutzen können. AMS gelten SLAs nicht.

Für Ressourcen, die Sie über Self-Service bereitstellen, bietet AMS Vorfallmanagement, detektive Kontrollen und Leitplanken, Berichterstattung, zugewiesene Ressourcen (Cloud Service Delivery Manager und Cloud Architect), Sicherheit und Zugriff sowie technischen Support bei Serviceanfragen. Darüber hinaus übernehmen Sie gegebenenfalls die Verantwortung für das Kontinuitätsmanagement, das Patch-Management, die Infrastrukturüberwachung und das Änderungsmanagement für Ressourcen, die außerhalb des AMS-Change-Management-Systems bereitgestellt oder konfiguriert wurden.

Erste Schritte mit dem SSP-Modus in AMS

Self-Service Provisioning ist einer der AMS-Modi für die Multi-Account-Landing landing zone (MALZ), die Sie verwenden können. Weitere Informationen finden Sie unter Übersicht der Modi.

Um Funktionen zur Self-Service-Bereitstellung bereitzustellen, hat AMS erweiterte IAM-Rollen mit Rechtegrenzen eingerichtet, um unbeabsichtigte Änderungen durch direkten Zugriff zu verhindern. AWS-Service Die Rollen verhindern nicht alle Änderungen, und Sie müssen Ihre internen Kontrollen und Compliance-Richtlinien einhalten und sicherstellen, dass alle AWS-Services verwendeten Rollen die erforderlichen Zertifizierungen erfüllen. Dies ist der Self-Service-Bereitstellungsmodus. Einzelheiten zu den AWS Compliance-Anforderungen finden Sie unter AWS Compliance.

Um Ihrem Landingzone-Anwendungskonto mit mehreren Konten einen Self-Service Provisioning Service hinzuzufügen, verwenden Sie den Befehl Verwaltung | AWS Service | Self-Provisioned Service | Änderungstyp hinzufügen (CT), entweder den für die Prüfung erforderlichen CT oder den automatisierten CT, wie für den Service angegeben.

> **Note**
>
> Um zu beantragen, dass AMS einen zusätzlichen Self-Service-Bereitstellungsservice anbietet, reichen Sie eine Serviceanfrage ein.

Verwenden Sie AMS SSP, um Amazon API Gateway in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon API Gateway zuzugreifen. Amazon API Gateway ist ein vollständig verwalteter Service, der Entwicklern die Erstellung, Veröffentlichung, Wartung, Überwachung und Sicherung APIs in jeder Größenordnung erleichtert. Mithilfe von können AWS Management Console Sie REST erstellen WebSocket APIs , die als Eingangstür für Anwendungen dienen, um auf Daten, Geschäftslogik oder Funktionen aus Ihren Back-End-Services zuzugreifen, z. B. Workloads, die auf Amazon Elastic Compute Cloud (Amazon EC2) ausgeführt werden, Code, der auf AWS Lambdabeliebigen Webanwendungen ausgeführt wird, oder Echtzeitkommunikationsanwendungen.

API Gateway übernimmt alle Aufgaben, die mit der Annahme und Verarbeitung von bis zu Hunderttausenden von gleichzeitigen API-Aufrufen verbunden sind, einschließlich Verkehrsmanagement, Autorisierung und Zugriffskontrolle, Überwachung und API-Versionsverwaltung. Für API Gateway fallen keine Mindestgebühren oder Startkosten an. Sie zahlen nur für die API-Aufrufe, die Sie erhalten, und die Menge der übertragenen Daten. Mit dem gestaffelten Preismodell von API Gateway können Sie Ihre Kosten senken, wenn Ihre API-Nutzung steigt. Weitere Informationen finden Sie unter Amazon API Gateway.

Häufig gestellte Fragen: API Gateway in AMS

F: Wie beantrage ich Zugriff auf Amazon API Gateway in meinem AMS-Konto?

Fordern Sie Zugriff auf API Gateway an, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_apigateway_author_role` `customer_apigateway_cloudwatch_role` Konto die folgenden IAM-Rollen zur Verfügung: und. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rollen in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon API Gateway in meinem AMS-Konto?

- Die API-Gateway-Konfiguration ist auf Ressourcen ohne `AMS-` `MC-` Präfixe beschränkt, um Änderungen an der AMS-Infrastruktur zu verhindern.
- `CREATE`Die Rechte für VPCLink sind deaktiviert, um die unregulierte Erstellung von Elastic Load Balancers zu verhindern. Falls VPCLinks erforderlich, finden Sie weitere Informationen unter Application Load Balancer | Erstellen.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon API Gateway in meinem AMS-Konto?

Dies hängt von der Art des API Gateway ab, das Sie bereitstellen möchten. Es kann sich um einen eigenständigen Dienst handeln, er kann aber auch Zugriff auf bestehende Dienste (z. B. Network Load Balancer) anfordern.

Verwenden Sie AMS SSP, um Alexa for Business in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf Funktionen von Alexa for Business zuzugreifen. Alexa for Business ist ein Dienst, der es Ihrem Unternehmen und Ihren Mitarbeitern ermöglicht, Alexa zu verwenden, um mehr Arbeit zu erledigen. Mit Alexa for Business können Sie Alexa als intelligenten Assistenten verwenden, um in Besprechungsräumen, an Ihrem Schreibtisch und sogar mit den Alexa-Geräten, die Sie bereits zu Hause oder unterwegs verwenden, produktiver zu sein. IT- und Facility-Manager können Alexa for Business verwenden, um die Auslastung der vorhandenen Besprechungsräume an ihrem Arbeitsplatz zu messen und zu erhöhen.

Weitere Informationen finden Sie unter Alexa for Business.

Häufig gestellte Fragen zu Alexa for Business in AWS Managed Services

F: Wie beantrage ich Zugriff auf Alexa for Business in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_alexa_console_role` Konto die folgende IAM-Rolle zur Verfügung:. A `customer_alexa_device_setup_user` wird auch für das von Alexa for Business bereitgestellte Geräteeinrichtungstool erstellt. Dieses Geräteeinrichtungstool kann dann zur Einrichtung Ihrer Geräte verwendet werden. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rollen in Ihre Verbundlösung integrieren.

Mit dem Alexa for Business-Gateway können Sie Alexa for Business mit Ihren Endpunkten der Cisco Webex- und Poly Group-Serie verbinden, um Besprechungen mit Ihrer Stimme zu steuern. Die Gateway-Software läuft auf Ihrer lokalen Hardware und leitet Konferenzanweisungen von Alexa for Business sicher an Ihren Cisco-Endpunkt weiter. Das Gateway benötigt zwei Paare von AWS Anmeldeinformationen, um mit Alexa for Business zu kommunizieren. Wir bieten zwei IAM-Benutzer mit beschränktem Zugriff: `customer_alexa_gateway_installer_user` und

`customer_alexa_gateway_execution_user` für Ihre Alexa for Business-Gateways einen für die Installation des Gateways und einen für den Betrieb des Gateways. Diese können angefordert werden, indem Sie einen RFC mit dem Änderungstyp Deployment | Advanced Stack components | Identity and Access Management (IAM) | Entität oder Richtlinie erstellen (Überprüfung erforderlich) einreichen (ct-3dpd8mdd9jn1r).

> **Note**
>
> Um Nutzungsberichte zu generieren und an Amazon S3 zu senden, geben Sie den Amazon S3 S3-Bucket-Namen im RFC für den selbst bereitgestellten Service an.

F: Welche Einschränkungen gelten für die Nutzung von Alexa for Business in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von Alexa for Business ist mit der selbst bereitgestellten Servicerolle Alexa for Business verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Alexa for Business in meinem AMS-Konto?

- Wenn Sie WPA2 Enterprise Wi-Fi verwenden möchten, um Ihre gemeinsam genutzten Geräte einzurichten, geben Sie diesen Netzwerksicherheitstyp im Geräte-Setup-Tool an, wofür ein erforderlich AWS Private Certificate Authority ist.
- AMS erstellt nur geheime Schlüssel, die mit dem Namespace „A4B“ beginnen. Dies ist nur auf diesen Namespace beschränkt.

F: Welche Funktionen von Alexa for Business sind separat erforderlich RFCs?

Um ein Alexa Voice Service (AVS) -Gerät bei Alexa for Business zu registrieren, gewähren Sie Zugriff auf den integrierten Gerätehersteller von Alexa. Dazu muss in der Alexa for Business Business-Konsole eine IAM-Rolle erstellt werden, die mit dem Änderungstyp Management | Other | Other bereitgestellt werden kann. Auf diese Weise kann der AVS-Gerätehersteller Geräte in Ihrem Namen bei Alexa for Business registrieren und verwalten.

Verwenden Sie AMS SSP, um Amazon AppStream 2.0 in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf Funktionen von Amazon AppStream AppStream 2.0 (2.0) zuzugreifen.

AppStream 2.0 ermöglicht es Ihnen, Ihre Desktop-Anwendungen zu verschieben AWS, ohne sie neu schreiben zu müssen. Sie können Ihre Anwendungen auf AppStream Version 2.0 installieren, Startkonfigurationen festlegen und Ihre Anwendungen Benutzern zur Verfügung stellen. AppStream 2.0 bietet eine große Auswahl an Optionen für virtuelle Maschinen, sodass Sie den Instanztyp auswählen können, der Ihren Anwendungsanforderungen am besten entspricht, und die Parameter für die automatische Skalierung so einstellen können, dass Sie die Anforderungen Ihrer Endbenutzer problemlos erfüllen können. AppStream 2.0 ermöglicht es Ihnen, Anwendungen in Ihrem eigenen Netzwerk zu starten, was bedeutet, dass Ihre Anwendungen mit Ihren vorhandenen AWS Ressourcen interagieren können.

Mit Amazon AppStream 2.0 können Sie Ihre Anwendungen mithilfe des Image Builders schnell und einfach installieren, testen und aktualisieren. Jede Anwendung, die auf Microsoft Windows Server 2012 R2, Windows Server 2016 oder Windows Server 2019 ausgeführt wird, wird unterstützt, und Sie müssen keine Änderungen vornehmen. Wenn Ihre Tests abgeschlossen sind, können Sie Konfigurationen für den Anwendungsstart und Standardbenutzereinstellungen festlegen und Ihr Image veröffentlichen, damit Benutzer darauf zugreifen können.

Weitere Informationen finden Sie unter AppStream 2.0.

AppStream 2.0 in AWS Managed Services — Häufig gestellte Fragen

F: Wie beantrage ich Zugriff auf AppStream 2.0 in meinem AMS-Konto?

Beantragen Sie Zugriff auf AppStream 2.0, indem Sie einen RFC mit dem Änderungstyp Management | AWS Service | Self-Provisioned Service | Add (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt `customer_appstream_console_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:.

A `customer_appstream_stream_role` wird auch zum Streamen von Anwendungen eingesetzt, bei denen Benutzer mit ihren Active Directory-Anmeldeinformationen authentifiziert werden müssen.

Nach der Bereitstellung in Ihrem Konto müssen Sie die Rollen in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Verwendung von AppStream 2.0 in meinem AMS-Konto?

- Die folgenden Funktionen müssen vom AMS-Supportteam konfiguriert werden und erfordern spezielle Funktionen RFCs. Anweisungen zur Anforderung zusätzlicher Funktionen finden Sie in Abschnitt 4.
  - Erstellen und Streamen von Schnittstellen-VPC-Endpunkten.

- Support für Amazon S3 S3-Endpunkte für Basisordner und Persistenz von Anwendungseinstellungen in einem privaten Netzwerk.
- Erstellung und Auswahl der IAM-Rolle, die auf allen Fleet-Streaming-Instances verfügbar sein wird.
- Beitritt zu AppStream 2.0-Flotten und Image Builder-Microsoft-Active-Directory-Domänen
- Erstellen von benutzerdefinierten AppStream 2.0-Nutzungsberichten.
- Benutzerdefiniertes Branding wird derzeit nicht unterstützt.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von AppStream 2.0 in meinem AMS-Konto?

Geben Sie bei der Übermittlung des RFC an Onboard AppStream 2.0 den Namen des Amazon S3 S3-Buckets an, der für den AppStream 2.0-Nutzungsbericht verwendet werden soll. Der Bucket-Name wird zu dem hinzugefügt`customer-appstream-usagereports-policy`, der beim Onboarding von AppStream 2.0 erstellt wurde.

F: Für welche AppStream 2.0-Funktionalität ist eine separate Version erforderlich? RFCs

- Um einen VPC-Schnittstellen-Endpunkt für AppStream 2.0 auszuwählen, reichen Sie einen RFC vom Typ Management | Other | Other | Update ein, um einen VPC-Endpunkt in Ihrem Konto zu erstellen. Schritte zum Erstellen benutzerdefinierter Endpoints für AppStream 2.0 finden Sie unter Creating and Streaming from Interface VPC Endpoints im AppStream 2.0-Benutzerhandbuch.
- Die Support von Amazon S3 S3-Endpunkten für Basisordner und die Persistenz von Anwendungseinstellungen in einem privaten Netzwerk kann konfiguriert werden, indem Amazon S3 S3-VPC-Endpunkte mit einem RFC vom Typ Management | Other | Other | Create change type angefordert werden. Der RFC muss den Amazon S3 S3-Ziel-Bucket, der den Inhalt des Home-Ordners hostet, bzw. die Amazon S3 S3-Buckets für Anwendungseinstellungen enthalten. Dieser RFC stellt AppStream 2.0 die Berechtigungen bereit, die für den Zugriff auf Amazon S3 S3-VPC-Endpunkte erforderlich sind. Schritte zum Erstellen benutzerdefinierter Endpunkte für Streams finden Sie unter Using Amazon S3 VPC Endpoints for Home Folders and Application Settings Persistence im AppStream 2.0-Benutzerhandbuch.
- Um eine IAM-Rolle zu erstellen und auszuwählen, die auf allen Fleet-Streaming-Instances verfügbar sein wird, reichen Sie einen RFC vom Typ Deployment | Advanced Stack Components | Identity and Access Management (IAM) | Entität oder Richtlinie erstellen (Überprüfung erforderlich) (ct-3dpd8mdd9jn1r) ein und fordern Sie die IAM-Rolle mit der erforderlichen Richtlinie an. Der Name der IAM-Rolle sollte immer mit dem Präfix „customer_appstream“ beginnen.

- Amazon AppStream 2.0-Flotten und Image Builder können mit Domains in Microsoft Active Directory verknüpft werden, indem ein RFC vom Typ Management | Other | Other | Update für die Erstellung eines Dienstkontos in Active Directory (AD) eingereicht wird. Die Mindestberechtigungen, die für den Beitritt zu Microsoft Active Directory erforderlich sind, sind in der AppStream 2.0-Dokumentation unter Gewähren von Berechtigungen zum Erstellen und Verwalten von Active Directory-Computerobjekten definiert.
- Um benutzerdefinierte AppStream 2.0-Nutzungsberichte zu erstellen, reichen Sie einen RFC für Management | Other | Other | Create Change Type RFC ein und fordern Sie Folgendes an:
  - "AppStreamUsageReports" Erstellung eines CFN-Stacks
  - „customer_appstream_usagereports_role“ muss im Konto bereitgestellt werden
  - Geben Sie außerdem die folgenden Details an:
    - Geben Sie den CRON-Ausdruck an, um die Ausführung des Crawlers zu planen. Standardmäßig ist es jeden Tag 23:00 UTC.
    - Amazon S3 S3-Bucket-ARN, der für Athena-Abfrageergebnisse verwendet werden soll. Dieser Bucket sollte das Präfix haben: `aws-athena-query-results`
    - Amazon S3 S3-Bucket ARN für AppStream 2.0-Nutzungsberichte, Protokolle.

  Nachdem die Rolle bereitgestellt wurde, integrieren Sie die Rolle in Ihre Verbundlösung und melden Sie sich an. Greifen Sie dann auf AWS GlueAWS Glue Athena zu, um mithilfe der Nutzungsbericht-Rolle benutzerdefinierte Berichte zu generieren. Einzelheiten zur Verwendung von AppStream 2.0-Nutzungsberichten finden Sie in der 2.0-Dokumentation unter Benutzerdefinierte Berichte erstellen und AppStream 2.0-Nutzungsdaten analysieren. AppStream

Verwenden Sie AMS SSP, um Amazon Athena in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Athena (Athena) zuzugreifen. Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten in Amazon S3 mithilfe von Standard-SQL analysieren können. Athena ist Serverless, weshalb auch keine Infrastruktur eingerichtet oder verwaltet werden muss – und Sie zahlen nur für tatsächlich ausgeführte Abfragen. Sie verweisen auf Ihre Daten in Amazon S3, definieren das Schema und beginnen mit der Abfrage mithilfe von Standard-SQL. Die meisten Ergebnisse werden innerhalb von Sekunden geliefert. Mit Athena sind keine komplexen extract-transform-load (ETL-) Jobs erforderlich, um Ihre Daten für die Analyse vorzubereiten. Dies

macht es für jeden mit SQL-Kenntnissen einfach, große Datensätze schnell zu analysieren. Weitere Informationen finden Sie unter Amazon Athena.

Häufig gestellte Fragen: Athena in AMS

F: Wie beantrage ich Zugriff auf Amazon Athena in meinem AMS-Konto?

Beantragen Sie Zugriff auf Athena, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_athena_console_role` Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Athena in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von Amazon Athena ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon Athena in meinem AMS-Konto?

Athena ist stark vom AWS Glue Dienst abhängig, da er die mit catalog/metastore AWS Glue erstellten Daten verwendet. Daher sind AWS Glue Berechtigungen im erfolgreichen Athena RFC enthalten.

Die Rolle `customer_athena_console_role` ist Voraussetzung für einen Amazon S3 S3-Bucket. Verwenden Sie das automatisierte CT `ct-1a68ck03fn98r` (Deployment | Advanced Stack Components | S3 storage | Create), um einen neuen Bucket zu erstellen. Wenn Sie dieses automatisierte CT verwenden, um einen S3-Bucket für Athena zu erstellen, muss der Bucket-Name mit einem Präfix `athena-query-results-*` beginnen.

Verwenden Sie AMS SSP, um Amazon Bedrock in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Bedrock zuzugreifen. Amazon Bedrock ist ein vollständig verwalteter Service, der leistungsstarke Basismodelle (FMs) von führenden KI-Startups bereitstellt und AWS Ihnen über eine einheitliche API zur Verfügung stellt. Sie können aus einer Vielzahl von Basismodellen wählen, um das Modell zu finden, das für Ihren Anwendungsfall am besten geeignet ist. Amazon Bedrock bietet außerdem eine breite Palette von Funktionen zur Entwicklung generativer KI-Anwendungen mit Sicherheits- und Datenschutzfunktionen und

verantwortungsvoller KI. Mit Amazon Bedrock können Sie auf einfache Weise mit den wichtigsten Basismodellen für Ihre Anwendungsfälle experimentieren und diese evaluieren, sie mithilfe von Techniken wie Feinabstimmung und Retrieval Augmented Generation (RAG) privat an Ihre Daten anpassen und Agenten erstellen, die Aufgaben mithilfe Ihrer Unternehmenssysteme und Datenquellen ausführen.

Mit der serverlosen Erfahrung von Amazon Bedrock können Sie schnell loslegen, Foundation-Modelle privat mit Ihren eigenen Daten anpassen und sie mithilfe von AWS-Tools einfach und sicher in Ihre Anwendungen integrieren und bereitstellen, ohne eine Infrastruktur verwalten zu müssen. Weitere Informationen finden Sie unter Amazon Bedrock.

Häufig gestellte Fragen: Amazon Bedrock in AMS

F: Wie beantrage ich Zugriff auf Amazon Bedrock in meinem AMS-Konto?

Um Zugriff auf Amazon Bedrock zu beantragen, reichen Sie einen RFC mit dem Änderungstyp Management | AWS Service | Self-Provisioned Service | Add (review erforderlich) (ct-3qe6io8t6jtny) ein. Dieser RFC stellt `customer_bedrock_console_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Bedrock in meinem AMS-Konto?

- Amazon Bedrock Knowledge Bases werden standardmäßig nicht als Teil der SSPS-Rolle unterstützt, da sie von Amazon OpenSearch Service Serverless abhängig sind, das derzeit nicht von AMS unterstützt wird.
- Bedrock Studio wird nicht unterstützt, da es von nicht unterstützten Diensten wie Amazon abhängig ist. DataZone

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon Bedrock in meinem AMS-Konto?

- Modellabonnements von Drittanbietern, für die AWS Marketplace Berechtigungen erforderlich sind, müssen über die Standardrolle (`AWSManagedServicesAdminRole`auf MALZ und `Customer_ReadOnly_Role` auf SALZ) ausgeführt werden. Das liegt daran, dass die Standardrolle AWS Marketplace Berechtigungen beinhaltet.
- Wenn Datenverschlüsselung verwendet wird, müssen Sie den AWS KMS Schlüssel-ARN angeben, wenn Sie die Erstellung der Konsolenrolle anfordern. Außerdem muss der Amazon S3 S3-Bucket „Bedrock“ im Namen haben.

Verwenden Sie AMS SSP, um Amazon CloudSearch in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf CloudSearch Amazon-Funktionen zuzugreifen. Amazon CloudSearch ist ein verwalteter Service in der AWS Cloud, mit dem Sie kostengünstig eine Suchlösung für Ihre Website oder Anwendung einrichten, verwalten und skalieren können. Amazon CloudSearch unterstützt 34 Sprachen und beliebte Suchfunktionen wie Hervorhebung, automatische Vervollständigung und Geodatensuche. Weitere Informationen finden Sie auf Amazon CloudSearch.

> **Note**
>
> AWS hat mit Wirkung zum 25. Juli 2024 den Zugang für Neukunden zu Amazon CloudSearch geschlossen. CloudSearch Amazon-Bestandskunden können den Service weiterhin wie gewohnt nutzen. AWS investiert weiterhin in Sicherheits-, Verfügbarkeits- und Leistungsverbesserungen für Amazon CloudSearch, aber wir planen nicht, neue Funktionen einzuführen.
> Um mehr über die Unterschiede zwischen Amazon CloudSearch und Amazon OpenSearch Service zu erfahren und zu erfahren, wie Sie zu OpenSearch Service wechseln können, wenden Sie sich an Ihren Cloud-Architekten (CA). Weitere Informationen zur Umstellung auf OpenSearch Service finden Sie unter Übergang von Amazon CloudSearch zu Amazon OpenSearch Service.

Häufig gestellte Fragen zu Amazon CloudSearch in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon CloudSearch in meinem AMS-Konto?

Beantragen Sie Zugriff auf Amazon, CloudSearch indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_csearch_admin_role` Konto `customer_csearch_dev_role` die folgenden IAM-Rollen zur Verfügung: und. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon CloudSearch in meinem AMS-Konto?

Die volle Funktionalität von Amazon CloudSearch ist in Ihrem AMS-Konto verfügbar. Alle von AMS unterstützten Datenbanklösungen werden derzeit auf Amazon unterstützt. CloudSearch Beachten

Sie, dass DynamoDB derzeit die einzige verwaltete AWS Datenbanklösung ist, die nicht indexiert werden kann.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon CloudSearch in meinem AMS-Konto?

Amazon ist CloudSearch darauf angewiesen, dass Amazon S3 mit Identitätsanbietern zusammenarbeitet, um Eingabedaten automatisch zu analysieren und die Tabellenfelder zu bestimmen. Der Zugriff auf Amazon S3 ist in diesem RFC nicht enthalten und muss separat in einer Serviceanfrage angefordert werden.

Verwenden Sie AMS SSP, um Amazon CloudWatch Synthetics in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon CloudWatch Synthetics zuzugreifen. Sie können Amazon CloudWatch Synthetics verwenden, um „Kanarien“ zur Überwachung Ihrer Endgeräte zu erstellen und. APIs

Canaries sind konfigurierbare Skripte, die in Node.js oder Python geschrieben sind und nach einem Zeitplan ausgeführt werden. Sie legen Lambda-Funktionen in Ihrem Konto an, die Node.js oder Python als Framework verwenden. Canarys arbeiten über HTTP- und HTTPS-Protokolle. Canaries überprüfen die Verfügbarkeit und Latenz Ihrer Endgeräte und können Ladezeitdaten und UI-Screenshots speichern. Sie überwachen Ihre REST APIs - und Website-Inhalte und können nach unbefugten Änderungen durch Phishing, Code-Injection und Cross-Site-Scripting suchen. URLs

Canaries verfolgen dieselben Wege und führen dieselben Aktionen aus wie ein Kunde, sodass Sie Ihr Kundenerlebnis kontinuierlich überprüfen können, auch wenn Sie keinen Kundenverkehr mit Ihren Anwendungen haben. Durch den Einsatz von Canarys können Sie Probleme entdecken, bevor Ihre Kunden sie entdecken. Weitere Informationen finden Sie unter Amazon CloudWatch: Synthetisches Monitoring verwenden.

Häufig gestellte Fragen zu Amazon CloudWatch Synthetics in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon CloudWatch Synthetics in meinem AMS-Konto?

Fordern Sie Zugriff auf Amazon CloudWatch Synthetics an, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto die folgende IAM-Rolle zur Verfügung:

„customer_cw_synthetics_console_role“ und „customer_cw_synthetics_canary_lambda_role“. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle „customer_cw_synthetics_console_role“ in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon CloudWatch Synthetics in meinem AMS-Konto?

Es gibt keine Einschränkungen für die Verwendung von Amazon CloudWatch Synthetics in Ihrem AMS-Konto. Das Erstellen von Rollen für Canaries außerhalb der von AMS bereitgestellten Servicerolle 'customer_cw_synthetics_canary_lambda_role' ist verboten.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon CloudWatch Synthetics in meinem AMS-Konto?

Die Kanaren erstellen und verwenden einen standardmäßigen Amazon CloudWatch Synthetics S3-Bucket: "cw-syn-results- -*${accountnumber}*“ *${default-region}*

Verwenden Sie AMS SSP, um Amazon Cognito Cognito-Benutzerpools in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Cognito Cognito-Benutzerpools zuzugreifen. Amazon Cognito Cognito-Benutzerpools bieten ein sicheres Benutzerverzeichnis, das auf Hunderte von Millionen von Benutzern skaliert werden kann. Als vollständig verwalteter Service können Amazon Cognito Cognito-Benutzerpools eingerichtet werden, ohne sich Gedanken über die Einrichtung der Serverinfrastruktur machen zu müssen. Mit diesem Service können Sie einen Pool von Endbenutzern verwalten, den Sie für die Integration in Ihre internen Anwendungen verwenden können. Dieser Service bietet Ihnen eine Alternative zu einer benutzerdefinierten Datenbank oder einem Verzeichnis von Endbenutzern für Web- oder Mobilanwendungen. Gleichzeitig bieten Amazon Cognito Cognito-Benutzerpools den vollen Funktionsumfang eines Verzeichnisdienstes wie Kennwortrichtlinien, Multi-Faktor-Authentifizierung, Kennwortwiederherstellung und Selbstanmeldung bei Diensten. Es ermöglicht der Anwendung auch, den Zugriff in anderen beliebten öffentlichen Diensten wie OpenID, Facebook, Amazon oder Google zu bündeln.

Amazon Cognito ist in zwei Hauptprodukte unterteilt. Amazon Cognito-Benutzerpools und Amazon Cognito Identity Provider. Dieser Abschnitt konzentriert sich auf Amazon Cognito Cognito-Benutzerpools, die Zugriff auf andere AWS Dienste wie Amazon S3 oder DynamoDB bieten. Mit diesem Service können Sie Amazon Cognito Cognito-Benutzerpools oder einen externen

Identitätsanbieter verwenden, um Zugriff auf AWS Dienste zu gewähren. Er ermöglicht auch den Zugriff auf AWS Dienste mithilfe eines anonymen Gastzugriffs. Aufgrund der Leistungsfähigkeit von Amazon Cognito Cognito-Benutzerpools würden sie manuell als Service case-by-case für Betriebsanleitungen verwaltet werden, um mögliche Sicherheitslücken im Konto zu vermeiden. Weitere Informationen finden Sie unter Amazon Cognito User Pools.

Häufig gestellte Fragen zu Amazon Cognito Cognito-Benutzerpools in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon Cognito Cognito-Benutzerpools in meinem AMS-Konto?

Die Implementierung von Amazon Cognito Cognito-Benutzerpools in AMS erfolgt in zwei Schritten:

1. Reichen Sie den Änderungstyp Management | Other | Other | Create (ct-1e1xtak34nx76) ein und fordern Sie die Erstellung der Amazon Cognito Cognito-Benutzerpools in Ihrem AMS-Konto an. Schließen Sie die folgenden Informationen ein:
   - AWS Region.
   - Name für den Cognito-Benutzerpool.
   - Wenn Sie anstelle des standardmäßigen internen Cognito-Mail-Service den Amazon Simple Email Service (Amazon SES) zum Senden von Nachrichten und Benachrichtigungen verwenden möchten, sollte der Kunde im Konto eine bereits validierte E-Mail-Adresse für den Amazon SES-Service angeben. Diese Adresse wird für die Felder „Von“ und „ANTWORT-TO“ der Nachricht verwendet. Sie müssen auch die Region angeben, in der Amazon SES aktiviert wurde (us-east-1, eu-west-1 oder us-west-2).
   - Wenn Sie SMS-Nachrichten für Einmalpasswörter und zur Bestätigung verwenden möchten, sollte der Kunde dies angeben.
2. Fordern Sie den Benutzerzugriff an, indem Sie Folgendes einreichen: Verwaltung | AWS Service | Selbst bereitgestellter Service | Änderungstyp hinzufügen (ct-1w8z66n899dct). Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen zur Verfügung: und. `customer_cognito_admin_role` `customer_cognito_importjob_role` Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren. Mit diesen Rollen können Sie die Amazon Cognito Cognito-Benutzerpools verwalten, Ihre Benutzer und Gruppen im Pool verwalten, Importjobs für Benutzer erstellen, die Benachrichtigungen und Abonnementnachrichten ändern, Anwendungen dem Benutzerpool zuordnen, das Hinzufügen von Verbunddiensten zum Pool selbst verwalten und bereits erstellte Pools löschen.

F: Was sind die Einschränkungen bei der Verwendung von Amazon Cognito Cognito-Benutzerpools in meinem AMS-Konto?

Sie können die Amazon Cognito Cognito-Benutzerpools nicht erstellen. Diese Aktion erfordert die Erstellung von IAM-Rollen, um die von Amazon Cognito verwendeten Dienste wie Amazon SES und Amazon Simple Notification Service (Amazon SNS) nutzen zu können.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Cognito Cognito-Benutzerpools in meinem AMS-Konto?

Wenn Sie Amazon SES verwenden möchten, um Nachrichten und Benachrichtigungen per E-Mail an Ihre Benutzerpools zu senden, sollten diese den Amazon SES SES-Service bereits im Konto aktivieren und die E-Mail-Adresse, die in den Feldern „FROM“ und „REPLY-TO“ der gesendeten E-Mails verwendet werden soll, bereits validieren. Weitere Informationen zur Validierung von E-Mail-Adressen mit Amazon SES finden Sie unter Verifizieren von E-Mail-Adressen in Amazon SES.

Verwenden Sie AMS SSP, um Amazon Comprehend in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Comprehend zuzugreifen. Amazon Comprehend ist ein Service zur Verarbeitung natürlicher Sprache (NLP), der maschinelles Lernen nutzt, um Erkenntnisse und Zusammenhänge im Text zu finden. Es sind keine Erfahrungen mit maschinellem Lernen erforderlich. Amazon Comprehend verwendet maschinelles Lernen, um Ihnen zu helfen, die Erkenntnisse und Zusammenhänge in Ihren unstrukturierten Daten aufzudecken. Der Service identifiziert die Sprache des Textes, extrahiert wichtige Phrasen, Orte, Personen, Marken oder Ereignisse, versteht, wie positiv oder negativ der Text ist, analysiert Text mithilfe von Tokenisierung und Wortarten und organisiert automatisch eine Sammlung von Textdateien nach Themen. Sie können auch die AutoML-Funktionen in Amazon Comprehend verwenden, um einen benutzerdefinierten Satz von Entitäten oder Textklassifizierungsmodellen zu erstellen, die speziell auf die Bedürfnisse Ihres Unternehmens zugeschnitten sind. Weitere Informationen finden Sie unter Amazon Comprehend.

Häufig gestellte Fragen zu Amazon Comprehend in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon Comprehend in meinem AMS-Konto?

Die Konsolen- und Datenzugriffsrollen von Amazon Comprehend können durch Einreichung von zwei AMS-Services angefordert werden: RFCs

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Management | AWS Service | Self-Provisioned Service | Add (Überprüfung erforderlich) (ct-3qe6io8t6jtny) angeben. Dieser RFC stellt Ihrem `customer_comprehend_console_role` Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Comprehend in meinem AMS-Konto?

Die Funktion „Neue IAM-Rolle erstellen“ über die Amazon Comprehend Comprehend-Konsole ist eingeschränkt. Andernfalls ist der volle Funktionsumfang von Amazon Comprehend in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Comprehend in meinem AMS-Konto?

Amazon S3 und AWS Key Management Service (AWS KMS) sind für die Verwendung von Amazon Comprehend erforderlich, wenn Amazon S3 S3-Buckets mit Schlüsseln verschlüsselt sind. AWS KMS

Verwenden Sie AMS SSP, um Amazon Connect in Ihrem AMS-Konto bereitzustellen

> **Note**
>
> Nach reiflicher Überlegung haben wir beschlossen, den Support für Amazon Connect Voice ID mit Wirkung zum 20. Mai 2026 einzustellen. Amazon Connect Voice ID akzeptiert ab dem 20. Mai 2025 keine Neukunden mehr. Als Bestandskunde mit einem Konto, das vor dem 20. Mai 2025 für den Service registriert wurde, können Sie die Amazon Connect Voice ID-Funktionen weiterhin nutzen. Nach dem 20. Mai 2026 können Sie Amazon Connect Voice ID nicht mehr verwenden.

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf Amazon Connect Connect-Funktionen zuzugreifen. Amazon Connect ist ein Omnichannel-Cloud-Kontaktzentrum, das Unternehmen dabei unterstützt, erstklassigen Kundenservice zu geringeren Kosten anzubieten. Amazon Connect bietet Kunden und Mitarbeitern ein nahtloses Sprach- und Chat-Erlebnis. Dazu gehören eine Reihe von Tools für kompetenzbasiertes Routing, leistungsstarke Echtzeit- und Verlaufsanalysen sowie easy-to-use intuitive Verwaltungstools — alles mit pay-as-you-go Preisgestaltung.

Sie können eine oder mehrere Instanzen der virtuellen Contact Center-Instanzen entweder in AMS-Landingzone-Konten mit mehreren Konten oder Landingzone-Konten mit nur einem Konto erstellen. Sie können bestehende SAML 2.0-Identitätsanbieter für den Agentenzugriff verwenden oder die native Unterstützung von Amazon Connect für das Benutzerlebenszyklusmanagement verwenden.

Darüber hinaus können Sie von der Amazon free/direct Connect-Konsole aus gebührenpflichtige Telefonnummern für jede Amazon Connect Connect-Instanz anfordern. Mithilfe einer easy-to-use grafischen Benutzeroberfläche können Sie umfangreiche Kontaktabläufe erstellen, um das gewünschte Kundenerlebnis und die gewünschte Weiterleitung zu erreichen. Die Kontaktflüsse können AWS Lambda Funktionen zur Integration in lokale Datenspeicher und APIs nutzen. Sie können Datenstreaming auch mit Kinesis Streams und Firehose aktivieren.

Die Anrufaufzeichnungen, Chat-Transkripte und Berichte werden in einem Amazon S3 S3-Bucket gespeichert, der mit einem AWS KMS Schlüssel verschlüsselt ist. Die Kontaktflussprotokolle können in CloudWatch Protokollgruppen gespeichert werden.

Weitere Informationen finden Sie unter Amazon Connect.

Häufig gestellte Fragen zu Amazon Connect in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon Connect in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) angeben. Dieser RFC stellt Ihrem `customer_connect_console_role` Konto `customer_connect_user_role` die folgenden IAM-Rollen zur Verfügung: und. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Nutzung von Amazon Connect in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von Amazon Connect ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon Connect in meinem AMS-Konto?

- Sie müssen einen AWS KMS Schlüssel und einen Amazon S3 S3-Bucket mit Standard-AMS RFCs erstellen. Der Amazon S3 S3-Bucket ist zum Speichern von Anrufaufzeichnungen und Chat-Transkripten erforderlich.
- Wenn Sie eine Integration mit Active Directory (AD) durchführen möchten, ist ein AD Connector für die Integration zwischen AMS-gehosteten Amazon Connect Connect-Instances und Ihren lokalen

Verzeichnisdiensten erforderlich. AD Connector kann in Ihrem Konto konfiguriert werden, indem Sie einen RFC „Management | Other | Other“ anfordern.

- Sie können die folgenden optionalen, selbst bereitgestellten Dienste auf der Grundlage Ihrer Anforderungen an den Kontaktablauf aktivieren.
  - AWS Lambda: Sie können Lambda-Funktionen verwenden, um die Kontaktflüsse zu erweitern, um vorhandene lokale Datenspeicher zu nutzen oder. APIs Sie können den selbst bereitgestellten Lambda-Dienst verwenden, um die Lambda-Funktionen zu erstellen.
  - Amazon Kinesis Data Streams: Sie können Datenstreams erstellen, um Datenstreaming zu externen Anwendungen zu ermöglichen. Sie können Kontaktnachverfolgungsdatensätze oder Agentenereignisse streamen.
  - Amazon Kinesis Data Firehose: Sie können Data Firehose erstellen, um umfangreiche Kontaktverfolgungsdatensätze an externe Anwendungen zu streamen.
  - Amazon Lex: Sie können Amazon Lex Chatbots nutzen, um intelligente Kontaktabläufe zu erstellen und dabei die Amazon Alexa-Services für ein umfassendes Kundenerlebnis und Automatisierung zu nutzen.
- F: Wie beantrage ich das Hinzufügen einer Länderliste für ausgehende oder eingehende Anrufe?

  Um eine Länderliste für ausgehende oder eingehende Anrufe hinzuzufügen, reichen Sie eine Serviceanfrage an AMS ein.

Verwenden Sie AMS SSP, um Amazon Data Firehose in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Data Firehose zuzugreifen. Firehose ist der einfachste Weg, Streaming-Daten zuverlässig in Data Lakes, Datenspeicher und Analysetools zu laden. Es kann Streaming-Daten erfassen, transformieren und in Amazon S3, Amazon Redshift, Amazon OpenSearch Service und Splunk laden und ermöglicht so Analysen nahezu in Echtzeit mit vorhandenen Business Intelligence-Tools und Dashboards, die Sie bereits heute verwenden. Es handelt sich um einen vollständig verwalteten Service, der sich automatisch an den Durchsatz Ihrer Daten anpasst und für den keine laufende Verwaltung erforderlich ist. Außerdem können die Daten vor dem Laden gebündelt, komprimiert, transformiert und verschlüsselt werden, wodurch der Speicherverbrauch am Zielort minimiert und die Sicherheit erhöht wird. Weitere Informationen finden Sie unter Was ist Amazon Data Firehose?

Häufig gestellte Fragen zu Firehose in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon Data Firehose in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) angeben. Dieser RFC stellt Ihrem `customer_kinesis_firehose_user_role` Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Firehose in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von Amazon Data Firehose ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Firehose in meinem AMS-Konto?

Für jeden Delivery-Stream müssen neue serviceverknüpfte IAM-Rollen angefordert werden. Sie können auch eine einzelne dienstverknüpfte Rolle für alle Streams wiederverwenden, indem Sie die Rollenrichtlinie mit den erforderlichen Ressourcenberechtigungen aktualisieren (einschließlich S3-Buckets/KMS-Schlüsseln/Lambda-Funktionen/Kinesis-Streams).

Nachdem Sie den RFC zum Hinzufügen von Firehose eingereicht haben, wird sich ein AMS Operations Engineer mit einer Serviceanfrage für die Ressourcen, die ARNs Sie mit Data Firehose verbinden möchten (z. B. S3, Lambda und Kinesis Streams) AWS KMS, mit Ihnen in Verbindung setzen.

Verwenden Sie AMS SSP, um Amazon DevOps Guru in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon DevOps Guru zuzugreifen. Amazon DevOps Guru ist ein vollständig verwalteter Betriebsservice, der es Entwicklern und Betreibern leicht macht, die Leistung und Verfügbarkeit ihrer Anwendungen zu verbessern. DevOpsMit Guru können Sie die mit der Identifizierung betrieblicher Probleme verbundenen administrativen Aufgaben auslagern, sodass Sie schnell Empfehlungen zur Verbesserung Ihrer Anwendung umsetzen können. DevOpsGuru

liefert reaktive Erkenntnisse, die Sie nutzen können, um Ihre Anwendung jetzt zu verbessern. Es bietet auch proaktive Einblicke, mit denen Sie betriebliche Probleme vermeiden können, die sich in future auf Ihre Anwendung auswirken könnten. DevOpsGuru nutzt maschinelles Lernen, um Ihre Betriebsdaten sowie Anwendungsmetriken und Ereignisse zu analysieren und Verhaltensweisen zu identifizieren, die von normalen Betriebsmustern abweichen. Sie werden benachrichtigt, wenn DevOps Guru ein betriebliches Problem oder Risiko feststellt. Für jedes Problem präsentiert DevOps Guru intelligente Empfehlungen zur Lösung aktueller und prognostizierter future betrieblicher Probleme.

Weitere Informationen finden Sie unter Was ist Amazon DevOps Guru.

Häufig gestellte Fragen zu Amazon DevOps Guru in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon DevOps Guru in meinem AMS-Konto?

Um Zugriff zu beantragen, reichen Sie den Änderungstyp Verwaltung | AWS Service | Selbstbereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) ein. Dieser RFC stellt Ihrem Konto die folgende IAM-Rolle zur `customer_devopsguru_role` Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon DevOps Guru in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von Amazon DevOps Guru ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon DevOps Guru in meinem AMS-Konto?

Es gibt keine Voraussetzungen. DevOpsGuru nutzt die folgenden AWS Dienste: Amazon CloudWatch Logs, RDS Insights, AWS X-Ray AWS Lambda, und AWS CloudTrail.

Verwenden Sie AMS SSP, um Amazon DocumentDB (mit MongoDB-Kompatibilität) in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf Funktionen von Amazon DocumentDB (mit MongoDB-Kompatibilität) zuzugreifen. Amazon DocumentDB (mit MongoDB-Kompatibilität) ist ein schneller, skalierbarer, hochverfügbarer und vollständig verwalteter Dokumentendatenbankservice, der MongoDB-Workloads

unterstützt. Amazon DocumentDB bietet Ihnen die Leistung, Skalierbarkeit und Verfügbarkeit, die Sie für den skalierbaren Betrieb geschäftskritischer MongoDB-Workloads benötigen. Amazon DocumentDB implementiert die Apache 2.0-Open-Source-API MongoDB 3.6, indem es die Antworten emuliert, die ein MongoDB-Client von einem MongoDB-Server erwartet, sodass Sie Ihre vorhandenen MongoDB-Treiber und -Tools mit Amazon DocumentDB verwenden können. In Amazon DocumentDB sind Speicher und Datenverarbeitung entkoppelt, sodass beide unabhängig voneinander skaliert werden können. Sie können die Lesekapazität auf Millionen von Anfragen pro Sekunde erhöhen, indem Sie bis zu 15 Read Replicas mit niedriger Latenz hinzufügen, unabhängig von der Größe Ihrer Daten. Amazon DocumentDB ist für eine Verfügbarkeit von 99,99% konzipiert und repliziert sechs Kopien Ihrer Daten in drei AWS Availability Zones (). AZs Sie können AWS Database Migration Service (DMS) kostenlos (für sechs Monate) verwenden, um Ihre lokalen oder Amazon Elastic Compute Cloud (Amazon EC2) MongoDB-Datenbanken praktisch ohne Ausfallzeiten zu Amazon DocumentDB zu migrieren. Weitere Informationen finden Sie unter Amazon DocumentDB (mit MongoDB-Kompatibilität).

Häufig gestellte Fragen zu Amazon DocumentDB in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon DocumentDB in meinem AMS-Konto?

Amazon DocumentDB DocumentDB-Konsolen- und Datenzugriffsrollen können durch die Einreichung von zwei AMS RFCs, Konsolenzugriff und Datenzugriff, beantragt werden:

Fordern Sie Zugriff auf Amazon DocumentDB an, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_documentdb_role` Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon DocumentDB in meinem AMS-Konto?

Amazon DocumentDB erfordert Amazon RDS-spezifische Berechtigungen. Da AMS Amazon RDS vollständig verwaltet, beinhaltet die IAM-Rolle für Amazon DocumentDB einige Einschränkungen für Aktionen auf Amazon RDS. Beachten Sie die folgenden Einschränkungen:

- Der Zugriff auf `DeleteDBInstance` und wurde `DeleteDBCluster` APIs eingeschränkt. Um diese Löschungen zu verwenden APIs, reichen Sie einen RFC mit dem Änderungstyp Management | Advanced Stack Components | Identity and Access Management (IAM) | Entität oder Richtlinie aktualisieren (Überprüfung erforderlich) ein (ct-27tuth19k52b4).

- Sie können keine Tags zu Amazon RDS-Instances hinzufügen oder daraus entfernen.
- Sie können Ihre Amazon DocumentDB DocumentDB-Instance nicht öffentlich machen.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon DocumentDB in meinem AMS-Konto?

Amazon S3 und AWS KMS sind für die Verwendung von Amazon DocumentDB erforderlich, wenn Amazon S3 S3-Buckets mit AWS KMS Schlüsseln verschlüsselt sind.

Verwenden Sie AMS SSP, um Amazon DynamoDB in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon DynamoDB (DynamoDB) zuzugreifen. Amazon DynamoDB ist eine Schlüsselwert- und Dokumentendatenbank, die in jeder Größenordnung eine Leistung im einstelligen Millisekundenbereich bietet. Es handelt sich um eine vollständig verwaltete, multiaktive Datenbank mit mehreren Regionen und integrierter Sicherheit, Sicherung und Wiederherstellung sowie In-Memory-Caching für Anwendungen im Internet. Weitere Informationen hierzu finden Sie unter Amazon DynamoDB.

Amazon DynamoDB Accelerator (DAX) ist ein Write-Through-Cache-Service, der das Hinzufügen eines Caches zu DynamoDB-Tabellen vereinfachen soll. DAX ist für Anwendungen konzipiert, die Lesevorgänge mit hoher Leistung erfordern.

Häufig gestellte Fragen zu DynamoDB in AWS Managed Services

F: Wie beantrage ich Zugriff auf DynamoDB und DAX in meinem AMS-Konto?

Fordern Sie Zugriff auf DynamoDB und DAX an, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen und -Richtlinien zur Verfügung:

- DynamoDB-Rollenname: `customer_dynamodb_role`

  Name der DAX-Dienstrolle: `customer_dax_service_role`
- Name der DynamoDB-Richtlinie: `customer_dynamodb_policy`

  DAX-Dienstrichtlinie: `customer_dax_service_policy`

Nach der Bereitstellung in Ihrem Konto müssen Sie die Lösung `customer_dynamodb_role` in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Verwendung von DynamoDB in meinem AMS-Konto?

Alle DynamoDB-Funktionen werden unterstützt, einschließlich DynamoDB Accelerator (DAX).

Beim Erstellen von Alarmen für eine bestimmte Tabelle muss dem Alarmnamen das Präfix „customer*“ vorangestellt werden, zum Beispiel. `customer-employee-table-high-put-latency`

Wenn Sie ein Amazon SNS SNS-Thema für DynamoDB erstellen, muss es den Namen haben:. `dynamodb`

Um das von DynamoDB erstellte Amazon SNS SNS-Thema zu löschen, reichen Sie einen RFC vom Änderungstyp Management | Other | Other | Update ein.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von DynamoDB in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Verwendung von DynamoDB in Ihrem AMS-Konto.

Verwenden Sie AMS SSP, um Amazon Elastic Container Registry in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Elastic Container Registry (Amazon ECR) zuzugreifen. Amazon Elastic Container Registry ist eine vollständig verwaltete Docker-Container-Registry, die Entwicklern das Speichern, Verwalten und Bereitstellen von Docker-Container-Images erleichtert. Amazon ECR ist in Amazon Elastic Container Service (Amazon ECS) integriert und vereinfacht so Ihren Arbeitsablauf von der Entwicklung bis zur Produktion. Mit Amazon ECR müssen Sie keine eigenen Container-Repositorys betreiben oder sich Gedanken über die Skalierung der zugrunde liegenden Infrastruktur machen. Amazon ECS hostet Ihre Images in einer hochverfügbaren und skalierbaren Architektur, sodass Sie Container für Ihre Anwendungen zuverlässig bereitstellen können. Die Integration mit AWS Identity and Access Management (IAM) ermöglicht die Kontrolle jedes Repositorys auf Ressourcenebene. Bei Amazon ECR fallen keine Vorabgebühren oder Verpflichtungen an. Sie zahlen nur für die Datenmenge, die Sie in Ihren Repositorys speichern, und für die Datenmenge, die ins Internet übertragen wird.

Weitere Informationen finden Sie unter Amazon Elastic Container Registry.

Häufig gestellte Fragen zu Amazon Elastic Container Registry in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon ECR in meinem AMS-Konto?

Fordern Sie Zugriff auf Amazon ECR an, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen zur Verfügung:, und mit den zugehörigen IAM-Richtlinien bzw. `customer_ecr_console_role` `customer_ecr_poweruser_instance_profile` `customer_ecr_console_policy` `customer_ecr_poweruser_instance_profile_policy` Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon ECR in meinem AMS-Konto?

Es gibt Einschränkungen in Bezug auf AMS-Namespaces für die Verwendung von Amazon ECR in Ihrem AMS-Konto. Container-Images dürfen nicht das Präfix „AMS-“ oder „Sentinel-“ haben.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon ECR in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten, um Amazon ECR in Ihrem AMS-Konto zu verwenden.

Verwenden Sie AMS SSP, um EC2 Image Builder in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf EC2 Image Builder Builder-Funktionen zuzugreifen. EC2 Image Builder ist ein vollständig verwalteter AWS Service, der es einfacher macht, die Erstellung, Verwaltung und Bereitstellung von benutzerdefinierten, sicheren und up-to-date „goldenen“ Server-Images zu automatisieren, die vorinstalliert und mit Software und Einstellungen vorkonfiguriert sind, um bestimmte IT-Standards zu erfüllen.

Sie können die AWS Management Console AWS CLI oder verwenden, APIs um benutzerdefinierte Images in Ihrem AWS Konto zu erstellen. Wenn Sie den verwenden AWS Management Console, führt Sie der Amazon EC2 Image Builder Builder-Assistent durch die folgenden Schritte:

- Stellen Sie Startartefakte bereit

- Software hinzufügen und entfernen
- Passen Sie Einstellungen und Skripts an
- Führen Sie ausgewählte Tests aus
- Verteilen Sie Bilder nach AWS Regionen

Die von Ihnen erstellten Images werden in Ihrem Konto erstellt und können fortlaufend für Betriebssystem-Patches konfiguriert werden. Weitere Informationen finden Sie unter EC2 Image Builder.

EC2 Häufig gestellte Fragen zu Image Builder in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf EC2 Image Builder in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Über diesen RFC wird die folgende IAM-Rolle in Ihrem Konto bereitgestellt:. `customer_ec2_imagebuilder_role` Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen für EC2 Image Builder?

AMS unterstützt die Verwendung von Service Defaults für die Infrastrukturkonfiguration nicht. Sie können eine neue Infrastrukturkonfiguration erstellen oder eine bestehende verwenden.

AMS unterstützt derzeit nicht die Erstellung von Container-Rezepten.

F: Was sind die Voraussetzungen oder Abhängigkeiten, um EC2 Image Builder zu aktivieren?

- EC2 Serviceverknüpfte Image Builder Builder-Rolle: Sie müssen eine dienstverknüpfte Rolle nicht manuell erstellen. Wenn Sie Ihre erste Image Builder-Ressource in der AWS Management Console, der AWS CLI oder der AWS API erstellen, erstellt Image Builder die serviceverknüpfte Rolle für Sie.
- Instanzen, die zum Erstellen von Images und zum Ausführen von Tests mit Image Builder verwendet werden, müssen Zugriff auf den Systems Manager Manager-Dienst haben. Der SSM-Agent wird auf dem Quell-Image installiert, sofern er noch nicht vorhanden ist, und er wird entfernt, bevor das Image erstellt wird.

- AWS IAM: Die IAM-Rolle, die Sie Ihrem Instanzprofil zuordnen, muss über Berechtigungen zum Ausführen der in Ihrem Image enthaltenen Build- und Testkomponenten verfügen. Die folgenden IAM-Rollenrichtlinien müssen der IAM-Rolle angehängt werden, die den Instanzprofilen zugeordnet ist: und. `EC2InstanceProfileForImageBuilder` `AmazonSSMManagedInstanceCore` Der Name der IAM-Rolle sollte das Schlüsselwort enthalten. `*imagebuilder*`
- Wenn Sie die Protokollierung konfigurieren, muss das in Ihrer Infrastrukturkonfiguration angegebene Instanzprofil über `s3:PutObject` Berechtigungen für den Ziel-Bucket (`arn:aws:s3:::{bucket-name}/*`) verfügen. Beispiel:

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::{bucket-name}/*"
        }
    ]
}
```

- Erstellen Sie ein SNS-Thema mit dem Namen „imagebuilder“, um alle Benachrichtigungen und Benachrichtigungen von EC2 Image Builder zu erhalten.

Verwenden Sie AMS SSP, um Amazon ECS AWS Fargate in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf AWS Fargate Funktionen von Amazon ECS zuzugreifen. AWS Fargate ist eine Technologie, die Sie mit Amazon ECS verwenden können, um Container auszuführen (siehe Container on AWS), ohne Server oder Cluster von EC2 Amazon-Instances verwalten zu müssen. Damit AWS Fargate müssen Sie keine Cluster von virtuellen Maschinen mehr bereitstellen, konfigurieren oder skalieren, um Container auszuführen. Auf diese Weise müssen keine Servertypen mehr ausgewählt werden, es muss nicht entschieden werden, wann die Cluster skaliert werden oder das Cluster-Packing optimiert werden.

Weitere Informationen finden Sie unter Amazon ECS auf AWS Fargate.

Häufig gestellte Fragen zu Amazon ECS on Fargate in AWS Managed Services

F: Wie beantrage ich in meinem AMS-Konto Zugriff auf Amazon ECS on Fargate?

Beantragen Sie Zugriff auf Amazon ECS auf Fargate, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen zur Verfügung: `customer_ecs_fargate_console_role` (falls keine vorhandene IAM-Rolle bereitgestellt wird, der die ECS-Richtlinie zugeordnet werden kann),,, und. `customer_ecs_fargate_events_service_role` `customer_ecs_task_execution_service_role` `customer_ecs_codedeploy_service_role` `AWSServiceRoleForApplicationAutoScaling_ECSService` Nach der Bereitstellung in Ihrem Konto müssen Sie die Rollen in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon ECS auf Fargate in meinem AMS-Konto?

- Die Überwachung und Protokollierung von Amazon ECS-Aufgaben liegt in Ihrer Verantwortung, da Aktivitäten auf Containerebene oberhalb des Hypervisors stattfinden und die Protokollierungsmöglichkeiten von Amazon ECS auf Fargate eingeschränkt sind. Als Benutzer von Amazon ECS auf Fargate empfehlen wir Ihnen, die notwendigen Schritte zu unternehmen, um die Protokollierung Ihrer Amazon ECS-Aufgaben zu aktivieren. Weitere Informationen finden Sie unter Aktivieren des awslogs-Protokolltreibers für Ihre Container.
- Für Sicherheit und Malware-Schutz auf Container-Ebene sind Sie ebenfalls verantwortlich. Amazon ECS on Fargate enthält weder Trend Micro noch vorkonfigurierte Netzwerksicherheitskomponenten.
- Dieser Service ist sowohl für Landingzone-Konten mit mehreren Konten als auch für AMS-Konten mit Einzelkonten verfügbar.
- Amazon ECS Service Discovery ist standardmäßig in der Rolle „Self-Provisioned“ eingeschränkt, da erhöhte Berechtigungen erforderlich sind, um private gehostete Route 53 53-Zonen zu erstellen. Um Service Discovery für einen Service zu aktivieren, reichen Sie den Änderungstyp Management | Other | Other | Update ein. Die Informationen, die zur Aktivierung von Service Discovery für Ihren Amazon ECS-Service erforderlich sind, finden Sie im Service Discovery-Handbuch.
- AMS verwaltet oder beschränkt derzeit keine Images, die für die Bereitstellung in Containern auf Amazon ECS Fargate verwendet werden. Sie können Images aus Amazon ECR, Docker Hub oder

einem anderen privaten Image-Repository bereitstellen. Aus diesem Grund haben wir empfohlen, öffentliche oder ungesicherte Images nicht bereitzustellen, da sie zu böswilligen Aktivitäten auf dem Konto führen können.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon ECS auf Fargate in meinem AMS-Konto?

- Im Folgenden sind Abhängigkeiten von Amazon ECS von Fargate aufgeführt. Es sind jedoch keine zusätzlichen Maßnahmen erforderlich, um diese Dienste mit Ihrer selbst bereitgestellten Rolle zu aktivieren:
  - CloudWatch Logs
  - CloudWatch Ereignisse
  - CloudWatch Alarme
  - CodeDeploy
  - App Mesh
  - Cloud Map
  - Route 53
- Abhängig von Ihrem Anwendungsfall stützt sich Amazon ECS auf die folgenden Ressourcen, die Sie möglicherweise benötigen, bevor Sie Amazon ECS on Fargate in Ihrem Konto verwenden können:
  - Sicherheitsgruppe, die mit dem Amazon ECS-Service verwendet werden soll. Sie können Deployment | Erweiterte Stack-Komponenten | Sicherheitsgruppe | Create (auto) (ct-3pc215bnwb6p7) verwenden oder, falls Ihre Sicherheitsgruppe spezielle Regeln erfordert, Deployment | Erweiterte Stack-Komponenten | Sicherheitsgruppe | Erstellen (Überprüfung erforderlich) verwenden (ct-1oxx2g2d7hc90). Hinweis: Die Sicherheitsgruppe, die Sie mit Amazon ECS auswählen, muss speziell für Amazon ECS erstellt werden, wo sich der Amazon ECS-Service oder -Cluster befindet. Weitere Informationen finden Sie im Abschnitt Sicherheitsgruppe unter Einrichtung mit Amazon ECS und Sicherheit in Amazon Elastic Container Service.
  - Application Load Balancer (ALB), Network Load Balancer (NLB), Classic Load Balancer (ELB) für den Lastenausgleich zwischen Aufgaben.
  - Zielgruppen für. ALBs
  - App-Mesh-Ressourcen (z. B. virtuelle Router, virtuelle Dienste, virtuelle Knoten) zur Integration in Ihren Amazon ECS-Cluster.

- Derzeit gibt es für AMS keine Möglichkeit, das Risiko, das mit der Unterstützung von Berechtigungen von Sicherheitsgruppen verbunden ist, automatisch zu minimieren, wenn diese außerhalb der standardmäßigen AMS-Änderungstypen erstellt werden. Wir empfehlen Ihnen, eine bestimmte Sicherheitsgruppe für die Verwendung mit Ihrem Fargate-Cluster anzufordern, um die Möglichkeit der Verwendung einer Sicherheitsgruppe einzuschränken, die nicht für die Verwendung mit Amazon ECS vorgesehen ist.

Verwenden Sie AMS SSP, um Amazon EKS AWS Fargate in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf AWS Fargate Funktionen von Amazon EKS zuzugreifen. AWS Fargate ist eine Technologie, die bedarfsgerecht dimensionierte Rechenkapazität für Container bereitstellt (Informationen zu Containern finden Sie unter Was sind Container?). Mit AWS Fargate müssen Sie keine Gruppen von virtuellen Maschinen mehr bereitstellen, konfigurieren oder skalieren, um Container auszuführen. Auf diese Weise müssen keine Servertypen mehr ausgewählt werden, es muss nicht entschieden werden, wann die Knotengruppen skaliert werden oder das Cluster-Packing optimiert werden.

Amazon Elastic Kubernetes Service (Amazon EKS) integriert Kubernetes mithilfe AWS Fargate von Controllern, die mithilfe des erweiterbaren AWS Upstream-Modells von Kubernetes erstellt wurden. Diese Controller werden als Teil der von Amazon EKS verwalteten Kubernetes-Steuerebene ausgeführt und sind für die Planung nativer Kubernetes-Pods auf Fargate verantwortlich. Die Fargate-Controller enthalten einen neuen Scheduler, der neben dem Standard-Kubernetes-Scheduler und zusätzlich zu mehreren mutierenden und validierenden Zugangscontrollern ausgeführt wird. Wenn Sie einen Pod starten, der die Kriterien für die Ausführung auf Fargate erfüllt, erkennen, aktualisieren und planen die im Cluster ausgeführten Fargate-Controller den Pod auf Fargate.

Weitere Informationen finden Sie unter Amazon EKS ab AWS Fargate sofort allgemein verfügbar und im Amazon EKS Best Practices Guide for Security (enthält „Empfehlungen“ wie „Unnötigen anonymen Zugriff überprüfen und widerrufen“ und mehr).

> **Tip**
>
> AMS hat einen Änderungstyp, Deployment | Advanced Stack Components | Identity and Access Management (IAM) | OpenID Connect-Anbieter erstellen (ct-30ecvfi3tq4k3), den

Sie mit Amazon EKS verwenden können. Ein Beispiel finden Sie unter Identity and Access Management (IAM) | OpenID Connect Provider erstellen.

Häufig gestellte Fragen zu Amazon EKS on AWS Fargate in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon EKS on Fargate in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) angeben. Dieser RFC stellt Ihrem Konto die folgende IAM-Rolle zur Verfügung.

- `customer_eks_fargate_console_role`.

  Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.
- Diese Servicerollen geben Amazon EKS on Fargate die Erlaubnis, andere AWS Dienste in Ihrem Namen anzurufen:
  - `customer_eks_pod_execution_role`
  - `customer_eks_cluster_service_role`

F: Welche Einschränkungen gelten für die Nutzung von Amazon EKS auf Fargate in meinem AMS-Konto?

- Das Erstellen von verwalteten oder EC2 selbstverwalteten Knotengruppen wird in AMS nicht unterstützt. Wenn Sie EC2 Worker Nodes verwenden möchten, wenden Sie sich an Ihren AMS Cloud Service Delivery Manager (CSDM) oder Cloud Architect (CA).
- AMS enthält keine Trend Micro- oder vorkonfigurierten Netzwerksicherheitskomponenten für Container-Images. Es wird von Ihnen erwartet, dass Sie vor der Verteilung Ihre eigenen Image-Suchdienste verwalten, um bösartige Container-Images zu erkennen.
- EKSCTL wird aufgrund von Interdependenzen nicht unterstützt. CloudFormation
- Während der Clustererstellung sind Sie berechtigt, die Protokollierung der Cluster-Steuerungsebene zu deaktivieren. Weitere Informationen finden Sie unter Amazon-EKS-Steuerebenen-Protokollierung. Wir empfehlen Ihnen, alle wichtigen API-, Authentifizierungs- und Audit-Logging bei der Clustererstellung zu aktivieren.
- Während der Cluster-Erstellung ist der Cluster-Endpunktzugriff für Amazon EKS-Cluster standardmäßig öffentlich. Weitere Informationen finden Sie unter Amazon EKS-Cluster-

Endpunktzugriffskontrolle. Wir empfehlen, Amazon EKS-Endpunkte auf privat zu setzen. Wenn Endgeräte für den öffentlichen Zugriff erforderlich sind, empfiehlt es sich, sie nur für bestimmte CIDR-Bereiche auf öffentlich zu setzen.

- AMS verfügt nicht über eine Methode, um Bilder, die für die Bereitstellung in Containern auf Amazon EKS Fargate verwendet werden, zu erzwingen oder einzuschränken. Sie können Images aus Amazon ECR, Docker Hub oder einem anderen privaten Image-Repository bereitstellen. Daher besteht das Risiko, dass ein öffentliches Image bereitgestellt wird, das böswillige Aktivitäten auf dem Konto ausführen könnte.
- Die Bereitstellung von EKS-Clustern über das Cloud Development Kit (CDK) oder CloudFormation Ingest wird in AMS nicht unterstützt.
- Sie müssen die erforderliche Sicherheitsgruppe mithilfe von ct-3pc215bnwb6p7 Deployment | Advanced Stack Components | Security Group | Create erstellen und in der Manifestdatei für die Erstellung von Ingresses referenzieren. Das liegt daran, dass die Rolle nicht autorisiert ist, Sicherheitsgruppen zu erstellen. `customer-eks-alb-ingress-controller-role`

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon EKS auf Fargate in meinem AMS-Konto?

Um den Service nutzen zu können, müssen die folgenden Abhängigkeiten konfiguriert werden:

- Für die Authentifizierung gegenüber dem Dienst aws-iam-authenticator müssen sowohl KUBECTL als auch installiert sein. Weitere Informationen finden Sie unter Clusterauthentifizierung verwalten.
- Kubernetes basiert auf einem Konzept, das als „Dienstkonten“ bezeichnet wird. Um die Funktionalität der Dienstkonten innerhalb eines Kubernetes-Clusters auf EKS nutzen zu können, ist ein RFC Management | Other | Other | Update mit den folgenden Eingaben erforderlich:
  - [Erforderlich] Name des Amazon EKS-Clusters
  - [Erforderlich] Amazon EKS-Cluster-Namespace, in dem das Servicekonto (SA) bereitgestellt wird.
  - [Erforderlich] Name der Amazon EKS-Cluster-SA.
  - [Erforderlich] Name der IAM-Richtlinie, der permissions/document zugeordnet werden muss.
  - [Erforderlich] Der Name der IAM-Rolle wird angefordert.
  - [Optional] OpenID Connect-Provider-URL. Weitere Informationen finden Sie unter
    - Aktivierung von IAM-Rollen für Dienstkonten auf Ihrem Cluster
    - Einführung detaillierter IAM-Rollen für Dienstkonten

- Wir empfehlen, dass Config-Regeln konfiguriert und überwacht werden
  - Öffentliche Cluster-Endpunkte
  - API-Protokollierung deaktiviert

  Es liegt in Ihrer Verantwortung, diese Konfigurationsregeln zu überwachen und zu korrigieren.

Wenn Sie einen ALB-Ingress-Controller bereitstellen möchten, reichen Sie einen RFC für das Update Management | Other | Other ein, um die erforderliche IAM-Rolle für die Verwendung mit dem ALB Ingress Controller-Pod bereitzustellen. Die folgenden Eingaben sind erforderlich, um IAM-Ressourcen zu erstellen, die dem ALB Ingress Controller zugeordnet werden sollen (schließen Sie diese in Ihren RFC ein):

- [Erforderlich] Name des Amazon EKS-Clusters
- [Optional] URL des OpenID Connect-Anbieters
- [Optional] Amazon EKS-Cluster-Namespace, in dem der Application Load Balancer (ALB) -Ingress Controller-Service bereitgestellt wird. [Standard: Kube-System]
- [Optional] Name des Amazon EKS-Cluster-Servicekontos (SA). [Standard: aws-load-balancer-controller]

Wenn Sie die Verschlüsselung von Envelope Secrets in Ihrem Cluster aktivieren möchten (was wir empfehlen), geben Sie den KMS-Schlüssel, den IDs Sie verwenden möchten, im Beschreibungsfeld des RFC an, um den Dienst hinzuzufügen (Management | Service | Self-provisioned AWS service | Add (ct-1w8z66n899dct)). Weitere Informationen zur Umschlagverschlüsselung finden Sie unter Amazon EKS fügt Umschlagverschlüsselung für geheime Daten mit AWS KMS hinzu.

Verwenden Sie AMS SSP, um Amazon EMR in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf Amazon EMR-Funktionen zuzugreifen. Amazon EMR ist die branchenführende Cloud-Big-Data-Plattform für die Verarbeitung riesiger Datenmengen mithilfe von Open-Source-Tools wie Apache Spark, Apache Hive, Apache, Apache Flink HBase, Apache Hudi und Presto. Mit Amazon EMR können Sie Analysen im Petabyte-Bereich zu weniger als der Hälfte der Kosten herkömmlicher On-Premises-Lösungen und mehr als dreimal schneller als Apache Spark-Standardlösungen durchführen. Für Aufträge mit kurzer Laufzeit können Sie Cluster hoch- und herunterfahren und pro Sekunde für die verwendeten Instances zahlen. Für Workloads mit langer

Laufzeit können Sie hochverfügbare Cluster erstellen, die automatisch skaliert werden, um der Nachfrage gerecht zu werden.

Sie können eine oder mehrere Instances der Amazon EMR-Cluster entweder in AMS-Landingzone-Konten mit mehreren Konten oder Landingzone-Konten mit einem Konto erstellen, um sowohl transiente als auch persistente Amazon EMR-Cluster zu unterstützen. Sie können auch die Kerberos-Authentifizierung aktivieren, um Benutzer aus einer lokalen Active Directory-Domäne zu authentifizieren.

Sie können mehrere Datenspeicher mit den Amazon EMR-Clustern nutzen, um anwendungsspezifische Hadoop-Tools und -Bibliotheken zu unterstützen. Die Amazon EMR-Cluster können mithilfe von OnDemand Spot-Instances erstellt und Autoscaling konfiguriert werden, um die Kapazität zu verwalten und die Kosten zu senken.

Die Cluster-Protokolldateien können zum Protokollieren und Debuggen in einem Amazon S3 S3-Bucket archiviert werden. Sie können auch auf die im Amazon EMR-Cluster gehosteten Weboberflächen zugreifen, um Hadoop-Administrationsanforderungen oder Notizbucherfahrungen für Kunden zu unterstützen.

Weitere Informationen finden Sie unter Amazon EMR.

Häufig gestellte Fragen zu Amazon EMR in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon EMR in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Self-Provisioned Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen zur Verfügung:

- `customer_emr_cluster_instance_profile`
- `customer_emr_cluster_autoscaling_role`
- `customer_emr_console_role`
- `customer_emr_cluster_service_role`

Nachdem es in Ihrem Konto bereitgestellt wurde, müssen Sie die customer_emr_console_role in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon EMR in meinem AMS-Konto?

Wir empfehlen Ihnen, bei der Erstellung von Amazon EMR auf einem EC2 Cluster von der AWS-Konsole aus die Option Create Cluster — Advanced zu verwenden. Amazon EMR-Cluster müssen erstellt werden, indem das Tag mit dem Schlüssel "for-use-with-amazon-emr-managed-policies" mit dem Wert „true“ hinzugefügt wird. Wählen Sie in den Sicherheitsoptionen die folgenden Konfigurationen aus:

- Wählen Sie benutzerdefinierte Rollen für Ihren Cluster aus:
  - EMR-Rolle: customer_emr_cluster_service_role
  - EC2 Instanzprofil: customer_emr_cluster_instance_profile
  - Auto Scaling Scaling-Rolle: customer_emr_cluster_autoscaling_role
- EC2 Sicherheitsgruppen:
  - Master: ams-emr-master-security -Gruppe
  - Kern und Aufgabe: -Gruppe ams-emr-worker-security
  - Servicezugriff: -group ams-emr-serviceaccess-security

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon EMR in meinem AMS-Konto?

AMS erstellt Standardsicherheitsgruppen für die Master-, Worker- und Services-Knoten von Amazon EMR.

Die Startvorlagen und Sicherheitsgruppen, die mit Amazon EMR-Clustern verwendet werden sollen, müssen den Tag-Schlüssel "for-use-with-amazon-emr-managed-policies" mit dem Wert „true“ haben.

Das standardmäßige Amazon EMR-Cluster-Instance-Profil ermöglicht den Zugriff auf Ressourcen wie S3-Buckets und Dynamodb-Tabellen, deren Namen „emr“ enthalten. Sie können zusätzliche IAM-Richtlinien anfordern, um zusätzliche Ressourcen für Amazon EMR zu nutzen. Die folgenden Ressourcen-ARNs können mit Amazon EMR-Jobs unter Verwendung des customer_emr_cluster_instance_profile verwendet werden:

- arn:aws:dynamodb: *:*:table/*emr*
- arn:aws:kinesis: *:*:stream/*emr*
- arn:aws:sns: *:*: *emr*arn:aws:sqs: *:*: *emr*
- arn:aws:sqs: *:*: *emr*
- arn:aws:sqs: *:*:AWS-* ElasticMapReduce
- arn:aws:sdb: *::domäne: *emr*

- arn:aws:s3: ::*emr*

Wenn Kerberos-Authentifizierung für den Amazon EMR-Cluster erforderlich ist:

- Geben Sie den Bereichsnamen an, der für jeden kerberisierten Amazon EMR-Cluster verwendet werden soll, und die lokalen Active Directory-IP-Adressen.
- Anforderungen an die Infrastruktur:

  Multi-Account Landing Zone (MALZ): Reichen Sie einen RFC ein, um ein neues verwaltetes Anwendungskonto oder eine neue VPC in einem vorhandenen Anwendungskonto zu erstellen.

  Single-Account Landing Zone (SALZ): Reichen Sie einen RFC ein, um ein neues Subnetz in Ihrer VPC zu erstellen.
- Konfigurieren Sie die eingehende Vertrauensstellung für den Bereich des Clusters im lokalen Active Directory.
- Reichen Sie einen RFC ein, um DNS-Zonen für den Bereich im Managed AD zu konfigurieren.
- Konfiguration des Bereichs:

  MALZ: Senden Sie einen Management | Other | Other | Update (ct-0xdawir96cy7k) -RFC, um den VPC-DHCP-Optionssatz so zu aktualisieren, dass er den Realmnamen als Domainnamensuffix verwendet.

  SALZ: Reichen Sie einen RFC für Management | Other | Other | Update (ct-0xdawir96cy7k) ein, um ein neues Amazon EMR-AMI zu generieren, das den spezifischen Bereich für das Domainnamensuffix verwendet.

Für die Bereitstellung von Amazon EMR Studio ist für die Rolle `customer_emr_cluster_service_role` eine Voraussetzung für einen Amazon Simple Storage Service-Bucket erforderlich. Um den Bucket zu erstellen, verwenden Sie das automatisierte CT `ct-1a68ck03fn98r` (Deployment | Advanced Stack Components | S3 storage | Create). Wenn Sie dieses automatisierte CT verwenden, um einen Amazon S3 S3-Bucket für Amazon EMR zu erstellen, muss der Bucket-Name mit dem Präfix `customer-emr-*` beginnen. Außerdem müssen Sie den Bucket in derselben AWS Region wie der Amazon EMR-Cluster erstellen.

Verwenden Sie AMS SSP, um Amazon EventBridge in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf EventBridge Amazon-Funktionen zuzugreifen. Amazon EventBridge ist ein serverloser Event-Bus-Service, der es einfach macht, Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen zu verbinden. EventBridge liefert einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, Software-as-a-Service (SaaS) -Anwendungen und AWS Diensten und leitet diese Daten an Ziele weiter, wie AWS Lambda z. Sie können Routing-Regeln einrichten, um festzulegen, wohin Ihre Daten gesendet werden sollen, um Anwendungsarchitekturen zu erstellen, die in Echtzeit auf alle Ihre Datenquellen reagieren. Mit EventBridge können Sie ereignisgesteuerte Architekturen erstellen, die lose gekoppelt und verteilt sind.

Weitere Informationen finden Sie auf Amazon EventBridge.

EventBridge in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf EventBridge in meinem AMS-Konto?

Beantragen Sie den Zugriff auf, EventBridge indem Sie einen RFC mit dem Änderungstyp Management | AWS-Service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_eventbridge_role` Konto `customer_eventbridge_scheduler_execution_role` die folgenden IAM-Rollen zur Verfügung: und. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

Die Ausführungsrolle `customer_eventbridge_scheduler_execution_role` ist eine IAM-Rolle, von der EventBridge Scheduler annimmt, um in Ihrem Namen mit anderen AWS-Services zu interagieren. Die mit dieser Rolle verknüpften Berechtigungsrichtlinien gewähren dem EventBridge Scheduler Zugriff auf das Aufrufen von Zielen.

> **Note**
>
> Standardmäßig verwendet EventBridge Scheduler AWS eigene Schlüssel EventBridge zum Verschlüsseln der Daten. Um einen vom Kunden verwalteten Schlüssel für die Verschlüsselung der Daten EventBridge zu verwenden, reichen Sie den RFC über den

Änderungstyp Management | AWS-Service | Self-provisioned service | Add (review required) Change Type (ct-3qe6io8t6jtny) für die Servicebereitstellung ein.

F: Welche Einschränkungen gelten für die Nutzung in meinem AMS-Konto? EventBridge

Sie müssen AMS einreichen RFCs und die folgenden Ressourcen erstellen: Servicerollen zum Auslösen des Batch-Jobs, SQS-Warteschlange, CodeBuild CodePipeline, und SSM-Befehle.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung EventBridge in meinem AMS-Konto?

Sie müssen mithilfe des Änderungstyps Deployment | Advanced Stack Components | Identity and Access Management (IAM) | Entität oder Richtlinie erstellen (Überprüfung erforderlich) (ct-3dpd8mdd9jn1r) eine EventBridge Servicerolle mit einem RFC anfordern, bevor Sie andere AWS Ressourcen wie AWS Batch Lambda-, Amazon SNS-, Amazon SQS- oder Amazon Logs-Ressourcen EventBridge zum Auslösen verwenden. CloudWatch Geben Sie die Dienste an, die aufgerufen werden sollen, wenn Sie Ihre Servicerolle anfordern. Informationen zu den Berechtigungen, die zum Aufrufen von Zielen erforderlich sind, finden Sie unter Verwenden ressourcenbasierter Richtlinien für. EventBridge

EventBridge ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem Mitglied ausgeführt wurden. AWS-Service EventBridge CloudTrail muss aktiviert sein und darf die Protokolldateien in S3-Buckets speichern. Hinweis: Alle AMS-Konten wurden CloudTrail aktiviert, sodass keine Maßnahmen erforderlich sind.

F: Für die Rolle customer_eventbridge_scheduler_execution_role ist ein Schlüssel erforderlich (optional, falls er für die Verschlüsselung verwendet wird). AWS Key Management Service Wie AWS KMS CMKs setze ich die Verschlüsselung von Daten im Ruhe/bei der Übertragung ein?

Standardmäßig verschlüsselt EventBridge Scheduler Ereignismetadaten und Nachrichtendaten, die er unter einem AWS eigenen Schlüssel speichert (Verschlüsselung im Ruhezustand). EventBridge Scheduler verschlüsselt auch Daten, die zwischen EventBridge Scheduler und anderen Diensten übertragen werden, mithilfe von Transport Layer Security (TLS) (Verschlüsselung bei der Übertragung).

Wenn Ihr spezieller Anwendungsfall erfordert, dass Sie die Verschlüsselungsschlüssel, die Ihre Daten auf EventBridge Scheduler schützen, kontrollieren und prüfen, können Sie einen vom Kunden verwalteten Schlüssel verwenden.

Sie müssen einen RFC mit dem Änderungstyp Verwaltung | AWS-Service | Self-provisioned Service | Add (review required) anfordern, bevor Sie Amazon EventBridge für die Aktivierung der Genehmigung verwenden. AWS KMS

Verwenden Sie AMS SSP, um Amazon Forecast in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Forecast (Forecast) zuzugreifen. Amazon Forecast ist ein vollständig verwalteter Service, der maschinelles Lernen nutzt, um hochgenaue Prognosen zu liefern.

> **Note**
>
> AWS hat mit Wirkung zum 29. Juli 2024 den Zugang für Neukunden zu Amazon Forecast geschlossen. Bestandskunden von Amazon Forecast können den Service weiterhin wie gewohnt nutzen. AWS investiert weiterhin in Sicherheits-, Verfügbarkeits- und Leistungsverbesserungen für Amazon Forecast, plant jedoch AWS nicht, neue Funktionen einzuführen.
> Wenn Sie Amazon Forecast verwenden möchten, wenden Sie sich an Ihren CSDM, damit dieser Ihnen weiterhelfen kann, wie Sie Ihre Nutzung von Amazon Forecast auf Amazon SageMaker Canvas umstellen können.

Forecast basiert auf derselben Technologie, die auch bei Amazon.com verwendet wird, und verwendet maschinelles Lernen, um Zeitreihendaten mit zusätzlichen Variablen zu kombinieren, um Prognosen zu erstellen. Forecast erfordert keine Erfahrung mit maschinellem Lernen, um loszulegen. Sie müssen nur historische Daten sowie alle zusätzlichen Daten angeben, von denen Sie glauben, dass sie sich auf Ihre Prognosen auswirken könnten. Beispielsweise kann sich die Nachfrage nach einer bestimmten Hemdfarbe mit den Jahreszeiten und dem Standort des Geschäfts ändern. Dieser komplexe Zusammenhang ist für sich genommen schwer zu ermitteln, aber maschinelles Lernen eignet sich hervorragend, um ihn zu erkennen. Sobald Sie Ihre Daten bereitgestellt haben, untersucht Forecast sie automatisch, ermittelt, was aussagekräftig ist, und erstellt ein Prognosemodell, mit dem Prognosen getroffen werden können, die bis zu 50% genauer sind als die alleinige Betrachtung von Zeitreihendaten.

Weitere Informationen finden Sie unter Amazon Forecast.

Häufig gestellte Fragen zu Amazon Forecast in AWS Managed Services

F: Wie beantrage ich Zugriff auf Forecast in meinem AMS-Konto?

Beantragen Sie Zugriff auf, AWS Firewall Manager indem Sie einen RFC mit dem Änderungstyp Management | AWS Service | Self-Provisioned Service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_forecast_admin_role` Konto die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Nutzung von Forecast in meinem AMS-Konto?

Der standardmäßige S3-Bucket-Zugriff ermöglicht Ihnen nur den Zugriff auf Buckets mit dem Benennungsmuster „customer-forecast-*“. Wenn Sie Ihre eigene Benennungskonvention für Daten-Buckets haben, besprechen Sie die Benennung von Buckets und die damit verbundene Einrichtung des Zugriffs mit Ihrem Cloud Architect (CA). Beispiel:

- Sie könnten Ihre spezifische Amazon Forecast-Servicerolle mit einer Benennung wie 'AmazonForecast- ExecutionRole -*' und dem zugehörigen richtigen S3-Bucket-Zugriff definieren. Weitere Informationen finden Sie in der IAM-Konsole unter AmazonForecast-ExecutionRole-Admin Servicerolle und IAM-Richtlinie customer_forecast_default_s3_access_policy.
- Möglicherweise müssen Sie den zugehörigen S3-Buckets-Zugriff der IAM-Verbundrolle zuordnen. Weitere Informationen finden Sie in der IAM-Richtlinie customer_forecast_default_s3_access_policy in der IAM-Konsole.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Forecast in meinem AMS-Konto?

- Vor der Verwendung von Forecast müssen die richtigen Amazon S3 S3-Buckets erstellt werden. Insbesondere erfolgt der Standardzugriff auf S3-Buckets nach dem Benennungsmuster „customer-forecast-*“
- Wenn Sie für S3-Buckets andere Benennungsmuster als „customer-forecast-*“ verwenden möchten, müssen Sie eine neue Servicerolle mit S3-Zugriffsberechtigungen für die Buckets erstellen:
  1. Es muss eine neue Servicerolle mit der Benennung 'AmazonForecast- - ExecutionRole {suffix}' erstellt werden.
  2. Es muss eine neue IAM-Richtlinie erstellt werden, die customer_forecast_default_s3_access_policy ähnelt und der neuen Servicerolle und der

zugehörigen Verbundadministratorrolle (z. B. 'customer_forecast_admin_role') zugeordnet werden soll

F: Wie kann ich die Datensicherheit bei der Nutzung von Amazon Forecast verbessern?

- Für die Datenverschlüsselung im Ruhezustand können AWS KMS Sie ein vom Kunden verwaltetes CMK bereitstellen, um den Datenspeicher auf dem Amazon S3 S3-Service zu schützen:
  - Aktivieren Sie die Standardverschlüsselung für den Bucket mit dem Bereitstellungsschlüssel und richten Sie die Bucket-Richtlinie so ein, dass die AWS KMS Datenverschlüsselung beim Eingeben von Daten akzeptiert wird.
  - Aktivieren Sie die Amazon Forecast-Servicerolle 'AmazonForecast- ExecutionRole -*' und die Verbundadministratorrolle (z. B. 'customer_forecast_admin_role') als Hauptbenutzer. AWS KMS
- Für die Datenverschlüsselung während der Übertragung können Sie das HTTPS-Protokoll einrichten, das bei der Übertragung von Objekten gemäß der Amazon S3 S3-Bucket-Richtlinie erforderlich ist.
- Weitere Einschränkungen der Zugriffskontrolle: Aktivieren Sie eine Bucket-Richtlinie für den genehmigten Zugriff für die Amazon Forecast-Servicerolle 'AmazonForecast- ExecutionRole -*' und die Administratorrolle (z. B. 'customer_forecast_admin_role').

F: Was sind die Best Practices bei der Verwendung von Amazon Forecast?

- Sie sollten ein gutes Verständnis Ihrer Datenklassifizierungspraktiken haben und die damit verbundenen Datensicherheitsanforderungen bei der Verwendung von S3-Buckets mit Amazon Forecast abbilden.
- Für die Amazon S3 S3-Bucket-Konfiguration empfehlen wir Ihnen dringend, die HTTPS-Durchsetzung in Ihrer S3-Bucket-Richtlinie zu aktivieren.
- Sie müssen wissen, dass die Admin-Rolle „customer_forecast_admin_role“ den permissiven Zugriff (Get/Delete/PutS3-Objekte) auf Amazon S3 S3-Buckets mit dem Namen „customer-forecast-*“ unterstützt. HINWEIS: Wenn Sie eine detaillierte Zugriffskontrolle für mehrere Teams benötigen, gehen Sie wie folgt vor:
  - Definieren Sie Ihre IAM-Identität für den teambasierten Zugriff (Rolle/Benutzer) mit geringsten Zugriffsrechten auf zugehörige Amazon S3 S3-Buckets.
  - Erstellen Sie team/project basierend AWS KMS CMKs und gewähren Sie den entsprechenden IAM-Identitäten den richtigen Zugriff. (Benutzerzugriff und 'AmazonForecast- ExecutionRole - {team/project}'.

- Richten Sie die S3-Bucket-Standardverschlüsselung mit der erstellten ein. AWS KMS CMKs
- Erzwingen Sie S3-API-Verkehr mit dem HTTPS-Protokoll in der S3-Bucket-Richtlinie.
- Erzwingen Sie die S3-Bucket-Konfiguration für den genehmigten Zugriff für verwandte IAM-Identitäten (Benutzerzugriff und 'AmazonForecast- ExecutionRole - {team/project}') auf die Buckets.

- Wenn Sie die 'customer_forecast_admin_role' für allgemeine Zwecke verwenden möchten, sollten Sie die zuvor aufgeführten Punkte berücksichtigen, um S3-Buckets zu schützen.

F: Wo sind Compliance-Informationen zu Amazon Forecast?

Weitere Informationen finden Sie im Compliance-Programm für AWS Dienste.

Verwenden Sie AMS SSP, um Amazon FSx in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf FSx Amazon-Funktionen zuzugreifen. Amazon FSx bietet vollständig verwaltete Dateisysteme von Drittanbietern. Amazon FSx bietet Ihnen die native Kompatibilität von Dateisystemen von Drittanbietern mit Funktionen für Workloads wie Windows-basierten Speicher, Hochleistungsrechnen (HPC), maschinelles Lernen und Electronic Design Automation (EDA). Amazon FSx automatisiert zeitaufwändige Verwaltungsaufgaben wie Hardwarebereitstellung, Softwarekonfiguration, Patching und Backups. Amazon FSx integriert die Dateisysteme mit Cloud-nativen AWS Diensten, wodurch sie für eine breitere Palette von Workloads noch nützlicher werden.

Amazon FSx stellt Ihnen zwei Dateisysteme zur Auswahl: Amazon FSx für Windows File Server für Windows-basierte Anwendungen und Amazon for Lustre FSx für rechenintensive Workloads. Weitere Informationen finden Sie auf Amazon FSx.

Häufig gestellte Fragen zu Amazon FSx in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon FSx in meinem AMS-Konto?

Beantragen Sie Zugriff auf Amazon, FSx indem Sie einen RFC mit dem Änderungstyp Management | AWS-Service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer_fsx_admin_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon FSx in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität des Dienstes ist verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon FSx in meinem AMS-Konto?

Es gibt keine Voraussetzungen. Für erweiterte Konfigurationen wie Multi-AZ müssen Sie jedoch die Dienste DFS-Replikation und DFS-Namespaces installieren und verwalten. Weitere Informationen finden Sie unter Bereitstellen von Multi-AZ-Dateisystemen.

F: Wie integriere ich mein FSx Amazon-Dateisystem in mein Managed AD für mehrere Konten in der landing zone?

Wenn Sie ein FSx Amazon-Dateisystem erstellen, können Sie Ihr MALZ Managed AD als „AWS Managed Microsoft Active Directory“ für die Windows-Authentifizierung angeben. Weitere Informationen finden Sie unter Amazon FSx mit AWS Directory Service für Microsoft Active Directory verwenden

Außerdem müssen Sie das Managed AD zuerst für das Anwendungskonto freigeben. Senden Sie dazu einen RFC mit dem Änderungstyp Management | Directory Service | Directory | Share directory (ct-369odosk0pd9w).

F: Welche Benutzer gehören zur Gruppe der Delegierten FSx Administratoren von AWS?

Nur IT-Dateiserveradministratoren. Diese Gruppe verfügt über Vollzugriffsrechte für alle Dateifreigaben.

F: Sollte ich die Standard-Dateifreigabe Share verwenden, die bei der Bereitstellung des FSx Systems erstellt wird?

Nein, wir empfehlen nicht, die standardmäßige Dateifreigabe Share wie bereitgestellt zu verwenden. Es gewährt allen Benutzern vollen Zugriff, was gegen das Prinzip der geringsten Rechte verstößt. Erstellen Sie stattdessen kleinere, benutzerdefinierte Dateifreigaben, die Ihren Geschäftsanforderungen entsprechen.

F: Wie kann ich benutzerdefinierte Dateifreigaben für bestimmte Organisationen in meinem Unternehmen erstellen?

Anweisungen zum Erstellen benutzerdefinierter Dateifreigaben finden Sie unter Dateifreigaben. Beschränken Sie den Zugriff auf jede Dateifreigabe nach dem Prinzip der geringsten Rechte.

Verwenden Sie AMS SSP, um Amazon FSx für OpenZFS in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon FSx for OpenZFS zuzugreifen. FSx for OpenZFS ist ein vollständig verwalteter Dateispeicherservice, der es einfach macht, Daten, die sich auf lokalen ZFS- oder anderen Linux-basierten Dateiservern befinden, nach AWS zu verschieben, ohne Ihren Anwendungscode oder die Art und Weise, wie Sie Daten verwalten, zu ändern. Es bietet einen äußerst zuverlässigen, skalierbaren, leistungsstarken und funktionsreichen Dateispeicher, der auf dem Open-Source-OpenZFS-Dateisystem basiert und die vertrauten Funktionen und Fähigkeiten von OpenZFS-Dateisystemen mit der Agilität, Skalierbarkeit und Einfachheit eines vollständig verwalteten AWS Dienstes bietet. Für Entwickler, die Cloud-native Anwendungen entwickeln, bietet es einfachen, leistungsstarken Speicher mit umfangreichen Funktionen für die Arbeit mit Daten.

FSx für OpenZFS sind Dateisysteme von Linux-, Windows- und macOS-Recheninstanzen und Containern aus breit zugänglich, die das branchenübliche NFS-Protokoll (v3, v4.0, v4.1, v4.2) verwenden. OpenZFS basiert AWS auf Graviton-Prozessoren und den neuesten AWS Festplatten- und Netzwerktechnologien (einschließlich AWS Scalable Reliable Datagram Networking und dem AWS Nitro-System) und bietet bis zu 1 Million IOPS mit FSx Latenzen von Hunderten von Mikrosekunden. Durch die vollständige Unterstützung von OpenZFS-Funktionen wie Instant point-in-time Snapshots und Datenklonen können Sie mit OpenZFS Ihre lokalen Dateiserver ganz einfach durch AWS Speicher ersetzen, der vertraute Dateisystemfunktionen bietet und die Notwendigkeit, langwierige Qualifizierungen durchzuführen und bestehende Anwendungen oder Tools zu ändern oder neu zu gestalten, überflüssig macht. FSx Und durch die Kombination der leistungsstarken Datenverwaltungsfunktionen von OpenZFS mit der hohen Leistung und Kosteneffizienz der neuesten AWS-Technologien ermöglicht OpenZFS Ihnen, FSx leistungsstarke, datenintensive Anwendungen zu erstellen und auszuführen.

Als vollständig verwalteter Service macht es OpenZFS einfach, FSx vollständig verwaltete Dateisysteme zu starten, auszuführen und zu skalieren, die die Dateiserver ersetzen AWS , die Sie vor Ort betreiben, und gleichzeitig für mehr Flexibilität und geringere Kosten sorgen. Mit FSx OpenZFS müssen Sie sich nicht mehr um die Einrichtung und Bereitstellung von Dateiservern und Speichervolumes, die Replikation von Daten, die Installation und das Patchen von Dateiserversoftware, die Erkennung und Behebung von Hardwarefehlern und die manuelle Durchführung von Backups kümmern. Es bietet auch eine umfassende Integration mit anderen AWS Diensten wie AWS Identity and Access Management (IAM), AWS Key Management Service (AWS KMS) CloudWatch, Amazon und AWS CloudTrail.

Amazon FSx stellt Ihnen zwei Dateisysteme zur Auswahl: Amazon FSx für Windows File Server für Windows-basierte Anwendungen und Amazon for Lustre FSx für rechenintensive Workloads. Weitere Informationen finden Sie auf Amazon FSx.

Häufig gestellte FSx Fragen zu Amazon für OpenZFS in AWS Managed Services

F: Wie beantrage ich Zugriff FSx zur Nutzung von OpenZFS in meinem AMS-Konto?

Fordern Sie Zugriff auf Amazon FSx OpenZFS an, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_fsx_ontap_admin_role` Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten FSx für die Nutzung von OpenZFS in meinem AMS-Konto?

Um die Sicherheitsgruppe auf den Amazon FSx Elastic Network Interfaces (ENIs) zu ersetzen, müssen Sie Management | Other | Other | Update einreichen, RFCs da Sicherheitsgruppen ein kritischer Perimeter für die AMS-Umgebung sind. Das ist die einzige Einschränkung.

F: Was sind die Voraussetzungen oder Abhängigkeiten FSx für die Nutzung von OpenZFS in meinem AMS-Konto?

Es gibt keine Voraussetzungen. Sie müssen es jedoch Verwenden Sie AMS SSP, um Amazon FSx in Ihrem AMS-Konto bereitzustellen installiert haben.

Verwenden Sie AMS SSP, um Amazon FSx für NetApp ONTAP in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon FSx for NetApp ONTAP zuzugreifen. Amazon FSx for NetApp ONTAP ist ein vollständig verwalteter Service, der äußerst zuverlässige, skalierbare, leistungsstarke und funktionsreiche Dateispeicherung bietet, die auf dem beliebten NetApp ONTAP-Dateisystem basiert. Er bietet die vertrauten Funktionen, Leistungen und Fähigkeiten APIs von NetApp Dateisystemen mit der Agilität, Skalierbarkeit und Einfachheit eines vollständig verwalteten Systems. AWS-Service

Amazon FSx for NetApp ONTAP bietet funktionsreichen, schnellen und flexiblen gemeinsamen Dateispeicher, auf den von Linux-, Windows- und macOS-Recheninstanzen aus, die vor Ort

AWS oder vor Ort ausgeführt werden, umfassend zugegriffen werden kann. FSx for ONTAP bietet leistungsstarken SSD-Speicher mit Latenzen unter einer Millisekunde und ermöglicht eine schnelle und einfache Verwaltung Ihrer Daten, indem Sie Ihre Dateien mit einem Klick auf eine Schaltfläche speichern, klonen und replizieren können. Außerdem werden Ihre Daten automatisch auf kostengünstigeren, elastischen Speicher aufgeteilt, sodass Sie keine Kapazität bereitstellen oder verwalten müssen. So können Sie SSD-Leistung für Ihren Workload erreichen, während Sie nur für einen kleinen Teil Ihrer Daten für SSD-Speicher bezahlen. Es bietet hochverfügbaren und langlebigen Speicher mit vollständig verwalteten Backups und Unterstützung für regionsübergreifende Notfallwiederherstellung. Außerdem unterstützt es beliebte Datensicherheits- und Antivirenanwendungen, die den Schutz und die Sicherung Ihrer Daten noch einfacher machen. Für Kunden, die NetApp ONTAP vor Ort verwenden, FSx ist ONTAP eine ideale Lösung, um Ihre dateibasierten Anwendungen von lokalen zu migrieren, zu sichern oder zu beschleunigen, AWS ohne dass Sie Ihren Anwendungscode oder die Art und Weise, wie Sie Ihre Daten verwalten, ändern müssen.

Als vollständig verwalteter Service macht es Amazon FSx for NetApp ONTAP einfach, zuverlässigen, leistungsstarken und sicheren gemeinsamen Dateispeicher in der Cloud zu starten und zu skalieren. Mit Amazon FSx for NetApp ONTAP müssen Sie sich keine Gedanken mehr über die Einrichtung und Bereitstellung von Dateiservern und Speichervolumes, die Replikation von Daten, die Installation und das Patchen von Dateiserversoftware, die Erkennung und Behebung von Hardwarefehlern, die Verwaltung von Failover und Failback sowie die manuelle Durchführung von Backups machen. Es bietet auch eine umfassende Integration mit anderen AWS-Services Anbietern wie Amazon AWS Identity and Access Management WorkSpaces AWS Key Management Service, und AWS CloudTrail.

Amazon FSx stellt Ihnen zwei Dateisysteme zur Auswahl: Amazon FSx für Windows File Server für Windows-basierte Anwendungen und Amazon for Lustre FSx für rechenintensive Workloads. Weitere Informationen finden Sie auf Amazon FSx.

Häufig gestellte FSx Fragen zu Amazon für NetApp ONTAP in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon FSx for NetApp ONTAP in meinem AMS-Konto?

Beantragen Sie Zugriff auf Amazon FSx for NetApp ONTAP, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto `customer_fsx_ontap_admin_role` die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon FSx for NetApp ONTAP in meinem AMS-Konto?

Um die Sicherheitsgruppe auf den elastischen Netzwerkschnittstellen von Amazon FSx for NetApp ONTAP (ENIs) zu ersetzen, müssen Sie Management | Other | Other | Update einreichen, RFCs da Sicherheitsgruppen ein kritischer Perimeter für die AMS-Umgebung sind. Das ist die einzige Einschränkung.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon FSx for NetApp ONTAP in meinem AMS-Konto?

Es gibt keine Voraussetzungen. Sie müssen es jedoch Verwenden Sie AMS SSP, um Amazon FSx in Ihrem AMS-Konto bereitzustellen installiert haben.

Verwenden Sie AMS SSP, um Amazon Inspector Classic in Ihrem AMS-Konto bereitzustellen

> **Note**
>
> Hinweis zum Ende des Supports: Am 20. Mai 2026 AWS wird der Support für Amazon Inspector Classic eingestellt. Nach dem 20. Mai 2026 können Sie nicht mehr auf die Amazon Inspector Classic-Konsole oder die Amazon Inspector Classic-Ressourcen zugreifen. Amazon Inspector Classic ist nicht mehr für neue Konten und Konten verfügbar, die in den letzten sechs Monaten keine Bewertung abgeschlossen haben. Für alle anderen Konten bleibt der Zugriff bis zum 20. Mai 2026 gültig. Danach können Sie nicht mehr auf die Amazon Inspector Classic-Konsole oder die Amazon Inspector Classic-Ressourcen zugreifen. Weitere Informationen finden Sie unter Ende des Supports für Amazon Inspector Classic.

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Inspector Classic zuzugreifen. Amazon Inspector Classic ist ein automatisierter Sicherheitsbewertungsservice, der dazu beiträgt, die Sicherheit und Konformität von Anwendungen zu verbessern, auf denen bereitgestellt wird AWS. Amazon Inspector Classic bewertet Anwendungen automatisch auf Sicherheitslücken, Sicherheitslücken und Abweichungen von bewährten Methoden. Nach der Durchführung einer Bewertung erstellt Amazon Inspector Classic eine detaillierte Liste der Sicherheitsergebnisse, die nach Schweregrad priorisiert sind. Diese Ergebnisse können direkt oder als Teil detaillierter Bewertungsberichte überprüft werden,

die über die Amazon Inspector Classic-Konsole oder API verfügbar sind. Weitere Informationen finden Sie unter Amazon Inspector Classic.

Häufig gestellte Fragen zu Amazon Inspector in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon Inspector Classic in meinem AMS-Konto?

Fordern Sie Zugriff auf Amazon Inspector Classic an, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto die IAM-Rolle zur Verfügung. `customer_inspector_admin_role` Die Rolle umfasst die AWS AmazonInspectorFullAccess -verwaltete Richtlinie. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Inspector Classic in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von Amazon Inspector Classic ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Inspector Classic in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten, um Amazon Inspector Classic in Ihrem AMS-Konto zu verwenden.

Verwenden Sie den neuen Amazon Inspector in AMS

Sie können den neuen Amazon Inspector jetzt in Ihrem AMS-Konto verwenden.

Für Amazon Inspector Classic `AmazonInspectorFullAccess` waren die `customer-inspector-admin-role-ssm-inspector-agent-policy` und erforderlich. Es wurde jedoch ein Update für die SSPS-Rolle vorgenommen`customer-inspector-admin-role`, das nun eine zusätzliche Rolle beinhaltet. `policyAmazonInspector2FullAccess` Diese neue Richtlinie ermöglicht API-Berechtigungen für die neue Version von Amazon Inspector.

Verwenden Sie AMS SSP, um Amazon Kendra in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Kendra zuzugreifen. Amazon Kendra ist ein

intelligenter Suchdienst, der natürliche Sprachverarbeitung und fortschrittliche Algorithmen für maschinelles Lernen verwendet, um spezifische Antworten auf Suchfragen aus Ihren Daten zurückzugeben. Im Gegensatz zur herkömmlichen schlüsselwortbasierten Suche verwendet Amazon Kendra seine Funktionen für semantisches und kontextuelles Verständnis, um festzustellen, ob ein Dokument für eine Suchabfrage relevant ist. Amazon Kendra gibt spezifische Antworten auf Fragen zurück, sodass Ihre Erfahrung der Interaktion mit einem menschlichen Experten sehr nahe kommt. Amazon Kendra ist hochgradig skalierbar, in der Lage, Leistungsanforderungen zu erfüllen, ist eng in andere AWS Dienste wie Amazon S3 und Amazon Lex integriert und bietet Sicherheit auf Unternehmensniveau. Weitere Informationen finden Sie unter Amazon Kendra;.

Häufig gestellte Fragen zu Amazon Kendra in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon Kendra in meinem AMS-Konto?

Um Zugriff auf Amazon Inspector Classic zu beantragen, reichen Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) ein. Dieser RFC stellt Ihrem Konto die IAM-Rolle zur Verfügung. `customer_kendra_console_role` Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Nutzung von Amazon Kendra in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von Amazon Kendra ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon Kendra in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten, um mit Amazon Kendra zu beginnen. Abhängig von Ihrem spezifischen Anwendungsfall benötigen Sie jedoch möglicherweise Zugriff auf andere AWS Dienste.

Verwenden Sie AMS SSP, um Amazon Kinesis Data Streams in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Kinesis Data Streams (KDS) zuzugreifen. Amazon Kinesis Data Streams ist ein hoch skalierbarer und langlebiger Echtzeit-Datenstreaming-Service. KDS kann kontinuierlich Gigabytes an Daten pro Sekunde aus Hunderttausenden von Quellen wie Website-Clickstreams, Datenbankereignisströmen, Finanztransaktionen, Social-Media-Feeds, IT-

Protokollen und Ereignissen zur Standortverfolgung erfassen. Die gesammelten Daten sind innerhalb von Millisekunden verfügbar, um Anwendungsfälle für Echtzeitanalysen wie Echtzeit-Dashboards, Erkennung von Anomalien in Echtzeit, dynamische Preisgestaltung und mehr zu ermöglichen. Weitere Informationen finden Sie unter Amazon Kinesis Data Streams.

Häufig gestellte Fragen zu Kinesis Data Streams in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon Kinesis Data Streams in meinem AMS-Konto?

Fordern Sie Zugriff auf Amazon Kinesis Data Streams an, indem Sie einen RFC mit dem Management | AWS-Service | Self-provisioned Service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer_kinesis_data_streaming_user_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Kinesis Data Streams in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von Amazon Kinesis Data Streams ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Kinesis Data Streams in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Kinesis Data Streams in Ihrem AMS-Konto.

Verwenden Sie AMS SSP, um Amazon Kinesis Video Streams in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Kinesis Video Streams (KVS) zuzugreifen. Amazon Kinesis Video Streams unterstützt Sie beim sicheren Streamen von Videos von verbundenen Geräten AWS für Analysen, maschinelles Lernen (ML), Wiedergabe und andere Verarbeitungszwecke. Kinesis Video Streams stellt automatisch die gesamte Infrastruktur bereit, die für die Aufnahme von Streaming-Videodaten von Millionen von Geräten erforderlich ist, und

skaliert sie elastisch. Außerdem speichert, verschlüsselt und indexiert es dauerhaft Videodaten in Ihren Streams und ermöglicht Ihnen den Zugriff auf Ihre Daten über. easy-to-use APIs Kinesis Video Streams ermöglicht Ihnen die Wiedergabe von Videos für die Live- und On-Demand-Anzeige und die schnelle Erstellung von Anwendungen, die durch die Integration mit Amazon Rekognition Video und Bibliotheken für ML-Frameworks wie Apache MxNet TensorFlow, und OpenCV die Vorteile von Computer Vision und Videoanalyse nutzen. Weitere Informationen finden Sie unter Amazon Kinesis Video Streams.

Häufig gestellte Fragen zu Amazon Kinesis Video Streams in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon Kinesis Video Streams in meinem AMS-Konto?

Fordern Sie Zugriff auf Amazon Kinesis Video Streams an, indem Sie einen RFC mit dem Management | AWS Service | Self-Provisioned Service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer_kinesis_video_streaming_user_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Kinesis Video Streams in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von Amazon Kinesis Video Streams ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Kinesis Video Streams in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Kinesis Video Streams in Ihrem AMS-Konto.

Verwenden Sie AMS SSP, um Amazon Lex in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf Amazon Lex Lex-Funktionen zuzugreifen. Amazon Lex ist ein Service zum Integrieren von Konversationsschnittstellen in jede Anwendung, die Sprache und Text verwendet.

Amazon Lex bietet fortschrittliche Deep-Learning-Funktionen wie automatische Spracherkennung (ASR) zur Umwandlung von Sprache in Text und Natural Language Understanding (NLU), um die Absicht des Textes zu erkennen, sodass Sie Anwendungen mit äußerst ansprechenden Benutzererlebnissen und lebensechten Konversationsinteraktionen entwickeln können. Mit Amazon Lex stehen dieselben Deep-Learning-Technologien, die Amazon Alexa unterstützen, jetzt allen Entwicklern zur Verfügung, sodass Sie schnell und einfach anspruchsvolle Konversationsbots oder Chatbots in natürlicher Sprache erstellen können. Weitere Informationen finden Sie unter Amazon Lex.

Häufig gestellte Fragen zu Amazon Lex in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon Lex in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie Folgendes einreichen: Verwaltung | AWS Service | Selbst bereitgestellter Service | Änderungstyp hinzufügen (ct-1w8z66n899dct). Dieser RFC stellt Ihrem Konto `customer_lex_author_role` die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Lex in meinem AMS-Konto?

Die Amazon Lex Lex-Integration mit Lambda ist auf Lambda-Funktionen ohne „AMS-“ -Präfix beschränkt, um jegliche Änderungen an der AMS-Infrastruktur zu verhindern.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Lex in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten, um Amazon Lex in Ihrem AMS-Konto zu verwenden.

Verwenden Sie AMS SSP, um Amazon MQ in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf Amazon MQ MQ-Funktionen zuzugreifen. Amazon MQ ist ein verwalteter Message Broker-Service für Apache ActiveMQ, der Sie bei der Einrichtung und dem Betrieb von Message Brokern in der Cloud unterstützt. Message Broker ermöglichen es verschiedenen Softwaresystemen, die häufig unterschiedliche Programmiersprachen und auf unterschiedlichen

Plattformen verwenden, zu kommunizieren und Informationen auszutauschen. Amazon MQ reduziert Ihre Betriebslast, indem es die Bereitstellung, Einrichtung und Wartung von ActiveMQ, einem beliebten Open-Source-Nachrichtenbroker, verwaltet. Wenn Sie Ihre aktuellen Anwendungen mit Amazon MQ verbinden, werden Industriestandards APIs und Protokolle für das Messaging verwendet, darunter JMS, NMS, AMQP, STOMP, MQTT und. WebSocket Die Verwendung von Standards bedeutet, dass in den meisten Fällen kein Messaging-Code neu geschrieben werden muss, wenn Sie zu migrieren. AWS Weitere Informationen finden Sie unter Was ist Amazon MQ?

Häufig gestellte Fragen zu Amazon MQ in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon MQ in meinem AMS-Konto?

Die Nutzung von Amazon MQ in Ihrem AMS-Konto erfolgt in zwei Schritten:

1. Stellen Sie den Amazon MQ Broker bereit. Reichen Sie dazu eine CFN-Vorlage mit dem Amazon MQ Broker über einen RFC mit Deployment | Ingestion | Stack from CloudFormation Template | Create change type (ct-36cn2avfrrj9v) ein, oder reichen Sie einen RFC mit dem Änderungstyp Management | Other | Other | Other | Create change type (ct-1e1xtak34nx76) ein und fordern Sie die Bereitstellung von Amazon MQ Broker in Ihrem Konto an.
2. Greifen Sie auf die Amazon MQ MQ-Konsole zu. Nachdem der Amazon MQ Broker bereitgestellt wurde, erhalten Sie Zugriff auf die Amazon MQ MQ-Konsole, indem Sie einen RFC mit Management | AWS service | Self-provisioned service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto die folgende IAM-Rolle zur Verfügung:. `customer_mq_console_role`

Nachdem die Rolle in Ihrem Konto bereitgestellt wurde, müssen Sie sie in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon MQ in meinem AMS-Konto?

Die volle Funktionalität von Amazon MQ ist in Ihrem AMS-Konto verfügbar. Die Bereitstellung von Amazon MQ Broker ist jedoch aufgrund der erforderlichen erhöhten Berechtigungen nicht im Rahmen der Richtlinie verfügbar. Einzelheiten zur Bereitstellung von Amazon MQ Broker in Ihren Konten finden Sie oben.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon MQ in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten, um Amazon MQ in Ihrem AMS-Konto zu verwenden.

Verwenden Sie AMS SSP, um Amazon Managed Service für Apache Flink in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Managed Service for Apache Flink zuzugreifen. Managed Service für Apache Flink ist der einfachste Weg, Streaming-Daten zu analysieren, umsetzbare Erkenntnisse zu gewinnen und auf Ihre Geschäfts- und Kundenanforderungen in Echtzeit zu reagieren. Amazon Managed Service für Apache Flink reduziert die Komplexität beim Erstellen, Verwalten und Integrieren von Streaming-Anwendungen mit anderen AWS Services. SQL-Benutzer können mithilfe von Vorlagen und einem interaktiven SQL-Editor problemlos Streaming-Daten abfragen oder ganze Streaming-Anwendungen erstellen. Java-Entwickler können mithilfe von Open-Source-Java-Bibliotheken und AWS -Integrationen schnell anspruchsvolle Streaming-Anwendungen erstellen, um Daten in Echtzeit zu transformieren und zu analysieren. Amazon Managed Service für Apache Flink kümmert sich um alles, was für die kontinuierliche Ausführung Ihrer Echtzeitanwendungen erforderlich ist, und skaliert automatisch, um dem Volumen und dem Durchsatz Ihrer eingehenden Daten zu entsprechen. Mit Amazon Managed Service für Apache Flink zahlen Sie nur für die Ressourcen, die Ihre Streaming-Anwendungen verbrauchen. Es gibt keine Mindestgebühr oder Einrichtungskosten. Weitere Informationen finden Sie unter Amazon Managed Service für Apache Flink.

Häufig gestellte Fragen zu Managed Service für Apache Flink in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon Managed Service für Apache Flink in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) angeben. Dieser RFC stellt Ihrem `customer_kinesis_analytics_application_role` Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Managed Service für Apache Flink in meinem AMS-Konto?

- Konfigurationen sind auf Ressourcen ohne „AMS-“ oder „MC-“ -Präfixe beschränkt, um jegliche Änderungen an der AMS-Infrastruktur zu verhindern.
- Die Erlaubnis, Kinesis Data Streams oder Firehose zu löschen oder neue zu erstellen, wurde aus der Richtlinie entfernt. Wir haben eine andere Richtlinie, die das ermöglicht.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Kinesis Data Streams in meinem AMS-Konto?

Es gibt einige Abhängigkeiten:

- Amazon Managed Service für Apache Flink erfordert, dass Kinesis Data Streams oder Firehose erstellt werden müssen, bevor eine Anwendung mit Managed Service für Apache Flink konfiguriert werden kann.
- Die ressourcenbasierten Richtlinienberechtigungen sollten auf eine bestimmte Eingabedatenquelle hinweisen.

Verwenden Sie AMS SSP, um Amazon Managed Streaming for Apache Kafka in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Managed Streaming for Apache Kafka (Amazon MSK) zuzugreifen. Amazon Managed Streaming for Apache Kafka ist ein vollständig verwalteter AWS Streaming-Datenservice, mit dem Sie ganz einfach Anwendungen erstellen und ausführen können, die Apache Kafka zur Verarbeitung von Streaming-Daten verwenden, ohne dass Sie Experte für den Betrieb von Apache Kafka-Clustern werden müssen. Amazon MSK verwaltet die Bereitstellung, Konfiguration und Wartung von Apache Kafka-Clustern und ZooKeeper Apache-Knoten für Sie. Amazon MSK zeigt auch wichtige Leistungskennzahlen von Apache Kafka in der AWS Konsole an.

Amazon MSK bietet mehrere Sicherheitsstufen für Ihre Apache Kafka-Cluster, darunter VPC-Netzwerkisolierung, AWS IAM für die API-Autorisierung auf Kontrollebene, Verschlüsselung im Ruhezustand, TLS-Verschlüsselung bei der Übertragung, TLS-basierte Zertifikatsauthentifizierung und Authentifizierung gesichert durch. SASL/SCRAM AWS Secrets Manager Weitere Informationen finden Sie unter Amazon MSK.

Häufig gestellte Fragen zu Amazon MSK in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon MSK in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbstbereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt die folgenden IAM-Richtlinien und Rollen für Ihr Konto bereit:

- `customer-msk-admin-policy.json`
- `AmazonMSKFullAccess`
- `customer-msk-admin-role.json`

Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Nutzung von Amazon MSK?

Damit Amazon MSK Brokerprotokolle an die von Ihnen konfigurierten Ziele senden kann, stellen Sie sicher, dass die `AmazonMSKFullAccess` Richtlinie mit Ihrer IAM-Rolle verknüpft ist. Es sind also bereits vollständige Zugriffsberechtigungen vorhanden.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon MSK?

Bevor Sie Ihren MSK-Cluster erstellen, müssen Sie über eine VPC und Subnetze innerhalb dieser VPC verfügen. Standardmäßig deckt AMS dies im Rahmen der standardmäßigen AMS-VPC-Erstellung ab.

Weitere Informationen zu den Einschränkungen von Amazon MSK finden Sie unter Amazon MSK Limits.

Verwenden Sie AMS SSP, um Amazon Managed Service für Prometheus in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Managed Service for Prometheus (AMP) zuzugreifen. Amazon Managed Service für Prometheus ist ein serverloser, Prometheus-kompatibler Service zur Überwachung von Containermetriken, der es einfacher macht, Containerumgebungen im großen Maßstab sicher zu überwachen. Mit Amazon Managed Service für Prometheus können Sie dasselbe Open-Source-Prometheus-Datenmodell und dieselbe Abfragesprache verwenden, die Sie heute verwenden, um die Leistung Ihrer containerisierten Workloads zu überwachen, und außerdem von verbesserter Skalierbarkeit, Verfügbarkeit und Sicherheit profitieren, ohne die zugrunde liegende Infrastruktur verwalten zu müssen.

Amazon Managed Service for Prometheus skaliert automatisch die Erfassung, Speicherung und Abfrage von Betriebsmetriken, wenn Workloads nach oben oder unten skaliert werden. Es lässt sich in AWS Sicherheitsdienste integrieren, um einen schnellen und sicheren Zugriff auf Daten zu ermöglichen. Weitere Informationen finden Sie unter Was ist Amazon Managed Service for Prometheus?

Häufig gestellte Fragen zu Amazon Managed Service für Prometheus in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon Managed Service for Prometheus in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) angeben. Dieser RFC stellt Ihrem `customer-prometheus-console-role` Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die `customer-prometheus-console-role` Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Managed Service for Prometheus in meinem AMS-Konto?

Alle Funktionen werden unterstützt.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon Managed Service for Prometheus in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten, um mit Amazon Managed Service for Prometheus zu beginnen. Abhängig von Ihrem spezifischen Anwendungsfall benötigen Sie jedoch möglicherweise Zugriff auf andere AWS Dienste.

Verwenden Sie AMS SSP, um Amazon Personalize in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Personalize zuzugreifen. Amazon Personalize ist ein Service für maschinelles Lernen, mit dem Entwickler auf einfache Weise individuelle Empfehlungen für Kunden erstellen können, die ihre Anwendungen verwenden.

Maschinelles Lernen wird zunehmend zur Verbesserung der Kundenbindung eingesetzt, indem personalisierte Produkt- und Inhaltsempfehlungen, maßgeschneiderte Suchergebnisse und gezielte

Marketingaktionen bereitgestellt werden. Die Entwicklung der Funktionen für maschinelles Lernen, die zur Erstellung dieser ausgeklügelten Empfehlungssysteme erforderlich sind, war für die meisten Unternehmen heute aufgrund der Komplexität jedoch unerreichbar. Amazon Personalize ermöglicht es Entwicklern, die noch keine Erfahrung mit maschinellem Lernen haben, mithilfe von Machine-Learning-Technologie, die durch jahrelangen Einsatz auf Amazon.com perfektioniert wurde, mühelos anspruchsvolle Personalisierungsfunktionen in ihre Anwendungen zu integrieren.

Mit Amazon Personalize stellen Sie einen Aktivitätsstream aus Ihrer Anwendung bereit — Klicks, Seitenaufrufe, Anmeldungen, Käufe usw. — sowie ein Inventar der Artikel, die Sie empfehlen möchten, wie Artikel, Produkte, Videos oder Musik. Sie können Amazon Personalize auch zusätzliche demografische Informationen von Ihren Benutzern wie Alter oder geografischer Standort zur Verfügung stellen. Amazon Personalize verarbeitet und untersucht die Daten, ermittelt, was sinnvoll ist, wählt die richtigen Algorithmen aus und trainiert und optimiert ein Personalisierungsmodell, das auf Ihre Daten zugeschnitten ist. Alle von Amazon Personalize analysierten Daten werden vertraulich und sicher behandelt und nur für Ihre individuellen Empfehlungen verwendet. Sie können mit der Bereitstellung personalisierter Empfehlungen über einen einfachen API-Aufruf beginnen. Sie zahlen nur für das, was Sie tatsächlich nutzen, und es fallen keine Mindestgebühren und keine Vorabverpflichtungen an.

Weitere Informationen finden Sie unter Amazon Personalize.

Häufig gestellte Fragen zu Amazon Personalize in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon Personalize in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Self-Provisioned Service | Add (review erforderlich) (ct-3qe6io8t6jtny) einreichen. Sie müssen dann angeben, welcher S3-Bucket die Daten enthält, die von personalize zur Generierung der Empfehlungen verwendet werden sollen. AWS Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen zur Verfügung`customer_personalize_console_role`: und. `customer_personalize_service_role`

- Sobald die in Ihrem Konto `customer_personalize_console_role` bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren. Sie können die `customer_personalize_console_policy` auch einer anderen vorhandenen Rolle zuordnen als`Customer_ReadOnly_Role`.
- Nachdem der `customer_personalize_service_role` Ihrem Konto zur Verfügung gestellt wurde, können Sie seinen ARN angeben, wenn Sie eine neue Datensatzgruppe erstellen.

Zu diesem Zeitpunkt wird AMS Operations diese Servicerolle auch in Ihrem Konto bereitstellen:`aws_code_pipeline_service_role_policy`.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Personalize in meinem AMS-Konto?

Die Amazon Personalize Personalize-Konfiguration ist auf Ressourcen ohne „ams-“ oder „mc-“ - Präfixe beschränkt, um jegliche Änderungen an der AMS-Infrastruktur zu verhindern.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Personalize in meinem AMS-Konto?

- Wenn der S3-Bucket, in dem Daten gespeichert sind, verschlüsselt ist, muss die KMS-Schlüssel-ID angegeben werden, damit wir der von Amazon Personalize verwendeten Rolle erlauben können, den Bucket zu entschlüsseln.

  Amazon Personalize unterstützt den KMS S3-Standardschlüssel nicht. Falls für die Verwendung von KMS erforderlich, erstellen Sie einen benutzerdefinierten Schlüssel und fügen Sie ihm die folgende Richtlinie hinzu, indem Sie einen RFC mit dem Änderungstyp KMS Key | Create (Überprüfung erforderlich) öffnen:

  JSON

```
{
    "Version":"2012-10-17",
    "Id": "key-consolepolicy-3",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "Service": "personalize.amazonaws.com"
            },
            "Action": "kms:*",
            "Resource": "*"
        }
    ]
}
```

- Ein S3-Bucket muss mit der folgenden Bucket-Richtlinie erstellt werden. Reichen Sie dazu einen RFC mit dem Änderungstyp S3 Storage | Create Policy ein. Diese Richtlinie ermöglicht Amazon Personalize den Zugriff auf Daten. Dieser Bucket enthält die Daten, die von Amazon Personalize verwendet werden sollen.

JSON

```
{
"Version":"2012-10-17",
"Id": "PersonalizeS3BucketAccessPolicy",
"Statement": [
{
"Sid": "PersonalizeS3BucketAccessPolicy",
"Effect": "Allow",
"Principal": {
"Service": "personalize.amazonaws.com"
},
"Action": [
"s3:GetObject",
"s3:ListBucket"
],
"Resource": [
"arn:aws:s3:::bucket-name",
"arn:aws:s3:::bucket-name/*"
]
}
]
}
```

Verwenden Sie AMS SSP, um Amazon QuickSight in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf QuickSight Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. QuickSight ist ein schneller, cloudgestützter Business Intelligence-Service, der allen Mitarbeitern Ihres Unternehmens Einblicke bietet. Da es sich um einen vollständig verwalteten Service handelt, QuickSight können Sie auf einfache Weise interaktive Dashboards erstellen und veröffentlichen, die Erkenntnisse aus maschinellem Lernen (ML) enthalten. Weitere Informationen finden Sie auf Amazon QuickSight.

QuickSight in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff QuickSight auf mein AMS-Konto?

Beantragen Sie den Zugriff, indem Sie Folgendes einreichen: Verwaltung | AWS Service | Selbst bereitgestellter Service | Änderungstyp hinzufügen (ct-1w8z66n899dct). Dieser RFC stellt Ihrem Konto `customer_quicksight_console_admin_role` die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung QuickSight in meinem AMS-Konto?

- AWS Sie können aufgrund der Abhängigkeit von den IAM-Richtlinien QuickSight nicht auf die Ressourceneinstellungen zugreifen. Das AMS-Team aktiviert jedoch jede Ressource für Sie als Antwort auf Ihre Anfrage zur Aktivierung des Dienstes.
- Der Ressourcenzugriff für einzelne Benutzer und Gruppen wird in diesem Modell nicht unterstützt, da diese Funktion es Benutzern ermöglicht, IAM-Berechtigungen zu ändern, was die AMS-Infrastruktur gefährden könnte.
- Die Möglichkeit, IAM-Identitäten von innen einzuladen, QuickSight wird aufgrund des Risikos, das mit der Änderung von IAM-Objekten verbunden ist, nicht unterstützt.
- QuickSight Der Service bietet zwei Editionen: Enterprise und Standard. Beide bieten eine Single Sign-On-Option (SSO), die von AMS unterstützt wird. Die Enterprise Edition bietet jedoch eine Option zur QuickSight Integration in Active Directory (AD). QuickSight on AMS unterstützt aufgrund von Inkompatibilitäten zwischen der AMS-Kontostruktur und den QuickSight Vertrauensanforderungen keine Integration mit AD.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung QuickSight in meinem AMS-Konto?

- Wenn AMS diesen RFC zum Hinzufügen erhält QuickSight, erhalten Sie eine Serviceanfrage mit zusätzlichen Informationen. Geben Sie dem Kunden folgende Informationen:
  - QuickSight Kontoname (zum Beispiel *`CustomerName`*`-quicksight`
  - QuickSight Edition (Standard oder Enterprise)
  - Die AWS Region, in der der QuickSight Service aktiviert werden soll (standardmäßig Ihre AWS AMS-Region).
  - Eine Benachrichtigungs-E-Mail-Adresse für das QuickSight Konto.
  - (Optional) Der S3-Bucket, in dem sich die zu analysierenden Datendateien befinden.

- Die VPC und das Subnetz IDs , mit denen eine Verbindung hergestellt wird, QuickSight unterstützen eine Funktion zum Hinzufügen einer VPC-Verbindung, die private Konnektivität zwischen QuickSight und Ressourcen innerhalb des Kontos ermöglicht.

Ein AMS-Betreiber führt den Anmeldevorgang in Ihrem Namen durch und konfiguriert zwei Funktionen: QuickSight

- Automatische Erkennung von Datenquellen.
- VPC-Verbindungen.

> **Note**
>
> Diese Aktionen müssen von einem AMS-Betreiber ausgeführt werden, da während des Anmeldevorgangs erhöhte IAM- und VPC-Berechtigungen erforderlich sind.

Verwenden Sie AMS SSP, um Amazon Rekognition in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Rekognition zuzugreifen. Amazon Rekognition macht es einfach, Bild- und Videoanalysen zu Ihren Anwendungen hinzuzufügen, und zwar mithilfe bewährter, hochgradig skalierbarer Deep-Learning-Technologie, für deren Verwendung kein Fachwissen im Bereich maschinelles Lernen erforderlich ist. Mit Amazon Rekognition können Sie Objekte, Personen, Text, Szenen und Aktivitäten in Bildern und Videos identifizieren und unangemessene Inhalte erkennen. Amazon Rekognition bietet außerdem hochgenaue Funktionen zur Gesichtsanalyse und Gesichtssuche, mit denen Sie Gesichter erkennen, analysieren und vergleichen können, und zwar für eine Vielzahl von Anwendungsfällen zur Benutzerverifizierung, Personenzählung und zur öffentlichen Sicherheit.

Mit Amazon Rekognition Custom Labels können Sie Objekte und Szenen in Bildern identifizieren, die speziell auf Ihre Geschäftsanforderungen zugeschnitten sind. Sie können beispielsweise ein Modell erstellen, um bestimmte Maschinenteile an Ihrer Montagelinie zu klassifizieren oder um ungesunde Pflanzen zu erkennen. Amazon Rekognition Custom Labels nimmt Ihnen die schwere Arbeit bei der Modellentwicklung ab, sodass keine Erfahrung mit maschinellem Lernen erforderlich ist. Sie

müssen lediglich Bilder von Objekten oder Szenen bereitstellen, die Sie identifizieren möchten, und der Service erledigt den Rest.

Weitere Informationen finden Sie unter Amazon Rekognition.

Häufig gestellte Fragen zu Amazon Rekognition in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon Rekognition in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) angeben. Dieser RFC stellt Ihrem `customer_rekognition_console_role & customer_rekognition_service_role` Konto die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon Rekognition in meinem AMS-Konto?

Der volle Funktionsumfang von Amazon Rekognition ist mit der selbst bereitgestellten Servicerolle Amazon Rekognition verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon Rekognition in meinem AMS-Konto?

Wenn Sie Kinesis Video Streams verwenden, die das Quell-Streaming-Video für einen Amazon Rekognition Video Video-Stream-Prozessor oder einen Datenstream als Ziel zum Schreiben von Daten in Kinesis Data Streams bereitstellen, geben Sie AMS bitte `kinesisStreamName` bei der Erstellung des RFC eine an.

Verwenden Sie AMS SSP, um Amazon SageMaker AI in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon SageMaker AI zuzugreifen. SageMaker KI bietet jedem Entwickler und Datenwissenschaftler die Möglichkeit, Modelle für maschinelles Lernen schnell zu erstellen, zu trainieren und einzusetzen. Amazon SageMaker AI ist ein vollständig verwalteter Service, der den gesamten Workflow für maschinelles Lernen abdeckt, um Ihre Daten zu kennzeichnen und aufzubereiten, einen Algorithmus auszuwählen, das Modell zu trainieren, es für die Bereitstellung abzustimmen und zu optimieren, Vorhersagen zu treffen und Maßnahmen zu ergreifen.

Ihre Modelle werden schneller, mit viel weniger Aufwand und geringeren Kosten in Produktion gehen. Weitere Informationen finden Sie unter Amazon SageMaker AI.

SageMaker Häufig gestellte Fragen zu KI in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf SageMaker KI in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Self-Provisioned Service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen und die Servicerolle zur Verfügung. `customer_sagemaker_admin_role` `AmazonSageMaker-ExecutionRole-Admin` Nachdem SageMaker KI in Ihrem Konto bereitgestellt wurde, müssen Sie die `customer_sagemaker_admin_role` Rolle in Ihre Verbundlösung integrieren. Sie können nicht direkt auf die Servicerolle zugreifen. Der SageMaker KI-Dienst verwendet sie bei der Ausführung verschiedener Aktionen, wie hier beschrieben: Rollen übergeben.

F: Was sind die Einschränkungen bei der Nutzung von SageMaker KI in meinem AMS-Konto?

- Die folgenden Anwendungsfälle werden von der AMS Amazon SageMaker AI IAM-Rolle nicht unterstützt:
  - SageMaker AI Studio wird derzeit nicht unterstützt.
  - SageMaker KI Ground Truth zur Verwaltung privater Belegschaften wird nicht unterstützt, da diese Funktion einen übermäßigen Zugriff auf Amazon Cognito Cognito-Ressourcen erfordert. Wenn die Verwaltung einer privaten Belegschaft erforderlich ist, können Sie eine benutzerdefinierte IAM-Rolle mit kombinierten SageMaker KI- und Amazon Cognito Cognito-Berechtigungen anfordern. Andernfalls empfehlen wir, Mitarbeiter der öffentlichen Hand (unterstützt von Amazon Mechanical Turk) oder AWS Marketplace Dienstleister für die Datenkennzeichnung zu beauftragen.
- Erstellung von VPC-Endpunkten zur Unterstützung von API-Aufrufen an SageMaker KI-Dienste (aws.sagemaker). {region} .notebook, com.amazonaws. {region} .sagemaker.api und com.amazonaws. {region} .sagemaker.runtime) wird nicht unterstützt, da Berechtigungen nicht nur auf KI-bezogene Dienste beschränkt werden können. SageMaker Um diesen Anwendungsfall zu unterstützen, reichen Sie einen RFC Management | Other | Other ein, um zugehörige VPC-Endpoints zu erstellen.
- SageMaker Die auto Skalierung von KI-Endpunkten wird nicht unterstützt, da SageMaker KI `DeleteAlarm` Berechtigungen für jede („*“) Ressource benötigt. Um Endpoint Auto Scaling zu

unterstützen, reichen Sie einen RFC Management | Other | Other ein, um Auto Scaling für einen SageMaker KI-Endpunkt einzurichten.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von SageMaker KI in meinem AMS-Konto?

- Die folgenden Anwendungsfälle erfordern vor der Verwendung eine spezielle Konfiguration:
  - Wenn ein S3-Bucket zum Speichern von Modellartefakten und Daten verwendet werden soll, müssen Sie einen S3-Bucket mit den erforderlichen Schlüsselwörtern (“ SageMaker „, „Sagemaker“, „sagemaker“ oder „aws-glue“) mit einem Deployment | Advanced stack components | S3 storage | Create RFC anfordern.
  - Wenn Elastic File Store (EFS) verwendet wird, muss der EFS-Speicher im selben Subnetz konfiguriert und von Sicherheitsgruppen zugelassen werden.
  - Wenn andere Ressourcen direkten Zugriff auf SageMaker KI-Dienste (Notebooks, API, Runtime usw.) benötigen, muss die Konfiguration wie folgt angefordert werden:
    - Senden eines RFC zur Erstellung einer Sicherheitsgruppe für den Endpunkt (Deployment | Erweiterte Stack-Komponenten | Sicherheitsgruppe | Create (auto)).
    - Verwaltung einreichen | Andere | Andere | RFC erstellen, um zugehörige VPC-Endpoints einzurichten.

F: Welche Benennungskonventionen werden für Ressourcen unterstützt, auf die sie direkt zugreifen **`customer_sagemaker_admin_role`** können? (Im Folgenden finden Sie Informationen zu Aktualisierungs- und Löschberechtigungen. Wenn Sie zusätzliche unterstützte Namenskonventionen für Ihre Ressourcen benötigen, wenden Sie sich zur Beratung an einen AMS Cloud Architect.)

- Ressource: `AmazonSageMaker-ExecutionRole-*` Rolle übergeben
  - Berechtigungen: Die selbst bereitgestellte SageMaker AI-Servicerolle unterstützt Ihre Verwendung der SageMaker AI-Servicerolle (`AmazonSageMaker-ExecutionRole-*`) mit AWS Glue AWS RoboMaker, und. AWS Step Functions
- Ressource: Secrets auf AWS Secrets Manager
  - Berechtigungen: Beschreiben, Erstellen, Abrufen und Aktualisieren von Geheimnissen mit einem `AmazonSageMaker-*` Präfix.
  - Berechtigungen: Beschreiben, Geheimnisse abrufen, wenn das `SageMaker` Ressourcen-Tag auf gesetzt ist`true`.

- Ressource: Repositorien aktiviert AWS CodeCommit
  - Berechtigungen: Repositorys mit einem Präfix erstellen/löschen. `AmazonSageMaker-*`
  - Berechtigungen: Git Pull/Push auf Repositorys mit den folgenden Präfixen, `*sagemaker**SageMaker*`, und. `*Sagemaker*`
- Ressource: Amazon ECR-Repositorys (Amazon Elastic Container Registry)
  - Berechtigungen: Berechtigungen: Legen Sie Repository-Richtlinien fest, löschen Sie sie und laden Sie Container-Images hoch, wenn die folgende Benennungskonvention für Ressourcen verwendet wird. `*sagemaker*`
- Ressource: Amazon S3 S3-Buckets
  - Berechtigungen: Objekt abrufen, speichern, löschen, mehrteiliges Hochladen von S3-Objekten abbrechen, wenn Ressourcen die folgenden Präfixe haben:`*SageMaker*`, und. `*Sagemaker* *sagemaker* aws-glue`
  - Berechtigungen: Ruft S3-Objekte ab, wenn das `SageMaker` Tag auf gesetzt ist. `true`
- Ressource: Amazon CloudWatch Log Group
  - Berechtigungen: Protokollgruppe oder Stream erstellen, Protokollereignis speichern, Auflisten, Aktualisieren, Erstellen, Löschen der Protokollzustellung mit dem folgenden Präfix:`/aws/sagemaker/*`.
- Ressource: Amazon CloudWatch Metric
  - Berechtigungen: Geben Sie Metrikdaten ein, wenn die folgenden Präfixe verwendet werden: `AWS/SageMaker` `AWS/SageMaker/aws/SageMaker`,`aws/SageMaker/`,`aws/sagemaker`,`aws/sagemaker/`, und`/aws/sagemaker/.`.
- Ressource: Amazon CloudWatch Dashboard
  - Berechtigungen: Create/Delete Dashboards, wenn die folgenden Präfixe verwendet werden:. `customer_*`
- Ressource: Thema Amazon SNS (Simple Notification Service)
  - Berechtigungen: Subscribe/Create Thema, wenn die folgenden Präfixe verwendet werden: `*sagemaker**SageMaker*`, und. `*Sagemaker*`

F: Was ist der Unterschied zwischen **`AmazonSageMakerFullAccess`** und**`customer_sagemaker_admin_role`**?

Das `customer_sagemaker_admin_role` `customer_sagemaker_admin_policy` bietet fast die gleichen Berechtigungen wie mit der AmazonSageMakerFullAccess Ausnahme:

- Erlaubnis zur Verbindung mit AWS RoboMaker Amazon Cognito und AWS Glue Ressourcen.
- SageMaker Automatische Skalierung von KI-Endpunkten. Sie müssen einen RFC mit dem Änderungstyp Management | Advanced Stack Components | Identity and Access Management (IAM) | Entität oder Richtlinie aktualisieren (Überprüfung erforderlich) (ct-27tuth19k52b4) einreichen, um Autoscaling-Berechtigungen vorübergehend oder dauerhaft zu erhöhen, da Autoscaling einen permissiven Zugriff auf den Service erfordert. CloudWatch

F: Wie verwende ich einen vom Kunden verwalteten Schlüssel bei der Datenverschlüsselung im Ruhezustand? AWS KMS

Sie müssen sicherstellen, dass die Schlüsselrichtlinie für die vom Kunden verwalteten Schlüssel ordnungsgemäß eingerichtet wurde, sodass zugehörige IAM-Benutzer oder -Rollen die Schlüssel verwenden können. Weitere Informationen finden Sie im Dokument mit den AWS KMS wichtigsten Richtlinien.

Verwenden Sie AMS SSP, um Amazon Simple Email Service in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Simple Email Service (Amazon SES) zuzugreifen. Amazon Simple Email Service ist ein Cloud-basierter E-Mail-Versandservice, der digitale Vermarkter und Anwendungsentwickler beim Versand von Marketing-, Benachrichtigungs- und Transaktions-E-Mails unterstützt.

Sie können die SMTP-Schnittstelle oder eine der Schnittstellen verwenden AWS SDKs , um Amazon SES direkt in Ihre vorhandenen Anwendungen zu integrieren. Sie können die E-Mail-Versandfunktionen von Amazon SES auch in die Software integrieren, die Sie bereits verwenden, z. B. Ticketsysteme und E-Mail-Clients.

Weitere Informationen finden Sie unter Amazon Simple Email Service.

Häufig gestellte Fragen zu Amazon SES in AWS Managed Services

F: Wie beantrage ich Zugriff auf Amazon SES in meinem AMS-Konto?

Fordern Sie Zugriff auf Amazon SES an, indem Sie einen RFC mit dem Änderungstyp Management | AWS-Service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer_ses_admin_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Amazon SES in meinem AMS-Konto?

- Sie müssen eine S3-Bucket-Richtlinie konfigurieren, damit Amazon SES Ereignisse im Bucket veröffentlichen kann.
- Sie müssen einen Standardschlüssel (AWS SES) verwenden oder einen CMK-Schlüssel konfigurieren, damit Amazon SES E-Mails verschlüsseln und Ereignisse an andere Serviceressourcen wie Amazon S3, Amazon SNS, Lambda und Firehose weiterleiten kann, die zum Konto gehören.

F: Welche Einschränkungen gelten für die Nutzung von Amazon SES in meinem AMS-Konto?

Sie müssen Spenden sammeln RFCs , um die folgenden Ressourcen zu erstellen:

- Ein SMTP-Benutzer und eine IAM-Servicerolle mit PutEvents Genehmigung für einen Kinesis Firehose-Stream.
- Sie müssen mithilfe von AMS-Änderungstypen neue AWS Ressourcen wie S3-Bucket, Firehose-Stream und SNS-Thema erstellen, damit die Ziele Ihrer Amazon SES SES-Regeln und Konfigurationssätze mit diesen Ressourcen funktionieren.
- SMTP-Anmeldeinformationen. Um neue SMTP-Anmeldeinformationen anzufordern, verwenden Sie den Change Type (Management | Other | Other | Create). AMS erstellt die Anmeldeinformationen und fügt sie für Sie zu Secrets Manager hinzu.

Verwenden Sie AMS SSP, um Amazon Simple Workflow Service in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Simple Workflow Service (Amazon SWF) zuzugreifen. Amazon Simple Workflow Service unterstützt Entwickler beim Erstellen, Ausführen und Skalieren von Hintergrundjobs mit parallel oder sequentiellen Schritten. Sie können sich Amazon SWF als vollständig verwalteten Status-Tracker und Aufgabenkoordinator in der Cloud vorstellen. Wenn die Ausführung der Schritte Ihrer Anwendung mehr als 500 Millisekunden in Anspruch nimmt, Sie den Status der Verarbeitung verfolgen müssen oder wenn Sie eine Aufgabe wiederherstellen oder erneut versuchen müssen, wenn eine Aufgabe fehlschlägt, kann Amazon SWF Ihnen helfen. Weitere Informationen finden Sie unter Amazon Simple Workflow Service.

Häufig gestellte Fragen zu Amazon SWF in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Amazon SWF in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie Folgendes einreichen: Verwaltung | AWS Service | Selbst bereitgestellter Service | Änderungstyp hinzufügen (ct-1w8z66n899dct). Dieser RFC stellt Ihrem Konto `customer_swf_role` die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Amazon SWF in meinem AMS-Konto?

Die `InvokeFunction` Lambda-Berechtigungen wurden in diesen Service aufgenommen. Das AMS`customer_deny_policy`, das allen AMS-Kundenrollen hinzugefügt wird, verweigert jedoch ausdrücklich den Zugriff auf AMS-Lambda-Funktionen und AMS-eigene Ressourcen. Um Ressourcen in Amazon SWF zu kennzeichnen oder die Markierung aufzuheben, reichen Sie einen Änderungstyp Management | Andere | Andere ein.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon SWF in meinem AMS-Konto?

Amazon SWF ist vom AWS Lambda Service abhängig, daher wurden im Rahmen dieser Rolle Berechtigungen zum Aufrufen von Lambda bereitgestellt, und es sind keine zusätzlichen Berechtigungen erforderlich, um Lambda von Amazon SWF aufzurufen. Andernfalls gibt es keine Voraussetzungen für die Verwendung von Amazon SWF.

Verwenden Sie AMS SSP, um Amazon Textract in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Textract zuzugreifen. Amazon Textract ist ein vollständig verwalteter Service für maschinelles Lernen, der automatisch gedruckten Text, Handschriften und andere Daten aus gescannten Dokumenten extrahiert. Er geht über die einfache optische Zeichenerkennung (OCR) hinaus, um Daten aus Formularen und Tabellen zu identifizieren, zu verstehen und zu extrahieren. Weitere Informationen finden Sie unter Amazon Textract.

Häufig gestellte Fragen zu Amazon Textract in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich die Einrichtung von Amazon Textract in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) angeben. Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen zur Verfügung:, und. `customer_textract_console_role` `customer_textract_human_review_execution_role` `customer_ec2_textract_instance_profile` Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle `customer_textract_console_role` in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Nutzung von Amazon Textract in meinem AMS-Konto?

Es gibt keine Einschränkungen für die Verwendung von Amazon Textract in Ihrem AMS-Konto.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Textract in meinem AMS-Konto?

Sie müssen die Erstellung eines S3-Buckets beantragen, indem Sie die folgenden Felder einreichen: RFC Deployment | Advanced Stack Components | S3 storage | Create (ct-1a68ck03fn98r).

Verwenden Sie AMS SSP, um Amazon Transcribe in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Amazon Transcribe zuzugreifen. Amazon Transcribe ist ein vollständig verwalteter und kontinuierlich geschulter automatischer Spracherkennungsdienst, der automatisch Texttranskripte mit Zeitstempel aus Audiodateien generiert. Amazon Transcribe macht es Entwicklern leicht, ihren Anwendungen speech-to-text Funktionen hinzuzufügen. Es ist für Computer praktisch unmöglich, Audiodaten zu suchen und zu analysieren. Daher muss aufgezeichnete Sprache in Text umgewandelt werden, bevor sie in Anwendungen verwendet werden kann. In der Vergangenheit mussten Kunden mit Transkriptionsanbietern zusammenarbeiten, bei denen sie teure Verträge unterzeichnen mussten, und es war schwierig, sie in ihre Technologie-Stacks zu integrieren, um diese Aufgabe zu erfüllen. Viele dieser Anbieter verwenden veraltete Technologien, die sich nicht gut an verschiedene Szenarien anpassen lassen, wie z. B. Telefonaudio mit niedriger Klangqualität, das in Kontaktzentren üblich ist, was zu einer schlechten Genauigkeit führt.

Amazon Transcribe verwendet einen Deep-Learning-Prozess namens automatische Spracherkennung (ASR), um Sprache schnell und präzise in Text umzuwandeln. Amazon Transcribe kann verwendet werden, um Kundendienstanrufe zu transkribieren, Untertitelung und Untertitelung

zu automatisieren und Metadaten für Medienressourcen zu generieren, um ein vollständig durchsuchbares Archiv zu erstellen. Sie können Amazon Transcribe Medical verwenden, um medizinische speech-to-text Funktionen zu klinischen Dokumentationsanwendungen hinzuzufügen. Weitere Informationen finden Sie unter Amazon Transcribe.

Häufig gestellte Fragen zu Amazon Transcribe in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich die Einrichtung von Amazon Transcribe in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) angeben. Dieser RFC stellt Ihrem `customer_transcribe_role` Konto die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Nutzung von Amazon Transcribe in meinem AMS-Konto?

Wenn Sie mit Transcribe arbeiten, müssen Sie „customer-transcribe*“ als Präfix für Ihre Buckets verwenden, sofern RA nicht anders angegeben.

Sie können keine IAM-Rolle in Amazon Transcribe erstellen.

Sie können keinen vom Service verwalteten S3-Bucket für Ausgabedaten in Standard-SSPS verwenden (falls dies erforderlich ist, wenden Sie sich bitte an Ihre Kontozertifizierungsstelle).

Sie müssen die Risikoakzeptanz einreichen, wenn Sie vom Kunden verwaltete KMS-Schlüssel verwenden möchten, die nicht unter den AMS-Namespace fallen.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Amazon Transcribe in meinem AMS-Konto?

S3 muss Zugriff auf die Buckets mit dem Namen „customer-transcribe*“ haben. KMS ist für die Verwendung von Amazon Transcribe erforderlich, wenn Ihre S3-Buckets mit KMS-Schlüsseln verschlüsselt sind. Wenn ein Bucket nicht verschlüsselt werden muss, kann "KMStranscribeAllow“ entfernt werden.

Verwenden Sie AMS SSP, um Amazon WorkSpaces in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf WorkSpaces Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. WorkSpaces ermöglicht Ihnen die

Bereitstellung virtueller, cloudbasierter Microsoft Windows- oder Amazon Linux-Desktops für Ihre Benutzer, bekannt als WorkSpaces. WorkSpaces macht die Beschaffung und Bereitstellung von Hardware oder die Installation komplexer Software überflüssig. Sie können nach Ihren Bedürfnissen Benutzer schnell und bequem hinzufügen oder entfernen. Benutzer greifen auf sie zu, WorkSpaces indem sie eine Client-Anwendung von einem unterstützten Gerät oder, für Windows WorkSpaces, einen Webbrowser verwenden, und melden sich mit ihren vorhandenen lokalen Active Directory (AD) -Anmeldeinformationen an.

Weitere Informationen finden Sie auf Amazon WorkSpaces.

WorkSpaces in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff WorkSpaces auf mein AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_workspaces_console_role` Konto die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung WorkSpaces in meinem AMS-Konto?

Die volle Funktionalität von Workspaces ist mit der von Amazon WorkSpaces selbst bereitgestellten Servicerolle verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung WorkSpaces in meinem AMS-Konto?

- WorkSpaces sind AWS regional begrenzt; daher muss der AD Connector in derselben AWS Region konfiguriert werden, in der die WorkSpaces Instanzen gehostet werden.

  Kunden können mit einer der folgenden beiden Methoden eine Verbindung WorkSpaces zum Kunden-AD herstellen:

  1. Verwenden des AD-Connectors zur Proxyauthentifizierung für den lokalen Active Directory-Dienst (bevorzugt):

     Konfigurieren Sie den Active Directory (AD) Connector in Ihrem AMS-Konto, bevor Sie Ihre WorkSpaces Instanz in Ihren lokalen Verzeichnisdienst integrieren. Der AD Connector fungiert als Proxy für Ihre vorhandenen AD-Benutzer (aus Ihrer Domain), mit denen Sie WorkSpaces

mithilfe vorhandener lokaler AD-Anmeldeinformationen eine Verbindung herstellen können. Dies wird bevorzugt, da sie direkt mit der lokalen Domäne des Kunden verknüpft WorkSpaces sind, die sowohl als Ressourcen- als auch als Benutzergesamtstruktur fungiert, was zu mehr Kontrolle auf Kundenseite führt.

Weitere Informationen finden Sie unter Bewährte Methoden für die Bereitstellung von Amazon WorkSpaces (Szenario 1).

2. Verwenden von AD Connector mit AWS Microsoft AD, Shared Services VPC und einer unidirektionalen Vertrauensstellung für lokale Umgebungen:

   Sie können Benutzer auch mit Ihrem lokalen Verzeichnis authentifizieren, indem Sie zunächst eine unidirektionale ausgehende Vertrauensstellung von AMS-verwaltetem AD zu Ihrem lokalen AD einrichten. WorkSpaces tritt AMS-verwaltetem AD über einen AD Connector bei. WorkSpaces Die Zugriffsberechtigungen werden dann über das von AMS verwaltete AD an die WorkSpaces Instanzen delegiert, ohne dass Sie eine wechselseitige Vertrauensstellung mit Ihrer lokalen Umgebung aufbauen müssen. In diesem Szenario befindet sich die Benutzergesamtstruktur im Kunden-AD und die Ressourcengesamtstruktur im AMS-verwalteten AD (Änderungen am AMS-verwalteten AD können über RFC angefordert werden). Beachten Sie, dass die Konnektivität zwischen WorkSpaces VPC und der MALZ Shared Services VPC, auf der AMS-verwaltetes AD ausgeführt wird, über Transit Gateway hergestellt wird.

   Weitere Informationen finden Sie unter Bewährte Methoden für die Bereitstellung von Amazon WorkSpaces (Szenario 6).

> **Note**
>
> Der AD Connector kann konfiguriert werden, indem ein RFC vom Typ Management | Other | Other | Create Change Type mit den erforderlichen AD-Konfigurationsdetails eingereicht wird. Weitere Informationen finden Sie unter AD Connector erstellen. Wenn Methode 2 verwendet wird, um eine Ressourcengesamtstruktur in AMS-verwaltetem AD zu erstellen, reichen Sie ein weiteres Management | Other | Other | Other | Create Change Type RFC in AMS Shared-Services-Konto ein, indem Sie das von AMS verwaltete AD ausführen.

Verwenden Sie AMS SSP, um AMS Code-Dienste in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem von AMS verwalteten Konto auf die Funktionen der AMS Code-Dienste zuzugreifen. AMS Code Services ist ein firmeneigenes Bündel von AWS-Code-Management-Services, wie im Folgenden beschrieben wird. Sie können wählen, ob Sie alle Services in AMS mit AMS Code-Services oder einzeln in AMS bereitstellen möchten.

Die AMS Code-Dienste umfassen die folgenden Dienste:

- AWS CodeCommit: Ein vollständig verwalteter Quellcodeverwaltungsdienst, der sichere Git-basierte Repositorys hostet. Dadurch können Teams in einem sicheren und hoch skalierbaren Ökosystem gemeinsam an Code arbeiten. CodeCommit macht es überflüssig, Ihr eigenes Quellcodeverwaltungssystem zu betreiben oder sich Gedanken über die Skalierung der Infrastruktur zu machen. Sie können CodeCommit auch zum sicheren Aufbewahren beliebiger Objekte von Quellcode bis hin zu Binärdateien verwenden. Außerdem wird das reibungslose Arbeiten mit vorhandenen Git-basierten Tools ermöglicht. Weitere Informationen hierzu finden Sie unter AWS CodeCommit.

  Informationen zur Bereitstellung in Ihrem AMS-Konto unabhängig von den AMS Code-Diensten finden Sie unterVerwenden Sie AMS SSP zur Bereitstellung AWS CodeCommit in Ihrem AMS-Konto.
- AWS CodeBuild: Ein vollständig verwalteter Dienst für kontinuierliche Integration, der Quellcode kompiliert, Tests durchführt und Softwarepakete erstellt, die sofort einsatzbereit sind. Mit CodeBuild müssen Sie Ihre eigenen Build-Server nicht bereitstellen, verwalten und skalieren. CodeBuild skaliert kontinuierlich und verarbeitet mehrere Builds gleichzeitig, sodass Ihre Builds nicht in einer Warteschlange warten müssen. Mit den vorkonfigurierten Build-Umgebungen gelingt der Einstieg leicht. Jedoch können Sie auch benutzerdefinierte Build-Umgebungen mit Ihren eigenen Entwicklungstools erstellen. Mit CodeBuild werden Ihnen die von Ihnen genutzten Rechenressourcen minutengenau berechnet. Weitere Informationen hierzu finden Sie unter AWS CodeBuild.

  Informationen zur Bereitstellung in Ihrem AMS-Konto unabhängig von den AMS Code-Diensten finden Sie unterVerwenden Sie AMS SSP zur Bereitstellung AWS CodeBuild in Ihrem AMS-Konto.
- AWS CodeDeploy: Ein vollständig verwalteter Bereitstellungsservice, der Softwarebereitstellungen für eine Vielzahl von Rechendiensten wie Amazon EC2 und Ihren lokalen Servern automatisiert.

AWS CodeDeploy unterstützt Sie bei der schnellen Veröffentlichung neuer Funktionen, hilft Ihnen, Ausfallzeiten bei der Anwendungsbereitstellung zu vermeiden, und bewältigt die Komplexität der Aktualisierung Ihrer Anwendungen. Sie können AWS CodeDeploy es verwenden, um Softwarebereitstellungen zu automatisieren, sodass fehleranfällige manuelle Operationen überflüssig werden. Der Service lässt sich an Ihre Bereitstellungsanforderungen anpassen. Weitere Informationen hierzu finden Sie unter AWS CodeDeploy.

Informationen zur Bereitstellung in Ihrem AMS-Konto unabhängig von den AMS Code-Diensten finden Sie unterVerwenden Sie AMS SSP zur Bereitstellung AWS CodeDeploy in Ihrem AMS-Konto.

- AWS CodePipeline: Ein vollständig verwalteter Continuous Delivery-Service, der Sie bei der Automatisierung Ihrer Release-Pipelines für schnelle und zuverlässige Anwendungs- und Infrastrukturupdates unterstützt. CodePipeline automatisiert die Erstellungs-, Test- und Bereitstellungsphasen Ihres Release-Prozesses bei jeder Codeänderung auf der Grundlage des von Ihnen definierten Release-Modells. Auf diese Weise können Sie Funktionen und Updates schnell und zuverlässig bereitstellen. Sie können problemlos Dienste von Drittanbietern wie GitHub oder Ihr eigenes benutzerdefiniertes Plugin integrieren AWS CodePipeline . Mit zahlen Sie nur für das AWS CodePipeline, was Sie nutzen. Es fallen keine Vorausleistungen an und Sie gehen keine langfristigen Verpflichtungen ein. Weitere Informationen hierzu finden Sie unter AWS CodePipeline.

  Informationen zur Bereitstellung in Ihrem AMS-Konto unabhängig von den AMS Code-Diensten finden Sie unterVerwenden Sie AMS SSP zur Bereitstellung AWS CodePipeline in Ihrem AMS-Konto.

Häufig gestellte Fragen zu AMS-Code-Services in AWS Managed Services

F: Wie beantrage ich Zugriff auf AMS Code-Services in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_code_suite_console_role` Konto die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihrer Verbundlösung integrieren. Zu diesem Zeitpunkt wird AMS Operations auch die`customer_codebuild_service_role`,`customer_codedeploy_service_role`, `aws_code_pipeline_service_role` Servicerollen in Ihrem Konto für CodeBuild CodeDeploy und CodePipeline Services bereitstellen. Wenn zusätzliche IAM-Berechtigungen für die erforderlich sind, reichen Sie eine AMS-Serviceanfrage ein. `customer_codebuild_service_role`

> **Note**
>
> Sie können diese Dienste auch separat hinzufügen. Weitere Informationen finden Sie unter Verwenden Sie AMS SSP zur Bereitstellung AWS CodeBuild in Ihrem AMS-Konto Verwenden Sie AMS SSP zur Bereitstellung AWS CodeDeploy in Ihrem AMS-KontoVerwenden Sie AMS SSP zur Bereitstellung AWS CodePipeline in Ihrem AMS-Konto, bzw..

F: Welche Einschränkungen gelten für die Nutzung der AMS Code-Dienste in meinem AMS-Konto?

- AWS CodeCommit: Die Trigger-Funktion CodeCommit ist aufgrund der damit verbundenen Rechte zum Erstellen von SNS-Themen deaktiviert. Die direkte Authentifizierung gegen CodeCommit ist eingeschränkt. Benutzer sollten sich mit Credential Helper authentifizieren. Einige KMS-Befehle sind ebenfalls eingeschränkt: kms: Encrypt, kms: Decrypt,,, und kms:ReEncrypt. kms: GenereteDataKey kms: GenerateDataKeyWithoutPlaintext kms: DescribeKey
- CodeBuild: Für den Zugriff auf AWS CodeBuild Konsolenadministratoren sind die Berechtigungen auf Ressourcenebene beschränkt. CloudWatch Aktionen sind beispielsweise auf bestimmte Ressourcen beschränkt und die `iam:PassRole` Berechtigungen werden kontrolliert.
- CodeDeploy: CodeDeploy Unterstützt derzeit nur Bereitstellungen auf Amazon EC2 /On-Premises. Bereitstellungen auf ECS und Lambda werden nicht CodeDeploy unterstützt.
- CodePipeline: CodePipeline Funktionen, Stufen und Anbieter sind auf Folgendes beschränkt:
  - Bereitstellungsphase: Amazon S3 und AWS CodeDeploy
  - Quellstufe: Amazon S3 AWS CodeCommit, Bit Bucket und GitHub
  - Build-Phase: AWS CodeBuild und Jenkins
  - Genehmigungsphase: Amazon SNS
  - Testphase: Jenkins AWS CodeBuild, Ghost Inspector UI-Tests BlazeMeter, Micro Focus StormRunner Load, Runscope API-Überwachung
  - Invoke Stage: Step Functions und Lambda

  > **Note**
  >
  > AMS Operations stellt das `customer_code_pipeline_lambda_policy` in Ihrem Konto bereit. Es muss mit der Lambda-Ausführungsrolle für die Lambda-Aufrufphase verknüpft werden. Geben Sie den service/execution Lambda-Rollennamen an, mit dem Sie diese Richtlinie hinzufügen möchten. Wenn es keine

benutzerdefinierte service/execution Lambda-Rolle gibt, erstellt AMS eine neue Rolle mit dem Namen`customer_code_pipeline_lambda_execution_role`, das ist eine Kopie von `customer_lambda_basic_execution_role` zusammen mit`customer_code_pipeline_lambda_policy`.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung der AMS Code-Dienste in meinem AMS-Konto?

- CodeCommit: Wenn S3-Buckets mit AWS KMS Schlüsseln verschlüsselt AWS KMS sind, müssen S3 verwendet AWS CodeCommit werden.
- CodeBuild: Wenn zusätzliche IAM-Berechtigungen für die definierte AWS CodeBuild Servicerolle erforderlich sind, fordern Sie diese über eine AMS-Serviceanfrage an.
- CodeDeploy: Keine.
- CodePipeline: Keine. AWS unterstützte Dienste—AWS CodeCommit AWS CodeBuild,, AWS CodeDeploy—müssen vor oder zusammen mit dem Start von CodePipeline gestartet werden. Dies wird jedoch von einem AMS-Techniker durchgeführt.

Verwenden Sie AMS SSP zur Bereitstellung AWS Amplify in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Amplify Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. Dabei AWS Amplify handelt es sich um eine Komplettlösung, mit der Frontend-Web- und Mobilentwickler auf einfache Weise Full-Stack-Anwendungen erstellen, verbinden und hosten können. Amplify bietet Flexibilität, um die Bandbreite der AWS Dienste zu nutzen, wenn sich Ihre Anwendungsfälle weiterentwickeln. Amplify bietet Produkte zur Erstellung von Fullstack-Apps für iOS, Android, Flutter, Web und React Native. Weitere Informationen hierzu finden Sie unter AWS Amplify.

AWS Amplify in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich AWS Amplify die Einrichtung in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen.

Dieser RFC stellt Ihrem `customer_amplify_console_role` Konto die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung für Ihr Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

Darüber hinaus müssen Sie eine Risikoakzeptanz angeben, da es AWS Amplify über Berechtigungen verfügt, die die Infrastruktur verändern. Arbeiten Sie dazu mit Ihrem Cloud Service Delivery Manager (CSDM) zusammen.

F: Welche Einschränkungen gelten für die Nutzung AWS Amplify in meinem AMS-Konto?

Sie müssen es `'amplify*'` als Präfix für Ihre Buckets verwenden, wenn Sie mit Amplify arbeiten, sofern RA nicht anders angegeben.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Amplify in meinem AMS-Konto?

Es gibt keine Voraussetzungen für die Nutzung von AWS Amplify in Ihrem AMS-Konto.

Nur Malz-Umgebungen: Die integrierte Standardrolle für Amplify ist „customer_amplify_console_role“. Um eine benutzerdefinierte Rolle zu verwenden, stellen Sie zunächst die IAM-Entitäten bereit. Erstellen Sie dann einen zusätzlichen RFC, um Ihre benutzerdefinierte Rolle zur Zulassungsliste der Service Control-Richtlinie für Anwendungskonten hinzuzufügen.

Verwenden Sie AMS SSP für die Bereitstellung AWS AppSync

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS AppSync Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS AppSync vereinfacht die Anwendungsentwicklung, indem Sie eine flexible API erstellen können, mit der Sie sicher auf Daten aus einer oder mehreren Datenquellen zugreifen, diese bearbeiten und kombinieren können. AWS AppSync ist ein verwalteter Dienst, der GraphQL verwendet, um es Anwendungen zu erleichtern, genau die Daten zu erhalten, die sie benötigen.

Mit AWS AppSync können Sie skalierbare Anwendungen, einschließlich solcher, die Aktualisierungen in Echtzeit erfordern, auf einer Reihe von Datenquellen wie NoSQL-Datenspeichern, relationalen Datenbanken APIs, HTTP und Ihren benutzerdefinierten Datenquellen erstellen. AWS Lambda Für mobile Apps und Web-Apps bietet es AWS AppSync zusätzlich lokalen Datenzugriff, wenn Geräte offline gehen, und Datensynchronisierung mit anpassbarer Konfliktlösung, wenn sie wieder online sind. Weitere Informationen hierzu finden Sie unter AWS AppSync.

AWS AppSync in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS AppSync auf mein AMS-Konto?

Beantragen Sie den Zugriff, indem Sie Folgendes einreichen: Verwaltung | AWS Service | Selbst bereitgestellter Service | Änderungstyp hinzufügen (ct-1w8z66n899dct). Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen zur Verfügung: und. `customer_appsync_service_role` `customer_appsync_author_role` Nach der Bereitstellung in Ihrem Konto müssen Sie sie `customer_appsync_author_role` in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der AWS AppSync Nutzung von?

- Beim Erstellen einer Datenquelle für AppSync den Kunden muss die zuvor erstellte Servicerolle angegeben werden. Die Erstellung einer neuen Rolle ist nicht zulässig. Daher wird der Zugriff verweigert zurückgegeben
- AppSync Rollen sind so konfiguriert, dass Berechtigungen auf Ressourcen beschränkt werden, die die Präfixe „AMS-“ oder „MC-“ enthalten, um jegliche Änderungen an der AMS-Infrastruktur zu verhindern.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung AWS AppSync?

Der Dienst ermöglicht die Verwendung mehrerer anderer Dienste als Datenquelle.
Die Grundberechtigungen, sie als solche zu verwenden, sind in der Dienstrolle (`customer_appsync_service_role`) enthalten, aber Sie müssen die Servicerolle manuell auswählen, wenn Sie den Dienst verwenden.

Verwenden Sie AMS SSP zur Bereitstellung AWS App Mesh in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS App Mesh Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS App Mesh bietet Netzwerke auf Anwendungsebene, sodass Ihre Dienste über verschiedene Arten von Computerinfrastrukturen hinweg einfach miteinander kommunizieren können. App Mesh standardisiert die Art und Weise, wie Ihre Dienste kommunizieren, bietet Ihnen end-to-end Transparenz und gewährleistet eine hohe Verfügbarkeit Ihrer Anwendungen.

AWS App Mesh macht es einfach, Dienste auszuführen, indem es konsistente Transparenz und Netzwerkverkehrskontrollen für Dienste bietet, die auf mehreren Arten von Computerinfrastrukturen basieren. App Mesh macht es überflüssig, den Anwendungscode zu aktualisieren, um zu ändern, wie Überwachungsdaten gesammelt oder der Datenverkehr zwischen Diensten weitergeleitet wird. App Mesh konfiguriert jeden Dienst für den Export von Überwachungsdaten und implementiert eine konsistente Kommunikationssteuerungslogik in Ihrer gesamten Anwendung. Dies macht es einfach, schnell den genauen Ort von Fehlern zu lokalisieren und den Netzwerkverkehr automatisch umzuleiten, wenn es zu Ausfällen kommt oder wenn Codeänderungen implementiert werden müssen. Weitere Informationen hierzu finden Sie unter AWS App Mesh.

AWS App Mesh in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS App Mesh auf mein AMS-Konto?

Beantragen Sie den Zugriff, indem Sie Folgendes einreichen: Verwaltung | AWS Service | Selbst bereitgestellter Service | Änderungstyp hinzufügen (ct-1w8z66n899dct). Dieser RFC stellt Ihrem Konto `customer_app_mesh_console_role` die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der AWS App Mesh Nutzung von?

Die volle Funktionalität von AWS App Mesh ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS App Mesh?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Verwendung AWS App Mesh in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Audit Manager in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Audit Manager zuzugreifen. Audit Manager hilft Ihnen dabei, Ihre AWS Nutzung kontinuierlich zu überprüfen, um die Bewertung von Risiken und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen. Audit Manager automatisiert die Sammlung von Beweisen, um die Bewertung zu erleichtern, ob Ihre Richtlinien, Verfahren und Aktivitäten effektiv funktionieren. Wenn es Zeit für ein Audit ist, hilft Ihnen Audit Manager dabei, die

Überprüfung Ihrer Kontrollen durch Interessengruppen zu verwalten und revisionstaugliche Berichte mit deutlich weniger manuellem Aufwand zu erstellen. Weitere Informationen finden Sie unter Audit Manager.

AWS Audit Manager in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS Audit Manager auf mein AMS-Konto?

Sie können den Zugriff beantragen, indem Sie die folgenden Felder einreichen: AWS Services RFC Management | AWS-Service | Self-Provisioned Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny). Dieser RFC `customer-audit-manager-admin-Role` stellt die folgende IAM-Rolle in Ihrem Konto bereit:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihrer Verbundlösung integrieren.

F: Welche Einschränkungen gibt es bei der Nutzung AWS Audit Manager?

Es gibt keine Einschränkungen für die Verwendung von AWS Audit Manager in Ihrem AMS-Konto. Die volle Funktionalität für AWS Audit Manager wird bereitgestellt.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung AWS Audit Manager?

1. Sie müssen AMS den S3-Bucket zur Verfügung stellen, in dem Sie sich befinden reports/assessments möchten.
2. Wenn Sie den Dienst verschlüsseln möchten, müssen Sie AMS den zu verwendenden KMS-CMK-ARN zur Verfügung stellen.
3. Wenn Sie eine SNS-Benachrichtigung an ein Thema senden möchten, müssen Sie den Namen des Themas oder ARN angeben.
4. (Optional) Wenn Sie Organizations als Teil Ihrer Multi-Account-Landingzone in Audit Manager aktivieren möchten und ein delegiertes Administratorkonto wünschen, gibt es eine zusätzliche Voraussetzung: Geben Sie im Beschreibungsfeld für RFC (Management | AWS Service | Compatible Service| Add) an, dass Sie das delegierte Administratorkonto als Teil des Audit Manager Manager-Setups verwenden möchten, und geben Sie die folgenden Details an:
   - KMS CMK ARN (ursprünglich zur Einrichtung von Audit Manager verwendet)
   - Delegierte Administratorkonto-ID für Audit Manager zur Verwendung als Teil dieser landing zone mit mehreren Konten (kann ein MALZ-Anwendungskonto sein)

Verwenden Sie AMS SSP zur Bereitstellung AWS Batch in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Batch Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Batch ermöglicht Entwicklern, Wissenschaftlern und Ingenieuren die einfache und effiziente Ausführung von Hunderttausenden von Batch-Computing-Jobs. AWS AWS Batch stellt dynamisch die optimale Menge und Art der Rechenressourcen (wie CPU- oder speicheroptimierte Instances) bereit, basierend auf dem Volumen und den spezifischen Ressourcenanforderungen der eingereichten Batch-Jobs. Mit müssen Sie keine Batch-Computing-Software oder Servercluster AWS Batch, die Sie für die Ausführung Ihrer Jobs verwenden, installieren und verwalten, sodass Sie sich auf die Analyse der Ergebnisse und die Lösung von Problemen konzentrieren können. Weitere Informationen hierzu finden Sie unter AWS Batch.

AWS Batch in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS Batch auf mein AMS-Konto?

1. Um Zugriff auf zu beantragen AWS Batch, reichen Sie RFC Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) ein. Dieser RFC stellt die folgenden IAM-Rollen und -Richtlinien in Ihrem Konto bereit:

IAM-Rollen:

- `customer_batch_console_role`
- `customer_batch_ecs_instance_role`
- `customer_batch_events_service_role`
- `customer_batch_service_role`
- `customer_batch_ecs_task_role`

Richtlinien:

- `customer_batch_console_role_policy`
- `customer_batch_service_role_policy`

- `customer_batch_events_service_role_policy`

2. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle `customer_batch_console_role` in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gibt es bei der Nutzung AWS Batch?

Bei der Erstellung der Compute-Umgebung sollten Sie EC2 Instanzen als „customer_batch“ oder „customer-batch“ kennzeichnen. Wenn die Instanzen nicht markiert sind, werden die Instanzen nicht per Batch beendet, wenn der Job abgeschlossen ist.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung AWS Batch?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Verwendung AWS Batch in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Certificate Manager in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf die Funktionen AWS Certificate Manager (ACM) in Ihrem verwalteten AMS-Konto zuzugreifen. AWS Certificate Manager ist ein Dienst, mit dem Sie öffentliche und private Secure Sockets Layer/Transport Layer Security (SSL/TLS) -Zertifikate zur Verwendung mit AWS Diensten und Ihren internen verbundenen Ressourcen bereitstellen, verwalten und bereitstellen können. SSL/TLS Zertifikate werden verwendet, um die Netzwerkkommunikation zu sichern und die Identität von Websites im Internet sowie von Ressourcen in privaten Netzwerken nachzuweisen. AWS Certificate Manager macht den zeitaufwändigen manuellen Prozess des Kaufs, Hochladens und SSL/TLS Erneuerns von Zertifikaten überflüssig.

Mit AWS Certificate Manager können Sie ein Zertifikat anfordern, es auf ACM-integrierten AWS Ressourcen wie Elastic Load Balancers, CloudFront Amazon-Distributionen und APIs auf API Gateway bereitstellen und die Verlängerung von Zertifikaten übernehmen lassen AWS Certificate Manager . Außerdem können Sie damit private Zertifikate für Ihre internen Ressourcen erstellen und den Lebenszyklus von Zertifikaten zentral verwalten. Öffentliche und private Zertifikate, die AWS Certificate Manager für die Verwendung mit ACM-integrierten Diensten bereitgestellt werden, sind kostenlos. Sie zahlen nur für die AWS Ressourcen, die Sie für die Ausführung Ihrer Anwendung erstellen. Mit AWS Private Certificate Authorityzahlen Sie monatlich für den Betrieb der AWS Private CA und für die privaten Zertifikate, die Sie ausstellen. Weitere Informationen finden Sie unter AWS Certificate Manager — AWS Dokumentation.

Häufig gestellte Fragen zu ACM in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS Certificate Manager auf mein AMS-Konto?

Beantragen Sie den Zugriff, indem Sie Folgendes einreichen: Verwaltung | AWS Service | Selbst bereitgestellter Service | Änderungstyp hinzufügen (ct-1w8z66n899dct). Dieser RFC stellt Ihrem Konto `customer_acm_create_role` die folgende IAM-Rolle zur Verfügung:. Sie können diese Rolle verwenden, um ACM-Zertifikate zu erstellen und zu verwalten. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

ACM-Zertifikate können mit den folgenden Änderungstypen erstellt werden, auch wenn Sie die `customer_acm_create_role` IAM-Rolle nicht hinzugefügt haben:

- ACM | Öffentliches Zertifikat erstellen
- ACM | Privates Zertifikat erstellen
- ACM-Zertifikat mit zusätzlichem | Erstellen SANs

F: Was sind die Einschränkungen bei der AWS Certificate Manager Verwendung von?

Sie müssen eine Änderungsanforderung (Request for Change, RFC) an AMS senden, um bestehende Zertifikate zu löschen oder zu ändern, da diese Aktionen vollen Administratorzugriff erfordern (verwenden Sie den Änderungstyp Verwaltung | Andere | Andere | Aktualisierung (ct-0xdawir96cy7k). Beachten Sie, dass die IAM-Richtlinie Rechte, die auf Tagnamen (mc*, ams* usw.) basieren, nicht ausschließen kann. Für Zertifikate fallen keine Kosten an, daher ist das Löschen unbenutzter Zertifikate nicht zeitaufwändig.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Certificate Manager?

Bestehender öffentlicher DNS-Name und Zugriff zum Erstellen von DNS-CNAME-Einträgen, diese müssen jedoch nicht im verwalteten Konto gehostet werden.

Verwenden Sie AMS SSP zur Bereitstellung AWS Private Certificate Authority in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Private Certificate Authority Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. Private Zertifikate werden zur Identifizierung und Sicherung der Kommunikation zwischen verbundenen Ressourcen

in privaten Netzwerken wie Servern, Mobil- und IoT-Geräten und -Anwendungen verwendet. AWS Private CA ist ein verwalteter privater CA-Dienst, mit dem Sie den Lebenszyklus Ihrer privaten Zertifikate einfach und sicher verwalten können. AWS Private CA bietet Ihnen einen hochverfügbaren Service für private Zertifizierungsstellen ohne die Vorabinvestitionen und laufenden Wartungskosten für den Betrieb Ihrer eigenen privaten Zertifizierungsstelle. AWS Private CA erweitert die Zertifikatsverwaltungsfunktionen von ACM auf private Zertifikate, sodass Sie öffentliche und private Zertifikate zentral erstellen und verwalten können. Mithilfe der AWS Management Console oder der ACM-API können Sie ganz einfach private Zertifikate für Ihre AWS Ressourcen erstellen und bereitstellen. Für EC2 Instances, Container, IoT-Geräte und lokale Ressourcen können Sie ganz einfach private Zertifikate erstellen und verfolgen und sie mit Ihrem eigenen clientseitigen Automatisierungscode bereitstellen. Sie haben auch die Flexibilität, private Zertifikate zu erstellen und diese für Anwendungen, die benutzerdefinierte Gültigkeitsdauer von Zertifikaten, Schlüsselalgorithmen oder Ressourcennamen erfordern, selbst zu verwalten. Weitere Informationen finden Sie unter. AWS Private CA

AWS Private CA in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS Private CA auf mein AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den AWS Services-RFC (Management | AWS Service | Compatible Service) einreichen. Über diesen RFC wird Ihrem Konto die folgende IAM-Rolle zugewiesen:. `customer_acm_pca_role` Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der AWS Private CA Nutzung von?

Derzeit kann AWS Resource Access Manager (AWS RAM) nicht verwendet werden, um Ihr AWS Private CA Cross-Konto zu teilen.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Private CA?

1. Wenn Sie eine CRL erstellen möchten, benötigen Sie einen S3-Bucket, in dem Sie sie speichern können. AWS Private CA hinterlegt die CRL automatisch in dem von Ihnen Amazon S3 S3-Bucket und aktualisiert sie regelmäßig. Es ist eine Voraussetzung, dass für den S3-Bucket die unten angegebene Bucket-Richtlinie gilt, bevor Sie eine CRL einrichten können. Um mit dieser Anfrage fortzufahren, erstellen Sie einen RFC mit ct-0fpjlxa808sh2 (Verwaltung | Erweiterte Stack-Komponenten | S3-Speicher | Aktualisierungsrichtlinie) wie folgt:

- Geben Sie den S3-Bucket-Namen oder den ARN an.
- Kopieren Sie die folgende Richtlinie auf RFC und `bucket-name` ersetzen Sie sie durch den gewünschten S3-Bucket-Namen.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"acm-pca.amazonaws.com"
         },
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetBucketAcl",
            "s3:GetBucketLocation"
         ],
         "Resource":[
            "arn:aws:s3:::bucket-name/*",
            "arn:aws:s3:::bucket-name"
         ]
      }
   ]
}
```

2. Wenn der obige S3-Bucket verschlüsselt ist, benötigt der Service Principal acm-pca.amazonaws.com Berechtigungen zum Entschlüsseln. Um mit dieser Anfrage fortzufahren, erstellen Sie einen RFC mit ct-3ovo7px2vsa6n (Management | Erweiterte Stack-Komponenten | KMS-Schlüssel | Update) wie folgt:

- Geben Sie den KMS-Schlüssel-ARN an, für den die Richtlinie aktualisiert werden muss.
- Kopieren Sie die folgende Richtlinie auf RFC und `bucket-name` ersetzen Sie sie durch den gewünschten S3-Bucket-Namen.

```
{
```

```
   "Sid":"Allow ACM-PCA use of the key",
   "Effect":"Allow",
   "Principal":{
      "Service":"acm-pca.amazonaws.com"
   },
   "Action":[
      "kms:GenerateDataKey",
      "kms:Decrypt"
   ],
   "Resource":"*",
   "Condition":{
      "StringLike":{
         "kms:EncryptionContext:aws:s3:arn":[
            "arn:aws:s3:::bucket_name/acm-pca-permission-test-key",
            "arn:aws:s3:::bucket_name/acm-pca-permission-test-key-private",
            "arn:aws:s3:::bucket_name/audit-report/*",
            "arn:aws:s3:::bucket_name/crl/*"
         ]
      }
   }
}
```

3. AWS Private CA CRLs unterstützt die S3-Einstellung „Öffentlichen Zugriff auf Buckets und Objekte blockieren, die über neue Zugriffskontrolllisten gewährt wurden (ACLs)“ nicht. Sie müssen diese Einstellung für das S3-Konto und den AWS Private CA Bucket deaktivieren, damit sie schreiben können, CRLs wie unter So erstellen und speichern Sie Ihre CRL für ACM Private CA sicher beschrieben. Wenn Sie deaktivieren möchten, erstellen Sie einen neuen RFC mit ct-0xdawir96cy7k (Verwaltung | Andere | Andere | Update) und fügen Sie eine Risikoakzeptanz hinzu. Wenn Sie Fragen zur Risikoakzeptanz haben, wenden Sie sich an Ihren Cloud Architect.

Verwenden Sie AMS SSP zur Bereitstellung AWS CloudEndure in Ihrem AMS-Konto

> **Note**
>
> Nach dem erfolgreichen Start von AWS Application Migration Service ist der CloudEndure Migrationsdienst nun in allen AWS Regionen nicht mehr verfügbar. Wir empfehlen unseren Kunden, ihn AWS Application Migration Service für Lift-and-Shift-Migrationen in GovCloud Regionen und in kommerzielle Regionen zu nutzen. Weitere Informationen finden Sie unter Was ist? AWS Application Migration Service .

Wenn Sie die verwenden möchten AWS Application Migration Service, wenden Sie sich an Ihre CA, damit sie Ihnen weiterhelfen kann.

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS CloudEndure Funktionen in Ihrem AMS-verwalteten Konto zuzugreifen. AWS CloudEndure Die Migration vereinfacht, beschleunigt und automatisiert umfangreiche Migrationen von physischer, virtueller und cloudbasierter Infrastruktur zu. AWS CloudEndure Disaster Recovery (DR) schützt vor Ausfallzeiten und Datenverlust aufgrund beliebiger Bedrohungen, einschließlich Ransomware und Serverbeschädigung.

AWS CloudEndure in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf CloudEndure in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_cloud_endure_user` Konto den folgenden IAM-Benutzer zur Verfügung:. Nachdem es in Ihrem Konto bereitgestellt wurde, werden der Zugriffsschlüssel und der geheime Schlüssel für den Benutzer in AWS Secrets Manager geteilt.

Diese Richtlinien werden auch für das Konto bereitgestellt: `customer_cloud_endure_policy` und. `customer_cloud_endure_deny_policy`

Darüber hinaus müssen Sie eine Risikoakzeptanz angeben, da die CloudEndure DR-Lösung für die Anwendungsintegration über Berechtigungen verfügt, die die Infrastruktur verändern. Arbeiten Sie dazu mit Ihrem Cloud Service Delivery Manager (CSDM) zusammen.

F: Welche Einschränkungen gelten für die Nutzung CloudEndure in meinem AMS-Konto?

Die Cloud-fähigen Replikations- und Konvertierungsinstanzen können nur in dem von Ihnen angegebenen Subnetz gestartet werden.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung CloudEndure in meinem AMS-Konto? Teilen Sie Folgendes über die bidirektionale RFC-Korrespondenz mit:

- VPC-Subnetzdetails für Replikations- und Konvertierungsinstanzen, die gestartet werden sollen.
- Der KMS-Schlüssel Amazon Resource Name (ARN), wenn die EBS-Volumes verschlüsselt sind.

Verwenden Sie AMS SSP zur Bereitstellung AWS CloudHSM in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS CloudHSM Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS CloudHSM hilft Ihnen dabei, die unternehmensinternen, vertraglichen und behördlichen Compliance-Anforderungen an die Datensicherheit zu erfüllen, indem spezielle Hardware Security Module (HSM) -Instanzen in der Cloud verwendet werden. AWS AWS, und AWS Marketplace-Partner bieten eine Vielzahl von Lösungen zum Schutz sensibler Daten innerhalb der AWS Plattform an. Für einige Anwendungen und Daten, die vertraglichen oder behördlichen Vorschriften zur Verwaltung kryptografischer Schlüssel unterliegen, kann jedoch zusätzlicher Schutz erforderlich sein. AWS CloudHSM ergänzt bestehende Datenschutzlösungen und ermöglicht es Ihnen, Ihre darin enthaltenen Verschlüsselungscodes zu schützen HSMs , die nach staatlichen Standards für sicheres Schlüsselmanagement entwickelt und validiert wurden. AWS CloudHSM ermöglicht es Ihnen, kryptografische Schlüssel, die für die Datenverschlüsselung verwendet werden, sicher zu generieren, zu speichern und zu verwalten, sodass nur Sie auf die Schlüssel zugreifen können. Weitere Informationen hierzu finden Sie unter AWS CloudHSM.

AWS CloudHSM in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS CloudHSM auf mein AMS-Konto?

Die Nutzung von in Ihrem AMS-Konto erfolgt in zwei Schritten:

1. Fordern Sie einen AWS CloudHSM Cluster an. Reichen Sie dazu einen RFC mit dem Änderungstyp Management | Other | Other | Create (ct-1e1xtak34nx76) ein. Geben Sie die folgenden Details an:
   - AWS Region.
   - ID/ARN. Provide a VPC ID/VPCVPC-ARN, der sich in demselben Konto befindet wie der RFC, den Sie einreichen.
   - Geben Sie mindestens zwei Availability Zones für den Cluster an.
   - EC2 Amazon-Instance-ID, die eine Verbindung zum HSM-Cluster herstellt.
2. Greifen Sie auf die AWS CloudHSM Konsole zu. Senden Sie dazu einen RFC mit dem Änderungstyp Management | AWS Service | Self-Provisioned Service | Add (ct-1w8z66n899dct).

Dieser RFC stellt Ihrem `customer_cloudhsm_console_role` Konto die folgende IAM-Rolle zur Verfügung:.

Nachdem die Rolle in Ihrem Konto bereitgestellt wurde, müssen Sie sie in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS CloudHSM in meinem AMS-Konto?

Der Zugriff auf die AWS CloudHSM Konsole bietet Ihnen nicht die Möglichkeit, Ihren Cluster zu erstellen, zu beenden oder wiederherzustellen. Um diese Dinge zu tun, reichen Sie den Änderungstyp Management | Andere | Andere | Änderungstyp erstellen (ct-1e1xtak34nx76) ein.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung in meinem AMS-Konto? AWS CloudHSM

Sie müssen TCP-Verkehr über Port 2225 über eine EC2 Amazon-Client-Instance innerhalb einer VPC zulassen oder Direct Connect VPN für lokale Server verwenden, die auf den HSM-Cluster zugreifen möchten. AWS CloudHSM ist in Bezug auf Sicherheitsgruppen und Netzwerkschnittstellen von Amazon EC2 abhängig. Für die Überwachung oder Prüfung von Protokollen stützt sich HSM auf CloudTrail (AWS API-Operationen) und CloudWatch Protokolle für alle lokalen HSM-Geräteaktivitäten.

F: Wer installiert Updates für den AWS CloudHSM Client und die zugehörigen Softwarebibliotheken?

Sie sind für die Installation der Bibliotheks- und Client-Updates verantwortlich. Sie sollten die Seite mit dem Versionsverlauf von CloudHSM auf Releases überprüfen und dann Updates mithilfe des CloudHSM-Client-Upgrades anwenden.

> **Note**
>
> Software-Patches für die HSM-Appliance werden vom Service immer automatisch angewendet. AWS CloudHSM

Verwenden Sie AMS SSP zur Bereitstellung AWS CodeBuild in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS CodeBuild Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS CodeBuild ist ein vollständig

verwalteter Continuous Integration Service, der Quellcode kompiliert, Tests durchführt und Softwarepakete erstellt, die sofort einsatzbereit sind. Mit CodeBuild müssen Sie Ihre eigenen Build-Server nicht bereitstellen, verwalten und skalieren. CodeBuild skaliert kontinuierlich und verarbeitet mehrere Builds gleichzeitig, sodass Ihre Builds nicht in einer Warteschlange warten müssen. Mit den vorkonfigurierten Build-Umgebungen gelingt der Einstieg leicht. Jedoch können Sie auch benutzerdefinierte Build-Umgebungen mit Ihren eigenen Entwicklungstools erstellen. Mit CodeBuild werden Ihnen die von Ihnen genutzten Rechenressourcen minutengenau berechnet. Weitere Informationen hierzu finden Sie unter AWS CodeBuild.

> **Note**
>
> Um CodeCommit, CodeBuild, und CodePipeline mit einem einzigen RFC zu integrieren CodeDeploy, reichen Sie den Änderungstyp Management | AWS Service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) ein und fordern Sie die drei Services an:, und. CodeBuild CodeDeploy CodePipeline Anschließend werden alle drei Rollen,, und in Ihrem Konto bereitgestellt. `customer_codebuild_service_role` `customer_codedeploy_service_role` `aws_code_pipeline_service_role` Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihrer Verbundlösung integrieren.

CodeBuild in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS CodeBuild auf mein AMS-Konto?

Die Nutzung von AWS CodeBuild in Ihrem AMS-Konto erfolgt in zwei Schritten:

1. Bereitstellung des `CodeBuild Service Role` For-Build-Prozesses zur Koordination mit AWS S3-Buckets, Amazon CloudWatch und Log-Gruppen
2. Fordern Sie Zugriff auf die Konsole an CodeBuild

Sie können beantragen, dass beide in Ihrem AMS-Konto eingerichtet werden, indem Sie einen RFC an Management | AWS Service | Self-Provisioned Service | Änderungstyp hinzufügen senden (ct-1w8z66n899dct). Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS CodeBuild in meinem AMS-Konto?

Für den Zugriff auf AWS CodeBuild Konsolenadministratoren sind die Berechtigungen auf Ressourcenebene beschränkt. CloudWatch Aktionen sind beispielsweise auf bestimmte Ressourcen beschränkt und die `iam:PassRole` Berechtigungen werden kontrolliert.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung CodeBuild in meinem AMS-Konto?

Wenn zusätzliche IAM-Berechtigungen für die definierte AWS CodeBuild Servicerolle erforderlich sind, fordern Sie diese über eine AMS-Serviceanfrage an.

Verwenden Sie AMS SSP zur Bereitstellung AWS CodeCommit in Ihrem AMS-Konto

> **Note**
>
> AWS hat mit Wirkung zum 25. Juli 2024 den AWS CodeCommit Zugang für Neukunden geschlossen. AWS CodeCommit Bestandskunden können den Service weiterhin wie gewohnt nutzen. AWS investiert weiterhin in Sicherheit, Verfügbarkeit und Leistungsverbesserungen für AWS CodeCommit, aber wir haben nicht vor, neue Funktionen einzuführen.
> Wenn Sie CodeCommit AWS-Git-Repositorys zu anderen Git-Anbietern migrieren möchten, wenden Sie sich an Ihren Cloud-Architekten (CA). Weitere Informationen zur Migration Ihrer Git-Repositorys finden Sie unter So migrieren Sie Ihr CodeCommit AWS-Repository zu einem anderen Git-Anbieter.

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS CodeCommit Funktionen in Ihrem AMS-verwalteten Konto zuzugreifen. AWS CodeCommit ist ein vollständig verwalteter Quellcodeverwaltungsdienst, der sichere Git-basierte Repositorys hostet. Er hilft Teams bei der Zusammenarbeit an Code in einem sicheren und hoch skalierbaren Ökosystem. CodeCommit macht es überflüssig, Ihr eigenes Quellcodeverwaltungssystem zu betreiben oder sich Gedanken über die Skalierung der Infrastruktur zu machen. Sie können damit alles CodeCommit , vom Quellcode bis hin zu Binärdateien, sicher speichern und es funktioniert nahtlos mit Ihren vorhandenen Git-Tools. Weitere Informationen hierzu finden Sie unter AWS CodeCommit.

> **Note**
>
> Um CodeCommit, CodeBuild, und CodePipeline mit einem einzigen RFC zu integrieren CodeDeploy, reichen Sie den Änderungstyp Management | AWS Service | Self-

provisioned service | Add (review required) (ct-3qe6io8t6jtny) ein und fordern Sie die drei Services an:, und. CodeBuild CodeDeploy CodePipeline Anschließend werden alle drei Rollen,, und in Ihrem Konto bereitgestellt. `customer_codebuild_service_role` `customer_codedeploy_service_role` `aws_code_pipeline_service_role` Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihrer Verbundlösung integrieren.

CodeCommit in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf CodeCommit in meinem AMS-Konto?

AWS CodeCommit Konsolen- und Datenzugriffsrollen können beantragt werden, indem zwei AWS Dienste RFCs, Konsolenzugriff und Datenzugriff eingereicht werden:

- Beantragen Sie den Zugriff auf, AWS CodeCommit indem Sie einen RFC mit dem Änderungstyp Management | AWS Service | Self-Provisioned Service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_codecommit_console_role` Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

  Für den Datenzugriff (z. B. für Trainings- und Entitätslisten) ist CTs für jede Datenquelle eine separate Angabe der S3-Datenquelle (verpflichtend), des Ausgabe-Buckets (verpflichtend) und des KMS (optional) erforderlich. Es gibt keine Einschränkungen bei der Schaffung von AWS CodeCommit Arbeitsplätzen, solange allen Datenquellen Zugriffsrollen gewährt wurden. Um Datenzugriff zu beantragen, reichen Sie einen RFC bei Management | Other | Other | Create (ct-1e1xtak34nx76) ein.

F: Welche Einschränkungen gelten für die Nutzung in meinem AMS-Konto? AWS CodeCommit

Die aktivierte CodeCommit Trigger-Funktion ist aufgrund der damit verbundenen Rechte zum Erstellen von SNS-Themen deaktiviert. Die direkte Authentifizierung gegen CodeCommit ist eingeschränkt. Benutzer sollten sich mit Credential Helper authentifizieren. Einige KMS-Befehle sind ebenfalls eingeschränkt:`kms:Encrypt`,,`kms:Decrypt`, `kms:ReEncrypt``kms:GenereteDataKey`, `kms:GenerateDataKeyWithoutPlaintext` und. `kms:DescribeKey`

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS CodeCommit in meinem AMS-Konto?

Wenn S3-Buckets mit KMS-Schlüsseln verschlüsselt sind, müssen S3 und KMS verwendet AWS CodeCommit werden.

Verwenden Sie AMS SSP zur Bereitstellung AWS CodeDeploy in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS CodeDeploy Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS CodeDeploy ist ein vollständig verwalteter Bereitstellungsservice, der Softwarebereitstellungen für eine Vielzahl von Rechendiensten wie Amazon EC2, AWS Fargate AWS Lambda, und Ihren lokalen Servern automatisiert. AWS CodeDeploy unterstützt Sie bei der schnellen Veröffentlichung neuer Funktionen, hilft Ihnen, Ausfallzeiten bei der Anwendungsbereitstellung zu vermeiden, und bewältigt die Komplexität der Aktualisierung Ihrer Anwendungen. Sie können AWS CodeDeploy damit Softwarebereitstellungen automatisieren, sodass fehleranfällige manuelle Operationen überflüssig werden. Der Service lässt sich an Ihre Bereitstellungsanforderungen anpassen. Weitere Informationen hierzu finden Sie unter AWS CodeDeploy.

> **Note**
>
> Um CodeCommit, CodeBuild, und CodePipeline mit einem einzigen RFC zu integrieren CodeDeploy, reichen Sie den Änderungstyp Management | AWS Service | Self-Provisioned Service | Add (Überprüfung erforderlich) (ct-3qe6io8t6jtny) ein und fordern Sie die drei Services an:, und. CodeBuild CodeDeploy CodePipeline Anschließend werden alle drei Rollen,, und in Ihrem Konto bereitgestellt. `customer_codebuild_service_role` `customer_codedeploy_service_role` `aws_code_pipeline_service_role` Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihrer Verbundlösung integrieren.

CodeDeploy in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf CodeDeploy in meinem AMS-Konto?

Beantragen Sie den Zugriff auf, CodeDeploy indem Sie einen RFC mit dem Änderungstyp Management | AWS-Service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_codedeploy_console_role` Konto `customer_codedeploy_service_role` die folgenden IAM-Rollen zur Verfügung: und. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die `customer_codedeploy_console_role` Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung CodeDeploy in meinem AMS-Konto?

Derzeit unterstützen wir Compute Platform nur als — Amazon EC2 /On-Premises. Blue/Green Bereitstellungen werden nicht unterstützt.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung CodeDeploy in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung CodeDeploy in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS CodePipeline in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS CodePipeline Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS CodePipeline ist ein vollständig verwalteter Continuous Delivery Service, der Sie bei der Automatisierung Ihrer Release-Pipelines für schnelle und zuverlässige Anwendungs- und Infrastrukturupdates unterstützt. CodePipeline automatisiert die Erstellungs-, Test- und Bereitstellungsphasen Ihres Release-Prozesses bei jeder Codeänderung auf der Grundlage des von Ihnen definierten Release-Modells. Auf diese Weise können Sie Funktionen und Updates schnell und zuverlässig bereitstellen. Sie können problemlos Dienste von Drittanbietern wie GitHub oder Ihr eigenes benutzerdefiniertes Plugin integrieren AWS CodePipeline . Mit zahlen Sie nur für das AWS CodePipeline, was Sie nutzen. Es fallen keine Vorausleistungen an und Sie gehen keine langfristigen Verpflichtungen ein. Weitere Informationen hierzu finden Sie unter AWS CodePipeline.

> **Note**
>
> Um CodeCommit, CodeBuild, und CodePipeline mit einem einzigen RFC zu integrieren CodeDeploy, reichen Sie den Änderungstyp Management | AWS Service | Self-Provisioned Service | Add (Überprüfung erforderlich) (ct-3qe6io8t6jtny) ein und fordern Sie die drei Dienste an:, und. CodeBuild CodeDeploy CodePipeline Anschließend werden alle drei Rollen,, und in Ihrem Konto bereitgestellt. `customer_codebuild_service_role` `customer_codedeploy_service_role` `aws_code_pipeline_service_role` Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihrer Verbundlösung integrieren. CodePipeline in AMS unterstützt „Amazon CloudWatch Events“ für Source Stage nicht, da für die Erstellung der Servicerolle und -richtlinie erweiterte Berechtigungen erforderlich sind,

wodurch das Modell mit den geringsten Rechten und der AMS-Change-Management-Prozess umgangen werden.

CodePipeline in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf CodePipeline in meinem AMS-Konto?

Beantragen Sie den Zugriff auf, CodePipeline indem Sie eine Serviceanfrage für das `customer_code_pipeline_console_role` entsprechende Konto einreichen. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

Zu diesem Zeitpunkt wird AMS Operations diese Servicerolle auch in Ihrem Konto bereitstellen:`aws_code_pipeline_service_role_policy`.

F: Welche Einschränkungen gelten für die Nutzung CodePipeline in meinem AMS-Konto?

Ja. CodePipeline Funktionen, Stufen und Anbieter sind auf Folgendes beschränkt:

1. Bereitstellungsphase: Beschränkt auf Amazon S3 und AWS CodeDeploy
2. Source Stage: Beschränkt auf Amazon S3 AWS CodeCommit, BitBucket, und GitHub
3. Build-Phase: Beschränkt auf AWS CodeBuild, und Jenkins
4. Genehmigungsphase: Beschränkt auf Amazon SNS
5. Testphase: Beschränkt auf Jenkins AWS CodeBuild BlazeMeter, Ghost Inspector UI Testing, Micro Focus StormRunner Load und Runscope API-Überwachung
6. Invoke Stage: Beschränkt auf Step-Funktionen und Lambda

> **Note**
>
> AMS Operations wird `customer_code_pipeline_lambda_policy` in Ihrem Konto bereitgestellt. Es muss mit der Lambda-Ausführungsrolle für die Lambda-Aufrufphase verknüpft sein. Bitte geben Sie den service/execution Lambda-Rollennamen an, mit dem Sie diese Richtlinie hinzufügen möchten. Wenn es keine benutzerdefinierte service/execution Lambda-Rolle gibt, erstellt AMS eine neue Rolle mit dem Namen`customer_code_pipeline_lambda_execution_role`, bei der es sich um eine Kopie von `customer_lambda_basic_execution_role` zusammen mit `customer_code_pipeline_lambda_policy` handelt.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung CodePipeline in meinem AMS-Konto?

AWS unterstützte Dienste AWS CodeCommit AWS CodeDeploy müssen vor oder zusammen mit dem Start von gestartet werden CodePipeline. AWS CodeBuild

Verwenden Sie AMS SSP zur Bereitstellung AWS Compute Optimizer in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Compute Optimizer Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Compute Optimizer empfiehlt optimale AWS Rechenressourcen für Ihre Workloads, um Kosten zu senken und die Leistung zu verbessern, indem maschinelles Lernen zur Analyse historischer Nutzungskennzahlen verwendet wird. Eine übermäßige Bereitstellung von Rechenleistung (Amazon EC2 und ASGs) kann zu unnötigen Infrastrukturkosten führen, und eine unzureichende Bereitstellung von Rechenleistung kann zu einer schlechten Anwendungsleistung führen. Compute Optimizer hilft Ihnen bei der Auswahl der optimalen EC2 Amazon-Instance-Typen, einschließlich derer, die Teil einer Amazon EC2 Auto Scaling Scaling-Gruppe sind, basierend auf Ihren Nutzungsdaten. Weitere Informationen hierzu finden Sie unter AWS Compute Optimizer.

Häufig gestellte Fragen zu Compute Optimizer in AWS Managed Services

F: Wie beantrage ich Zugriff auf Compute Optimizer in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Self-Provisioned Service | Add (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_compute_optimizer_readonly_role` Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Verwendung von Compute Optimizer in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von AWS Compute Optimizer ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Compute Optimizer in meinem AMS-Konto?

- Sie müssen einen RFC (Management | Other | Other | Update) einreichen, mit dem AMS Ops autorisiert wird, den Dienst in dem Konto zu aktivieren. Während der Bereitstellung wird eine Service Linked Role (SLR) erstellt, um die Erfassung von Metriken und die Generierung von Berichten zu ermöglichen. Die Spiegelreflexkamera trägt die Bezeichnung "“ AWSServiceRoleForComputeOptimizer. Weitere Informationen finden Sie unter Verwenden von dienstverknüpften Rollen für AWS Compute Optimizer
- CloudWatch Metriken müssen für die folgenden Metriken aktiviert sein:
  - CPU-Auslastung: Der Prozentsatz der zugewiesenen EC2 Amazon-Recheneinheiten, die auf der Instance verwendet werden. Diese Metrik identifiziert die Rechenleistung, die zum Ausführen einer Anwendung auf einer ausgewählten Instance erforderlich ist.
  - Speicherauslastung: Die Speichermenge, die während des Probenahmezeitraums auf irgendeine Weise genutzt wurde. Diese Metrik identifiziert den Arbeitsspeicher, der für die Ausführung einer Anwendung auf einer ausgewählten Instanz erforderlich ist. Die Speicherauslastung wird nur für Ressourcen analysiert, auf denen der Unified CloudWatch Agent installiert ist. Weitere Informationen finden Sie unter Aktivieren der Speicherauslastung mit dem CloudWatch Agenten (S. 10).
  - Netzwerkeingang: Die Anzahl der Byte, die von der Instance auf allen Netzwerkschnittstellen empfangen wurden. Diese Metrik identifiziert das Volumen des eingehenden Netzwerkverkehrs zu einer einzelnen Instance.
  - Netzwerkausgang: Die Anzahl der Byte, die von der Instance an alle Netzwerkschnittstellen gesendet wurden. Diese Metrik identifiziert das Volumen des ausgehenden Netzwerkverkehrs von einer einzelnen Instance.
  - Lokales Laufwerk input/output (I/O): Die Anzahl der input/output Operationen für das lokale Laufwerk. Diese Metrik identifiziert die Leistung des Root-Volumes einer Instance

Verwenden Sie AMS SSP zur Bereitstellung AWS DataSync in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS DataSync Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS DataSync verschiebt große Datenmengen online zwischen lokalem Speicher und Amazon S3, Amazon Elastic File System (Amazon Elastic File System) oder Amazon FSx. Manuelle Aufgaben im Zusammenhang mit Datenübertragungen können Migrationen verlangsamen und den IT-Betrieb belasten. DataSync macht viele dieser Aufgaben überflüssig oder erledigt sie automatisch, darunter die Erstellung von Skripten, die Planung und Überwachung von Übertragungen, die Validierung von Daten und die

Optimierung der Netzwerkauslastung. Der DataSync Software-Agent stellt eine Verbindung zu Ihrem Network File System (NFS) und Server Message Block (SMB) -Speicher her, sodass Sie Ihre Anwendungen nicht ändern müssen. DataSync kann Hunderte von Terabyte und Millionen von Dateien mit Geschwindigkeiten übertragen, die bis zu zehnmal schneller sind als Open-Source-Tools, über das Internet oder über Links. AWS Direct Connect Sie können DataSync damit aktive Datensätze oder Archive in die Cloud migrieren AWS, Daten zur zeitnahen Analyse und Verarbeitung in die Cloud übertragen oder Daten replizieren, um die Geschäftskontinuität zu AWS gewährleisten.

Weitere Informationen hierzu finden Sie unter AWS DataSync.

DataSync in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf DataSync in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_datasync_console_role` Konto die folgende IAM-Rolle zur Verfügung:.

Nach der Bereitstellung in Ihrem Konto müssen Sie die Rollen in Ihre Verbundlösung integrieren.

Die CloudWatch Protokollgruppe, die zum Streamen von Aufgabenprotokollen verwendet werden soll, ist „/aws/datasync“.

F: Welche Einschränkungen gelten für die Nutzung DataSync in meinem AMS-Konto?

Die volle Funktionalität von AWS DataSync ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung DataSync in meinem AMS-Konto?

- Amazon S3 ARNs (Amazon Resource Names) sind für alle S3-Buckets erforderlich, die mit DataSync Aufgaben verknüpft sind, die mithilfe der DataSync Service-Rolle `customer_datasync_service_role` ausgeführt werden.
- VPC-Endpunkte und Sicherheitsgruppen für DataSync Agenten müssen vor der Verwendung von VPC-Endpunkten mit einem RFC mit dem Änderungstyp Management | Other | Other | Create (ct-1e1xtak34nx76) angefordert werden.
- AWS DataSync Agenten werden in AMS als Appliance ausgeführt. Der AWS DataSync Agent wird vom Service gepatcht und aktualisiert. Einzelheiten finden Sie in den AWS DataSync häufig gestellten Fragen.

- Um einen AWS DataSync Agenten zu starten, reichen Sie einen RFC mit dem Änderungstyp Management | Other | Other | Create (ct-1e1xtak34nx76) ein und fordern Sie die Bereitstellung des Agenten an. Geben Sie die AWS DataSync Amazon EC2 AMI-ID, den Instance-Typ, das Subnetz und die Sicherheitsgruppe an und verweisen Sie entweder auf ein vorhandenes EC2 Amazon-Schlüsselpaar oder fordern Sie die Erstellung eines neuen Schlüsselpaars an.

> **Note**
>
> AMS stellt den AWS DataSync Agenten manuell im Namen des Kunden bereit und benötigt den WIGS-Aufnahmeprozess auf dem AWS DataSync Amazon AMI nicht. EC2

Verwenden Sie AMS SSP zur Bereitstellung AWS Device Farm in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Device Farm Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Device Farm ist ein Service zum Testen von Anwendungen, mit dem Sie die Qualität Ihrer Web- und mobilen Apps verbessern können, indem Sie sie mit einer Vielzahl von Desktop-Browsern und echten Mobilgeräten testen, ohne eine Testinfrastruktur bereitstellen und verwalten zu müssen. Der Dienst ermöglicht es Ihnen, Ihre Tests gleichzeitig auf mehreren Desktop-Browsern oder realen Geräten auszuführen, um die Ausführung Ihrer Testsuite zu beschleunigen, und generiert Videos und Protokolle, mit denen Sie Probleme mit Ihrer App schnell identifizieren können.

Weitere Informationen hierzu finden Sie unter AWS Device Farm.

AWS Device Farm in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf AWS Device Farm in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_devicefarm_role` Konto die folgende IAM-Rolle zur Verfügung:.

Nach der Bereitstellung in Ihrem Konto müssen Sie die Rollen in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Device Farm in meinem AMS-Konto?

Vollzugriff auf den AWS Device Farm Service ist möglich, mit Ausnahme der Verwendung des AMS-Namespace im Tag „Name“.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Device Farm in meinem AMS-Konto?

Keine.

Verwenden Sie AMS SSP zur Bereitstellung AWS Elastic Disaster Recovery in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Elastic Disaster Recovery Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Elastic Disaster Recovery minimiert Ausfallzeiten und Datenverluste durch schnelle, zuverlässige Wiederherstellung von lokalen und cloudbasierten Anwendungen mit erschwinglichem Speicher, minimalem Rechenaufwand und minimaler Wiederherstellung. point-in-time Sie können die IT-Resilienz erhöhen, wenn Sie AWS Elastic Disaster Recovery lokale oder cloudbasierte Anwendungen replizieren, die auf unterstützten Betriebssystemen ausgeführt werden. Verwenden Sie den AWS Management Console , um Replikations- und Starteinstellungen zu konfigurieren, die Datenreplikation zu überwachen und Instanzen für Drills oder Recovery zu starten.

Weitere Informationen hierzu finden Sie unter AWS Elastic Disaster Recovery.

AWS Elastic Disaster Recovery in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf AWS Elastic Disaster Recovery in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_drs_console_role` Konto die folgende IAM-Rolle zur Verfügung:.

Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Elastic Disaster Recovery in meinem AMS-Konto?

Es gibt keine Einschränkungen für die Nutzung AWS Elastic Disaster Recovery in Ihrem AMS-Konto.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Elastic Disaster Recovery in meinem AMS-Konto?

- Nachdem Sie Zugriff auf die Konsolenrolle haben, müssen Sie den Elastic Disaster Recovery-Dienst initialisieren, um die erforderlichen IAM-Rollen innerhalb des Kontos zu erstellen.

  - Sie müssen den Änderungstyp Verwaltung | Anwendungen | IAM-Instanzprofil | Create (Überprüfung erforderlich) Change Type ct-0ixp4ch2tiu04 RFC einreichen, um einen Klon des Instance-Profils zu erstellen und die Richtlinie anzuhängen. `customer-mc-ec2-instance-profile` `AWSElasticDisasterRecoveryEc2InstancePolicy` Sie müssen angeben, an welche Computer die neue Richtlinie angehängt werden soll.
  - Wenn die Instanz nicht das Standard-Instanzprofil verwendet, kann AMS die Verbindung `AWSElasticDisasterRecoveryEc2InstancePolicy` durch Automatisierung herstellen.
- Für die kontoübergreifende Wiederherstellung müssen Sie einen kundeneigenen KMS-Schlüssel verwenden. Der KMS-Schlüssel des Quellkontos muss gemäß der Richtlinie aktualisiert werden, um den Zugriff auf das Zielkonto zu ermöglichen. Weitere Informationen finden Sie unter Teilen des EBS-Verschlüsselungsschlüssels mit dem Zielkonto.
- Die KMS-Schlüsselrichtlinie muss aktualisiert werden, damit der `customer_drs_console_role` Benutzer die Richtlinie einsehen kann, wenn Sie nicht zwischen den Rollen wechseln möchten.
- Für die konto- und regionsübergreifende Notfallwiederherstellung muss AMS das Quell - und das Zielkonto als vertrauenswürdige Konten einrichten und die Rollen Failback und In-Right-Sizing über bereitstellen AWS . AWS CloudFormation

Verwenden Sie AMS SSP zur Bereitstellung AWS Elemental MediaConvert in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Elemental MediaConvert Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Elemental MediaConvert ist ein dateibasierter Videotranskodierungsdienst mit Funktionen in Broadcast-Qualität. Damit können Sie video-on-demand (VOD) -Inhalte für die Übertragung und die Übertragung auf mehreren Bildschirmen in großem Maßstab erstellen. Der Service kombiniert erweiterte Video- und Audiofunktionen mit einer einfachen Webservice-Oberfläche und pay-as-you-go Preisgestaltung. Mit AWS Elemental MediaConvert können Sie sich auf die Bereitstellung überzeugender Medienerlebnisse konzentrieren, ohne sich Gedanken über die Komplexität des Aufbaus und Betriebs Ihrer eigenen Videoverarbeitungsinfrastruktur machen zu müssen.

Weitere Informationen hierzu finden Sie unter AWS Elemental MediaConvert.

MediaConvert in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf MediaConvert in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_mediaconvert_author_role` Konto die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

Es wird eine zweite Rolle bereitgestellt`customer_MediaConvert_Default_Role`, die von verwendet wird, um aus dem S3-Quell-Bucket zu lesen und die Ausgabe MediaConvert in den S3-Ziel-Bucket zu schreiben sowie das API-Gateway aufzurufen, falls Sie Digital Rights Management (DRM) benötigen.

F: Welche Einschränkungen gelten für die Nutzung MediaConvert in meinem AMS-Konto?

Es gibt keine Einschränkungen für die Verwendung von MediaConvert in AMS.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung MediaConvert in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung MediaConvert in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Elemental MediaLive in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Elemental MediaLive Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Elemental MediaLive ist ein Dienst zur Live-Videoverarbeitung in Rundfunkqualität. Damit können Sie hochwertige Videostreams für die Übertragung auf Fernsehgeräten und mit dem Internet verbundene Multiscreen-Geräte wie Tablets TVs, Smartphones und Set-Top-Boxen erstellen. Der Dienst kodiert Ihre Live-Videostreams in Echtzeit, verwendet eine größere Live-Videoquelle und komprimiert sie in kleinere Versionen, um sie an Ihre Zuschauer zu verteilen. Mit AWS Elemental MediaLive können Sie ganz einfach Streams sowohl für Live-Events als auch für Rund-um-die-Uhr-Kanäle mit erweiterten Übertragungsfunktionen, hoher Verfügbarkeit und Preisgestaltung einrichten. pay-as-you-go AWS Elemental MediaLive ermöglicht es Ihnen, sich darauf zu konzentrieren, überzeugende Live-Videoerlebnisse für Ihre Zuschauer zu schaffen, ohne die Komplexität des Aufbaus und Betriebs einer Videoverarbeitungsinfrastruktur in Sendequalität.

Weitere Informationen hierzu finden Sie unter AWS Elemental MediaLive.

MediaLive in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf MediaLive in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_medialive_author_role` Konto die folgende IAM-Rolle zur Verfügung:.

Im Rahmen dieses RFC wird Ihrem Konto eine zweite Rolle zugewiesen. Diese `customer_medialive_service_role` Rolle kann Ihren Media Live-Kanälen und Eingaben zugewiesen werden, um mit anderen Diensten wie Amazon S3 und CloudWatch Logs zu interagieren. MediaStore

Nachdem die Rollen in Ihrem Konto bereitgestellt wurden, müssen Sie die Rollen in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung MediaLive in meinem AMS-Konto?

Es gibt keine Einschränkungen für die Verwendung von MediaLive in AMS.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung MediaLive in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung MediaLive in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Elemental MediaPackage in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Elemental MediaPackage Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Elemental MediaPackage bereitet Ihr Video zuverlässig für die Übertragung über das Internet vor und schützt es. AWS Elemental MediaPackage Erstellt aus einem einzigen Videoeingang Videostreams, die für die Wiedergabe auf verbundenen Mobiltelefonen TVs, Computern, Tablets und Spielekonsolen formatiert sind. Es macht es einfach, beliebte Videofunktionen für Zuschauer (Start, Pause, Rücklauf usw.) zu implementieren, wie sie häufig auf zu finden sind. DVRs AWS Elemental MediaPackage kann Ihre Inhalte auch mithilfe von Digital Rights Management (DRM) schützen. AWS Elemental MediaPackage skaliert automatisch als Reaktion auf die Auslastung, sodass Ihre Zuschauer immer ein großartiges Erlebnis haben, ohne dass Sie im Voraus genau vorhersagen müssen, wie viel Kapazität Sie benötigen.

Weitere Informationen hierzu finden Sie unter AWS Elemental MediaPackage.

MediaPackage in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf AWS Elemental MediaPackage in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_mediapackage_author_role` Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

Eine zweite Rolle wird bereitgestellt`customer_mediapackage_service_role`, die Ihren Media Live-Kanälen und -Eingängen zugewiesen werden kann, um mit anderen Diensten wie S3 und Secrets Manager zu interagieren.

F: Welche Einschränkungen gelten für die Nutzung MediaPackage in meinem AMS-Konto?

Es gibt keine Einschränkungen für die Verwendung von MediaPackage in AMS.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung MediaPackage in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung MediaPackage in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Elemental MediaStore in Ihrem AMS-Konto

> **Note**
>
> AWS Hat nach reiflicher Überlegung die Entscheidung getroffen MediaStore, das Unternehmen mit Wirkung zum 13. November 2025 einzustellen. Wenn Sie ein aktiver Kunde von sind MediaStore, können Sie den Service bis zum 13. November 2025 MediaStore wie gewohnt nutzen. Dann endet der Support für den Service. Nach diesem Datum können Sie keine der Funktionen dieses Dienstes mehr nutzen MediaStore .

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Elemental MediaStore Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Elemental

MediaStore ist ein für Medien optimierter AWS Speicherdienst. Er bietet Ihnen die Leistung, Konsistenz und geringe Latenz, die für die Bereitstellung von Live-Streaming-Videoinhalten erforderlich sind. AWS Elemental MediaStore fungiert als Ursprungsspeicher in Ihrem Video-Workflow. Seine hohen Leistungsfähigkeiten erfüllen die Anforderungen der anspruchsvollsten Workloads für die Medienbereitstellung in Kombination mit langfristiger, kostengünstiger Speicherung. Weitere Informationen hierzu finden Sie unter AWS Elemental MediaStore.

MediaStore in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf MediaStore in meinem AMS-Konto?

Beantragen Sie den Zugriff auf, MediaStore indem Sie einen RFC mit dem Änderungstyp Management | AWS-Service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer_mediastore_author_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Als Teil dieses RFC wird eine zweite Rolle in Ihrem Konto bereitgestellt, eine `MediaStoreAccessLogs` Rolle, die vom MediaStore Dienst zur Anmeldung von Aktivitäten verwendet wird CloudWatch, sofern Sie diese Funktion aktivieren. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rollen in Ihre Verbundlösung integrieren.

Zu diesem Zeitpunkt wird AMS Operations diese Servicerolle auch in Ihrem Konto bereitstellen:`aws_code_pipeline_service_role_policy`.

F: Welche Einschränkungen gelten für die Nutzung MediaStore in meinem AMS-Konto?

Es gibt keine Einschränkungen für die Verwendung von MediaStore in AMS.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung MediaStore in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung MediaStore in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Elemental MediaTailor in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Elemental MediaTailor Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Elemental MediaTailor ermöglicht es Videoanbietern, individuell zugeschnittene Werbung in ihre Videostreams einzufügen, ohne dabei Abstriche bei der Übertragungsqualität machen zu müssen. quality-of-service

Mit AWS Elemental MediaTailor erhalten die Zuschauer Ihres Live- oder On-Demand-Videos jeweils einen Stream, der Ihre Inhalte mit auf sie personalisierten Anzeigen kombiniert. Im Gegensatz zu anderen personalisierten Werbelösungen wird AWS Elemental MediaTailor Ihr gesamter Stream — Video und Werbung — jedoch in sendegerechter Videoqualität geliefert, um das Erlebnis für Ihre Zuschauer zu verbessern. AWS Elemental MediaTailor bietet automatisierte Berichte, die sowohl auf kunden- als auch auf serverseitigen Kennzahlen zur Anzeigenbereitstellung basieren, um Werbeimpressionen und Zuschauerverhalten genau zu messen. Sie können unerwartete, stark nachgefragte Zuschauerereignisse ganz einfach monetarisieren, ohne dass Vorabkosten anfallen. AWS Elemental MediaTailor Es verbessert auch die Anzeigenbereitstellungsraten, sodass Sie mit jedem Video mehr Geld verdienen können, und es funktioniert mit einer Vielzahl von Netzwerken zur Inhaltsbereitstellung, Anzeigenentscheidungsservern und Client-Geräten.

Weitere Informationen hierzu finden Sie unter AWS Elemental MediaTailor.

MediaTailor in häufig gestellten Fragen zu AWS Managed Services

F: Wie beantrage ich Zugriff auf MediaTailor in meinem AMS-Konto?

Beantragen Sie den Zugriff auf, MediaTailor indem Sie einen RFC mit dem Änderungstyp Management | AWS-Service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer-mediatailor-role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung MediaTailor in meinem AMS-Konto?

Es gibt keine Einschränkungen für die Verwendung von MediaTailor in AMS.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung MediaTailor in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung MediaTailor in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Global Accelerator in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf die Funktionen von Global Accelerator zuzugreifen. Global Accelerator ist ein

Service auf Netzwerkebene, mit dem Sie Beschleuniger erstellen, um die Verfügbarkeit und Leistung von Internetanwendungen zu verbessern, die von einem globalen Publikum verwendet werden. Weitere Informationen finden Sie unter Global Accelerator.

Häufig gestellte Fragen zu Global Accelerator in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich die Einrichtung von Global Accelerator in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den AWS Services-RFC (Management | AWS Service | Self-Provisioned Service) einreichen. Über diesen RFC werden die folgenden IAM-Rollen in Ihrem Konto bereitgestellt:. `customer_global_accelerator_console_role` Nach der Bereitstellung in Ihrem Konto müssen Sie die Konsolenrolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Global Accelerator in meinem AMS-Konto?

Global Accelerator ist ein globaler Service, der Endgeräte in mehreren AWS Regionen unterstützt, die in der AWS Regionentabelle aufgeführt sind.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von Global Accelerator in meinem AMS-Konto?

Wenn Sie Ihren Accelerator mit Global Accelerator einrichten, ordnen Sie die statischen IP-Adressen regionalen Endpunkten in einer oder mehreren AWS Regionen zu. Bei Standardbeschleunigern sind die Endpunkte Network Load Balancers, Application Load Balancers, EC2 Amazon-Instances oder Elastic IP-Adressen. Bei benutzerdefinierten Routing-Beschleunigern sind Endpunkte Virtual Private Cloud (VPC) -Subnetze mit einer oder mehreren Instanzen. EC2

Verwenden Sie AMS SSP zur Bereitstellung AWS Glue in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Glue Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Glue ist ein vollständig verwalteter ETL-Service (Extrahieren, Transformieren und Laden), mit dem Sie Ihre Daten für Analysen vorbereiten und laden können. Sie können einen ETL-Job mit ein paar Klicks in der erstellen und ausführen AWS Management Console. Sie zeigen AWS Glue auf Ihre Daten, die auf gespeichert sind AWS, AWS Glue und entdecken Ihre Daten und speichern die zugehörigen Metadaten (z. B. Tabellendefinition und Schema) im AWS Glue Data Catalog. Nach der Katalogisierung sind Ihre Daten sofort durchsuchbar, abfragbar und für ETL-Aktionen verfügbar. Weitere Informationen hierzu finden Sie unter AWS Glue.

AWS Glue in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich AWS Glue die Einrichtung in meinem AMS-Konto?

Beantragen Sie den Zugriff auf, AWS Glue indem Sie einen RFC mit dem Management | AWS-Service | Selbstbereitgestellter Service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen zur Verfügung:

- `customer_glue_console_role`
- `customer_glue_service_role`

Zu den vorherigen Rollen gehören die folgenden beigefügten Richtlinien:

- `customer_glue_secrets_manager_policy`
- `customer_glue_deny_policy`

Nachdem die Rollen in Ihrem Konto bereitgestellt wurden, müssen Sie sie in Ihre Verbundlösung integrieren.

Für den Zugriff auf Crawler-, Jobs- und Entwicklungsendpunkte (Rollen, die für bestimmte Anwendungsfälle benötigt werden), reichen Sie einen RFC mit Deployment | Advanced Stack Components | Identity and Access Management (IAM) | Entität oder Richtlinie erstellen (ct-3dpd8mdd9jn1r) ein.

F: Welche Einschränkungen gelten für die Nutzung in meinem AMS-Konto? AWS Glue

Es gibt keine Einschränkungen. Die volle Funktionalität von AWS Glue ist in Ihrem AMS-Konto verfügbar. Für eine interaktive Umgebung, in der Sie ETL-Skripts erstellen und testen können, verwenden Sie Notebooks on AWS Glue Studio. AWS Glue Interaktive Sitzungen und Job Notebooks sind serverlose Funktionen AWS Glue , die Sie in der AWS Glue Servicerolle verwenden können AWS Glue und die diese nutzen.

AWS Glue vor 2.0: AWS Glue Notebooks sind eine nicht verwaltete Ressource, die EC2 Amazon-Instances in einem Konto startet. Es hat sich bewährt, Ihre eigenen EC2 Amazon-Instances zu starten und die Software zu installieren, die zur Unterstützung einer Notebook-Umgebung und -Entwicklung erforderlich ist. Weitere Informationen finden Sie unter Tutorial: Einrichten eines lokalen

Apache Zeppelin-Notebooks zum Testen und Debuggen von ETL-Skripts und Verwenden von Entwicklungsendpunkten für die Entwicklung von Skripts.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Glue in meinem AMS-Konto?

AWS Glue ist von Amazon S3, CloudWatch, und CloudWatch Logs abhängig. Transitive Abhängigkeiten variieren je nach Datenquelle, und andere AWS Glue Servicefunktionen können miteinander interagieren (Beispiel: Amazon Redshift, Amazon RDS, Athena).

Verwenden Sie AMS SSP zur Bereitstellung AWS Lake Formation in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Lake Formation Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Lake Formation ist ein Service, der es einfach macht, innerhalb weniger Tage einen sicheren Data Lake einzurichten. Ein Data Lake ist ein zentralisiertes, kuratiertes und gesichertes Repository, in dem alle Ihre Daten gespeichert werden, sowohl in seiner ursprünglichen Form als auch für die Analyse vorbereitet. Mit einem Data Lake können Sie Datensilos aufschlüsseln und verschiedene Arten von Analysen kombinieren, um Erkenntnisse zu gewinnen und bessere Geschäftsentscheidungen zu leiten.

Das Erstellen eines Data Lake mit Lake Formation ist so einfach wie das Definieren von Datenquellen und die Datenzugriffs- und Sicherheitsrichtlinien, die Sie anwenden möchten. Lake Formation hilft Ihnen dann, Daten aus Datenbanken und Objektspeicher zu sammeln und zu katalogisieren, die Daten in Ihren neuen Amazon S3-Data Lake zu verschieben, Ihre Daten mithilfe von Algorithmen für Machine Learning zu bereinigen und zu klassifizieren und den sicheren Zugriff auf Ihre sensiblen Daten zu sichern. Ihre Benutzer können auf einen zentralen Datenkatalog zugreifen (Einzelheiten finden Sie in den AWS Glue häufig gestellten Fragen), in dem die verfügbaren Datensätze und ihre entsprechende Verwendung beschrieben werden. Ihre Benutzer nutzen diese Datensätze dann mit Analyse- und Machine-Learning-Diensten ihrer Wahl, wie Amazon Redshift, Amazon Athena und (in der Betaversion) Amazon EMR für Apache Spark. Lake Formation baut auf den Funktionen auf, die in verfügbar sind AWS Glue.

Weitere Informationen hierzu finden Sie unter AWS Lake Formation.

Häufig gestellte Fragen zu Lake Formation in AWS Managed Services

F: Wie beantrage ich Zugriff auf AWS Lake Formation in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_lakeformation_data_analyst_role` Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rollen in Ihre Verbundlösung integrieren.

Darüber hinaus sind die folgenden zwei Rollen optional:

- `customer_lakeformation_admin_role`
- `customer_lakeformation_workflow_role`

Bei Administratorberechtigungen können Sie wählen, ob Sie die Rolle `customer_lakeformation_admin_role` als Teil desselben SSPS-Änderungstyps (ct-3qe6io8t6jtny) integrieren möchten.

Wenn Sie Blueprints in der AWS Lake Formation Konsole erstellen möchten, müssen Sie den RFC Management | Other | Other (ct-1e1xtak34nx76) einreichen, um den bereitzustellen. `customer_lakeformation_workflow_role` Im RFC müssen Sie den S3-Bucket-Namen angeben, wenn der Bucket bei der Erstellung von Blueprints eine Quelle ist. Der S3-Bucket ist anwendbar AWS CloudTrail, wenn der Blueprint-Typ Classic Load Balancer Logs oder Application Load Balancer Logs ist.

F: Welche Einschränkungen gelten für die Nutzung AWS Lake Formation in meinem AMS-Konto?

Die volle Funktionalität von Lake Formation ist in AMS verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Lake Formation in meinem AMS-Konto?

Lake Formation ist in den AWS Glue Dienst integriert, sodass AWS Glue Benutzer nur auf die Datenbanken und Tabellen zugreifen können, für die sie Lake Formation Formation-Berechtigungen haben. Darüber hinaus können AWS Athena- und Amazon Redshift Redshift-Benutzer nur die AWS Glue Datenbanken und Tabellen abfragen, für die sie Lake Formation Formation-Berechtigungen haben.

Verwenden Sie AMS SSP zur Bereitstellung AWS Lambda in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Lambda Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Lambda ermöglicht es Ihnen, Code auszuführen, ohne Server bereitzustellen oder zu verwalten. Sie zahlen nur für die Rechenzeit, die Sie verbrauchen. Es fallen keine Gebühren an, wenn Ihr Code nicht ausgeführt wird. Mit Lambda können Sie Code für praktisch jede Art von Anwendung oder Back-End-Dienst ausführen, und das alles ohne Verwaltungsaufwand. Laden Sie Ihren Code hoch und Lambda kümmert sich um alles, was für die Ausführung und Skalierung Ihres Codes mit hoher Verfügbarkeit erforderlich ist. Sie können Ihren Code so einrichten, dass er automatisch von anderen AWS Diensten ausgelöst wird, oder ihn direkt von einer beliebigen Web- oder mobilen App aus aufrufen. Weitere Informationen hierzu finden Sie unter AWS Lambda.

Häufig gestellte Fragen zu Lambda in AWS Managed Services

F: Wie beantrage ich Zugriff auf AWS Lambda in meinem AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Selbst bereitgestellter Service | Hinzufügen (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_lambda_admin_role` Konto `customer_lambda_basic_execution_role` die folgenden IAM-Rollen zur Verfügung: und. Nachdem es in Ihrem Konto bereitgestellt wurde, müssen Sie die Rollen in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Lambda in meinem AMS-Konto?

- Eine Lambda-Funktion ist so konzipiert, dass sie von Ereignisquellen aufgerufen wird. Eine Liste der Dienste, die als Lambda-Ereignisquelle verwendet werden können, finden Sie unter AWS Lambda Mit anderen Diensten verwenden. Derzeit sind nicht alle diese Dienste in AMS-Konten verfügbar. Wenn Sie einen Dienst benötigen, der nicht verfügbar ist, arbeiten Sie mit Ihrem AMS CSDM zusammen, um eine Ausnahme einzureichen.
- Standardmäßig stellt Ihnen AMS eine grundlegende Lambda-Initiierungsrolle zur Verfügung, die die `AWSXrayWriteOnlyAccess` Berechtigungen `AWSLambdaBasicExecutionRole` und enthält. Weitere Informationen finden Sie unter AWS Lambda Initiation Role. Wenn Sie zusätzliche Berechtigungen benötigen, z. B. die Möglichkeit, Lambda-Funktionen in Ihrer AMS-VPC bereitzustellen, reichen Sie einen RFC mit dem Änderungstyp Management | AWS-Service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) ein.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung in meinem AMS-Konto? AWS Lambda

Für den Einstieg gibt es keine Voraussetzungen oder Abhängigkeiten. Abhängig von Ihrem spezifischen Anwendungsfall benötigen Sie jedoch möglicherweise Zugriff auf andere AWS Dienste, um Ereignisquellen zu erstellen, oder zusätzliche Berechtigungen für Ihre Funktion, um verschiedene Aktionen auszuführen. AWS Lambda Wenn zusätzliche Berechtigungen erforderlich sind, reichen Sie einen RFC mit dem Änderungstyp Management | AWS-Service | Self-provisioned service | Add (review required) ein (Überprüfung erforderlich) (ct-3qe6io8t6jtny).

F: Was muss ich tun, um eine Lambda-Funktion in einem meiner Konten auszuführen?

Verwenden Sie die folgenden Richtlinien, um eine Lambda-Funktion in einem Core-Konto bereitzustellen:

- Stellen Sie sicher, dass SSPS for AWS Lambda integriert ist.
- Es gibt keine spezifischen Einschränkungen, die diese Bereitstellung im Rahmen der AMS-Verantwortlichkeiten verbieten, solange Ihre AMS-Ressourcen geschützt und gesetzeskonform sind.
- Wenn Sie möchten, dass AMS die Lambda-Funktion erstellt, müssen Sie zuerst die dafür vorgesehene SSPS-Rolle verwenden. AWS Lambda Wenn Sie dann weiterhin AMS-Unterstützung bei der Bereitstellung oder Unterstützung der Funktion benötigen, wenden Sie sich an Ihre Zertifizierungsstelle und starten Sie den Out-of-Scope-Prozess (OOS).

Verwenden Sie AMS SSP zur Bereitstellung AWS License Manager in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS License Manager Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS License Manager lässt sich in AWS Services integrieren, um die Verwaltung von Lizenzen für mehrere AWS Konten, IT-Kataloge und lokale Lizenzen über ein einziges Konto zu vereinfachen. AWS AWS License Manager ermöglicht es Administratoren, benutzerdefinierte Lizenzregeln zu erstellen, die die Bedingungen ihrer Lizenzvereinbarungen emulieren, und setzt diese Regeln dann durch, wenn eine Amazon-Instance gestartet EC2 wird. Mit diesen Regeln können Sie Lizenzverstöße einschränken, indem Sie den Start der Instance physisch unterbinden oder Administratoren über den Verstoß informieren. AWS License Manager Weitere Informationen hierzu finden Sie unter AWS License Manager.

Häufig gestellte Fragen zum License Manager in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich AWS License Manager die Einrichtung in meinem AMS-Konto?

Beantragen Sie Zugriff auf, AWS License Manager indem Sie einen RFC mit dem Änderungstyp Management | AWS Service | Self-Provisioned Service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_license_manager_role` Konto die folgende IAM-Rolle zur Verfügung:. Sobald die IAM-Rolle License Manager in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS License Manager in meinem AMS-Konto?

Sie können AWS License Manager Regeln mit Ihren eigenen verknüpfen (gefiltert unter „Mein Eigentum“). AMIs Wenn Sie sich dafür entscheiden, eine Limit-Zuordnung zu einem AMI zu erzwingen (Beispiel: kann nur 100 vCPUs dieses AMI unterstützen) und das Limit ausschöpfen, werden future Starts mit diesem AMI blockiert und es wird die Fehlermeldung „Keine Lizenzen verfügbar“ zurückgegeben. Dies ist das beabsichtigte Verhalten dieses Dienstes (die Lizenzerschöpfung wird nicht zugelassen). Falls Sie das Limit ausgeschöpft haben, das AMI aber erneut starten müssen, müssen Sie die in konfigurierte Regel ändern AWS License Manager.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS License Manager in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung AWS License Manager in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Migration Hub in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Migration Hub Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Migration Hub bietet einen zentralen Ort, an dem Sie den Fortschritt der Anwendungsmigrationen für mehrere Lösungen und Partnerlösungen verfolgen können. AWS Mithilfe von Migration Hub können Sie die Migrationstools AWS und Partner-Migrationstools auswählen, die Ihren Anforderungen am besten entsprechen, und gleichzeitig einen Überblick über den Status der Migrationen in Ihrem gesamten Anwendungsportfolio erhalten. Migration Hub bietet auch wichtige Kennzahlen und Fortschritte für einzelne Anwendungen, unabhängig davon, welche Tools für die Migration verwendet werden. Auf diese Weise können Sie schnell über den Fortschritt all Ihrer Migrationen informiert werden, Probleme einfach identifizieren

und beheben und den Gesamtzeit- und Arbeitsaufwand für Ihre Migrationsprojekte reduzieren. Weitere Informationen hierzu finden Sie unter AWS Migration Hub.

Häufig gestellte Fragen zu Migration Hub in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Migration Hub in meinem AMS-Konto?

Fordern Sie Zugriff auf Migration Hub an, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer_migrationhub_author_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen für Migration Hub?

Keine.

F: Was sind die Voraussetzungen für die Aktivierung von Migration Hub?

Es gibt keine Voraussetzungen, um mit der Nutzung von Migration Hub in Ihrem AMS-Konto zu beginnen. Während der Verwaltung des Service sind jedoch möglicherweise Berechtigungen außerhalb von Migration Hub erforderlich, z. B. Schreibberechtigungen für Amazon S3 zum Hochladen von Serverinformationen.

Verwenden Sie AMS SSP zur Bereitstellung AWS Outposts in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Outposts Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Outposts ist ein vollständig verwalteter Service, der AWS Infrastruktur, AWS Dienste und Tools auf praktisch jedes Rechenzentrum APIs, jeden Colocation-Bereich oder jede lokale Einrichtung ausdehnt und so für ein einheitliches Hybrid-Erlebnis sorgt. AWS Outposts eignet sich gut für Workloads, die einen Zugriff auf lokale Systeme mit geringer Latenz, lokale Datenverarbeitung oder lokalen Datenspeicher erfordern. Weitere Informationen hierzu finden Sie unter AWS Outposts.

AWS Outposts in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich AWS Outposts die Einrichtung in meinem AMS-Konto?

Beantragen Sie Zugriff auf, AWS Outposts indem Sie einen RFC mit dem Änderungstyp Management | AWS Service | Self-Provisioned Service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_outposts_role` Konto die folgende IAM-Rolle zur Verfügung:. Sobald die Rolle in Ihrem Konto bereitgestellt wurde, müssen Sie sie in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Outposts in meinem AMS-Konto?

Es gibt keine Einschränkungen für die Verwendung AWS Outposts in Ihrem AMS-Konto.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Outposts in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Outposts in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Resilience Hub in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Resilience Hub Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Resilience Hub hilft Ihnen dabei, Ihre AWS Anwendungen proaktiv vorzubereiten und vor Störungen zu schützen. Der Resilience Hub bietet Resilienzbeurteilungen und -validierungen, die in Ihren Softwareentwicklungszyklus integriert werden können, um Schwachstellen bei der Ausfallsicherheit aufzudecken. Resilience Hub hilft Ihnen bei der Einschätzung, ob Ihre Anwendungen die Ziele für die Wiederherstellungszeit (RTO) und die Zielvorgaben für den Wiederherstellungspunkt (Recovery Point Objective, RPO) erfüllen können, und hilft Ihnen, Probleme zu lösen, bevor sie in Betrieb genommen werden. Nachdem Sie eine AWS Anwendung in der Produktion bereitgestellt haben, können Sie Resilience Hub verwenden, um die Ausfallsicherheit Ihrer Anwendung weiter zu verfolgen. Wenn ein Ausfall auftritt, sendet Resilience Hub eine Benachrichtigung an den Betreiber, um den zugehörigen Wiederherstellungsprozess zu starten.

AWS Resilience Hub in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS Resilience Hub auf mein AMS-Konto?

Beantragen Sie Zugriff auf Resilience Hub, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen und -Richtlinien zur Verfügung:

IAM roles

- `customer_resiliencehub_console_role`
- `customer_resiliencehub_service_role`

Richtlinien

- `customer_resiliencehub_console_policy`
- `customer_resiliencehub_service_policy`

Nachdem die Rolle in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle `customer_resiliencehub_console_role` in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Resilience Hub in meinem AMS-Konto?

Es gibt keine Einschränkungen. Die volle Funktionalität von Resilience Hub ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Resilience Hub in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Verwendung von Resilience Hub in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Secrets Manager in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Secrets Manager Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Secrets Manager hilft Ihnen beim Schutz von Geheimnissen, die Sie für den Zugriff auf Ihre Anwendungen, Dienste und IT-Ressourcen benötigen. Mit diesem Service können Sie Datenbankanmeldedaten, API-Schlüssel und andere Geheimnisse während ihres gesamten Lebenszyklus problemlos rotieren, verwalten und abrufen. Benutzer und Anwendungen rufen Geheimnisse mit einem Aufruf des Secrets Manager ab APIs, sodass sensible Informationen nicht mehr im Klartext hartcodiert werden müssen. Secrets Manager bietet geheime Rotation mit integrierter Integration für Amazon RDS, Amazon Redshift und Amazon DocumentDB. Der Service ist auch auf andere Arten von Geheimnissen erweiterbar, einschließlich API-Schlüsseln und Tokens. OAuth Weitere Informationen hierzu finden Sie unter AWS Secrets Manager.

> **Note**
>
> Standardmäßig können AMS-Betreiber auf Geheimnisse zugreifen AWS Secrets Manager , die mit dem AWS KMS Standardschlüssel (CMK) des Kontos verschlüsselt wurden. Wenn Sie möchten, dass AMS Operations nicht auf Ihre Geheimnisse zugreifen kann, verwenden Sie ein benutzerdefiniertes CMK mit einer AWS Key Management Service (AWS KMS) - Schlüsselrichtlinie, die Berechtigungen definiert, die den im Secret gespeicherten Daten entsprechen.

Häufig gestellte Fragen zu Secrets Manager in AWS Managed Services

F: Wie beantrage ich Zugriff auf AWS Secrets Manager in meinem AMS-Konto?

Fordern Sie Zugriff auf Secrets Manager an, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt Ihrem `customer_secrets_manager_console_role` `customer-rotate-secrets-lambda-role` Konto die folgenden IAM-Rollen zur Verfügung: und. Die `customer_secrets_manager_console_role` wird als Admin-Rolle für die Bereitstellung und Verwaltung der Secrets verwendet und `customer-rotate-secrets-lambda-role` wird als Lambda-Ausführungsrolle für die Lambda-Funktionen verwendet, die die Secrets rotieren. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die `customer_secrets_manager_console_role` Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Secrets Manager in meinem AMS-Konto?

Der volle Funktionsumfang von AWS Secrets Manager ist in Ihrem AMS-Konto verfügbar, ebenso wie die automatische Rotation von Geheimnissen. Beachten Sie jedoch, dass das Einrichten Ihrer Rotation mithilfe von „Create a new Lambda function to perform rotation“ nicht unterstützt wird, da für die Erstellung des AWS CloudFormation Stacks erhöhte Berechtigungen erforderlich sind (Erstellung der IAM-Rolle und Lambda-Funktion), wodurch der Change-Management-Prozess umgangen wird. AMS Advanced unterstützt nur „Eine bestehende Lambda-Funktion zur Rotation verwenden“, bei der Sie Ihre Lambda-Funktionen so verwalten, dass Geheimnisse mithilfe der Lambda-SSPS-Admin-Rolle rotiert werden. AWS AMS Advanced erstellt oder verwaltet Lambda nicht, um die Geheimnisse rotieren zu lassen.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Secrets Manager in meinem AMS-Konto?

Die folgenden Namespaces sind für AMS reserviert und im Rahmen des direkten Zugriffs auf nicht verfügbar: AWS Secrets Manager

- arn:aws:secretsmanager: *:*:secret:ams-shared/*
- arn:aws:secretsmanager: *:*:secret:customer-shared/*
- arn:aws:secretsmanager: *:*:secret:ams/*

Schlüssel mit Secrets Manager (AMS SSPS) teilen

Die Weitergabe von Geheimnissen an AMS im Klartext eines RFC, einer Serviceanfrage oder eines Vorfallberichts führt zu einem Vorfall mit der Offenlegung von Informationen. AMS löscht diese Informationen aus dem Fall und fordert Sie auf, die Schlüssel neu zu generieren.

Sie können AWS Secrets Manager(Secrets Manager) unter diesem Namespace verwenden,`customer-shared`.

Häufig gestellte Fragen zum Teilen von Schlüsseln mit Secrets Manager

F: Welche Arten von Geheimnissen müssen mit Secrets Manager geteilt werden?

Einige Beispiele sind vorab genutzte Schlüssel für die VPN-Erstellung, vertrauliche Schlüssel wie Authentifizierungsschlüssel (IAM, SSH), Lizenzschlüssel und Passwörter.

F: Wie kann ich die Schlüssel mithilfe von Secrets Manager mit AMS teilen?

1. Melden Sie sich mit Ihrem Verbundzugriff und der entsprechenden Rolle bei der AWS Management-Konsole an:

   für SALZ, das `Customer_ReadOnly_Role`

   für MALZ,`AWSManagedServicesChangeManagementRole`.
2. Navigieren Sie zur AWS Secrets Manager Konsole und klicken Sie auf Neues Geheimnis speichern.
3. Wählen Sie Andere Art von Secrets aus.
4. Geben Sie den geheimen Wert als Klartext ein und verwenden Sie die standardmäßige KMS-Verschlüsselung. Klicken Sie auf Weiter.
5. Geben Sie den geheimen Namen und die Beschreibung ein. Der Name beginnt immer mit customer-shared/. Zum Beispiel customer-shared/mykey2022. Klicken Sie auf Weiter.

6. Lassen Sie die automatische Rotation deaktiviert und klicken Sie auf Weiter.
7. Überprüfen Sie es und klicken Sie auf Speichern, um das Geheimnis zu speichern.
8. Antworten Sie uns über die Serviceanfrage, den RFC oder den Vorfallbericht mit dem geheimen Namen, damit wir das Geheimnis identifizieren und abrufen können.

F: Welche Berechtigungen sind für die gemeinsame Nutzung der Schlüssel mit Secrets Manager erforderlich?

SALZ: Suchen Sie nach der `customer_secrets_manager_shared_policy` verwalteten IAM-Richtlinie und stellen Sie sicher, dass das Richtliniendokument mit dem Dokument übereinstimmt, das in den folgenden Erstellungsschritten angehängt wurde. Vergewissern Sie sich, dass die Richtlinie den folgenden IAM-Rollen zugeordnet ist:. `Customer_ReadOnly_Role`

MALZ: Stellen Sie sicher`AMSSecretsManagerSharedPolicy`, dass der `AWSManagedServicesChangeManagementRole` Rolle, zugeordnet ist, die Ihnen die `GetSecretValue` Aktion im `ams-shared` Namespace ermöglicht.

Beispiel:

```
{
 "Action": "secretsmanager:*",
 "Resource": [
 "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
 "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
 ],
 "Effect": "Allow",
 "Sid": "AllowAccessToSharedNameSpaces"
 }
```

> **Note**
>
> Die erforderlichen Berechtigungen werden erteilt, wenn Sie einen AWS Secrets Manager als Self-Service bereitgestellten Dienst hinzufügen.

Verwenden Sie AMS SSP zur Bereitstellung AWS Security Hub in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Security Hub Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Security Hub bietet Ihnen einen umfassenden Überblick über Ihren Sicherheitsstatus AWS und Ihre Einhaltung der Sicherheitsstandards und Best Practices der Sicherheitsbranche. Security Hub zentralisiert und priorisiert Sicherheits- und Compliance-Erkenntnisse aus AWS Konten, Diensten und unterstützten Drittanbietern, um Sie bei der Analyse Ihrer Sicherheitstrends und der Identifizierung der Sicherheitsprobleme mit der höchsten Priorität zu unterstützen. Weitere Informationen hierzu finden Sie unter AWS Security Hub.

Häufig gestellte Fragen zu Security Hub in AWS Managed Services

F: Wie beantrage ich Zugriff auf AWS Security Hub in meinem AMS-Konto?

Fordern Sie Zugriff auf Security Hub an, indem Sie einen RFC mit dem Änderungstyp Management | AWS-Service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer_securityhub_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung von Security Hub in meinem AMS-Konto?

Die Archivierungsfunktion wurde als potenzielles Sicherheits- und Betriebsrisiko eingestuft und im Rahmen der Sicherheitsfunktion des selbst bereitgestellten Dienstes eingeschränkt.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Security Hub in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Security Hub in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Service Catalog AppRegistry in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AppRegistry Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AppRegistry ermöglicht die Anwendungssuche, Berichterstattung und Verwaltungsaktionen von einem zentralen Ort aus. Entwickler erstellen selten Anwendungen in einem einzigen AWS Konto. In der Regel trennen

sie Anwendungsressourcen nach Lebenszyklusphasen wie Entwicklung, Test und Produktion. AppRegistry ermöglicht es Ihnen, all Ihre Ressourcensammlungen in den von Ihnen definierten AWS Konten zu gruppieren und anzuzeigen.

Mit AppRegistry können Sie Ihre AWS Anwendungen, die Sammlung von Ressourcen, die Ihren Anwendungen zugeordnet sind, und Anwendungsattributgruppen speichern. Weitere Informationen finden Sie unter Was ist AppRegistry.

Häufig gestellte Fragen: AWS Service Catalog AppRegistry im AMS

F: Wie beantrage ich Zugriff AWS Service Catalog AppRegistry auf mein AMS-Konto?

Beantragen Sie den Zugriff auf, AppRegistry indem Sie einen RFC mit dem Änderungstyp Verwaltung | AWS Service | Self-Provisioned Service | Add (Überprüfung erforderlich) (ct-3qe6io8t6jtny) einreichen. Dieser RFC stellt `customer-appregistry-console-role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihrer Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Service Catalog AppRegistry in meinem AMS-Konto?

Der volle Zugriff auf den AppRegistry Dienst wird gewährt, mit Ausnahme der Verwendung des AMS-Namespace im `'Name'` Tag.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Service Catalog AppRegistry in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung AppRegistry in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Shield Advanced in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Shield Advanced Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Shield Advanced ist ein verwalteter Service zum Schutz vor verteilten Denial of Service (DDoS), der Anwendungen schützt, auf denen ausgeführt wird. AWS Shield Advanced bietet eine ständig aktive Erkennung und automatische Inline-Abwehrmaßnahmen, die Ausfallzeiten und Latenz von Anwendungen minimieren, sodass Sie nicht den AWS Support in Anspruch nehmen müssen, um vom DDo S-Schutz

zu profitieren. Es gibt zwei Stufen: AWS Shield Standard und Advanced; AMS bietet Shield Advanced an. Weitere Informationen finden Sie unter Shield Advanced.

Alle AWS Kunden profitieren ohne zusätzliche Kosten vom automatischen Schutz von AWS Shield Standard. AWS Shield Standard schützt vor den häufigsten, häufig auftretenden Netzwerk- und DDo Transport-Layer-S-Angriffen, die auf Ihre Website oder Anwendungen abzielen. Wenn Sie Amazon CloudFront und Amazon Route 53 verwenden AWS Shield Standard , erhalten Sie umfassenden Verfügbarkeitsschutz vor allen bekannten Infrastrukturangriffen (Layer 3 und 4).

Für einen besseren Schutz vor Angriffen auf Ihre Anwendungen, die auf Ressourcen von Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (ELB) CloudFront AWS Global Accelerator, Amazon und Amazon Route 53 ausgeführt werden, können Sie abonnieren AWS Shield Advanced.

Zusätzlich zu den mitgelieferten Schutz auf Netzwerk- und Transportebene AWS Shield Advanced bietet es zusätzliche Erkennung und Abwehr großer und ausgeklügelter DDo S-Angriffe, Einblicke in Angriffe nahezu in Echtzeit und die Integration mit AWS WAF einer Firewall für Webanwendungen. AWS Shield Standard AWS Shield Advanced bietet Ihnen außerdem rund um die Uhr Zugriff auf das AWS Shield Response Team (SRT) und Schutz vor DDo S-bedingten Spitzen in Ihren Gebühren für Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (Elastic Load Balancing) CloudFront AWS Global Accelerator, Amazon und Amazon Route 53.

Häufig gestellte Fragen zu Shield Advanced in AWS Managed Services

F: Wie beantrage ich Zugriff auf Shield Advanced in meinem AMS-Konto?

Fordern Sie Zugriff auf Shield Advanced an, indem Sie einen RFC mit dem Änderungstyp Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_shield_role` `aws_drt_shield_role` Konto die folgenden IAM-Rollen zur Verfügung: und. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rollen in Ihre Verbundlösung integrieren.

Nachdem die Rollen in Ihrem Konto bereitgestellt wurden, können Sie sie verwenden, `customer_shield_role` um Ihr Abonnement AWS Shield Advanced in Ihrem Konto zu bestätigen.

> **Note**
>
> Beachten Sie, dass mit der Nutzung von eine monatliche Gebühr und eine einjährige Verpflichtung verbunden sind. AWS Shield Advanced Darüber hinaus berechtigt die Verwendung AWS Shield Advanced in AMS AMS zur Eskalation an den AWS Shield (SRT),

der bei eskalierten Distributed-Denial-of-Service (S) -Vorfällen Änderungen an den Firewall-Regeln (AWS WAF) Ihrer Webanwendung vornehmen kann. DDo Diese Änderungen werden in Abstimmung mit AMS vorgenommen.

F: Welche Einschränkungen gelten für die Nutzung von Shield Advanced in meinem AMS-Konto?

Dies ist zwar keine Einschränkung, Sie sollten sich jedoch darüber im Klaren sein, dass bei Verwendung von Shield Advanced die bereitgestellt wird`aws_drt_shield_role`, sodass AWS Shield Teams (SRT) bei eskalierten DDo S-Vorfällen Notfalländerungen an AWS WAF Regeln innerhalb von AMS-Konten vornehmen können. Dies wird von AMS für die schnellste Behebung von S-Angriffen empfohlen und würde nach einer DDo AMS-Eskalation an das SRT erfolgen.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von Shield Advanced in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten, um Shield Advanced in Ihrem AMS-Konto zu verwenden.

Verwenden Sie AMS SSP zur Bereitstellung AWS Snowball Edge in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf Snowball Edge-Funktionen zuzugreifen. Snowball Edge ist eine Datentransportlösung im Petabyte-Bereich, die Geräte verwendet, die so konzipiert sind, dass sie sicher sind, um große Datenmengen in die und aus der Cloud zu übertragen. AWS Snowball Edge bewältigt häufig auftretende Herausforderungen im Zusammenhang mit umfangreichen Datenübertragungen, darunter hohe Netzwerkkosten, lange Übertragungszeiten und Sicherheitsbedenken. Sie können Snowball Edge verwenden, um Analysedaten, Genomikdaten, Videobibliotheken, Bildrepositorys und Backups zu migrieren und Teile von Rechenzentrumsabschaltungen, Bandaustauschprojekten oder Anwendungsmigrationsprojekten zu archivieren. Die Übertragung von Daten mit Snowball Edge ist einfach, schnell, sicherer und kann nur ein Fünftel der Kosten für die Übertragung von Daten über Highspeed-Internet kosten.

Mit Snowball Edge müssen Sie keinen Code schreiben oder Hardware kaufen, um Ihre Daten zu übertragen. Verwenden Sie zunächst die AWS Management Console, um einen Importauftrag für Snowball zu erstellen, und ein Snowball-Gerät wird Ihnen automatisch zugeschickt. Sobald es ankommt, schließen Sie das Gerät an Ihr lokales Netzwerk an, laden Sie den Snowball-Client („Client“) herunter und führen Sie ihn aus, um eine Verbindung herzustellen, und wählen Sie dann

mit dem Client die Dateiverzeichnisse aus, die Sie auf das Gerät übertragen möchten. Der Client verschlüsselt dann die Dateien und überträgt sie mit hoher Geschwindigkeit auf das Gerät. Sobald die Übertragung abgeschlossen ist und das Gerät zur Rücksendung bereit ist, wird das E Ink-Versandetikett automatisch aktualisiert und Sie können den Auftragsstatus mit Amazon Simple Notification Service (Amazon SNS), Textnachrichten oder direkt in der Konsole verfolgen. Weitere Informationen hierzu finden Sie unter AWS Snowball Edge.

Häufig gestellte Fragen zu Snowball Edge in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS Snowball Edge auf mein AMS-Konto?

Die Implementierung von Snowball Edge in AMS erfolgt in zwei Schritten:

1. Reichen Sie einen Änderungstyp Management | Andere | Andere | Erstellen Sie einen (ct-1e1xtak34nx76) -Änderungstyp und fordern Sie eine Servicerolle für Snowball Edge für Ihr AMS-Konto an.
2. Beantragen Sie Benutzerzugriff, indem Sie die folgenden Optionen einreichen: Verwaltung | AWS Dienst | Selbst bereitgestellter Dienst | Änderungstyp hinzufügen (ct-1w8z66n899dct). Dieser RFC stellt Ihrem Konto die folgenden IAM-Rollen zur Verfügung:, und. `customer_snowball_console_role` `customer_snowball_export_role` `customer_snowball_import_role` Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Snowball Edge in meinem AMS-Konto?

Die volle Funktionalität von AWS Snowball Edge ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Snowball Edge in meinem AMS-Konto?

Sie müssen über das oben angegebene Servicerollenkonto verfügen.

Verwenden Sie AMS SSP zur Bereitstellung AWS Step Functions in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Step Functions Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Step Functions ist

ein Webservice, mit dem Sie die Komponenten verteilter Anwendungen und Microservices mithilfe visueller Workflows koordinieren können. Sie erstellen Anwendungen aus einzelnen Komponenten, die jeweils eine diskrete Funktion oder Aufgabe ausführen, sodass Sie Anwendungen schnell skalieren und verändern können. Step Functions bietet eine zuverlässige Möglichkeit, Komponenten zu koordinieren und die Funktionen Ihrer Anwendung Schritt für Schritt durchzugehen. Step Functions bietet eine grafische Konsole, mit der Sie die Komponenten Ihrer Anwendung als eine Reihe von Schritten visualisieren können. Sie löst jeden Schritt automatisch aus, verfolgt ihn und versucht es erneut, wenn Fehler auftreten, sodass Ihre Anwendung jedes Mal in der richtigen Reihenfolge und wie erwartet ausgeführt wird. Step Functions protokolliert den Status jedes Schritts, sodass Sie Probleme schnell diagnostizieren und debuggen können, wenn etwas schief geht. Weitere Informationen hierzu finden Sie unter AWS Step Functions.

Häufig gestellte Fragen zu Step Functions in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS Step Functions auf mein AMS-Konto?

Beantragen Sie den Zugriff auf, AWS Step Functions indem Sie einen RFC mit Management | AWS Service | Self-Provisioned Service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_step_functions_role` Konto die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Step Functions in meinem AMS-Konto?

Die volle Funktionalität von AWS Step Functions ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Step Functions in meinem AMS-Konto?

Zur Laufzeit muss die von Step Functions verwendete Rolle Zugriff auf die von der Step-Funktion verwendeten Dienste haben. Beispielsweise könnte eine Schrittfunktion von Lambda-Funktionen abhängen. Jemand, der eine Step-Funktion erstellt, erstellt wahrscheinlich gleichzeitig Lambda-Funktionen und müsste auch Zugriff auf diesen Dienst anfordern.

Verwenden Sie AMS SSP, um AWS Systems Manager Parameter Store in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf AWS Systems Manager Parameter Store-Funktionen zuzugreifen.

AWS Systems Manager Der Parameter Store bietet sicheren, hierarchischen Speicher für die Verwaltung von Konfigurationsdaten und Geheimnissen. Sie können Daten wie Passwörter, Datenbankzeichenfolgen und Lizenzcodes als Parameterwerte speichern. Sie können Werte als Klartext oder als verschlüsselte Daten speichern. Anschließend können Sie anhand des eindeutigen Namens, den Sie beim Erstellen des Parameters angegeben haben, auf die Werte verweisen. Parameter Store ist hochgradig skalierbar, verfügbar und langlebig und wird von der AWS Cloud unterstützt. Weitere Informationen finden Sie unter AWS Systems Manager Parameter Store.

> **Note**
>
> Wenn Sie einen dedizierten Geheimspeicher mit Lebenszyklusmanagement wünschen, verwenden Sie Verwenden Sie AMS SSP zur Bereitstellung AWS Secrets Manager in Ihrem AMS-Konto anstelle von Parameter Store. Secrets Manager hilft Ihnen dabei, Ihre Sicherheits- und Compliance-Anforderungen zu erfüllen, indem Sie Secrets automatisch rotieren lassen können. Secrets Manager bietet eine integrierte Integration für MySQL, PostgreSQL und Amazon Aurora auf Amazon RDS, die durch die Anpassung von Lambda-Funktionen auf andere Arten von Geheimnissen erweiterbar ist.

AWS Systems Manager Häufig gestellte Fragen zum Speichern von Parametern in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Systems Manager Parameter Store in meinem AMS-Konto?

Beantragen Sie den Zugriff auf den AWS Systems Manager Parameterspeicher, indem Sie einen RFC an folgende Adresse senden: Management | AWS Service | Self-Provisioned Service | Änderungstyp hinzufügen (ct-1w8z66n899dct). Dieser RFC stellt `customer_systemsmanager_parameterstore_console_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Verwendung von AWS Systems Manager Parameter Store in meinem AMS-Konto?

Sie müssen AWS verwaltete Schlüssel verwenden. Der Zugriff ist auf die Erstellung benutzerdefinierter KMS-Schlüssel beschränkt. Wenn jedoch ein benutzerdefinierter Schlüssel

erforderlich ist, reichen Sie einen RFC ein, um einen vom Kunden verwalteten Schlüssel (CMK) zu erstellen. Verwenden Sie dabei Deployment | Advanced Stack Components | KMS-Schlüssel | Änderungstyp erstellen (ct-1d84keiri1jhg) mit dieser IAM-Rolle als Wert für die Parameter und. `customer_systemsmanager_parameterstore_console_role` `IAMPrincipalsRequiringDecryptPermissions` `IAMPrincipalsRequiringEncryptPermissionsPrincipal` Nachdem der KMS-Schlüssel erstellt wurde, können Sie damit eine sichere Zeichenfolge erstellen.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von AWS Systems Manager Parameter Store in meinem AMS-Konto?

Es gibt keine Voraussetzungen. SSM Parameter Store ist jedoch darauf angewiesen, dass KMS eine sichere Zeichenfolge erstellt, sodass Sie die im Parameter Store gespeicherten Werte ver- und entschlüsseln können.

Verwenden Sie AMS SSP, um AWS Systems Manager Automation in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf AWS Systems Manager Automatisierungsfunktionen zuzugreifen. AWS Systems Manager Die Automatisierung vereinfacht allgemeine Wartungs- und Bereitstellungsaufgaben von Amazon Elastic Compute Cloud-Instances und anderen AWS Ressourcen mithilfe von Runbooks, Aktionen und Servicekontingenten. Sie ermöglicht es Ihnen, Automatisierungen in großem Umfang zu erstellen, auszuführen und zu überwachen. Eine Systems Manager-Automatisierung ist eine Art von Systems Manager Manager-Dokument, das die Aktionen definiert, die Systems Manager auf Ihren verwalteten Instanzen ausführt. Ein Runbook, mit dem Sie allgemeine Wartungs- und Bereitstellungsaufgaben wie das Ausführen von Befehlen oder Automatisierungsskripten in Ihren verwalteten Instanzen ausführen. Systems Manager umfasst Funktionen, mit denen Sie mithilfe von Amazon Elastic Compute Cloud-Tags auf große Gruppen von Instances abzielen können, sowie Geschwindigkeitssteuerungen, mit denen Sie Änderungen gemäß den von Ihnen definierten Grenzwerten implementieren können. Die Runbooks werden mit JavaScript Object Notation (JSON) oder YAML geschrieben. Mit dem Document Builder in der Systems Manager-Automation-Konsole können Sie jedoch ein Runbook erstellen, ohne nativen JSON- oder YAML-Code erstellen zu müssen. Alternativ können Sie von Systems Manager bereitgestellte Runbooks mit vordefinierten Schritten verwenden, die Ihren Anforderungen entsprechen. Weitere Informationen finden Sie in der Dokumentation unter Arbeiten mit Runbooks. AWS Systems Manager

> **Note**
>
> Systems Manager Automation unterstützt zwar 20 Aktionstypen, die im Runbook verwendet werden können, aber eine begrenzte Anzahl von Aktionen, die Sie beim Erstellen von Runbooks verwenden können, können Sie in Ihrem AMS Advanced-Konto verwenden. Ebenso kann eine begrenzte Anzahl von Runbooks, die von Systems Manager bereitgestellt werden, entweder direkt oder in Ihrem eigenen Runbook verwendet werden. Einzelheiten finden Sie in den folgenden häufig gestellten Fragen zu den Einschränkungen.

AWS Systems Manager Häufig gestellte Fragen zur Automatisierung in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf Systems Manager Automation in meinem AMS-Konto?

Beantragen Sie Zugriff auf AWS Systems Manager Automation, indem Sie einen RFC über Management | AWS Service | Self-Provisioned Service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer_systemsmanager_automation_console_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Was sind die Einschränkungen bei der Nutzung von AWS Systems Manager Automation in meinem AMS-Konto?

Sie müssen Ihr Runbook mit einer begrenzten Anzahl von von Systems Manager unterstützten Aktionen zur Automatisierung nur verfassen, um and/or Befehlsskripts innerhalb Ihrer verwalteten Instanzen auszuführen. Die Aktionen, die Ihnen zur Verfügung stehen, sowie etwaige Einschränkungen werden im Folgenden beschrieben.

AWS Systems Manager Einschränkungen der Automatisierung

Aktion	Beschreibung	Einschränkung
aws: assertAwsResource Eigentum —	Bestätigen Sie einen AWS Ressourcen- oder Ereigniss tatus	Nur EC2 Instanzen

Aktion	Beschreibung	Einschränkung
aws:aws:branch —	Führen Sie bedingte Automatisierungsschritte aus	Keine Einschränkung
AWS: CreateTags —	Tags für Ressourcen erstellen AWS	Nur für SSM-Automatisierungs-Runbooks, die Sie erstellen
AWS: ExecuteAutomation —	Führen Sie eine weitere Automatisierung aus	Nur das Automatisierungs-Runbook, das Sie erstellen
aws:ExecuteScript —	Führen Sie ein Skript aus	Das einzige Skript, das keine API-Aufrufe an Dienste tätigt
aws:pause —	Eine Automatisierung pausieren	Keine Einschränkung
aws:RunCommand —	Führen Sie einen Befehl auf einer verwalteten Instanz aus	Verwenden Sie nur das vom System Manager bereitgestellte Dokument - AWS-RunShellScript und AWS-RunPowerShellScript
aws:sleep —	Eine Automatisierung verzögern	Keine Einschränkung
als: waitForAws ResourceProperty —	Warte auf eine AWS Ressourceneigenschaft	Nur EC2 Instanzen

Sie können sich auch dafür entscheiden, Befehle oder Skripte direkt mit dem von Systems Manager bereitgestellten Runbook AWS RunShellScript und AWS auszuführen, RunPowerShellScript indem Sie die Funktion „Befehl ausführen“ in der Systems Manager Manager-Konsole verwenden. Sie können diese Runbooks auch in Ihrem Runbook verschachteln, um zusätzliche Prüfungen vor der Nachbearbeitung oder eine komplexe Automatisierungslogik zu and/or ermöglichen.

Die Rolle folgt dem Prinzip der geringsten Rechte und gewährt nur die erforderlichen Berechtigungen zum Verfassen, Ausführen und Abrufen von Ausführungsdetails von Runbooks, die auf die Ausführung von and/or Befehlsskripten in Ihren verwalteten Instances abzielen. Sie gewährt keine

Genehmigung für andere Funktionen, die der AWS Systems Manager Dienst bereitstellt. Mit dieser Funktion können Sie Automatisierungs-Runbooks erstellen, die Ausführung der Runbooks kann jedoch nicht auf AMS-eigene Ressourcen ausgerichtet werden.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung von AWS Systems Manager Automation in meinem AMS-Konto?

Es gibt keine Voraussetzungen. Sie müssen jedoch sicherstellen, dass Ihre internen and/or Compliance-Kontrollen bei der Erstellung von Runbooks eingehalten werden. Wir empfehlen außerdem, Runbooks gründlich zu testen, bevor Sie sie mit Produktionsressourcen ausführen.

F: Kann die Systems Manager Manager-Richtlinie mit anderen IAM-Rollen verknüpft **`customer_systemsmanager_automation_policy`** werden?

Nein, im Gegensatz zu anderen Self-Provision-fähigen Diensten kann diese Richtlinie nur der bereitgestellten Standardrolle zugewiesen werden. `customer_systemsmanager_automation_console_role`

Im Gegensatz zu den Richtlinien anderer SSPS-Rollen kann diese SSM-SSPS-Richtlinie nicht mit anderen benutzerdefinierten IAM-Rollen gemeinsam genutzt werden, da dieser AMS-Dienst nur zum Ausführen von Befehlen oder Automatisierungsskripten innerhalb Ihrer verwalteten Instanzen dient. Wenn diese Berechtigungen mit anderen benutzerdefinierten IAM-Rollen verknüpft werden könnten, möglicherweise mit Berechtigungen für andere Dienste, könnte sich der Umfang der zulässigen Aktionen auf verwaltete Dienste erstrecken und die Sicherheitslage Ihres Kontos potenziell beeinträchtigen.

Wenden Sie sich an Ihren jeweiligen Cloud-Architekten oder Service Delivery Manager, um alle Änderungsanträge (RFCs) anhand unserer technischen AMS-Standards zu bewerten. Weitere Informationen finden Sie unter RFC-Sicherheitsüberprüfungen.

> **Note**
>
> AWS Systems Manager ermöglicht es Ihnen, Runbooks zu verwenden, die mit Ihrem Konto geteilt werden. Wir empfehlen Ihnen, Vorsicht walten zu lassen und eine Due-Diligence-Prüfung durchzuführen, wenn Sie gemeinsam genutzte Runbooks verwenden. Stellen Sie außerdem sicher, dass Sie vor der Ausführung der Runbooks den Inhalt überprüfen, um zu verstehen, welche Runbooks ausgeführt command/scripts werden. Einzelheiten finden Sie unter Bewährte Methoden für gemeinsam genutzte SSM-Dokumente.

Verwenden Sie AMS SSP zur Bereitstellung AWS Transfer Family in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt in Ihrem AMS-verwalteten Konto auf Funktionen AWS Transfer Family (Transfer Family) zuzugreifen. AWS Transfer Family ist ein vollständig verwalteter AWS Service, mit dem Sie Dateien über das Secure File Transfer Protocol (SFTP) in den und aus dem Amazon Simple Storage Service (Amazon S3) -Speicher übertragen können. SFTP wird auch als Secure Shell (SSH) File Transfer Protocol bezeichnet. SFTP wird für den Datenaustausch zwischen unterschiedlichen Branchen wie Finanzdienstleistungen, Gesundheitswesen, Werbung, Einzelhandel usw. eingesetzt.

Mit AWS SFTP erhalten Sie Zugriff auf einen SFTP-Server, AWS ohne eine Serverinfrastruktur betreiben zu müssen. Sie können diesen Service verwenden, um Ihre SFTP-basierten Workflows zu migrieren und AWS gleichzeitig die Clients und Konfigurationen Ihrer Endbenutzer unverändert beizubehalten. Sie verknüpfen Ihren Hostnamen zunächst mit dem SFTP-Serverendpunkt, fügen dann Ihre Benutzer hinzu und gewähren ihnen die richtige Zugriffsebene. Danach werden die Übertragungsanfragen Ihrer Benutzer direkt von Ihrem AWS SFTP-Serverendpunkt aus bearbeitet. Weitere Informationen finden Sie unter Einen AWS Transfer for SFTPSFTP-fähigen Server erstellen.

AWS Transfer for SFTP in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS Transfer for SFTP auf mein AMS-Konto?

Beantragen Sie den Zugriff auf, AWS Transfer for SFTP indem Sie einen RFC mit Management | AWS Service | Self-Provisioned Service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Über diesen RFC werden die folgenden IAM-Rollen und eine Richtlinie in Ihrem Konto bereitgestellt:

- `customer_transfer_author_role`. Mit dieser Rolle können Sie den SFTP-Dienst über die Konsole verwalten.
- `customer_transfer_sftp_server_logging_role`. Diese Rolle ist so konzipiert, dass sie an den SFTP-Server angehängt werden kann. Sie ermöglicht dem SFTP-Server das Abrufen von Protokollen. CloudWatch
- `customer_transfer_sftp_user_role`. Diese Rolle ist so konzipiert, dass sie den SFTP-Benutzern zugewiesen werden kann. Sie ermöglicht den SFTP-Benutzern die Interaktion mit dem S3-Bucket.

- `policy customer_transfer_scope_down_policy`. Bei dieser Richtlinie handelt es sich um eine Scopedown-Richtlinie, die auf den SFTP-Benutzer angewendet werden kann, um seinen Zugriff auf den S3-Bucket auf seine Home-Ordner zu beschränken.
- `customer_transfer_sftp_efs_user_role`. Diese Rolle ist so konzipiert, dass sie den SFTP-Benutzern zugewiesen werden kann. Es ermöglicht den SFTP-Benutzern die Interaktion mit dem EFS-Dateisystem.

Nachdem es in Ihrem Konto bereitgestellt wurde, müssen Sie die Rollen in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Transfer for SFTP in meinem AMS-Konto?

AWS Die Übertragung für die SFTP-Konfiguration ist auf Ressourcen ohne „AMS-“ oder „MC-“ -Präfixe beschränkt, um jegliche Änderungen an der AMS-Infrastruktur zu verhindern.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Transfer for SFTP in meinem AMS-Konto?

- Sie benötigen einen Amazon S3 S3-Bucket mit einem Namen, der das Schlüsselwort „transfer“ enthält, bevor Sie den AWS Transfer for SFTP Server und die Benutzer erstellen können.
- Um einen „Customer Identify Provider“ zu verwenden, müssen Sie das API Gateway, die Lambda-Funktion und Ihr Benutzer-Repository (AD, Secrets Manager usw.) bereitstellen. Weitere Informationen finden Sie unter Aktivieren der Kennwortauthentifizierung für die AWS Transfer for SFTP Verwendung von AWS Secrets Manager und die Arbeit mit Identitätsanbietern.

Verwenden Sie AMS SSP zur Bereitstellung AWS Transit Gateway in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Transit Gateway Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS Transit Gateway ist ein Service, mit dem Sie Ihre Amazon Virtual Private Cloud (VPCs) und Ihre lokalen Netzwerke mit einem einzigen Gateway verbinden können. Wenn Sie die Anzahl der Workloads erhöhen AWS, auf denen ausgeführt wird, müssen Sie in der Lage sein, Ihre Netzwerke auf mehrere Konten zu skalieren, und Amazon VPCs muss mit dem Wachstum Schritt halten können. Heute können Sie Amazon-Paare VPCs mithilfe von Peering verbinden. Die Verwaltung der point-to-point Konnektivität in vielen Amazon-Ländern ohne die Möglichkeit VPCs, die Konnektivitätsrichtlinien zentral zu verwalten, kann jedoch betrieblich kostspielig und umständlich sein. Für lokale Konnektivität müssen Sie Ihr AWS

VPN mit jeder einzelnen Amazon-VPC verbinden. Die Entwicklung dieser Lösung kann zeitaufwändig und schwierig zu verwalten sein, wenn die Anzahl der Lösungen auf Hunderte VPCs ansteigt. Weitere Informationen hierzu finden Sie unter AWS Transit Gateway.

AWS Transit Gateway in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS Transit Gateway auf mein AMS-Konto?

Beantragen Sie den Zugriff auf, AWS Transit Gateway indem Sie einen RFC mit Management | AWS Service | Self-Provisioned Service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem `customer_tgw_console_role` Konto die folgende IAM-Rolle zur Verfügung:. Nach der Bereitstellung in Ihrem Konto müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Transit Gateway in meinem AMS-Konto?

Die volle Funktionalität von AWS Transit Gateway ist in Ihrem AMS-Landezone-Konto mit einem Konto verfügbar, mit Ausnahme von Änderungen der Routentabelle für das Transit Gateway Gateway-Routing. Fordern Sie Änderungen an der Routentabelle an, indem Sie Folgendes einreichen: Management | Sonstige | Änderungstyp erstellen (ct-1e1xtak34nx76).

> **Note**
>
> Dieser Dienst wird nur für die landing zone mit einem Konto (SALZ) unterstützt, nicht für die landing zone mit mehreren Konten (MALZ).

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Transit Gateway in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Transit Gateway in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung von AWS WAF Web Application Firewall in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS WAF Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. AWS WAF ist eine Firewall für

Webanwendungen (AWS WAF), mit der Sie Ihre Webanwendungen vor häufigen Web-Exploits schützen können, die die Verfügbarkeit von Anwendungen beeinträchtigen, die Sicherheit gefährden oder übermäßig viele Ressourcen verbrauchen könnten. AWS WAF gibt Ihnen die Kontrolle darüber, welcher Datenverkehr zu Ihren Webanwendungen zugelassen oder blockiert werden soll, indem Sie anpassbare Websicherheitsregeln definieren. Sie können AWS WAF damit benutzerdefinierte Regeln erstellen, die gängige Angriffsmuster wie SQL-Injection oder Cross-Site-Scripting blockieren, sowie Regeln, die auf Ihre spezifische Anwendung zugeschnitten sind.

Weitere Informationen finden Sie unter AWS WAF — Web Application Firewall.

AMS unterstützt keine Überwachung (CloudWatch Alarme/Ereignisse/MMS-Warnungen) für AWS WAF. Es liegt in der Natur des AWS WAF Systems, dass Sie benutzerdefinierte Regeln für Ihre Anwendungen erstellen müssen. AMS kann Alarme nicht quantifizieren und für Sie erstellen, ohne den Kontext Ihrer Anwendung zu berücksichtigen. Weitere Informationen finden Sie unter AWS WAF — Web Application Firewall.

AWS WAF in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich AWS WAF die Einrichtung in meinem AMS-Konto?

Beantragen Sie den Zugriff auf, AWS WAF indem Sie einen RFC mit dem Management | AWS-Service | Selbstbereitgestellter Service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer_waf_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nachdem die AWS WAF IAM-Rolle in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gibt es bei der Nutzung? AWS WAF

Nachdem die Berechtigungen bereitgestellt wurden, steht Ihnen der volle Funktionsumfang von AWS WAF zur Verfügung.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung AWS WAF?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Verwendung AWS WAF in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS Well-Architected Tool in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS Well-Architected Tool Funktionen in Ihrem von AMS verwalteten Konto zuzugreifen. Auf diese AWS Well-Architected Tool Weise können Sie den Status Ihrer Workloads überprüfen und sie mit den neuesten AWS Best Practices für die Architektur vergleichen. Das Tool basiert auf dem AWS Well-Architected Framework, das Cloud-Architekten beim Aufbau einer sicheren, leistungsstarken, belastbaren und effizienten Anwendungsinfrastruktur unterstützt. Dieses Framework bietet Ihnen einen konsistenten Ansatz zur Bewertung von Architekturen, wurde in Zehntausenden von Workload-Überprüfungen verwendet, die vom AWS Lösungsarchitekturteam durchgeführt wurden, und bietet Anleitungen zur Implementierung von Designs, die im Laufe der Zeit an die Anwendungsanforderungen angepasst werden. Weitere Informationen hierzu finden Sie unter AWS Well-Architected Tool.

AWS WA Tool in häufig gestellten Fragen zu AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS Well-Architected Tool auf mein AMS-Konto?

Beantragen Sie den Zugriff auf, AWS Well-Architected Tool indem Sie einen RFC mit dem Management | AWS-Service | Selbstbereitgestellter Service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer_well_architected_tool_console_admin_role` Ihrem Konto die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

F: Welche Einschränkungen gelten für die Nutzung AWS Well-Architected Tool in meinem AMS-Konto?

Die volle Funktionalität von AWS Well-Architected Tool ist in Ihrem AMS-Konto verfügbar.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Well-Architected Tool in meinem AMS-Konto?

Es gibt keine Voraussetzungen oder Abhängigkeiten für die Nutzung AWS Well-Architected Tool in Ihrem AMS-Konto.

Verwenden Sie AMS SSP zur Bereitstellung AWS X-Ray in Ihrem AMS-Konto

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um direkt auf AWS X-Ray (X-Ray) -Funktionen in Ihrem verwalteten AMS-Konto zuzugreifen. AWS X-Ray hilft Entwicklern dabei, verteilte Produktionsanwendungen zu analysieren und zu debuggen, z. B. solche, die mit einer Microservices-Architektur erstellt wurden. Mit X-Ray können Sie die Leistung Ihrer Anwendung und der zugrunde liegenden Dienste nachvollziehen, um die Hauptursache von Leistungsproblemen und Fehlern zu identifizieren und zu beheben. X-Ray bietet eine end-to-end Übersicht der Anfragen, während sie Ihre Anwendung durchlaufen, und zeigt eine Übersicht der Ihrer Anwendung zugrunde liegenden Komponenten. Mit X-Ray können Sie sowohl Anwendungen in der Entwicklung als auch in der Produktion analysieren, von einfachen dreistufigen Anwendungen bis hin zu komplexen Microservices-Anwendungen, die aus Tausenden von Diensten bestehen. Weitere Informationen hierzu finden Sie unter AWS X-Ray.

Häufig gestellte Fragen zu X-Ray in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff AWS X-Ray auf mein AMS-Konto?

Beantragen Sie den Zugriff, indem Sie den Änderungstyp Verwaltung | AWS Service | Self-Provisioned Service | Add (ct-1w8z66n899dct) einreichen. Dieser RFC stellt Ihrem Konto `customer_xray_console_role` die folgende IAM-Rolle zur Verfügung:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren. Darüber hinaus müssen Sie über die `customer_xray_daemon_write_instance_profile` Möglichkeit verfügen, Daten von Ihren EC2 Amazon-Instances an X-Ray zu übertragen. Dieses Instance-Profil wird erstellt, wenn Sie das erhaltencustomer_xray_console_role.

Sie können eine Serviceanfrage an AMS Operations senden, um sie dem `customer_xray_daemon_write_policy` vorhandenen Instance-Profil zuzuweisen, oder Sie können das Instance-Profil verwenden, das erstellt wird, wenn AMS Operations X-Ray für Sie aktiviert.

F: Welche Einschränkungen gelten für die Nutzung AWS X-Ray in meinem AMS-Konto?

Die volle Funktionalität von AWS X-Ray ist in Ihrem AMS-Konto verfügbar, mit Ausnahme der Verschlüsselung mit dem AWS KMS-Schlüssel (KMS-Schlüssel). AWS X-Ray verschlüsselt standardmäßig alle Trace-Daten. Standardmäßig verschlüsselt X-Ray Traces und zugehörige Daten

im Ruhezustand. Wenn Sie Daten im Ruhezustand mit einem Schlüssel verschlüsseln müssen, können Sie entweder einen verwalteten AWS KMS-Schlüssel (aws/xray) oder einen vom Kunden verwalteten KMS-Schlüssel wählen. Reichen Sie für KMS Customer-Managed Key for X-Ray Encryption Folgendes ein: Management | Other | Other | Create change type (ct-1e1xtak34nx76).

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Nutzung in meinem AMS-Konto? AWS X-Ray

AWS X-Ray ist von Amazon S3 und CloudWatch Logs abhängig CloudWatch, die bereits in AMS-Konten implementiert sind. Transitive Abhängigkeiten variieren je nach Datenquellen und anderen AWS Diensten AWS X-Ray , mit denen Funktionen interagieren können (z. B. Amazon Redshift, Amazon RDS, Athena).

Verwenden Sie AMS SSP, um VM Import/Export in Ihrem AMS-Konto bereitzustellen

Verwenden Sie den AMS Self-Service Provisioning (SSP) -Modus, um Import/Exportcapabilities direkt in Ihrem AMS-verwalteten Konto auf VM zuzugreifen. Import/Export Mit VM können Sie auf einfache Weise VM-Images aus Ihrer vorhandenen Umgebung in EC2 Amazon-Instances importieren und sie zurück in Ihre lokale Umgebung exportieren. Dieses Angebot ermöglicht es Ihnen, Ihre bestehenden Investitionen in die virtuellen Maschinen, die Sie zur Erfüllung Ihrer Anforderungen an IT-Sicherheit, Konfigurationsmanagement und Compliance entwickelt haben, zu nutzen, indem Sie diese virtuellen Maschinen EC2 als ready-to-use Instances zu Amazon bringen. Sie können importierte Instances auch zurück in Ihre lokale Virtualisierungsinfrastruktur exportieren, sodass Sie Workloads in Ihrer gesamten IT-Infrastruktur bereitstellen können. Weitere Informationen finden Sie unter VM Import/Export.

Häufig gestellte Fragen Import/Export zu virtuellen Maschinen in AWS Managed Services

Häufig gestellte Fragen und Antworten:

F: Wie beantrage ich Zugriff auf virtuelle Maschinen Import/Export in meinem AMS-Konto?

Beantragen Sie den Zugriff auf die VM, Import/Export indem Sie einen RFC mit Management | AWS Service | Self-Provisioned Service | Änderungstyp hinzufügen (ct-1w8z66n899dct) einreichen. Dieser RFC stellt `customer_vmimport_policy` die folgende IAM-Richtlinie für Ihr Konto bereit:. Nachdem sie in Ihrem Konto bereitgestellt wurde, müssen Sie die Rolle in Ihre Verbundlösung integrieren.

Eine zusätzliche Rolle, die Import/Export VM-Dienstrolle, ist erforderlich, damit der Dienst Aktionen in Ihrem Konto ausführen kann.

F: Was sind die Einschränkungen bei der Verwendung von VM Import/Export in meinem AMS-Konto?

- Funktionen zum Importieren von benutzerdefinierten Maschinenabbildern und Datenvolumen sind beide in AMS VM Import/Export verfügbar. Die Berechtigungen für S3 wurden jedoch so eingeschränkt, dass Aktionen auf Buckets beschränkt werden, die dem Namen entsprechen, um den Zugriff auf `customer-vmimport-*` Informationen innerhalb des Kontos einzuschränken.
- Der Import von Images und Snapshots wird in AMS VM Import/Export unterstützt. Die Funktionen für den Instanzimport und den Instanzexport sind jedoch aus Sicherheitsgründen nicht verfügbar.
- Darüber hinaus wurde die Exportfunktion deaktiviert, um das Risiko des Exports eingeschränkter und sensibler Daten zu minimieren.

F: Was sind die Voraussetzungen oder Abhängigkeiten für die Verwendung von VM Import/Export in meinem AMS-Konto?

- Sie müssen ein unterstütztes Festplatten-Image für den Import in die AWS Umgebung bereitstellen. Weitere Informationen finden Sie unter Import/Export VM-Anforderungen.
- Auf die VM kann Import/Export nicht über die AWS Konsole zugegriffen werden. Sie müssen über AWS CLI, AWS -Tools für PowerShell oder den auf diesen Dienst zugreifen AWS SDKs. Oder Sie können ein Instanzprofil anfordern, indem Sie den Änderungstyp ct-117rmp64d5mvb einreichen: Bereitstellung | Erweiterte Stack-Komponenten | Identity and Access Management (IAM) | Instanzprofil erstellen. EC2 Dieses Instanzprofil ermöglicht es den Tools, Befehle von einer Instanz aus auszuführen.

Vom Kunden verwalteter Modus

Der kundenverwaltete Modus von AWS Managed Services (AMS) bietet ein flexibles Governance-Modell, das an Ihre Anforderungen angepasst werden kann. Dies kann als Ausweichoption für Dienste und Anwendungen angesehen werden, die AMS nicht für Sie ausführen kann. AMS betreibt keine Infrastruktur, die in Konten gehostet wird, die in diesem Modus erstellt wurden. In diesem Modus können Sie jedoch die zentralisierte Verwaltung mehrerer Konten nutzen. In diesem Modus können die folgenden Funktionen der Landing Zone für mehrere Konten genutzt werden:

- Automatisierte Kontobereitstellung

- Konnektivität über Transit Gateway im Netzwerkkonto
- Bibliothek mit AMS-Konfigurationsregeln
- Speichern Sie Kopien der Protokolle im Protokollkonto
- Zusammenfassung der vom Kunden verwalteten Guard Duty-Benachrichtigungen im Sicherheitskonto
- Konsolidierte Fakturierung
- Aktivierung benutzerdefinierter Service Control-Richtlinien.

Beispiel: Wenn Sie Workloads auf Ubuntu Pro ausführen möchten, bei dem es sich nicht um ein von AMS verwaltetes Betriebssystem handelt, können Sie ein vom Kunden verwaltetes Konto zum Hosten verwenden. Sie können Workloads auch über vom Kunden verwaltete Konten konsolidieren, um den Mengenrabatt auf reservierte Instances/Sharing Pläne zu nutzen, der durch gemeinsame Nutzung innerhalb einer AWS-Organisation verfügbar ist.

Erste Schritte mit dem vom Kunden verwalteten Modus

Der AMS-Modus „Customer Managed“ ist über ein spezielles Anwendungskonto mit mehreren Konten für die landing zone verfügbar.

Einzelheiten, einschließlich der Erstellung eines vom Kunden verwalteten Anwendungskontos, finden Sie unter Kundenverwaltete Anwendungskonten.

AMS- und AWS Service Catalog

Service Catalog in AWS Managed Services (AMS) ermöglicht es Unternehmen, Kataloge von AWS-Informationstechnologie (IT) -Services zu erstellen und zu verwalten. IT-Administratoren können Kataloge mit zugelassenen Produkten in ihren Konten erstellen, verwalten und an Endbenutzer verteilen, die dann in einem personalisierten Serviceportal auf die Produkte zugreifen können, die sie benötigen. Administratoren können kontrollieren, welche Benutzer Zugriff auf jedes Produkt haben, um die Einhaltung der Unternehmensrichtlinien durchzusetzen. Administratoren können auch Rollen einrichten, sodass Endbenutzer nur IAM-Zugriff auf Service Catalog benötigen, um genehmigte Ressourcen bereitzustellen. Service Catalog ermöglicht es Ihrem Unternehmen, von mehr Flexibilität und geringeren Kosten zu profitieren, da Endbenutzer in einem Katalog, den Sie kontrollieren, nur die Produkte finden und auf den Markt bringen können, die sie benötigen.

Service Catalog bietet Ihnen eine Alternative zum AMS Request for Change (RFC) -Prozess für die Bereitstellung und Aktualisierung von Ressourcen in Ihren AMS-verwalteten Konten. AMS verwaltet

alle Aufgaben des Infrastrukturbetriebs, die für den skalierbaren Betrieb von AWS für alle über Service Catalog bereitgestellten Infrastrukturressourcen erforderlich sind, einschließlich Sicherheit, Compliance, Bereitstellung, Verfügbarkeit, Patch, Überwachung, Warnung, Berichterstattung, Reaktion auf Vorfälle und Kostenoptimierung. Die Verwendung von Service Catalog in Ihrem AMS-verwalteten Konto bietet Ihnen einen Mechanismus zur zentralen Verwaltung häufig bereitgestellter IT-Services und hilft Ihnen dabei, eine konsistente Governance zu erreichen, während Benutzer schnell nur die genehmigten IT-Services bereitstellen können, die sie in ihren verwalteten Umgebungen benötigen.

Erste Schritte mit Service Catalog

Um mit Service Catalog in AMS zu beginnen, reichen Sie eine Serviceanfrage über die AMS-Konsole ein, um Zugriff auf Service Catalog anzufordern. Nach dem Absenden der Anfrage werden drei IAM-Rollen zusammen mit einem AMS-verwalteten Stack, der das CloudFormation Makro enthält, das das AMS aufruft `Transform` (zuvor beschrieben), in Ihren Konten bereitgestellt, sodass wir die Produkte in unseren Systemen registrieren und Operationen mit der über Service Catalog bereitgestellten Infrastruktur ausführen können. Zu den drei bereitgestellten IAM-Rollen gehören eine Rolle für IT-Administratoren zur Verwaltung von Produkten als Service Catalog-Administratoren, eine Rolle für Anwendungsbesitzer und Endbenutzer zum Konfigurieren, Starten und Verwalten von Produkten sowie eine Rolle, die als Starteinschränkung verwendet wird und die Berechtigungen definiert, die Service Catalog beim Starten oder Aktualisieren Ihres Produkts verwendet.

Service Catalog in AMS, bevor Sie beginnen

Ersetzt Service Catalog den bestehenden AMS Request for Change (RFC) -Prozess?

> In Konten, für die Service Catalog aktiviert ist, fungiert er als Change-Management-System, in dem Sie IT-Services in Ihrem AMS-Konto über Ihren vordefinierten Produktkatalog bereitstellen und aktualisieren. AMS stellt einen portfolio/product Standardkatalog bereit, und Ihre IT-Administratoren können Ihren eigenen erstellen und konfigurieren. Service Catalog bestätigt nur Stacks, die über Service Catalog bereitgestellt wurden. Ebenso können Dienste, die über Service Catalog bereitgestellt werden, nicht über den AMS RFC-Prozess geändert werden, da Änderungen außerhalb von Service Catalog dazu führen, dass der Stack von der genehmigten Produktkonfiguration abweicht.

Kann ich die über den Service Catalog bereitgestellten Stacks in der AMS-Konsole sehen?

> Ja. Sie können alle über den Servicekatalog bereitgestellten Stacks in der AMS-Konsole einsehen. Stacks, die über Service Catalog bereitgestellt werden, sind leicht anhand der Stack-

ID „SC-“ zu identifizieren. Stacks sind zwar in der AMS-Konsole sichtbar, sie können jedoch nicht über den AMS-RFC-Prozess aktualisiert werden. Der Zugriff auf das AMS-Change-Management-System (RFCs) ist ausschließlich auf Zugriffsanforderungen, Patch-Orchestrierung und Datensicherung beschränkt. RFCs

Wenn ich einen Stack über Service Catalog and/or aktualisiere, gibt es dann einen entsprechenden RFC in der AMS-Konsole?

Der einzige RFC, der in der AMS-Konsole angezeigt wird, ist ein RFC zur Registrierung des Stacks bei AMS, wenn ein Stack zum ersten Mal bereitgestellt wird. Dieser RFC wird automatisch durch den AMS-Validierungsprozess abgelegt, der ausgelöst wird, wenn ein Stack über Service Catalog gestartet wird. Alle anderen Bereitstellungen und Änderungen werden direkt in Service Catalog verfolgt und sind in der Service Catalog-Konsole sichtbar. Darüber hinaus können Sie die Funktion „Bereitgestellter Produktplan“ in Service Catalog verwenden, um die Liste der Änderungen anzuzeigen, die vor der Bereitstellung oder Aktualisierung des Produkts an den Ressourcen vorgenommen werden.

Muss ich etwas Spezielles für die Bereitstellung von Produkten in meinem AMS-verwalteten Konto tun?

Ja. Alle Service Catalog-Produkte, die in AMS-Konten bereitgestellt werden, müssen diese JSON-Zeile in der CFN-Vorlage enthalten, die dieses Produkt definiert:

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
{"Ref":"AWS::StackId"}}}
```

Dieser Codeausschnitt löst die AMS-Validierungen aus, die erforderlich sind, bevor die Ressource in Ihrem AMS-verwalteten Konto bereitgestellt werden kann. CloudFormation Es liegt in Ihrer Verantwortung, diese Codezeile als Teil der Produktdefinition aufzunehmen. Wenn es nicht enthalten ist, schlägt die Bereitstellung fehl und die folgende Fehlermeldung wird angezeigt: „Produkt konnte nicht erstellt werden. Dieses Konto wird von AMS verwaltet. Alle Produkte in AMS-Konten müssen den `Transform` AMS-Code in der Vorlage enthalten.“

Gibt es Service Catalog-Funktionen, die AMS-Kunden bei der Markteinführung nicht and/or eingeschränkt zur Verfügung stehen?

Ja, die folgenden SC-Funktionen sind für AMS-Kunden bei der ersten Markteinführung nicht verfügbar:

- Kontoerstellung über Service Catalog

- Möglichkeit, alle AWS-Services über Service Catalog auf einem von AMS verwalteten Konto zu starten. Die Verfügbarkeit von AWS-Services ist auf AMS-unterstützte Services (verwaltet und selbst bereitgestellt) beschränkt. Weitere Informationen zu AMS-unterstützten Services finden Sie in der AMS-Servicebeschreibung.
- Service Catalog IT Service Manager (ITSM) -Konnektoren kommunizieren nicht mit AMS-Vorfallberichten und Serviceanfragen.
- Möglichkeit, Service Catalog-Schnellstarts und Referenzarchitekturen ohne Änderungen zu nutzen. Denken Sie daran, dass Service Catalog-Produkte für AMS-Konten diese JSON-Codezeile enthalten müssen:

  ```
  "Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
  {"Ref":"AWS::StackId"}}}
  ```

  in der CNF-Vorlage. Beachten Sie, dass diese Zeile nicht Teil einer typischen CloudFormation AWS-Vorlage ist und explizit hinzugefügt werden muss.
- Terraform wird derzeit von AMS nicht für die Bereitstellung von Service Catalog-Produkten unterstützt.
- AWS-CFN-Stacksets werden in AMS nicht unterstützt.
- Sie können keine benutzerdefinierten IAM-Rollen erstellen.
- Serviceaktionen sind beschränkt auf:
  - AWS- RebootRdsInstance
  - AWS-Neustart-Instanz EC2
  - AWS-Startinstanz EC2
  - AWS- StartRdsInstance
  - AWS-Stopp-Instanz EC2
  - AWS- StopRdsInstance
  - AWS- CreateImage
  - AWS- CreateRdsSnapshot
  - AWS- CreateSnapshot

  > **Note**
  >
  > Bei der Erstellung von Serviceaktionen können Sie die Ausführungsrolle so konfigurieren, dass sie die Berechtigungen des Endbenutzers, die Startrolle oder

eine benutzerdefinierte IAM-Rolle Ihrer Wahl ist. Die ausgewählte Ausführungsrolle muss über ausreichende Berechtigungen verfügen, um die Dienstaktion auszuführen, und sie muss über eine Berechtigung verfügen TrustPolicy , mit der sie von Service Catalog übernommen werden kann. Andernfalls schlägt die Dienstaktion zur Ausführungszeit fehl. Wir empfehlen die Verwendung von AWSManagedServicesServiceCatalogLaunchRole, die über die richtigen Berechtigungen und die richtige Vertrauensrichtlinie für die Verwendung als Serviceaktion verfügt.

Wofür muss ich das AMS RFC-System weiterhin verwenden?

Bei allgemeiner Verfügbarkeit (GA) müssen Sie weiterhin RFCS verwenden, um die folgenden Aktionen auszuführen:

- Patch Orchestrator konfigurieren
- Konfiguration von Backup-Richtlinien
- Instanzzugriff anfordern
- Erstellung und Zuweisung von Sicherheitsgruppen, die nicht den AMS-Richtlinien entsprechen.
- Workload Ingest (WIGS) durchführen
- Erstellen von IAM-Rollen

Kann ich die Service Catalog-CLI verwenden, um in meinem AMS-verwalteten Konto auf Service Catalog zuzugreifen?

Ja, Service Catalog APIs ist über die CLI verfügbar und aktiviert. Aktionen von der Verwaltung von Service Catalog-Artefakten bis hin zur Bereitstellung und Beendigung dieser Artefakte sind verfügbar. Weitere Informationen finden Sie unter AWS Service Catalog Resources oder laden Sie das neueste AWS-SDK oder CLI herunter.

Wer erstellt, verwaltet und verteilt Kundenkataloge mit zugelassenen Produkten?

Der Katalogadministrator, der and/or IT-Administrator oder die zugewiesene Ressource des Kunden, ist für die Verwaltung Ihrer Servicekatalog-Kataloge und genehmigten Produkte verantwortlich.

Kann ich AMS verwenden? AMIs

AMS, AMIs die nach März 2020 verkauft wurden, können über den AWS Service Catalog bereitgestellt werden.

Wie migriere ich mithilfe von Service Catalog zu AMS?

Um Ihren Workload mithilfe von Service Catalog zu AMS zu migrieren, folgen Sie zunächst dem Workload Ingest (WIGs) -Prozess, um ein AMI in AMS zu erstellen. Sie verwenden das von WIGS erstellte AMI, um ein Produkt im Service Catalog zu erstellen. Eine Anleitung dazu finden Sie unter AWS Service Catalog — Erste Schritte.

Onboarding der AMS Multi-Account-Landingzone (MALZ)

MALZ Netzwerkarchitektur

Über die Landezone-Netzwerkarchitektur mit mehreren Konten

Bevor Sie mit dem Onboarding-Prozess in der AWS Managed Services (AMS) Multi-Account landing zone (MALZ) beginnen, ist es wichtig, die Basisarchitektur oder landing zone, die AMS in Ihrem Namen erstellt, sowie deren Komponenten und Funktionen zu verstehen.

Bei der AMS Multi-Account-Landing Zone handelt es sich um eine Multi-Account-Architektur, die mit der Infrastruktur vorkonfiguriert ist, um Authentifizierung, Sicherheit, Vernetzung und Protokollierung zu erleichtern.

> **Note**
>
> Kostenschätzungen finden Sie unter Grundkomponenten der AMS-Landezonenumgebung mit mehreren Konten.

Themen

- Service-Region
- Organisationseinheiten
- Richtlinien zur Servicesteuerung und AWS-Organisation

Das folgende Diagramm zeigt auf grober Ebene die Kontostruktur und die Aufteilung der Infrastruktur in die einzelnen Konten:

Service-Region

Alle Ressourcen innerhalb einer AMS-Landezone mit mehreren Konten werden aufgrund der aktuellen regionsübergreifenden Beschränkungen mit Active Directory und Transit Gateway in einer einzigen AWS-Region Ihrer Wahl bereitgestellt.

Organisationseinheiten

Eine typische AMS-Landezone mit mehreren Konten besteht aus vier Organisationseinheiten der obersten Ebene ()OUs:

- Die zentrale Organisationseinheit (OU) (wird verwendet, um Konten zu gruppieren und als eine einzige Einheit zu verwalten)
- Die Organisationseinheit der Anwendungen
- Die vom Kunden verwaltete Organisationseinheit
- Sie beschleunigen die OU

Mit der von AMS verwalteten landing zone für mehrere Konten können Sie auch benutzerdefinierte AWS-Konten OUs für die Gruppierung und Organisation erstellen und ihnen benutzerdefinierte SCPs Konten zuordnen. Beispiele hierfür finden Sie unter Verwaltungskonto | Benutzerdefiniertes Konto erstellen OUs und Verwaltungskonto erstellen | Benutzerdefiniertes SCP erstellen (Überprüfung erforderlich). AMS bietet vier bestehende Konten, in denen OUs neue Konten angefordert werden können: Accelerate, Applications > Managed, Applications > Development OUs und Customer-managed.

- Beschleunigen Sie OU:

  Dies ist eine Organisationseinheit der obersten Ebene in der AMS Multi-Account-Landing landing zone (MALZ). Konten unter dieser Organisationseinheit werden von AMS mit einem RFC (Bereitstellung | Verwaltete landing zone | Verwaltungskonto | Accelerate-Konto erstellen, Typ-ID ändern: ct-2p93tyd5angmi) bereitgestellt. In diesen Accelerate-Anwendungskonten können Sie von beschleunigten Betriebsdiensten wie Überwachung und Warnmeldungen, Vorfallmanagement, Sicherheitsmanagement und Backup-Management profitieren. Weitere Informationen finden Sie unter AMS Accelerate-Konten.

- Anwendungen > verwaltete Organisationseinheit:

  In dieser untergeordneten Organisationseinheit der Anwendungs-OU werden die Konten vollständig von AMS verwaltet, einschließlich aller betrieblichen Aufgaben. Zu den operativen Aufgaben gehören die Verwaltung von Serviceanfragen, das Vorfallmanagement, das Sicherheitsmanagement, das Kontinuitätsmanagement, das Patch-Management, die Kostenoptimierung, die Überwachung und das Eventmanagement. Diese Aufgaben werden für das Management Ihrer Infrastruktur ausgeführt. Bei Bedarf OUs können mehrere untergeordnete

Objekte erstellt werden, bis die maximale Anzahl an verschachtelten Elementen für AWS-Organisationen erreicht OUs ist. Einzelheiten finden Sie unter Kontingente für AWS Organizations.

- Anwendungen > OU für Entwicklung:

  Unter dieser Unter-OU der Anwendungs-OU in der von AMS verwalteten landing zone handelt es sich bei Konten um Konten im Entwicklermodus, die Ihnen erweiterte Berechtigungen zur Bereitstellung und Aktualisierung von AWS-Ressourcen außerhalb des AMS-Change-Management-Prozesses gewähren. Diese Organisationseinheit unterstützt bei Bedarf auch die Erstellung neuer untergeordneter Organisationseinheiten.

- vom Kunden verwaltete Organisationseinheit:

  Dies ist eine Organisationseinheit der obersten Ebene in der AMS-Landezone für mehrere Konten. Konten unter dieser Organisationseinheit werden von AMS mit einem RFC bereitgestellt. Bei diesen Konten sind Sie für den Betrieb von Workloads und AWS-Ressourcen verantwortlich. Diese Organisationseinheit unterstützt bei Bedarf auch die Einrichtung neuer untergeordneter Organisationseinheiten.

Als bewährte Methode empfehlen wir, Konten anhand ihrer Funktionen OUs und Richtlinien unter diesen und individuell angeforderten Unterkonten zu gruppieren. OUs

Richtlinien zur Servicesteuerung und AWS-Organisation

AWS stellt Service-Kontrollrichtlinien (SCPs) für die Berechtigungsverwaltung in einer AWS-Organisation bereit. SCPs werden verwendet, um zusätzliche Richtlinien dafür zu definieren, welche Aktionen Benutzer in welchen Fällen ausführen können. OUs Standardmäßig stellt AMS eine Reihe von in der Verwaltung SCPs bereitgestellten Konten bereit, die Schutz auf verschiedenen Standard-OU-Ebenen bieten. Für SCP-Einschränkungen wenden Sie sich bitte an Ihren CSDM.

Sie können auch benutzerdefinierte erstellen SCPs und diese an bestimmte anhängen. OUs Sie können von Ihrem Verwaltungskonto aus mit dem Änderungstyp ct-33ste5yc7hprs angefordert werden. AMS überprüft dann die angeforderten benutzerdefinierten Daten, bevor sie auf das Ziel angewendet werden. SCPs OUs Beispiele finden Sie unter Verwaltungskonto | Benutzerdefiniertes Konto OUs und Verwaltungskonto erstellen | Benutzerdefiniertes SCP erstellen (Überprüfung erforderlich).

Wählen Sie ein MALZ oder mehrere MALZs

Die folgende Tabelle enthält einige allgemeine Überlegungen zur Entscheidung zwischen einer einzelnen landing zone mit mehreren Konten (MALZ) und mehreren Landezonen mit mehreren Konten (z. B. zwei Landezonen mit mehreren Konten — Prod und Non-Prod). Im Allgemeinen hängt die Wahl von den individuellen Bedürfnissen, gesetzlichen Anforderungen und Betriebspraktiken ab.

Einzelne landing zone mit mehreren Konten im Vergleich zu mehreren Landezonen mit mehreren Konten

Entität	Einzelne AMS-Landezone	Mehrere (zwei oder mehr) Landezonen
Grundkosten	Niedriger, optimierter Preis von etwa 3.000 USD pro Monat.	Höher, zusätzliche Kosten von etwa 3.000 USD pro Umgebung.
Fakturierung	Einzelrechnung aufgrund eines einzigen Abrechnungs-/Verwaltungskontos.	Separate Rechnung für jede landing zone mit mehreren Konten. Derzeit unterstützt AWS Org keine Multi-Management-Konten mit einer einzigen Rechnung.
Portabilität vorhandener Reserved Instances () RIs	Niedrig. AWS ist RIs derzeit nicht für mehrere Rechnungskonten konvertierbar. Sie würden eine bestehende landing zone RIs für mehrere Konten wiederverwenden.	Niedriger. Sie würden es wiederverwenden und RIs in allen landing zone mit mehreren Konten verteilen.
Rabatte bei der Staffelung von Produkten	Hoch. Siehe Mengenrabatte.	Niedrig. Siehe Mengenrabatte.
Gemeinkosten bei der Ersteinrichtung (im project/migration Zeitplan)	Niedrig. Active Directory-, Netzwerk- und Single Sign-On-Integrationen (SSO) nur einmal.	Hoch. Sie würden Active Directory-, Netzwerkintegration- und SSO-Integrationen für jede landing zone durchführen. Dies könnte zu potenziellen Verzögerungen bei Migration sprojekten führen.

Entität	Einzelne AMS-Landezone	Mehrere (zwei oder mehr) Landezonen
Konfiguri erbarkeit gängiger Dienste	Geringer Aufwand. Sie konfigurieren common/shared Dienste wie DNS, Backup, Überwachung, Protokollierung usw.	Hoher Aufwand. Zusätzliche Planung ist erforderlich, um zu klären, wo die gemeinsame Infrastruktur oder die gemeinsamen Dienste installie rt werden sollen. Verkehr, der über mehrere Transit-Gateways (TGWs) in jeder landing zone fließt, könnte zu zusätzlichen Kosten führen.
Skalierbarkeit	Mittel. AMS hat derzeit ein praktisches Limit von 150 Konten pro landing zone mit mehreren Konten. Mehrere Teams oder Anbieter, die Anwendungen in demselben Konto ausführen, könnten Zugriff auf Stacks haben, die unterschi edlichen Teams gehören. Diese Einschränkung kann verringert werden, indem der Zugriff auf anwendung sspezifische Stacks auf der ServiceNo w Ebene gesteuert wird (durch Integrati on der AMS ServiceNow Connector -Anwendung und Verwendung von Tags). Fragen Sie die technischen Delivery Manager (TDMs) oder Cloud-Architekten (CAs) von AMS, wie Sie das umsetzen können.	Hoch. Möglichkeit, mehrere landing zone mit mehreren Konten zu nutzen, um die Konten zu verteilen und gleichzeitig eine Trennung auf Konto- oder Anwendungsebene zu erreichen . Die Verwaltung einer großen Anzahl von Konten könnte zu Betriebs- oder Kostengemeinkosten führen.
Operation elles Risiko	(Hängt davon ab) Niedrig. Operative Integration und Einsatzbereitschaft nur einmal. Geringere Wahrscheinlichkeit von Prozessabweichungen.	(Hängt davon ab) Niedrig. Vielfältige Integrations- und Betriebsaktivitäte n. Verschiebungen in mehreren Landezonen während des Berichtsz eitraums könnten zu operationellen Risiken führen.

Entität	Einzelne AMS-Landezone	Mehrere (zwei oder mehr) Landezonen
Mehrere AWS-Regionen	Eine einzige AWS-Region. Die AMS-Landezone für mehrere Konten ist auf eine einzige AWS-Region beschränkt. Um mehrere AWS-Regionen abzudecken, verwenden Sie mehrere landing zone mit mehreren Konten.	Mehrere AWS-Regionen. Bei mehreren Landing Zones mit mehreren Konten können Sie jedes MALZ in einer Region einsetzen und sie über Transit Gateway (TGW) -Peering miteinander verbinden.
Kontomigration oder Portabilität	Ja. Das Verschieben von Konten von einer Organisationseinheit zu einer anderen innerhalb derselben AWS-Organisation ist möglich.	Nein. AMS unterstützt keine Migration eines Kontos zwischen Landing Zones, also zwischen AWS Organizations. Workloads können mit Transit Gateway (TGW) oder VPC-Peering über Landingzonen verteilt werden.
Änderungsmanagement	Mittel. Destruktive Änderungen an gängigen Komponenten wie TGW, Active Directory (AD) oder Outbound (Egress) können sich auf alle Workloads in einer landing zone mit mehreren Konten auswirken. Änderungen an AMS-verwalteten Komponenten werden jedoch intern getestet und in fortlaufenden Updates veröffentlicht.	Niedrig. Destruktive Änderungen an gängigen Komponenten wie TGW, AD oder Outbound (Egress) können sich nur auf die Workloads in dieser speziellen landing zone mit mehreren Konten auswirken.
Daten- und Zugriffskontrollen	(Hängt davon ab) Geringe Kontrolle, wenn Sie für Prod- und Nicht-Prod-Workloads eine Verbindung zu verschiedenen lokalen ADs und Netzwerken herstellen möchten. SAML-Verbund, TGW-Domänen und Sicherheitsgruppen (SGs) können ebenfalls bei der Implementierung der erforderlichen Kontrollen helfen.	(Hängt davon ab) Hohe Kontrolle, wenn Sie für Prod-Workloads und Non-Prod-Workloads eine Verbindung zu verschiedenen lokalen ADs und Netzwerken herstellen möchten. Verwenden Sie separate Landezonen, um strenge Compliance-Anforderungen zu erfüllen.

Entität	Einzelne AMS-Landezone	Mehrere (zwei oder mehr) Landezonen
Einhaltung von Vorschriften und Sicherheit	(Hängt davon ab) Niedrig, wenn strenge Compliance-Anforderungen zur vollständigen Trennung materieller und immaterieller Arbeitslasten bestehen. Präventive und detektive Kontrollen nach AMS-Standard sind vorhanden.	(Hängt davon ab) Eine landing zone mit mehreren Konten könnte dazu beitragen, strenge Compliance-Anforderungen zu erfüllen, indem materielle und immaterielle Arbeitslasten vollständig getrennt werden. Präventive und detektive Kontrollen nach AMS-Standard sind vorhanden.

Empfehlung: Ohne strikte Einhaltung oder regionsübergreifende Anforderungen würde ein Start mit einer einzigen AMS-Landezone für mehrere Konten ein ausgewogenes Verhältnis zwischen Kosten, Sicherheit, betrieblicher Exzellenz und Komplexität der Migration bieten. Sie können jederzeit eine zusätzliche landing zone einrichten, falls Konto- oder Geschäftsbeschränkungen auftreten.

Einzelne landing zone mit mehreren Konten im Vergleich zu landing zone mit mehreren Konten FAQs

Einige häufig gestellte Fragen bei der Einrichtung einer einzelnen landing zone mit mehreren Konten oder mehrerer Landezonen mit mehreren Konten:

Frage 1: Kann ich mit einer einzigen Landingzone für mehrere Konten beginnen und dann zu einer landing zone mit mehreren Konten wechseln, wenn Kontolimits oder geschäftliche Einschränkungen auftreten?

A: Ja. Sie können jederzeit eine weitere landing zone für mehrere Konten einrichten:

- Es muss ein neues Konto für Rechnungszahler eingerichtet werden (derzeit unterstützt AWS keine Konten mit mehreren Zahlern in einer einzigen AWS-Organisation).
- Der Aufbau der Basisbasis für mehrere Konten dauert bis zu 2 Wochen, sobald der Fragebogen zur landing zone für mehrere Konten ausgefüllt ist.
- Jede landing zone mit mehreren Konten bedeutet zusätzliche Betriebskosten von ~3.000 USD/Monat.
- Für die Einrichtung eines neuen MALZ ist eine Integration von N/W, AD, DNS und SSO erforderlich.

- Alle Reserved Instances (RIs) und Kostensparpläne müssen für die neue landing zone mit mehreren Konten eingerichtet werden (RIs sind nicht übertragbar).
- Die AMS-Landingzone mit mehreren Konten unterstützt keine Migration eines Kontos zwischen Landingzone-Konten mit mehreren Konten, z. B. zwischen AWS-Organisationen. Das Verschieben von Anwendungen von einem Konto auf ein anderes ist jedoch mithilfe von Standardmigrationsmethoden möglich.

Frage 2: Welchen Ansatz verfolgt AMS gegenüber MALZ in Bezug updates/changes auf underlying/shared Infrastruktur und Quantifizierung des Risikos für Kunden? Geben Sie detailliert an, welche Zusicherungen im Prozess enthalten sind. Wie können sich Kunden darauf verlassen, dass MALZ keine Auswirkungen auf updates/changes die Kunden hat? Gibt es Maßnahmen, die der Kunde ergreifen muss, um Störungen zu verhindern?

A: AMS folgt einer strikten Änderungsmethodik und verwendet interne Tools, die es uns ermöglichen, Änderungen an den Kundenumgebungen zu definieren, zu überprüfen, zu planen und durchzuführen.

Der Prozess zur Veröffentlichung von Updates setzt Code-Reviews, Integrationstests, die Bereitstellung in Gamma- und Beta-Umgebungen sowie zusätzliche Backzeit und Tests in Beta- und Gamma-Umgebungen vor der Veröffentlichung in Kundenumgebungen durch. Alle Versionen beinhalten Rollback-Verfahren und werden vom Release-Team und dem Team, das die Änderung erstellt und angefordert hat, genau überwacht. Der Umfang der Releases beschränkt sich auf Stacks, die AMS gehören und von AMS bereitgestellt werden. Im Durchschnitt führen wir mindestens eine Veröffentlichung pro Woche durch.

Darüber hinaus gilt:

- AMS SLA sind anwendbar. Gemäß der AMS-Servicebeschreibung unterliegt jeder Vorfall, der nach einer gemeinsamen Wartung der Infrastruktur auftritt, der entsprechenden Vereinbarung zur Lösung oder Gutschrift.
- Kunden benötigen keine besonderen Präventivmaßnahmen, um Störungen der gemeinsamen Infrastruktur zu verhindern. Kunden haben nur Leseberechtigungen für AWS Org- oder Core OU-Konten, sodass Kunden keine zerstörerischen Änderungen an der MALZ-Kernumgebung vornehmen können. Alle Kundenanfragen an die Core-Infrastruktur müssen von AMS geprüft und genehmigt werden.
- Kunden können bestimmte Änderungen auf Organisationsebene testen, z. B. SCPs/Roles auf Ebene einzelner Konten, die keine Produkte sind, bevor sie Änderungen auf Ebene der App-Organisationseinheit weitergeben. Es steht auf der AMS-Roadmap, mehrere Apps zuzulassen

OUs (Q2 2020), wodurch das Risiko einiger Änderungen auf ORGANISATIONSEBENE weiter verringert würde. Das MALZ-Team hat bereits eine separate Organisationseinheit für Konten im „Build-Modus“ veröffentlicht, um eine klare Trennung der Kundenrechte und separate Kontrollen zu gewährleisten.

- Bei den meisten dieser Änderungen handelt es sich um Änderungen, die es AMS ermöglichen, die Arbeitslast effektiv und effizient zu verwalten, ohne dass sie sich unbedingt auf die Arbeitslast der Kunden auswirken. Wenn AMS der Ansicht ist, dass eine Änderung der gemeinsamen Infrastruktur Auswirkungen auf die Arbeitslast der Kunden haben kann, werden sie dann auf das Änderungsfenster der Kunden abgestimmt.

Allgemeine Empfehlung: Beginnen Sie mit mehreren Landezonen für mehrere Konten, wenn:

- Wenn es Ihnen hilft, eine bestimmte Konformität zu erreichen.
- Wenn Sie Multi-Region verwenden müssen.
- Wenn Sie unterschiedliche lokale Workloads ADs und Netzwerke für Workloads und für externe Prod/Material Workloads haben. Prod/Non-Material workloads, to clearly segregate b/w

Landing Zone-Konten mit mehreren Konten

Themen

- Verwaltungskonto
- Netzwerkkonto
- Shared Services-Konto
- Konto protokollieren und archivieren
- Sicherheitskonto
- Arten von Anwendungskonten
- AMS Tools-Konto (Workloads migrieren)

Verwaltungskonto

Das Verwaltungskonto ist Ihr erstes AWS-Konto, wenn Sie mit dem Onboarding bei AMS beginnen. Es verwendet AWS Organizations als Verwaltungskonto (auch bekannt als das Zahlungskonto, das die Gebühren aller Mitgliedskonten bezahlt), wodurch das Konto Mitgliedskonten erstellen

und finanziell verwalten kann. Es enthält das AWS-Landing landing zone (ALZ) -Framework, Kontokonfigurationsstapelsätze, AWS Organization Service Control Policies (SCPs) usw.

Weitere Informationen zur Verwendung eines Verwaltungskontos finden Sie unter Bewährte Methoden für das Verwaltungskonto.

Das folgende Diagramm bietet einen allgemeinen Überblick über die im Verwaltungskonto enthaltenen Ressourcen.

Ressourcen im Verwaltungskonto

Abgesehen von den oben genannten Standardservices werden beim Onboarding keine zusätzlichen AWS-Ressourcen im Verwaltungskonto erstellt. Die folgenden Eingaben sind beim Onboarding bei AMS erforderlich:

- Verwaltungskonto-ID: AWS-Konto-ID, die ursprünglich von Ihnen erstellt wurde.
- E-Mails für Kernkonten: Geben Sie die E-Mails an, die den einzelnen Kernkonten zugeordnet werden sollen: Networking, Shared Services, Logging und Sicherheitskonto.
- Serviceregion: Geben Sie die AWS-Region an, in der alle Ressourcen Ihrer AMS-Landezone bereitgestellt werden.

Netzwerkkonto

Das Netzwerkkonto dient als zentraler Knotenpunkt für das Netzwerk-Routing zwischen AMS-Landingzone-Konten mit mehreren Konten, Ihrem lokalen Netzwerk und ausgehendem Datenverkehr ins Internet. Darüber hinaus enthält dieses Konto öffentliche DMZ-Bastionen, über die AMS-Techniker auf Hosts in der AMS-Umgebung zugreifen können. Einzelheiten finden Sie im folgenden allgemeinen Diagramm des Netzwerkkontos.

Architektur von Netzwerkkonten

Das folgende Diagramm zeigt die AMS-Landingzone-Umgebung mit mehreren Konten und zeigt den Netzwerkdatenverkehr zwischen den Konten. Es ist ein Beispiel für eine Konfiguration mit hoher Verfügbarkeit.

AMS konfiguriert alle Netzwerkaspekte für Sie auf der Grundlage unserer Standardvorlagen und der von Ihnen beim Onboarding ausgewählten Optionen. Ein standardmäßiges AWS-Netzwerkdesign wird auf Ihr AWS-Konto angewendet, und eine VPC wird für Sie erstellt und entweder über VPN oder Direct Connect mit AMS verbunden. Weitere Informationen zu Direct Connect finden Sie unter AWS Direct Connect. Zum Standard VPCs gehören die DMZ, Shared Services und ein Anwendungssubnetz. Während des Onboarding-Prozesses VPCs können zusätzliche Informationen angefordert und erstellt werden, die Ihren Anforderungen entsprechen (z. B. Kundenabteilungen, Partner). Nach dem Onboarding erhalten Sie ein Netzwerkdiagramm: ein Umgebungsdokument, das erklärt, wie Ihr Netzwerk eingerichtet wurde.

> **Note**
>
> Informationen zu Standard-Servicelimits und Einschränkungen für alle aktiven Services finden Sie in der Dokumentation zu AWS-Servicelimits.

Unser Netzwerkdesign basiert auf dem „Prinzip der geringsten Rechte“ von Amazon. Um dies zu erreichen, leiten wir den gesamten eingehenden und ausgehenden Verkehr durch eine DMZ, mit Ausnahme des Datenverkehrs, der aus einem vertrauenswürdigen Netzwerk stammt. Das einzige vertrauenswürdige Netzwerk ist das, das zwischen Ihrer lokalen Umgebung und der VPC mithilfe and/or eines VPN und AWS Direct Connect (DX) konfiguriert wurde. Der Zugriff wird durch die Verwendung von Bastion-Instances gewährt, wodurch ein direkter Zugriff auf Produktionsressourcen verhindert wird. Alle Ihre Anwendungen und Ressourcen befinden sich in privaten Subnetzen, die über öffentliche Load Balancer erreichbar sind. Öffentlicher Ausgangsverkehr fließt über die NAT-Gateways in der Ausgangs-VPC (im Netzwerkkonto) zum Internet Gateway und dann zum Internet. Alternativ kann der Datenverkehr über Ihr VPN oder Direct Connect in Ihre lokale Umgebung fließen.

Private Netzwerkkonnektivität zur AMS-Landezonenumgebung mit mehreren Konten

AWS bietet private Konnektivität entweder über VPN-Konnektivität (Virtual Private Network) oder über Standleitungen mit AWS Direct Connect. Die private Konnektivität in Ihrer Umgebung mit mehreren Konten wird mit einer der im Folgenden beschriebenen Methoden eingerichtet:

- Zentralisierte Edge-Konnektivität mit Transit Gateway
- Direct Connect (DX) and/or VPN mit virtuellen privaten Clouds verbinden (VPCs)

Zentralisierte Edge-Konnektivität mit Transit Gateway

AWS Transit Gateway ist ein Service, mit dem Sie Ihre VPCs und Ihre lokalen Netzwerke mit einem einzigen Gateway verbinden können. Transit Gateway (TGW) kann verwendet werden, um Ihre bestehende Edge-Konnektivität zu konsolidieren und sie über einen einzigen ingress/egress Punkt weiterzuleiten. Das Transit-Gateway wird im Netzwerkkonto Ihrer AMS-Umgebung mit mehreren Konten erstellt. Weitere Informationen zu Transit Gateway finden Sie unter AWS Transit Gateway.

Das AWS Direct Connect (DX) -Gateway wird verwendet, um Ihre DX-Verbindung über eine virtuelle Transitschnittstelle mit dem VPCs oder VPNs , die an Ihr Transit-Gateway angeschlossen sind, zu verbinden. Sie ordnen ein Direct-Connect-Gateway dem Transit Gateway zu. Erstellen Sie anschließend eine virtuelle Transitschnittstelle für Ihre AWS Direct Connect Connect-Verbindung zum Direct Connect-Gateway. Informationen zu virtuellen DX-Schnittstellen finden Sie unter Virtuelle Schnittstellen von AWS Direct Connect.

Diese Konfiguration bietet die folgenden Vorteile. Sie haben folgende Möglichkeiten:

- Verwalten Sie eine einzelne Verbindung für mehrere VPCs oder VPNs , die sich in derselben AWS-Region befinden.
- Werben Sie für Präfixe von On-Premise zu AWS und von AWS zu On-Premise.

> **Note**
>
> Informationen zur Verwendung eines DX mit AWS-Services finden Sie im Abschnitt Classic im Resiliency Toolkit. Weitere Informationen finden Sie unter Transit Gateway Gateway-Verknüpfungen.

Um die Stabilität Ihrer Konnektivität zu erhöhen, empfehlen wir, dass Sie mindestens zwei virtuelle Transitschnittstellen von verschiedenen AWS Direct Connect Connect-Standorten an das Direct Connect-Gateway anschließen. Weitere Informationen finden Sie in der AWS Direct Connect Connect-Resilienzempfehlung.

DX oder VPN mit dem Konto verbinden VPCs

Mit dieser Option werden die landing zone Zone-Umgebungen VPCs in Ihrem AMS mit mehreren Konten direkt mit Direct Connect oder VPN verbunden. Der Datenverkehr fließt direkt von Direct Connect oder VPN, ohne das Transit-Gateway zu passieren. VPCs

Ressourcen im Netzwerkkonto

Wie im Netzwerkkontodiagramm dargestellt, werden die folgenden Komponenten im Konto erstellt und erfordern Ihre Eingabe.

Das Netzwerkkonto enthält zwei VPCs: Egress VPC und DMZ VPC, auch bekannt als Perimeter-VPC.

AWS-Netzwerkmanager

AWS Network Manager ist ein Service, mit dem Sie Ihre Transit-Gateway-Netzwerke (TGW) ohne zusätzliche Kosten für AMS visualisieren können. Es bietet eine zentrale Netzwerküberwachung sowohl für AWS-Ressourcen als auch für lokale Netzwerke, eine zentrale globale Ansicht ihres privaten Netzwerks in einem Topologiediagramm und auf einer geografischen Karte sowie Nutzungsmetriken wie den in/out, packets in/out, packets dropped, and alerts for changes in the topology, routing, and up/down Byte-Verbindungsstatus. Weitere Informationen finden Sie unter AWS Network Manager.

Verwenden Sie eine der folgenden Rollen, um auf diese Ressource zuzugreifen:

- AWSManagedServicesCaseRole
- AWSManagedServicesReadOnlyRole
- AWSManagedServicesChangeManagementRole

Ausgangs-VPC

Die Egress-VPC wird hauptsächlich für den ausgehenden Datenverkehr ins Internet verwendet und besteht aus public/private Subnetzen in bis zu drei Verfügbarkeitszonen (). AZs Network Address Translation (NAT) -Gateways werden in den öffentlichen Subnetzen bereitgestellt, und Transit Gateway (TGW) VPC-Anlagen werden in den privaten Subnetzen erstellt. Ausgehender oder ausgehender Internetverkehr aus allen Netzwerken wird über TGW durch das private Subnetz geleitet, wo er dann über VPC-Routing-Tabellen an ein NAT weitergeleitet wird.

Für Sie VPCs , die öffentlich zugängliche Anwendungen in einem öffentlichen Subnetz enthalten, ist der aus dem Internet stammende Datenverkehr in dieser VPC enthalten. Rückverkehr wird nicht an die TGW- oder Egress-VPC weitergeleitet, sondern über das Internet-Gateway (IGW) in der VPC zurückgeleitet.

> **Note**
>
> Netzwerk-VPC-CIDR-Bereich: Wenn Sie eine VPC erstellen, müssen Sie einen IPv4 Adressbereich für die VPC in Form eines CIDR-Blocks (Classless Inter-Domain Routing) angeben, z. B. 10.0.16.0/24. Dies ist der primäre CIDR-Block für Ihre VPC.
> Das AMS Multi-Account-Landingzone-Team empfiehlt den Bereich 24 (mit mehr IP-Adressen), um einen gewissen Puffer für den Fall bereitzustellen, dass in future andere Ressourcen/Appliances eingesetzt werden.

Verwaltete Palo Alto-Ausgangsfirewall

AMS bietet eine Managed Palo Alto Egress Firewall-Lösung, die das Filtern von ausgehendem Internetverkehr für alle Netzwerke in der Multi-Account Landing Zone-Umgebung (mit Ausnahme von öffentlich zugänglichen Diensten) ermöglicht. Diese Lösung kombiniert die branchenführende Firewall-Technologie (Palo Alto VM-300) mit den Infrastrukturmanagementfunktionen von AMS zur Bereitstellung, Überwachung, Verwaltung, Skalierung und Wiederherstellung der Infrastruktur in konformen Betriebsumgebungen. Dritte, einschließlich Palo Alto Networks, haben keinen Zugriff auf die Firewalls. Sie werden ausschließlich von AMS-Technikern verwaltet.

Steuerung des Verkehrs

Die verwaltete Firewall-Lösung für ausgehenden Datenverkehr verwaltet eine Domain-Zulassungsliste, die aus AMS-erforderlichen Domänen für Dienste wie Backup und Patch sowie aus Ihren definierten Domänen besteht. Wenn ausgehender Internetverkehr an die Firewall weitergeleitet wird, wird eine Sitzung geöffnet, der Datenverkehr wird ausgewertet, und wenn er einer zulässigen Domain entspricht, wird der Datenverkehr an das Ziel weitergeleitet.

Architektur

Die verwaltete Firewall-Lösung für ausgehenden Datenverkehr folgt einem Hochverfügbarkeitsmodell, bei dem je nach Anzahl der Verfügbarkeitszonen () zwei bis drei Firewalls eingesetzt werden. AZs Die Lösung nutzt einen Teil des IP-Bereichs der Standard-Ausgangs-VPC, stellt aber auch eine VPC-

Erweiterung (/24) für zusätzliche Ressourcen bereit, die für die Verwaltung der Firewalls erforderlich sind.

Netzwerkfluss

Auf hoher Ebene bleibt das Routing des öffentlichen ausgehenden Datenverkehrs unverändert, mit Ausnahme der Art und Weise, wie der Datenverkehr von der ausgehenden VPC ins Internet geleitet wird:

1. Ausgangsverkehr, der für das Internet bestimmt ist, wird über die VPC-Routentabelle an das Transit Gateway (TGW) gesendet
2. TGW leitet den Verkehr über die TGW-Routentabelle an die Ausgangs-VPC weiter
3. VPC leitet den Verkehr über die Routentabellen des privaten Subnetzes ins Internet weiter.
    a. In der standardmäßigen Multi-Account-Landingzone-Umgebung wird der Internetverkehr direkt an ein NAT-Gateway (Network Address Translation) gesendet. Die verwaltete Firewall-Lösung konfiguriert die Routing-Tabellen für private Subnetze neu, sodass die Standardroute (0.0.0.0/0) stattdessen auf eine Firewall-Schnittstelle verweist.

Die Firewalls selbst enthalten drei Schnittstellen:

1. Vertrauenswürdige Schnittstelle: Private Schnittstelle für den Empfang von Datenverkehr, der verarbeitet werden soll.
2. Nicht vertrauenswürdige Schnittstelle: Öffentliche Schnittstelle zum Senden von Datenverkehr ins Internet. Da die Firewalls NAT ausführen, akzeptieren externe Server Anfragen von diesen öffentlichen IP-Adressen.
3. Verwaltungsschnittstelle: Private Schnittstelle für Firewall-API, Updates, Konsole usw.

Während des gesamten Routings wird der Verkehr innerhalb derselben Availability Zone (AZ) aufrechterhalten, um den AZ-übergreifenden Verkehr zu reduzieren. Der Verkehr wird nur dann überquert AZs , wenn ein Failover auftritt.

Änderung der Zulassungsliste

Nach dem Onboarding `ams-allowlist` wird eine standardmäßige Zulassungsliste mit dem Namen erstellt, die für AMS erforderliche öffentliche Endpunkte sowie öffentliche Endpunkte für das Patchen von Windows- und Linux-Hosts enthält. Sobald der Betrieb abgeschlossen ist, können Sie in der AMS-Konsole unter der Kategorie Management | Managed Firewall | Outbound (Palo Alto) RFCs erstellen, um Zulassungslisten zu erstellen oder zu löschen oder die Domänen zu ändern. Beachten Sie, dass dies nicht geändert werden kann. `ams-allowlist` Die RFCs werden vollständig automatisiert behandelt (sie sind nicht manuell).

Benutzerdefinierte Sicherheitsrichtlinie

Sicherheitsrichtlinien bestimmen anhand von Datenverkehrsattributen wie der Quell- und Zielsicherheitszone, der Quell- und Ziel-IP-Adresse und dem Dienst, ob eine Sitzung blockiert oder zugelassen wird. Benutzerdefinierte Sicherheitsrichtlinien werden vollständig automatisiert unterstützt RFCs. CTs Informationen zum Erstellen oder Löschen von Sicherheitsrichtlinien finden Sie in der Kategorie Management | Managed Firewall | Outbound (Palo Alto). Das CT zum Bearbeiten einer vorhandenen Sicherheitsrichtlinie finden Sie unter der Kategorie Bereitstellung | Managed Firewall | Outbound (Palo Alto). Sie können neue Sicherheitsrichtlinien erstellen, Sicherheitsrichtlinien ändern oder Sicherheitsrichtlinien löschen.

> **Note**
>
> Die Standardsicherheitsrichtlinie `ams-allowlist` kann nicht geändert werden

CloudWatch PA-Dashboards für ausgehenden Datenverkehr

Zwei Dashboards bieten eine aggregierte Ansicht von Palo Alto (PA). Das AMS-MF-PA-Egress-Config-Dashboard bietet eine Übersicht über die PA-Konfiguration, Links zu Zulassungslisten und eine Liste aller Sicherheitsrichtlinien einschließlich ihrer Attribute. CloudWatch Das AMS-MF-PA-Egress-Dashboard kann so angepasst werden, dass Verkehrsprotokolle gefiltert werden. Um beispielsweise ein Dashboard für eine Sicherheitsrichtlinie zu erstellen, können Sie einen RFC mit einem Filter wie dem folgenden erstellen:

```
fields @timestamp, @message
| filter @logStream like /pa-traffic-logs/
| filter @message like /<Security Policy Name>/
| parse @message
 "*,*,*,
```

```
 as x1, @x2, @x3, @x4, @type, @x6, @x7, @source_ip, @destination_ip, @source_nat_ip,
 @dest_nat_ip, @rule, @x13, @x14, @application, @x16, @from_zone, @to_zone,
 @x19, @x20, @x21, @x22, @session_id, @x24, @source_port, @destination_port,
 @source_nat_port, @destination_nat_port, @x29, @protocol, @action, @bytes,
 @bytes_sent, @bytes_recieved, @packets, @x36, @x37, @category, @x39, @x40, @x41,
 @source_country, @destination_country, @x44, @packets_sent, @packets_recieved,
 @session_end_reason, @x48, @x49, @x50
| display @timestamp, @rule, @action, @session_end_reason, @protocol, @source_ip,
 @destination_ip, @source_port, @destination_port, @session_id, @from_zone,
 @to_zone, @category, @bytes_sent, @bytes_recieved, @packets_sent, @packets_recieved,
 @source_country, @destination_country
```

Failover-Modell

Die Firewall-Lösung umfasst zwei bis drei Palo Alto (PA) -Hosts (einer pro AZ). Healthy Check Canaries wird nach einem konstanten Zeitplan ausgeführt, um den Zustand der Hosts zu bewerten. Wenn ein Host als fehlerhaft identifiziert wird, wird AMS benachrichtigt, und der Datenverkehr für diese AZ wird durch Änderung der Routing-Tabelle automatisch auf einen fehlerfreien Host in einer anderen AZ umgeleitet. Da der Workflow zur Integritätsprüfung ständig ausgeführt wird, wird der Datenverkehr wieder auf die richtige AZ mit dem fehlerfreien Host umgeleitet, wenn der Host aufgrund vorübergehender Probleme oder manueller Behebung wieder funktionsfähig ist.

Skalierung

AMS überwacht die Firewall auf Durchsatz- und Skalierungsgrenzen. Wenn die Durchsatzgrenzen die unteren Schwellenwerte (CPU/Netzwerk) überschreiten, erhält AMS eine Warnung. Ein niedriger Schwellenwert deutet darauf hin, dass die Ressourcen fast ausgelastet sind und ein Punkt erreicht ist, an dem AMS die Messwerte im Laufe der Zeit auswertet und Skalierungslösungen vorschlägt.

Backup und Backup

Backups werden beim ersten Start, nach allen Konfigurationsänderungen und in regelmäßigen Abständen erstellt. Beim ersten Start werden Backups pro Host erstellt, aber Konfigurationsänderungen und regelmäßige Intervall-Backups werden auf allen Firewall-Hosts durchgeführt, wenn der Backup-Workflow aufgerufen wird. AMS-Techniker können zusätzliche Backups außerhalb dieser Fenster erstellen oder auf Anfrage Backup-Details bereitstellen.

AMS-Techniker können bei Bedarf die Wiederherstellung von Konfigurations-Backups durchführen. Wenn eine Wiederherstellung erforderlich ist, erfolgt sie auf allen Hosts, um die Konfiguration zwischen den Hosts synchron zu halten.

Eine Wiederherstellung kann auch erfolgen, wenn ein Host eine Instanz vollständig recyceln muss. Eine automatische Wiederherstellung des neuesten Backups erfolgt, wenn eine neue EC2 Instanz bereitgestellt wird. Im Allgemeinen werden Hosts nicht regelmäßig recycelt und sind für schwerwiegende Ausfälle oder erforderliche AMI-Swaps reserviert. Host-Wiederverwendungen werden manuell initiiert, und Sie werden benachrichtigt, bevor eine Wiederverwertung stattfindet.

Abgesehen von den Backups der Firewall-Konfiguration werden Ihre spezifischen Regeln für die Zulassungsliste separat gesichert. Eine Sicherungskopie wird automatisch erstellt, wenn Ihre definierten Regeln für die Zulassungsliste geändert werden. Die Wiederherstellung der Sicherungskopie auf der Zulassungsliste kann bei Bedarf von einem AMS-Techniker durchgeführt werden.

Aktualisierungen

Die AMS Managed Firewall Solution erfordert im Laufe der Zeit verschiedene Updates, um das System zu verbessern, zusätzliche Funktionen hinzuzufügen oder das Firewall-Betriebssystem (OS) oder die Firewall-Software zu aktualisieren.

Die meisten Änderungen wirken sich nicht auf die Betriebsumgebung aus, z. B. die Aktualisierung der Automatisierungsinfrastruktur. Andere Änderungen wie die Rotation der Firewall-Instanz oder das Betriebssystem-Update können jedoch zu Störungen führen. Wenn eine mögliche Betriebsunterbrechung aufgrund von Updates bewertet wird, stimmt sich AMS mit Ihnen ab, um die Wartungsfenster zu berücksichtigen.

Zugriff durch den Bediener

AMS-Betreiber verwenden ihre ActiveDirectory Anmeldeinformationen, um sich beim Palo Alto-Gerät anzumelden, um Operationen durchzuführen (z. B. Patchen, Reagieren auf ein Ereignis usw.). Die Lösung behält die standardmäßigen AMS-Operator-Authentifizierungs- und Konfigurationsänderungsprotokolle bei, um die auf den Palo Alto-Hosts ausgeführten Aktionen nachzuverfolgen.

Standardprotokolle

Standardmäßig befinden sich die von der Firewall generierten Protokolle für jede Firewall im lokalen Speicher. Im Laufe der Zeit werden lokale Protokolle je nach Speicherauslastung gelöscht. Die AMS-Lösung ermöglicht den Versand von Protokollen von den Maschinen in Echtzeit an CloudWatch Protokolle. Weitere Informationen finden Sie unterCloudWatch Integration von Protokollen.

Die AMS-Techniker haben weiterhin die Möglichkeit, Protokolle bei Bedarf direkt von den Maschinen abzufragen und zu exportieren. Darüber hinaus können Protokolle an ein kundeneigenes Panorama gesendet werden. Weitere Informationen finden Sie unterPanoramaintegration.

Die Lösung erfasst die folgenden Protokolle:

RFC-Statuscodes

Protokolltyp	Beschreibung
Datenverkehr	Zeigt einen Eintrag für den Start und das Ende jeder Sitzung an. Jeder Eintrag enthält Datum und Uhrzeit, Quell- und Zielzonen, Adressen und Ports, den Namen der Anwendung, den Namen der auf den Flow angewendeten Sicherheitsregel, die Regelaktion (Zulassen, Verweigern oder Löschen), die Eingangs- und Ausgangsschnittstelle, die Anzahl der Byte und den Grund für das Sitzungsende. In der Spalte Typ wird angegeben, ob der Eintrag für den Beginn oder das Ende der Sitzung bestimmt ist oder ob die Sitzung verweigert oder abgebrochen wurde. Ein „Drop“ bedeutet, dass die Sicherheitsregel, die den Datenverkehr blockiert hat, eine „beliebige“ Anwendung angegeben hat, während ein „Deny“ bedeutet, dass die Regel eine bestimmte Anwendung identifiziert hat. Wenn der Datenverkehr unterbrochen wird, bevor die Anwendung identifiziert wurde, z. B. wenn eine Regel den gesamten Datenverkehr für einen bestimmten Dienst blockiert, wird die Anwendung als „nicht zutreffend“ angezeigt.
Bedrohung	Zeigt einen Eintrag für jeden von der Firewall generierten Sicherhei tsalarm an. Jeder Eintrag enthält Datum und Uhrzeit, einen Namen oder eine URL der Bedrohung, die Quell- und Zielzonen, Adressen und Ports, den Namen der Anwendung sowie die Alarmaktion (zulassen oder blockieren) und den Schweregrad. In der Spalte Typ wird die Art der Bedrohung angegeben, z. B. „Virus“ oder „Spyware“, in der Spalte Name die Beschreibung oder URL der Bedrohung und in der Spalte Kategorie die Bedrohungskategorie (z. B. „Keylogger“) oder URL-Kategorie.

Protokolltyp	Beschreibung
URL-Filterung	Zeigt Protokolle für URL-Filter an, die den Zugriff auf Websites kontrollieren und festlegen, ob Benutzer Anmeldeinformationen an Websites senden können.
Konfiguration	Zeigt für jede Konfigurationsänderung einen Eintrag an. Jeder Eintrag enthält Datum und Uhrzeit, den Administratorbenutzernamen, die IP-Adresse, von der aus die Änderung vorgenommen wurde, den Clienttyp (Webinterface oder CLI), die Art der Befehlsausführung, ob der Befehl erfolgreich war oder nicht, den Konfigurationspfad und die Werte vor und nach der Änderung.
System (System)	Zeigt einen Eintrag für jedes Systemereignis an. Jeder Eintrag enthält Datum und Uhrzeit, den Schweregrad des Ereignisses und eine Beschreibung des Ereignisses.
Alarme	Das Alarmprotokoll zeichnet detaillierte Informationen zu Alarmen auf, die vom System generiert werden. Die Informationen in diesem Protokoll werden auch unter Alarme gemeldet. Weitere Informationen finden Sie unter „Alarmeinstellungen definieren“.
Authentifizierung	Zeigt Informationen zu Authentifizierungsereignissen an, die auftreten , wenn Endbenutzer versuchen, auf Netzwerkressourcen zuzugreifen, deren Zugriff durch Authentifizierungsrichtlinienregeln gesteuert wird. Benutzer können diese Informationen verwenden, um Zugriffsprobleme zu beheben und die Benutzerauthentifizierungsrichtlinie nach Bedarf anzupassen. In Verbindung mit Korrelationsobjekten können Benutzer auch Authentifizierungsprotokolle verwenden, um verdächtige Aktivitäten im Netzwerk des Benutzers zu identifizieren, z. B. Brute-Force-Angriffe. Optional können Benutzer Authentifizierungsregeln so konfigurieren, dass Authentifizierungs-Timeouts protokolliert werden. Diese Timeouts beziehen sich auf den Zeitraum, in dem sich ein Benutzer nur einmal für eine Ressource authentifizieren muss, aber wiederholt darauf zugreifen kann. Anhand von Informationen zu den Timeouts können Benutzer entscheiden, ob und wie sie angepasst werden sollen.

Protokolltyp	Beschreibung
Vereinheitlicht	Zeigt die neuesten Protokolleinträge für Verkehr, Bedrohung, URL-Filterung, WildFire Übermittlungen und Datenfilterung in einer einzigen Ansicht an. Die kollektive Protokollansicht ermöglicht es Benutzern, diese verschiedenen Protokolltypen gemeinsam zu untersuchen und zu filtern (anstatt jeden Protokollsatz einzeln zu durchsuchen). Oder Benutzer können wählen, welche Protokolltypen angezeigt werden sollen: Klicken Sie auf den Pfeil links neben dem Filterfeld und wählen Sie Traffic, Bedrohung, URL, Daten, and/or Wildfire aus, um nur die ausgewählten Protokolltypen anzuzeigen.

Verwaltung von Ereignissen

AMS überwacht kontinuierlich die Kapazität, den Zustand und die Verfügbarkeit der Firewall. Von der Firewall generierte Metriken sowie AWS/AMS generierte Metriken werden verwendet, um Alarme zu erstellen, die von den Betriebstechnikern von AMS empfangen werden, die das Problem untersuchen und lösen. Die aktuellen Alarme decken die folgenden Fälle ab:

Ereignisalarme:

- CPU-Auslastung der Firewall-Datenebene
  - CPU-Auslastung — CPU der Datenebene (Verarbeitung des Datenverkehrs)
- Die Auslastung der Firewall-Pakete auf Datenebene liegt bei über 80%
  - Paketauslastung — Datenebene (Verarbeitung des Datenverkehrs)
- Nutzung der Firewall-Sitzung auf der Datenebene
- Firewall-Datenebene-Sitzung aktiv
- Aggregierte Firewall-CPU-Auslastung
  - CPU-Auslastung für alle CPUs
- Failover von AZ
  - Alarmt, wenn in einer AZ ein Failover auftritt
- Ungesunder Syslog-Host
  - Der Syslog-Host schlägt die Integritätsprüfung fehl

Management-Alarme:

- Ausfallalarm des Health Check Monitors
  - Wenn der Workflow zur Integritätsprüfung unerwartet fehlschlägt
  - Dies gilt für den Workflow selbst, nicht für den Fall, dass eine Firewall-Integritätsprüfung fehlschlägt
- Alarm bei Ausfall der Passwortrotation
  - Wenn die Passwortrotation fehlschlägt
  - Das API-/Service-Benutzerkennwort wird alle 90 Tage gewechselt

Metriken

Alle Metriken werden erfasst und CloudWatch im Netzwerkkonto gespeichert. Diese können angezeigt werden, indem Sie Konsolenzugriff auf das Netzwerkkonto erhalten und zur CloudWatch Konsole navigieren. Einzelne Metriken können auf der Registerkarte Metriken oder in einer einzigen Dashboard-Ansicht mit ausgewählten Metriken angezeigt werden. Aggregierte Metriken können angezeigt werden, indem Sie zur Registerkarte Dashboard navigieren und AMS-MF-PA-Egress-Dashboard auswählen.

Benutzerdefinierte Metriken:

- Zustandsprüfung
  - Namespace: AMS/MF/PA/Egress
    - PARouteTableConnectionsByA-Z
    - PAUnhealthyByInstance
    - PAUnhealthyAggregatedByAZ
    - PAHealthCheckLockState
- Firewall generiert
  - Namespace:/AMS/MF/PA/Egress<instance-id>
    - DataPlaneCPUUtilizationPakt
    - DataPlanePacketBuffferUtilization
    - Pfanne GPGateway UtilizationPct
    - panSessionActive
    - panSessionUtilization

CloudWatch Integration von Protokollen

CloudWatch Durch die Integration von Protokollen werden Protokolle von den Firewalls in Logs weitergeleitet, wodurch das Risiko des Verlusts von CloudWatch Protokollen aufgrund der lokalen Speichernutzung verringert wird. Protokolle werden in Echtzeit ausgefüllt, sobald sie von den Firewalls generiert werden, und können bei Bedarf über die Konsole oder API eingesehen werden.

Komplexe Abfragen können für die Protokollanalyse erstellt oder mit CloudWatch Insights als CSV exportiert werden. Darüber hinaus bietet das benutzerdefinierte AMS Managed CloudWatch Firewall-Dashboard auch eine Schnellansicht bestimmter Verkehrsprotokollabfragen und eine grafische Darstellung der Zugriffe und der Richtlinieneinflüsse im Zeitverlauf. Die Verwendung von CloudWatch Protokollen ermöglicht auch die native Integration in andere AWS-Services wie AWS Kinesis.

> **Note**
>
> PA-Protokolle können nicht direkt an einen vorhandenen lokalen Syslog-Collector oder einen Syslog-Collector eines Drittanbieters weitergeleitet werden. Die AMS Managed Firewall-Lösung ermöglicht den Versand von Protokollen von den PA-Maschinen in Echtzeit an AWS CloudWatch Logs. Sie können die CloudWatch Logs Insight-Funktion verwenden, um Ad-hoc-Abfragen auszuführen. Darüber hinaus können Protokolle an die Panorama-Managementlösung Ihres Palo Alto gesendet werden. CloudWatch Protokolle können mithilfe von CloudWatch Abonnementfiltern auch an andere Ziele weitergeleitet werden. Erfahren Sie im folgenden Abschnitt mehr über Panorama. Weitere Informationen über Splunk finden Sie unter Integration mit Splunk.

Panoramaintegration

AMS Managed Firewall kann optional in Ihr bestehendes Panorama integriert werden. Auf diese Weise können Sie Firewallkonfigurationen von Panorama aus anzeigen oder Protokolle von der Firewall an das Panorama weiterleiten. Die Panorama-Integration mit AMS Managed Firewall ist schreibgeschützt, und Konfigurationsänderungen an den Firewalls von Panorama aus sind nicht zulässig. Panorama wird vollständig von Ihnen verwaltet und konfiguriert. AMS ist nur für die Konfiguration der Firewalls für die Kommunikation mit dem System verantwortlich.

Lizenzen

Der Preis der AMS Managed Firewall hängt von der Art der verwendeten Lizenz (stündlich oder Bring Your Own License, BYOL) und der Instanzgröße ab, in der die Appliance ausgeführt wird. Sie

müssen die Instance-Größe und die Lizenzen der Palo Alto-Firewall, die Sie bevorzugen, über den AWS Marketplace bestellen.

- Marketplace-Lizenzen: Akzeptieren Sie die Allgemeinen Geschäftsbedingungen des VM-Series Next-Generation Firewall Bundle 1 über das Netzwerkkonto in MALZ.
- BYOL-Lizenzen: Akzeptieren Sie die Nutzungsbedingungen der VM-Series Next-Generation Firewall (BYOL) über das Netzwerkkonto in MALZ und geben Sie den „BYOL-Authentifizierungscode“, den Sie nach dem Kauf der Lizenz erhalten haben, an AMS weiter.

Einschränkungen

Derzeit unterstützt AMS Firewalls der Serien VM-300 oder VM-500. Konfigurationen finden Sie hier: Modelle der VM-Serie auf EC2 AWS-Instances,

> **Note**
>
> Die AMS-Lösung wird im Active-Active-Modus ausgeführt, da jede PA-Instance in ihrer AZ den ausgehenden Datenverkehr für ihre jeweilige AZ abwickelt. Bei zwei AZs Instanzen verarbeitet jede PA-Instance also ausgehenden Datenverkehr mit bis zu 5 Gbit/s und bietet effektiv einen Gesamtdurchsatz von 10 Gbit/s über zwei. AZs Das Gleiche gilt für alle Grenzwerte in jeder AZ. Sollte die AMS-Zustandsprüfung fehlschlagen, verlagern wir den Verkehr von der AZ mit der fehlerhaften PA auf eine andere AZ, und beim Austausch der Instance wird die Kapazität auf die verbleibenden AZs Grenzwerte reduziert.
> AMS unterstützt derzeit keine anderen Palo Alto-Pakete, die auf dem AWS Marketplace erhältlich sind. Sie können beispielsweise nicht nach dem „VM-Series Next-Generation Firewall Bundle 2“ fragen. Beachten Sie, dass die AMS Managed Firewall-Lösung, die Palo Alto verwendet, derzeit nur ein Angebot zur Filterung des ausgehenden Datenverkehrs bietet, sodass die Verwendung erweiterter Pakete der VM-Serie keine zusätzlichen Funktionen oder Vorteile bieten würde.

Anforderungen für das Onboarding

- Sie müssen die Allgemeinen Geschäftsbedingungen der VM-Series Next-Generation Firewall von Palo Alto im AWS Marketplace lesen und akzeptieren.
- Sie müssen die Instance-Größe, die Sie verwenden möchten, auf der Grundlage Ihrer erwarteten Arbeitslast bestätigen.

- Sie müssen einen /24-CIDR-Block angeben, der nicht zu Konflikten mit Netzwerken in Ihrer Multi-Account-Landing Zone-Umgebung oder vor Ort führt. Sie muss derselben Klasse angehören wie die Egress-VPC (die Lösung stellt eine /24-VPC-Erweiterung für die Egress-VPC VPC).

Preise

Die Basiskosten für die Infrastruktur von AMS Managed Firewall sind in drei Hauptfaktoren aufgeteilt: die EC2 Instanz, die die Palo Alto-Firewall hostet, die Softwarelizenz, die Lizenzen der Palo Alto VM-Serie und Integrationen. CloudWatch

Die folgenden Preise basieren auf der Firewall der Serie VM-300.

- EC2 Instanzen: Die Palo Alto-Firewall wird in einem Hochverfügbarkeitsmodell mit 2-3 EC2 Instanzen ausgeführt, wobei die Instanz auf den erwarteten Workloads basiert. Die Kosten für die Instanz hängen von der Region und der Anzahl der ab AZs
  - Bsp. us-east-1, m5.xlarge, 3 AZs
    - 0,192$ * 24 * 30 * 3 = 414,72$
  - https://aws.amazon.com/ec2/Preise/auf Abfrage/
- Palo Alto-Lizenzen: Die Softwarelizenzkosten einer Palo Alto VM-300-Firewall der nächsten Generation hängen von der Anzahl der AZ sowie vom Instanztyp ab.
  - Bsp. us-east-1, m5.xlarge, 3 AZs
    - 0,87$ * 24 * 30 * 3 = 1879,20$
    - https://aws.amazon.com/marketplace/PP/B083M7JPKB? ref_=srh_res_product_title #pdp - Preisgestaltung
- CloudWatch Integration von Protokollen: Die Protokollintegration nutzt SysLog Server (-t3.medium), NLB und CloudWatch Protokolle. EC2 CloudWatch Die Kosten für die Server hängen von der Region und der Anzahl der Server ab AZs, und die Kosten für die NLB/CloudWatch Protokolle variieren je nach Auslastung des Datenverkehrs.
  - Bsp. us-east-1, t3.medium, 3AZ
    - 0,0416$ * 24 * 30 * 3 = 89,86$
  - https://aws.amazon.com/ec2/Preise/auf Abfrage/
  - https://aws.amazon.com/cloudwatch/Preisgestaltung/

Umkreis (DMZ) VPC

Die Perimeter- oder DMZ-VPC enthält die Ressourcen, die AMS-Betriebsingenieure für den Zugriff auf AMS-Netzwerke benötigen. Es enthält öffentliche Subnetze in 2-3 AZs Bereichen mit SSH-Bastions-Hosts in einer Auto Scaling Scaling-Gruppe (ASG), in die sich die Techniker von AMS Operations einloggen oder einen Tunnel durchqueren können. Die Sicherheitsgruppen, die den DMZ-Bastionen zugeordnet sind, enthalten Port-22-Regeln für eingehenden Datenverkehr von Amazon Corp Networks.

DMZ-VPC-CIDR-Bereich: Wenn Sie eine VPC erstellen, müssen Sie einen IPv4 Adressbereich für die VPC in Form eines CIDR-Blocks (Classless Inter-Domain Routing) angeben, z. B. 10.0.16.0/24. Dies ist der primäre CIDR-Block für Ihre VPC.

> **Note**
>
> Das AMS-Team empfiehlt den Bereich von 24 (mit mehr IP-Adressen), um einen gewissen Puffer für den Fall bereitzustellen, dass in future andere Ressourcen, wie z. B. eine Firewall, bereitgestellt werden.

AWS Transit Gateway

AWS Transit Gateway (TGW) ist ein Service, mit dem Sie Ihre Amazon Virtual Private Clouds (VPCs) und Ihre lokalen Netzwerke mit einem einzigen Gateway verbinden können. Transit Gateway ist das Netzwerk-Backbone, das das Routing zwischen AMS-Kontonetzwerken und externen Netzwerken abwickelt. Informationen zu Transit Gateway finden Sie unter AWS Transit Gateway.

Geben Sie die folgenden Eingaben ein, um diese Ressource zu erstellen:

- Transit Gateway-ASN-Nummer *: Geben Sie die private Autonome Systemnummer (ASN) für Ihr Transit Gateway an. Dabei sollte es sich um die ASN für die AWS-Seite einer BGP-Sitzung (Border Gateway Protocol) handeln. Der Bereich liegt zwischen 64512 und 65534 für 16-Bit. ASNs

Shared Services-Konto

Das Shared Services-Konto dient als zentraler Knotenpunkt für die meisten AMS-Datenebenendienste. Das Konto enthält die Infrastruktur und die Ressourcen, die für Access Management (AD) und Endpoint Security Management (Trend Micro) erforderlich sind, und es enthält

die Kundenbastionen (SSH/RDP). Die folgende Grafik bietet einen allgemeinen Überblick über die im Shared Services-Konto enthaltenen Ressourcen.

Die Shared Services-VPC besteht aus dem AD-Subnetz, dem EPS-Subnetz und dem Customer-Bastions-Subnetz in den drei Verfügbarkeitszonen (). AZs Die in der Shared Services-VPC erstellten Ressourcen sind unten aufgeführt und erfordern Ihre Eingabe.

- Shared Services VPC CIDR-Bereich: Wenn Sie eine VPC erstellen, müssen Sie einen IPv4 Adressbereich für die VPC in Form eines CIDR-Blocks (Classless Inter-Domain Routing) angeben, z. B. 10.0.1.0/24. Dies ist der primäre CIDR-Block für Ihre VPC.

  > **Note**
  >
  > Das AMS-Team empfiehlt den Bereich /23.

- Active Directory-Details: Microsoft Active Directory (AD) wird für user/resource Verwaltung, Authentifizierung/Autorisierung und DNS für all Ihre AMS-Landingzone-Konten mit mehreren Konten verwendet. AMS AD ist außerdem mit einer unidirektionalen Vertrauensstellung für Ihr Active Directory für eine vertrauensbasierte Authentifizierung konfiguriert. Die folgende Eingabe ist erforderlich, um das AD zu erstellen:
  - Domain Fully Qualified Domain Name (FQDN): Der vollqualifizierte Domainname für das AWS Managed Microsoft AD-Verzeichnis. Die Domain sollte keine bestehende Domain oder untergeordnete Domain einer bestehenden Domain in Ihrem Netzwerk sein.
  - Domain-NetBIOS-Name: Wenn Sie keinen NetBIOS-Namen angeben, verwendet AMS standardmäßig den ersten Teil Ihres Verzeichnis-DNS als Namen. Zum Beispiel corp für das Verzeichnis DNS corp.example.com.

- Trend Micro — Endpoint Protection Security (EPS): Trend Micro Endpoint Protection (EPS) ist die Hauptkomponente von AMS für die Betriebssystemsicherheit. Das System besteht aus Deep Security Manager (DSM), EC2 Instanzen, EC2 Relay-Instanzen und einem Agenten, der auf allen Datenebenen und EC2 Kundeninstanzen präsent ist.

  Sie müssen das `EPSMarketplaceSubscriptionRole` im Shared Services-Konto verwenden und entweder das Trend Micro Deep Security (BYOL) AMI oder Trend Micro Deep Security (Marketplace) abonnieren.

Die folgenden Standardeingaben sind erforderlich, um EPS zu erstellen (falls Sie die Standardwerte ändern möchten):

- Relay-Instanztyp: Standardwert — m5.large
- DSM-Instanztyp: Standardwert — m5.xlarge
- DB-Instance-Größe: Standardwert — 200 GB
- RDS-Instance-Typ: Standardwert — db.m5.large

- Kundenbastionen: Im Shared Services-Konto stehen Ihnen SSH- oder RDP-Bastionen (oder beide) zur Verfügung, um auf andere Hosts in Ihrer AMS-Umgebung zugreifen zu können. Um als Benutzer auf das AMS-Netzwerk zuzugreifen (SSH/RDP), you must use "customer" Bastions as the entry point. The network path originates from the on-premise network, goes through DX/ VPNzum Transit Gateway (TGW)) und wird dann zur Shared Services-VPC weitergeleitet. Sobald Sie auf die Bastion zugreifen können, können Sie zu anderen Hosts in der AMS-Umgebung springen, sofern die Zugriffsanfrage genehmigt wurde.
  - Die folgenden Eingaben sind für SSH-Bastionen erforderlich.
    - Gewünschte Instanzkapazität von SSH Bastion: Standardwert: 2.
    - Maximale Anzahl an SSH Bastion-Instanzen: Standardwert: 4.
    - Minimale Anzahl an SSH-Bastion-Instanzen: Standardwert -2.
    - SSH Bastion-Instanztyp: Standardwert — m5.large (kann geändert werden, um Kosten zu sparen; zum Beispiel ein t3.medium).
    - SSH Bastion Ingress CIDRs: IP-Adressbereiche, von denen aus Benutzer in Ihrem Netzwerk auf SSH Bastions zugreifen.
  - Die folgenden Eingaben sind für Windows RDP-Bastionen erforderlich.
    - RDP-Bastion-Instanztyp: Standardwert — t3.medium.
    - Gewünschte Mindestanzahl an Sitzungen für RDP Bastion: Standardwert: 2.
    - Maximale Anzahl an RDP-Sitzungen: Standardwert -10.
    - RDP Bastion-Konfigurationstyp: Sie können eine der folgenden Konfigurationen wählen
      - SecureStandard = Ein Benutzer erhält eine Bastion und nur ein Benutzer kann sich mit der Bastion verbinden.
      - SecureHA = Ein Benutzer erhält zwei Bastionen in zwei verschiedenen AZs, mit denen er sich verbinden kann, und nur ein Benutzer kann sich mit der Bastion verbinden.

    - SharedStandard = Ein Benutzer erhält eine Bastion, mit der er sich verbinden kann, und zwei Benutzer können sich gleichzeitig mit derselben Bastion verbinden.
    - shareDHA = Ein Benutzer erhält zwei Bastionen in zwei verschiedenen AZs, mit denen er sich verbinden kann, und zwei Benutzer können sich gleichzeitig mit derselben Bastion verbinden.
  - Kunden-RDP-Eingang CIDRs: IP-Adressbereiche, von denen aus Benutzer in Ihrem Netzwerk auf RDP Bastions zugreifen.

Aktualisierungen für gemeinsame Dienste: Landing Zone für mehrere Konten

AMS wendet auf monatlicher Basis und ohne vorherige Ankündigung Datenebenen-Releases auf verwaltete Konten an.

AMS verwendet die zentrale Organisationseinheit, um gemeinsam genutzte Dienste wie Zugriff, Netzwerk, EPS, Protokollspeicherung und Alert-Aggregation in Ihrer Multi-Account-Landing Zone bereitzustellen. AMS ist für die Behebung von Sicherheitslücken, das Patchen und die Bereitstellung dieser gemeinsamen Dienste verantwortlich. AMS aktualisiert regelmäßig die Ressourcen, die für die Bereitstellung dieser gemeinsamen Dienste verwendet werden, sodass Benutzer Zugriff auf die neuesten Funktionen und Sicherheitsupdates haben. Die Updates erfolgen in der Regel monatlich. Zu den Ressourcen, die Teil dieser Updates sind, gehören:

- Konten, die Teil der Kernorganisationseinheit sind.

  Das Verwaltungskonto, das Shared Services-Konto, das Netzwerkkonto, das Sicherheitskonto und das Protokollarchivkonto verfügen über Ressourcen für RDP- und SSH-Bastionen, Proxys, Management-Hosts und Endpoint Security (EPS), die normalerweise jeden Monat aktualisiert werden. AMS verwendet unveränderliche EC2 Bereitstellungen als Teil der Shared Services-Infrastruktur.
- Neues AMS AMIs mit den neuesten Updates.

> **Note**
>
> AMS-Operatoren verwenden bei der Ausführung von Änderungen an der Datenebene einen internen Alarmunterdrückungsänderungstyp (CT), und der RFC für diesen CT wird in Ihrer RFC-Liste angezeigt. Dies liegt daran, dass bei der Bereitstellung der Datenebenenversion verschiedene Infrastrukturen heruntergefahren, neu gestartet oder offline geschaltet werden können oder dass CPU-Spitzen oder andere Auswirkungen der Bereitstellung auftreten

können, die Alarme auslösen, die während der Bereitstellung der Datenebene irrelevant sind. Sobald die Bereitstellung abgeschlossen ist, wird überprüft, ob die gesamte Infrastruktur ordnungsgemäß funktioniert, und die Alarme werden wieder aktiviert.

Konto protokollieren und archivieren

Das Log Archive-Konto dient als zentrale Anlaufstelle für die Archivierung von Protokollen in Ihrer AMS-Landingzone-Umgebung mit mehreren Konten. Das Konto enthält einen S3-Bucket, der Kopien der AWS CloudTrail - und AWS Config-Protokolldateien von jedem der AMS-Landingzone-Umgebungskonten mit mehreren Konten enthält. Sie könnten dieses Konto für Ihre zentralisierte Logging-Lösung mit AWS Firehose oder Splunk usw. verwenden. Der Zugriff von AMS auf dieses Konto ist auf einige wenige Benutzer beschränkt. Der Zugriff ist auf Prüfer und Sicherheitsteams beschränkt, die für Compliance-Untersuchungen und forensische Untersuchungen im Zusammenhang mit Kontoaktivitäten zuständig sind.

Sicherheitskonto

Das Sicherheitskonto ist die zentrale Anlaufstelle für Operationen im Zusammenhang mit der Wohnungssicherheit und die zentrale Anlaufstelle für die Weiterleitung von Benachrichtigungen und Warnmeldungen an die AMS-Steuerflugzeugdienste. Darüber hinaus beherbergt das Sicherheitskonto das Amazon Guard Duty-Verwaltungskonto und den AWS Config-Aggregator.

Arten von Anwendungskonten

Anwendungskonten sind AWS-Konten innerhalb der von AMS verwalteten landing zone Zone-Architektur, die Sie zum Hosten Ihrer Workloads verwenden. AMS bietet drei Arten von Anwendungskonten an:

- Von AMS verwaltete Anwendungskonten
- AMS Accelerate-Konten
- Vom Kunden verwaltete Anwendungskonten

Anwendungskonten werden OUs in AWS Organizations je nach Art des Anwendungskontos unterschiedlich gruppiert:

- Stamm-OU:
  1. Anwendungen (OU)
     - Verwaltete Organisationseinheit: Von AMS verwaltete Konten
     - Entwicklungs-OU: Von AMS verwaltete Konten mit aktiviertem Entwicklermodus
  2. Accelerate OU: AMS Accelerate Application-Konten
  3. Kundenverwaltete Organisationseinheit: Vom Kunden verwaltete Anwendungskonten

Anwendungskonten werden über einen RFC bereitgestellt, der vom Verwaltungskonto aus übermittelt wird:

- Anwendungskonto mit VPC erstellen ct-1zdasmc2ewzrs
- Accelerate-Konto erstellen ct-2p93tyd5angmi
- Erstellen Sie ein vom Kunden verwaltetes Anwendungskonto ct-3pwbixz27n3tn

Von AMS verwaltete Anwendungskonten

Anwendungskonten, die vollständig von AMS verwaltet werden, werden als AMS-verwaltete Anwendungskonten bezeichnet, bei denen einige oder alle betrieblichen Aufgaben, wie z. B. Verwaltung von Serviceanfragen, Vorfallmanagement, Sicherheitsmanagement, Kontinuitätsmanagement (Backup), Patchmanagement, Kostenoptimierung oder Überwachung und Eventmanagement der Infrastruktur, von AMS ausgeführt werden.

Die Anzahl der von AMS ausgeführten Aufgaben hängt vom ausgewählten Change-Management-Modus ab. Von AMS verwaltete Konten unterstützen verschiedene Modi für das Änderungsmanagement:

- RFC-Modus
- Direkter Änderungsmodus in AMS
- AMS- und AWS Service Catalog
- AMS Advanced-Entwicklermodus
- Self-Service-Bereitstellungsmodus in AMS

Weitere Informationen zum Änderungsmanagement und zu den verschiedenen Modi finden Sie unter. Verwaltungsmodi ändern

Es gibt einige AWS-Services, die Sie in Ihrem AMS-verwalteten Konto ohne AMS-Management verwenden können. Die Liste dieser AWS-Services und wie Sie sie Ihrem AMS-Konto hinzufügen können, finden Sie im Abschnitt Self-Service-Bereitstellung.

AMS Accelerate-Konten

AMS Accelerate ist der AMS-Betriebsplan, mit dem die AWS-Infrastruktur betrieben werden kann, die Workloads unterstützt. Sie können von den Betriebsservices von AMS Accelerate wie Überwachung und Warnung, Incident Management, Sicherheitsmanagement und Backup-Management profitieren, ohne eine neue Migration durchführen zu müssen, Ausfallzeiten zu erleben oder Ihre Nutzung von AWS zu ändern. AMS Accelerate bietet auch ein optionales Patch-Add-on für EC2 basierte Workloads, die regelmäßig gepatcht werden müssen.

Mit AMS Accelerate haben Sie die Freiheit, alle AWS-Services nativ oder mit Ihren bevorzugten Tools zu verwenden, zu konfigurieren und bereitzustellen. Sie verwenden Ihre bevorzugten Zugriffs- und Änderungsmechanismen, während AMS konsequent bewährte Verfahren anwendet, die Ihnen helfen, Ihr Team zu skalieren, Kosten zu optimieren, Sicherheit und Effizienz zu erhöhen und die Ausfallsicherheit zu verbessern.

> **Note**
>
> AMS Accelerate-Konten in AMS Advanced verfügen weder über AMS Change Management (RFCs) noch über die AMS Advanced-Konsole. Stattdessen verfügen sie über die AMS Accelerate-Konsole und Funktionen.

Accelerate-Konten können nur über Ihr AMS-Landing landing zone Management-Konto mit mehreren Konten bereitgestellt werden. Accelerate bietet verschiedene betriebliche Funktionen. Weitere Informationen finden Sie in der Leistungsbeschreibung von Accelerate.

- Sie werden weiterhin einige der Funktionen der Kernkonten mit mehreren Konten (MALZ) nutzen können, z. B. zentrale Protokollierung, Einzelabrechnung, Config Aggregator im Sicherheitskonto und. SCPs
- AMS Accelerate bietet einige AMS Advanced-Dienste wie EPS, Access Management, Change Management und Provisioning nicht an. Wir empfehlen Ihnen, die nächsten Schritte zu befolgen, um Zugriff auf das Transit Gateway (TGW) zu erhalten und es zu konfigurieren.

Weitere Informationen zu Accelerate finden Sie unter Was ist Accelerate.

Erstellen Sie Ihr Accelerate-Konto

Gehen Sie wie folgt vor, um ein Accelerate-Konto zu erstellen: Accelerate-Konto erstellen.

Zugriff auf Ihr Accelerate-Konto

Nachdem Sie ein Accelerate-Konto in Ihrem MALZ-Konto (Multi-Account landing zone) bereitgestellt haben, können Sie in dem Konto eine Rolle mit administrativen Zugriffsberechtigungen übernehmen. `AccelerateDefaultAdminRole`

So greifen Sie auf das neue Accelerate-Konto zu:

1. Melden Sie sich bei der IAM-Konsole für das Verwaltungskonto mit der `CustomerDefaultAssumeRole` Rolle an.
2. Wählen Sie in der IAM-Konsole in der Navigationsleiste Ihren Benutzernamen aus.
3. Wählen Sie Switch Role. Wenn Sie diese Option erstmalig auswählen, wird eine Seite mit weiteren Informationen angezeigt. Lesen Sie sich diese Informationen durch und klicken Sie dann auf Switch Role (Rolle wechseln). Wenn Sie die Cookies Ihres Browsers löschen, kann die Seite erneut angezeigt werden.
4. Geben Sie auf der Seite „Rolle wechseln“ die Accelerate-Konto-ID und den Namen der Rolle ein, die Sie annehmen möchten:`AccelerateDefaultAdminRole`.

Nachdem Sie nun Zugriff haben, können Sie neue IAM-Rollen erstellen, um weiterhin auf Ihre Umgebung zuzugreifen. Wenn Sie SAML Federation für Ihr Accelerate-Konto nutzen möchten, finden Sie weitere Informationen unter Aktivieren des Zugriffs auf die AWS-Managementkonsole für SAML 2.0-Verbundbenutzer.

Ihr Accelerate-Konto mit Transit Gateway verbinden

AMS verwaltet die Netzwerkeinrichtung eines Accelerate-Kontos nicht. Sie haben die Möglichkeit, Ihr eigenes Netzwerk mit AWS zu verwalten APIs (siehe Netzwerklösungen) oder eine Verbindung zum von AMS verwalteten MALZ-Netzwerk herzustellen, indem Sie das bestehende Transit Gateway (TGW) verwenden, das in AMS MALZ bereitgestellt wird.

> **Note**
>
> Sie können nur dann eine VPC mit dem TGW verbinden, wenn sich das Accelerate-Konto in derselben AWS-Region befindet. Weitere Informationen finden Sie unter Transit-Gateways.

Um Ihr Accelerate-Konto zu Transit Gateway hinzuzufügen, fordern Sie mithilfe des Änderungstyps Bereitstellung | Verwaltete landing zone | Netzwerkkonto | Statische Route hinzufügen (ct-3r2ckznmt0a59) eine neue Route an. Geben Sie folgende Informationen an:

- Blackhole: True bedeutet, dass das Ziel der Route nicht verfügbar ist. Tun Sie dies, wenn der Verkehr für die statische Route vom Transit Gateway unterbrochen werden soll. False, um den Verkehr an die angegebene TGW-Anhangs-ID weiterzuleiten. Der Standardwert ist „false“.
- DestinationCidrBlock: Der IPV4 CIDR-Bereich, der für Zielübereinstimmungen verwendet wird. Routing-Entscheidungen basieren auf der genauesten Übereinstimmung. Beispiel: 10.0.2.0/24.
- TransitGatewayAttachmentId: Die TGW-Anhangs-ID, die als Ziel für die Routentabelle dient. Wenn Blackhole den Wert false hat, ist dieser Parameter erforderlich, andernfalls lassen Sie diesen Parameter leer. Beispiel: tgw-attach-04eb40d1e14ec7272.
- TransitGatewayRouteTableId: Die ID der TGW-Routentabelle. Beispiel: tgw-rtb-06ddc751c0c0c881c.

Erstellen Sie Routen in den TGW-Routentabellen, um eine Verbindung zu dieser VPC herzustellen:

1. Standardmäßig kann diese VPC mit keiner anderen VPCs in Ihrem MALZ-Netzwerk kommunizieren.
2. Entscheiden Sie mit Ihrem Lösungsarchitekten, mit was VPCs diese Accelerate-VPC kommunizieren soll.
3. Bereitstellung einreichen | Verwaltete landing zone | Netzwerkkonto | Änderungstyp für statische Route (ct-3r2ckznmt0a59) hinzufügen, geben Sie folgende Informationen an:
   - Blackhole: True bedeutet, dass das Ziel der Route nicht verfügbar ist. Tun Sie dies, wenn der Verkehr für die statische Route vom Transit Gateway unterbrochen werden soll. False, um den Verkehr an die angegebene TGW-Anhangs-ID weiterzuleiten. Der Standardwert ist „false“.
   - DestinationCidrBlock: Der IPV4 CIDR-Bereich, der für Zielübereinstimmungen verwendet wird. Routing-Entscheidungen basieren auf der genauesten Übereinstimmung. Beispiel: 10.0.2.0/24.
   - TransitGatewayAttachmentId: Die TGW-Anhangs-ID, die als Ziel für die Routentabelle dient. Wenn Blackhole den Wert false hat, ist dieser Parameter erforderlich, andernfalls lassen Sie diesen Parameter leer. Beispiel: tgw-attach-04eb40d1e14ec7272.
   - TransitGatewayRouteTableId: Die ID der TGW-Routentabelle. Beispiel: tgw-rtb-06ddc751c0c0c881c.

Eine neue Accelerate-Account-VPC mit dem AMS Multi-Account Landing Zone-Netzwerk verbinden (einen TGW-VPC-Anhang erstellen):

1. Öffnen Sie in Ihrem landing zone Networking-Konto mit mehreren Konten die Amazon VPC-Konsole.
2. Klicken Sie im Navigationsbereich auf Transit Gateways. Notieren Sie sich die TGW-ID des Transit-Gateways, das Sie sehen.
3. Öffnen Sie in Ihrem Accelerate-Konto die Amazon VPC-Konsole.
4. Wählen Sie im Navigationsbereich Transit Gateway Gateway-Anlagen > Transit Gateway Gateway-Anlage erstellen. Treffen Sie diese Entscheidungen:
   - Wählen Sie für die Transit Gateway Gateway-ID die Transit-Gateway-ID aus, die Sie in Schritt 2 aufgezeichnet haben.
   - Wählen Sie bei Attachment type (Anhangstyp) die Option VPC aus.
   - Geben Sie unter VPC Attachment (VPC-Anfügung) optional einen Namen für Attachment name tag (Anfügungs-Namens-Tag) ein.
   - Wählen Sie aus, ob DNS-Support und IPv6 Support aktiviert werden sollen.
   - Wählen Sie für VPC ID die VPC aus, die dem Transit-Gateway angefügt werden soll. Dieser VPC muss mindestens ein Subnetz zugeordnet sein.
   - Wählen Sie unter Subnetz ein Subnetz für jede Availability Zone aus IDs, das vom Transit-Gateway zur Weiterleitung des Datenverkehrs verwendet werden soll. Sie müssen mindestens ein Subnetz auswählen. Sie können nur ein Subnetz pro Availability Zone auswählen.
5. Wählen Sie Create attachment (Anhang erstellen) aus. Notieren Sie sich die ID des neu erstellten TGW-Anhangs.

Zuordnen des TGW-Anhangs zu einer Routentabelle:

1. Entscheiden Sie, welcher TGW-Routentabelle Sie die VPC zuordnen möchten. Wir empfehlen, eine neue Anwendungsroutentabelle für das Accelerate-Konto VPCs mithilfe des Änderungstyps Deployment | Managed landing zone | Netzwerkkonto | Transit-Gateway-Routentabelle erstellen (ct-3dscwaeyi6cup) zu erstellen.
2. Reichen Sie einen RFC Management | Managed landing zone | Networking Account | TGW-Attachment (ct-3nmhh0qr338q6) für das Netzwerkkonto ein, um den VPC- oder TGW-Anhang der ausgewählten Routentabelle zuzuordnen.

Erstellen Sie Routen in den TGW-Routentabellen, um eine Verbindung zu dieser VPC herzustellen:

1. Standardmäßig kann diese VPC mit keiner anderen VPCs in Ihrem Landingzone-Netzwerk mit mehreren Konten kommunizieren.
2. Entscheiden VPCs Sie mit Ihrem Lösungsarchitekten, mit was diese Accelerate-Account-VPC kommunizieren soll.
3. Bereitstellung einreichen | Verwaltete landing zone | Netzwerkkonto | Fügen Sie statische Route (ct-3r2ckznmt0a59) RFC für das Netzwerkkonto hinzu, um die benötigten TGW-Routen zu erstellen.

Konfiguration Ihrer VPC-Routing-Tabellen so, dass sie auf das AMS landing zone Transit Gateway für mehrere Konten verweisen:

1. Entscheiden Sie gemeinsam mit Ihrem Lösungsarchitekten, welchen Verkehr Sie an das AMS Multi-Account Landing Zone-Transit-Gateway senden möchten.
2. Bereitstellung einreichen | Verwaltete landing zone | Netzwerkkonto | Fügen Sie statische Route (ct-3r2ckznmt0a59) RFC für das Netzwerkkonto hinzu, um die benötigten TGW-Routen zu erstellen.

Vom Kunden verwaltete Anwendungskonten

Sie können Konten erstellen, die AMS nicht standardmäßig verwaltet. Diese Konten werden als vom Kunden verwaltete Konten bezeichnet und geben Ihnen die volle Kontrolle über den Eigenbetrieb der Infrastruktur innerhalb der Konten, während Sie gleichzeitig die Vorteile der zentralisierten Architektur nutzen können, die von AMS verwaltet wird.

Kundenverwaltete Konten haben keinen Zugriff auf die AMS-Konsole oder einen der von uns angebotenen Dienste (Patch, Backup usw.).

Kundenverwaltete Konten können nur über Ihr AMS-Landingzone-Verwaltungskonto mit mehreren Konten bereitgestellt werden.

Verschiedene AMS-Modi funktionieren unterschiedlich mit Anwendungskonten. Weitere Informationen zu den Modi finden Sie unter AWS Managed Services Services-Modi.

Informationen zur Erstellung Ihres kundenverwalteten Anwendungskontos finden Sie unter Verwaltungskonto | Kundenverwaltetes Anwendungskonto erstellen.

Um ein vom Kunden verwaltetes Anwendungskonto zu löschen, verwenden Sie Verwaltungskonto | Offboard-Anwendungskonto. (Das Confirm Offboarding CT gilt nicht für vom Kunden verwaltete Anwendungskonten.)

Zugriff auf Ihr vom Kunden verwaltetes Konto

Nachdem Sie ein vom Kunden verwaltetes Konto (CMA) in der landing zone mit mehreren Konten (MALZ) bereitgestellt haben, befindet sich im Konto eine AdministratorrolleCustomerDefaultAdminRole,, die Sie über den SAML-Verbund übernehmen müssen, um das Konto zu konfigurieren.

So greifen Sie auf die CMA zu:

1. Melden Sie sich bei der IAM-Konsole für das Verwaltungskonto mit der Rolle an CustomerDefaultAssumeRole.
2. Wählen Sie in der IAM-Konsole in der Navigationsleiste Ihren Benutzernamen aus.
3. Wählen Sie Switch Role. Wenn Sie diese Option erstmalig auswählen, wird eine Seite mit weiteren Informationen angezeigt. Lesen Sie sich diese Informationen durch und klicken Sie dann auf Switch Role (Rolle wechseln). Wenn Sie die Cookies Ihres Browsers löschen, kann die Seite erneut angezeigt werden.
4. Geben Sie auf der Seite „Rolle wechseln“ die ID des vom Kunden verwalteten Kontos und den Namen der Rolle ein, die Sie übernehmen möchten: CustomerDefaultAdminRole.

Nachdem Sie nun Zugriff haben, können Sie neue IAM-Rollen erstellen, um weiterhin auf Ihre Umgebung zuzugreifen. Wenn Sie SAML Federation für Ihr CMA-Konto nutzen möchten, finden Sie weitere Informationen unter Aktivieren des Zugriffs auf die AWS-Managementkonsole für SAML 2.0-Verbundbenutzer.

Verbinden Sie Ihre CMA mit Transit Gateway

AMS verwaltet nicht die Netzwerkeinrichtung von vom Kunden verwalteten Konten (CMAs). Sie haben die Möglichkeit, Ihr eigenes Netzwerk mit AWS zu verwalten APIs (siehe Networking Solutions) oder eine Verbindung zu dem von AMS verwalteten Mehrkonto-Landingzone-Netzwerk herzustellen, indem Sie das bestehende Transit Gateway (TGW) verwenden, das in AMS MALZ bereitgestellt wird.

> **Note**
>
> Sie können nur dann eine VPC mit dem TGW verbinden, wenn sich die CMA in derselben AWS-Region befindet. Weitere Informationen finden Sie unter Transit-Gateways.

Um Ihre CMA zu Transit Gateway hinzuzufügen, fordern Sie eine neue Route mit dem Änderungstyp Netzwerkkonto | Statische Route hinzufügen (ct-3r2ckznmt0a59) an und geben Sie folgende Informationen an:

- Blackhole: True bedeutet, dass das Ziel der Route nicht verfügbar ist. Tun Sie dies, wenn der Verkehr für die statische Route vom Transit Gateway unterbrochen werden soll. False, um den Verkehr an die angegebene TGW-Anhangs-ID weiterzuleiten. Der Standardwert ist „false“.
- DestinationCidrBlock: Der IPV4 CIDR-Bereich, der für Zielübereinstimmungen verwendet wird. Routing-Entscheidungen basieren auf der genauesten Übereinstimmung. Beispiel: `10.0.2.0/24`.
- TransitGatewayAttachmentId: Die TGW-Anhangs-ID, die als Ziel für die Routentabelle dient. Wenn Blackhole den Wert false hat, ist dieser Parameter erforderlich, andernfalls lassen Sie diesen Parameter leer. Beispiel: `tgw-attach-04eb40d1e14ec7272`.
- TransitGatewayRouteTableId: Die ID der TGW-Routentabelle. Beispiel: `tgw-rtb-06ddc751c0c0c881c`.

Verbindung einer neuen kundenverwalteten VPC mit dem AMS Multi-Account Landing Zone-Netzwerk (Erstellen eines TGW-VPC-Anhangs):

1. Öffnen Sie in Ihrem landing zone Networking-Konto mit mehreren Konten die Amazon VPC-Konsole.
2. Wählen Sie im Navigationsbereich Transit Gateways aus. Notieren Sie sich die TGW-ID des Transit-Gateways, das Sie sehen.
3. Öffnen Sie in Ihrem vom Kunden verwalteten Konto die Amazon VPC-Konsole.
4. Wählen Sie im Navigationsbereich Transit Gateway Gateway-Anlagen > Transit Gateway Gateway-Anlage erstellen. Treffen Sie diese Entscheidungen:
    a. Wählen Sie für die Transit Gateway Gateway-ID die Transit-Gateway-ID aus, die Sie in Schritt 2 aufgezeichnet haben.
    b. Wählen Sie bei Attachment type (Anhangstyp) die Option VPC aus.

c. Geben Sie unter VPC Attachment (VPC-Anfügung) optional einen Namen für Attachment name tag (Anfügungs-Namens-Tag) ein.

d. Wählen Sie aus, ob DNS-Support und IPv6 Support aktiviert werden sollen.

e. Wählen Sie für VPC ID die VPC aus, die dem Transit-Gateway angefügt werden soll. Dieser VPC muss mindestens ein Subnetz zugeordnet sein.

f. Wählen Sie unter Subnetz ein Subnetz für jede Availability Zone aus IDs, das vom Transit-Gateway zur Weiterleitung des Datenverkehrs verwendet werden soll. Sie müssen mindestens ein Subnetz auswählen. Sie können nur ein Subnetz pro Availability Zone auswählen.

5. Wählen Sie Create attachment (Anhang erstellen) aus. Notieren Sie sich die ID des neu erstellten TGW-Anhangs.

Zuordnen des TGW-Anhangs zu einer Routentabelle:

Entscheiden Sie, mit welcher TGW-Routentabelle Sie die VPC verknüpfen möchten. Wir empfehlen, eine neue Anwendungsroutentabelle für Customer Managed zu erstellen, VPCs indem Sie einen RFC für Bereitstellung | Verwaltete landing zone | Netzwerkkonto | Transit-Gateway-Routentabelle erstellen (ct-3dscwaeyi6cup) einreichen. Um die VPC- oder TGW-Anlage der ausgewählten Routing-Tabelle zuzuordnen, reichen Sie einen RFC Deployment | Managed landing zone | Networking Account | Associate TGW Attachment (ct-3nmhh0qr338q6) für das Netzwerkkonto ein.

Erstellen Sie Routen in den TGW-Routentabellen, um eine Verbindung zu dieser VPC herzustellen:

1. Standardmäßig kann diese VPC mit keiner anderen VPCs in Ihrem Multi-Account-Landingzone-Netzwerk kommunizieren.
2. Entscheiden Sie mit Ihrem Lösungsarchitekten, mit was VPCs diese vom Kunden verwaltete VPC kommunizieren soll. Bereitstellung einreichen | Verwaltete landing zone | Netzwerkkonto | Fügen Sie statische Route (ct-3r2ckznmt0a59) RFC für das Netzwerkkonto hinzu, um die benötigten TGW-Routen zu erstellen.

> **Note**
>
> Dieses CT (ct-3r2ckznmt0a59) erlaubt es nicht EgressRouteDomain, statische Routen zur Core-Routentabelle hinzuzufügen. Wenn Ihre CMA ausgehenden Verkehr zulassen muss, reichen Sie einen Management | Other | Other (MOO) -RFC mit ct-0xdawir96cy7k ein.

Konfiguration Ihrer VPC-Routentabellen so, dass sie auf das AMS Multi-Account Landing Zone-Transit-Gateway verweisen:

Entscheiden Sie gemeinsam mit Ihrem Lösungsarchitekten, welchen Verkehr Sie an das AMS Multi-Account Landing Zone-Transit-Gateway senden möchten. Aktualisieren Sie Ihre VPC-Routentabellen, um Traffic an den zuvor erstellten TGW-Anhang zu senden

Holen Sie sich operative Hilfe mit Ihren vom Kunden verwalteten Konten

AMS kann Ihnen helfen, die Workloads zu verwalten, die Sie in Ihren vom Kunden verwalteten Konten bereitgestellt haben, indem das Konto in AMS Accelerate integriert wird. Mit AMS Accelerate können Sie von operativen Services wie Überwachung und Alarmierung, Incident Management, Sicherheitsmanagement und Backup-Management profitieren, ohne eine neue Migration durchführen zu müssen, Ausfallzeiten zu haben oder Ihre Nutzung zu ändern. AWS AMS Accelerate bietet auch ein optionales Patch-Add-on für EC2 basierte Workloads, die regelmäßig gepatcht werden müssen. Mit AMS Accelerate nutzen, konfigurieren und implementieren Sie weiterhin alle AWS Dienste nativ oder mit Ihren bevorzugten Tools, wie Sie es mit AMS Advanced Customer Managed Accounts tun. Sie verwenden Ihre bevorzugten Zugriffs- und Änderungsmechanismen, während AMS bewährte Methoden anwendet, die Ihnen helfen, Ihr Team zu skalieren, Kosten zu optimieren, Sicherheit und Effizienz zu erhöhen und die Ausfallsicherheit zu verbessern. Weitere Informationen finden Sie in der Leistungsbeschreibung von Accelerate.

Um Ihr kundenverwaltetes Konto in Accelerate einzubinden, wenden Sie sich an Ihren CSDM und folgen Sie den Schritten unter Erste Schritte mit AMS Accelerate.

> **Note**
>
> AMS Accelerate-Konten in AMS Advanced verfügen weder über das AMS-Änderungsmanagement (Änderungsanträge oder RFCs) noch über die AMS Advanced-Konsole. Stattdessen verfügen sie über die AMS Accelerate-Konsole und -Funktionalität.

AMS Tools-Konto (Workloads migrieren)

Ihr Konto für Landing Zone-Tools mit mehreren Konten (mit VPC) beschleunigt die Migration, verbessert Ihre Sicherheitsposition, reduziert Kosten und Komplexität und standardisiert Ihr Nutzungsmuster.

Ein Tools-Konto bietet Folgendes:

- Eine klar definierte Grenze für den Zugriff auf Replikationsinstanzen für Systemintegratoren außerhalb Ihrer Produktions-Workloads.
- Ermöglicht die Einrichtung einer isolierten Kammer, um einen Workload auf Malware oder unbekannte Netzwerkrouten zu überprüfen, bevor er einem Konto mit anderen Workloads zugeordnet wird.
- Da es sich um ein definiertes Konto handelt, bietet es eine schnellere Einarbeitung und Einrichtung für die Migration von Workloads.
- Isolierte Netzwerkrouten zur Sicherung des Datenverkehrs vor Ort -> -> Tools-Konto CloudEndure -> AMS-aufgenommenes Image. Sobald ein Image aufgenommen wurde, können Sie es über einen AMS Management | Advanced Stack Components | AMI | Share (ct-1eiczxw8ihc18) -RFC für das Zielkonto freigeben.

Übergeordnetes Architekturdiagramm:

Verwenden Sie den Änderungstyp Deployment | Managed landing zone | Management account | Tools account (with VPC) erstellen (ct-2j7q1hgf26x5c), um schnell ein Tools-Konto bereitzustellen und einen Workload Ingestion-Prozess in einer Multi-Account-Landingzone-Umgebung zu instanziieren. Siehe Verwaltungskonto, Tools-Konto: Erstellen (mit VPC).

> **Note**
>
> Wir empfehlen, zwei Verfügbarkeitszonen (AZs) einzurichten, da es sich um einen Migrationshub handelt.
> Standardmäßig erstellt AMS die folgenden zwei Sicherheitsgruppen (SGs) in jedem Konto. Vergewissern Sie sich, dass diese beiden vorhanden SGs sind. Wenn sie nicht vorhanden sind, öffnen Sie bitte eine neue Serviceanfrage beim AMS-Team, um sie anzufordern.
>
> - SentinelDefaultSecurityGroupPrivateOnlyEgressAll
> - InitialGarden-SentinelDefaultSecurityGroupPrivateOnly

Stellen Sie sicher, dass CloudEndure Replikationsinstanzen im privaten Subnetz erstellt werden, in dem es Routen zurück zum Standort gibt. Sie können dies überprüfen, indem Sie sicherstellen, dass die Routing-Tabellen für das private Subnetz über eine Standardroute zurück zu TGW verfügen. Bei einem CloudEndure Computer-Cutover sollte jedoch das „isolierte“ private Subnetz verwendet werden, in dem es keine Route zurück zum lokalen Standort gibt, sondern nur ausgehender Internetverkehr zulässig ist. Es ist wichtig sicherzustellen, dass die Umstellung im isolierten Subnetz erfolgt, um mögliche Probleme mit den Ressourcen vor Ort zu vermeiden.

Voraussetzungen:

1. Entweder Plus - oder Premium-Supportstufe.
2. Das Anwendungskonto IDs für den KMS-Schlüssel, auf dem AMIs sie bereitgestellt werden.
3. Das Tools-Konto, das wie zuvor beschrieben erstellt wurde.

AWS Service zur Anwendungsmigration (AWS MGN)

AWS Der Application Migration Service (AWS MGN) kann in Ihrem MALZ Tools-Konto über die `AWSManagedServicesMigrationRole` IAM-Rolle verwendet werden, die bei der Bereitstellung des Tools-Kontos automatisch erstellt wird. Sie können AWS MGN verwenden, um Anwendungen und Datenbanken zu migrieren, die auf unterstützten Versionen von Windows- und Linux-Betriebssystemen laufen.

Die meisten up-to-date Informationen zum AWS-Region Support finden Sie in der Liste der AWS regionalen Dienste.

Falls Ihr bevorzugtes AWS-Region Produkt derzeit nicht von AWS MGN unterstützt wird oder das Betriebssystem, auf dem Ihre Anwendungen ausgeführt werden, derzeit nicht von AWS MGN unterstützt wird, sollten Sie in Erwägung ziehen, stattdessen die CloudEndure Migration in Ihrem Tools-Konto zu verwenden.

Beantragen Sie die MGN-Initialisierung AWS

AWS MGN muss vor der ersten Verwendung von AMS initialisiert werden. Um dies für ein neues Tools-Konto zu beantragen, reichen Sie einen RFC Management | Other | Other aus dem Tools-Konto mit den folgenden Angaben ein:

```
RFC Subject=Please initialize AWS MGN in this account
RFC Comment=Please click 'Get started' on the MGN welcome page here:

    https://console.aws.amazon.com/mgn/home?region=MALZ_PRIMARY_REGION#/welcome using
 all default values
    to 'Create template' and complete the initialization process.
```

Sobald AMS den RFC erfolgreich abgeschlossen und AWS MGN in Ihrem Tools-Konto initialisiert hat, können Sie die Standardvorlage `AWSManagedServicesMigrationRole` für Ihre Anforderungen bearbeiten.

Zugriff auf das neue AMS Tools-Konto aktivieren

Sobald das Tools-Konto erstellt wurde, stellt AMS Ihnen eine Konto-ID zur Verfügung. Ihr nächster Schritt besteht darin, den Zugriff auf das neue Konto zu konfigurieren. Dazu gehen Sie wie folgt vor:

1. Aktualisieren Sie die entsprechenden Active Directory-Gruppen auf das entsprechende Konto IDs.

   Neuen, von AMS erstellten Konten wird die ReadOnly Rollenrichtlinie sowie eine Rolle zugewiesen, über die Benutzer Dateien ablegen können. RFCs

   Für das Tools-Konto stehen außerdem eine zusätzliche IAM-Rolle und ein zusätzlicher Benutzer zur Verfügung:

   - IAM-Rolle: `AWSManagedServicesMigrationRole`
   - IAM-Benutzer: `customer_cloud_endure_user`
2. Fordern Sie Richtlinien und Rollen an, damit die Mitglieder des Serviceintegrationsteams Tools der nächsten Generation einrichten können.

   Navigieren Sie zur AMS-Konsole und legen Sie Folgendes ab RFCs:

   a. KMS-Schlüssel erstellen. Verwenden Sie entweder KMS-Schlüssel erstellen (auto) oder KMS-Schlüssel erstellen (Überprüfung erforderlich).

      Wenn Sie KMS zum Verschlüsseln aufgenommener Ressourcen verwenden, bietet die Verwendung eines einzigen KMS-Schlüssels, der mit den übrigen Landingzone-Anwendungskonten für mehrere Konten gemeinsam genutzt wird, Sicherheit für aufgenommene Bilder, sodass sie im Zielkonto entschlüsselt werden können.

   b. Teilen Sie den KMS-Schlüssel.

Verwenden Sie den Änderungstyp Verwaltung | Erweiterte Stack-Komponenten | KMS-Schlüssel | Teilen (Überprüfung erforderlich) (ct-05yb337abq3x5), um anzufordern, dass der neue KMS-Schlüssel für Ihre Anwendungskonten freigegeben wird, in denen die Daten gespeichert werden. AMIs

Beispielgrafik einer endgültigen Kontoeinrichtung:

Beispiel für eine vorab genehmigte IAM-Richtlinie von CloudEndure AMS

Um eine vorab von AMS genehmigte CloudEndure IAM-Richtlinie einzusehen:
Entpacken Sie die WIGS Cloud Endure Landing Zone-Beispieldatei und öffnen Sie die. `customer_cloud_endure_policy.json`

Testen der Konnektivität und end-to-end Einrichtung des AMS Tools-Kontos

1. Beginnen Sie mit der Konfiguration CloudEndure und Installation des CloudEndure Agenten auf einem Server, der auf AMS repliziert wird.
2. Erstellen Sie ein Projekt in CloudEndure.
3. Geben Sie die AWS Anmeldeinformationen ein, die Sie bei der Erfüllung der Voraussetzungen über den Secrets Manager gemeinsam genutzt haben.
4. In den Replikationseinstellungen:
   a. Wählen Sie für die Option Wählen Sie die Sicherheitsgruppen aus, die auf die Replikationsserver angewendet werden sollen, beide AMS- „Sentinel“ -Sicherheitsgruppen (Nur privat und EgressAll) aus.
   b. Definieren Sie Umtauschoptionen für die Maschinen (Instanzen). Weitere Informationen finden Sie in Schritt 5. Überschneiden
   c. Subnetz: Privates Subnetz.
5. Sicherheitsgruppe:
   a. Wählen Sie beide AMS-Sicherheitsgruppen „Sentinel“ aus (Nur privat und EgressAll).
   b. Cutover-Instanzen müssen mit dem von AMS verwalteten Active Directory (MAD) und mit öffentlichen Endpunkten kommunizieren: AWS
      i. Elastische IP: Keine
      ii. Öffentliche IP: nein
      iii. IAM-Rolle: customer-mc-ec 2-Instanzen-Profil

c. Legen Sie Tags gemäß Ihrer internen Tagging-Konvention fest.

6. Installieren Sie den CloudEndure Agenten auf dem Computer und suchen Sie in der EC2 Konsole nach der Replikationsinstanz, die in Ihrem AMS-Konto angezeigt werden soll.

Der AMS-Aufnahmeprozess:

AMS Tools Kontohygiene

Sie sollten aufräumen, nachdem Sie mit dem Konto fertig sind, das AMI gemeinsam genutzt haben und die replizierten Instances nicht mehr benötigen:

- Nach der Inanspruchnahme der WIGs Instance:
  - Cutover-Instance: Stoppen oder beenden Sie diese Instanz mindestens, nachdem die Arbeit abgeschlossen ist, über die AWS-Konsole
  - AMI-Backups vor der Ingestion: Wird entfernt, sobald die Instance aufgenommen und die On-Premise-Instance beendet wurde
  - AMS-Ingested Instances: Schalten Sie den Stack aus oder beenden Sie ihn, sobald das AMI gemeinsam genutzt wurde
  - AMS-Ingested AMIs: Wird gelöscht, sobald die gemeinsame Nutzung mit dem Zielkonto abgeschlossen ist
- Bereinigung am Ende der Migration: Dokumentieren Sie die Ressourcen, die im Entwicklermodus bereitgestellt wurden, um sicherzustellen, dass die Bereinigung regelmäßig erfolgt, zum Beispiel:
  - Sicherheitsgruppen
  - Ressourcen, die über Cloud-Formation erstellt wurden
  - Netzwerk ACK
  - Subnetz
  - VPC
  - Routing-Tabelle
  - Rollen
  - Benutzer und Konten

Migration im großen Maßstab - Migration Factory

Weitere Informationen finden Sie unter Einführung in die AWS CloudEndure Migration Factory-Lösung.

MALZ: Onboarding von Kernkonten

Die wichtigsten Aufgaben, die Sie beim Onboarding in ein AWS Landingzone-Kernkonto mit mehreren Konten erledigen müssen, lauten wie folgt:.

Themen

- Erstellen Sie ein AWS Landingzone-Kernkonto mit mehreren Konten in AMS
- Erstellen Sie eine IAM-Rolle für AMS, um auf Ihr Konto zuzugreifen
- Sichern Sie das neue Konto mit Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer in AMS
- Abonnieren AWS Marketplace Sie Trend Micro Endpoint Protection (EPS)
- Netzwerk einrichten
- Zugangsverwaltung einrichten

Bei Fragen zum Onboarding wenden Sie sich an Ihren Cloud Architect.

Erstellen Sie ein AWS Landingzone-Kernkonto mit mehreren Konten in AMS

Die AMS-Landingzone mit mehreren Konten erfordert die Bereitstellung eines neuen Amazon Web Services (AWS) -Kontos, das als Verwaltungskonto in der AMS-Landingzone-Umgebung mit mehreren Konten fungiert. Gehen Sie folgendermaßen vor AWS-Konto, um ein Konto step-by-step zu erstellen: Wie erstelle und aktiviere ich ein neues Amazon Web Services Services-Konto?

Die einfachen Schritte sind: Gehen Sie zu Konto erstellen, klicken Sie auf Jetzt registrieren und klicken Sie auf der sich öffnenden Seite auf Neues erstellen AWS-Konto. Folgen Sie den Anweisungen auf dem Bildschirm, einschließlich der Annahme eines Telefonanrufs und der Eingabe einer PIN über die Telefontastatur. Sie müssen auch eine Kreditkarte eingeben. AMS verwendet dieses Konto als Verwaltungskonto oder Zahlerkonto für Ihre neue landing zone mit mehreren Konten.

Note

Sprechen Sie nach dem Onboarding mit Ihrem Cloud Service Delivery Manager (CSDM) darüber, wie Sie die Abrechnung von Ihrer Kreditkarte auf ein Rechnungssystem verlagern können. Die folgenden Informationen werden benötigt:

- Name der Rechnungsfirma
- Name der Kontaktperson für die Abrechnung
- Telefonnummer des Abrechnungskontakts
- E-Mail-Adresse des Abrechnungskontakts
- Rechnungsadresse

Ihr CSDM hilft Ihnen bei diesem Update. Wenn Sie den Vorgang abgeschlossen haben und die Zahlungsmethode ändern möchten, finden Sie weitere Informationen unter Verwaltung Ihrer AWS Zahlungsmethoden.

Note

Verknüpfen Sie Ihr neues Konto nicht mit einem bestehenden Verwaltungs- oder Zahlerkonto. Stellen Sie sicher, dass Ihr Konto nicht Teil eines bestehenden Kontos ist AWS Organizations. Weitere Informationen finden Sie unter Was ist AWS Organizations?

Important

Es ist sehr wichtig, dass Sie sicherstellen, dass dem Konto eine E-Mail-Adresse (eine Verteilerliste, keine E-Mail-Adresse einer Person) und eine Telefonnummer zugeordnet sind, damit Sie Antworten auf potenzielle Sicherheitsvorfälle erhalten. Die Telefonnummer und E-Mail-Adresse für das Konto können nicht geändert werden, ohne das Kontopasswort zurückzusetzen, was für ein AMS-Root-Konto ein erhebliches Unterfangen darstellt.
Um sicherzustellen, dass diese Werte stabil sind, ist es wichtig, Kontaktinformationen auszuwählen, die nicht mit Personen verknüpft sind, da diese sich ändern können. Wählen Sie einen E-Mail-Alias, der auf eine Gruppe verweisen kann. Gehen Sie bei der Auswahl

einer Telefonnummer genauso vor: Wählen Sie eine Nummer, die auf eine Gruppe oder auf eine Nummer verweisen kann, die dem Unternehmen gehört und nicht auf eine Einzelperson.

Nähere Informationen zu den Fragen, die Ihnen bei der Einbindung Ihres Core-Kontos in die AMS-Landezone für mehrere Konten gestellt werden, finden Sie unterAnhang: Liste der Überlegungen zum Onboarding in der Multi-Account-Landezone (MALZ).

Erstellen Sie eine IAM-Rolle für AMS, um auf Ihr Konto zuzugreifen

Nachdem Sie Ihr neues Konto erfolgreich erstellt haben AWS-Konto, besteht der nächste Schritt darin, AMS Zugriff auf das neue Konto zu gewähren, um Ihre AMS-Umgebung zu erstellen und zu konfigurieren und laufende Änderungs- und Bereitstellungsanforderungen zu erfüllen. Einzelheiten finden Sie unter Delegieren des AWS kontenübergreifenden Zugriffs mithilfe von IAM-Rollen.

AWS Identity and Access Management (IAM) ist ein Webservice, mit dem Sie den Zugriff Ihrer Benutzer auf AWS Ressourcen sicher kontrollieren können. Sie verwenden IAM, um zu kontrollieren, wer Ihre AWS Ressourcen nutzen kann (Authentifizierung) und welche Ressourcen sie auf welche Weise verwenden können (Autorisierung).

Aktivieren Sie den IAM-Zugriff auf die Konsole AWS

1. Melden Sie sich mit Ihren Root-Kontoanmeldeinformationen (der E-Mail-Adresse und dem Passwort, mit denen Sie Ihr Konto erstellt haben AWS-Konto) bei der AWS Management Console an. Melden Sie sich nicht mit anderen IAM-Anmeldeinformationen an. Die Startseite der AWS Management-Konsole wird geöffnet.
2. Öffnen Sie in der oberen Navigationsleiste das Dropdownmenü für Ihren Kontonamen und wählen Sie dann Konto aus. Die Startseite für die Abrechnung wird geöffnet.
3. Scrollen Sie nach unten zu IAM-Benutzer- und Rollenzugriff zu den Abrechnungsinformationen und wählen Sie Bearbeiten aus. Der Bereich „IAM-Zugriff aktivieren“ wird geöffnet.
4. Aktivieren Sie das Kontrollkästchen und wählen Sie dann Aktualisieren. Sie können nun IAM-Richtlinien verwenden, um zu steuern, auf welche Seiten ein Benutzer zugreifen kann.

Erstellen Sie eine IAM-Rolle, die AMS verwenden kann

1. Besorgen Sie sich eine JSON- oder YAML-Datei, die eine IAM-Rolle definiert, die AMS zur Erstellung Ihrer Infrastruktur verwenden kann. Entweder:

- Ihr AMS Cloud Architect (CA) stellt Ihnen eine JSON- oder YAML-Datei zur Verfügung.
- Sie können onboarding_iam_roles.zip herunterladen und eine der folgenden Optionen wählen:
  - onboarding_role_admin.json (kürzer, gewährt vollen Administratorzugriff)
  - onboarding_role_minimal.json (länger, gewährt die geringsten Rechte)

2. Melden Sie sich bei der an und öffnen Sie die Konsole unter /cloudformation. AWS Management ConsoleAWS CloudFormation https://console.aws.amazon.com

3. Wählen Sie Stapel erstellen aus. Sie sehen die folgende Seite.

4. Wählen Sie Vorlagendatei hochladen, laden Sie die JSON- oder YAML-Datei der IAM-Rolle hoch und wählen Sie dann Weiter aus. Sie sehen die folgende Seite.

5. Gehen Sie **`ams-onboarding-role`** in den Bereich Stackname und scrollen Sie weiter nach unten und wählen Sie Weiter, bis Sie diese Seite erreichen.

6. Stellen Sie sicher, dass das Kontrollkästchen aktiviert ist, und wählen Sie dann Stapel erstellen aus.
7. Stellen Sie sicher, dass der Stack erfolgreich erstellt wurde.

Sichern Sie das neue Konto mit Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer in AMS

Dieser Abschnitt wurde redigiert, da er sensible AMS-Sicherheitsinformationen enthält. Diese Informationen sind in der AMS-Konsolendokumentation verfügbar. Um auf AWS Artifact zuzugreifen, können Sie sich an Ihren CSDM wenden, um Anweisungen zu erhalten, oder gehen Sie zu Erste Schritte mit AWS Artifact.

Abonnieren AWS Marketplace Sie Trend Micro Endpoint Protection (EPS)

Trend Micro Endpoint Protection (EPS) ist die Hauptkomponente von AMS für die Betriebssystemsicherheit. Um EPS einzurichten, sobald die Erstellung der AMS-Landing landing zone

gestartet wurde, müssen Sie sich beim Shared Services Core-Konto anmelden und das Trend Micro Deep Security AMI abonnieren AWS Marketplace. Ihr CSDM oder CA berät Sie gerne.

1. Melden Sie sich mit der Rolle oder dem Benutzer, den Sie im Onboarding-Fragebogen für angegeben haben, bei der AWS Konsole an `CustomerEPSSubscriptionIAMRoleOrUser`
2. Navigieren Sie zum Bildschirm „Rolle wechseln“.

   - Konto: Von AMS bereitgestellt
   - Rolle: `EPSMarketplaceSubscriptionRole`
   - Anzeigename: EPS-Abonnementsitzung

   Gehen Sie wie folgt vor, nachdem Sie die Rolle in der Konsole gewechselt haben AWS Marketplace, um Trend Micro Deep Security in der zu abonnieren:

   1. Navigieren Sie zum AWS Marketplace.
   2. Wählen Sie unter AWS Marketplace Produkte suchen, die Ihren Anforderungen entsprechen, die folgenden Optionen aus:
      a. Anbieter: Trend Micro
      b. Preisplan: Bring Your Own License, falls Sie über eine Lizenz verfügen, oder By Hosts Billing
      c. Liefermethoden: Amazon Machine Image
   3. Klicken Sie im rechten Bereich auf Weiter abonnieren.
   4. Lesen Sie die Allgemeinen Geschäftsbedingungen und klicken Sie in der oberen rechten Ecke auf Nutzungsbedingungen akzeptieren.
   5. Melden Sie sich vom Konto ab und bestätigen Sie mit Ihrem Cloud Architect, dass der Vorgang abgeschlossen wurde.

An diesem Punkt stellt AMS die Infrastruktur in Ihrer AMS-Umgebung bereit, und die Umgebung ist einsatzbereit, sobald Sie Ihr Netzwerk angeschlossen und Ihren Zugriff eingerichtet haben.

Netzwerk einrichten

Netzwerke in der AMS-Umgebung werden hauptsächlich über das Netzwerk-Kernkonto verwaltet.

Es gibt mehrere Prozesse, die abgeschlossen werden müssen, um das Netzwerk für AWS Managed Services (AMS) einzurichten:

- Zuweisen von IP-Speicherplatz für Ihre AMS-Umgebung
- Einrichtung einer privaten Netzwerkkonnektivität für AWS
- Richten Sie Ihre Firewall so ein, dass AMS-Operationen möglich sind

Zuweisen von IP-Speicherplatz für Ihre AMS-Umgebung

Sie sollten bereits mit Ihrem Cloud-Architekten zusammengearbeitet haben, um den IP-Bereich für Ihre AMS-Umgebung zu definieren und gleichzeitig den Onboarding-Fragebogen auszufüllen.

Einrichtung einer privaten Netzwerkkonnektivität AWS zu AMS

AWS bietet private Konnektivität mithilfe von VPN-Konnektivität und Standleitungen über AWS Direct Connect. Private Konnektivität kann auf zwei Arten eingerichtet werden:

- Zentralisierte Edge-Konnektivität mit Transit Gateway
- Direct Connect and/or VPN mit dem Konto verbinden VPCs

Zentralisierte Edge-Konnektivität mit Transit Gateway

AWS Transit Gateway ist ein Service, mit dem Sie Ihre Amazon Virtual Private Clouds (VPCs) und Ihre lokalen Netzwerke mit einem einzigen Gateway verbinden können. Transit Gateway kann verwendet werden, um Ihre bestehende Edge-Konnektivität zu konsolidieren und sie über einen einzigen ingress/egress Punkt weiterzuleiten. Weitere Informationen finden Sie unter AWS Transit Gateway.

Direct Connect mit Transit Gateway verbinden

Sie können Ihre bestehende Direct Connect-Verbindung verwenden oder eine neue Direct Connect-Verbindung in einem Ihrer vorhandenen AWS Konten erstellen. Die Direct Connect-Verbindung sollte eine dedizierte oder gehostete Verbindung sein, die mit 1 Gbit/s oder mehr läuft.

> **Note**
>
> Informationen zur Verwendung von Direct Connect mit AWS Diensten finden Sie unter Erste Schritte an einem AWS Direct Connect-Standort.

Um eine bestehende dedizierte Direct Connect-Verbindung zu verwenden, dürfen auf der Verbindung nicht mehr als 3 virtuelle Transitschnittstellen erstellt werden. Dies liegt daran, dass AWS Direct Connect für dedizierte Verbindungen ein Limit von 4 virtuellen Transitschnittstellen pro Verbindung gilt.

Weitere Informationen zu Direct Connect-Limits finden Sie unter AWS Direct Connect-Limits.

Nachdem die Direct Connect-Verbindung verfügbar ist, passiert Folgendes:

1. AMS erstellt ein Direct Connect Gateway im Netzwerkkonto. Sie müssen eine ASN-Nummer (Autonomous System Number) für das Direct Connect Gateway und die Präfixe angeben, die vom Direct Connect Gateway angekündigt werden müssen. Diese ASN wird als Amazon ASN verwendet.
2. Sie erstellen eine neue Transit-VIF und legen den Besitzer der virtuellen Schnittstelle als Netzwerkkonto fest.
3. AMS meldet sich beim Netzwerkkonto an und akzeptiert den Verbindungsvorschlag.
4. AMS verknüpft das Transit-Gateway mit dem Direct Connect-Gateway.
5. AMS ordnet den Anhang der lokalen Transit Gateway Gateway-Routingtabelle zu.

> **Note**
>
> Die für das Direct Connect Gateway und das Transit Gateway bereitgestellte ASN muss unterschiedlich sein.

Um die Stabilität Ihrer Konnektivität zu erhöhen, empfiehlt es sich, mindestens zwei virtuelle Transitschnittstellen von verschiedenen AWS Direct Connect-Standorten an das Direct Connect-Gateway anzuschließen. Weitere Informationen finden Sie unter AWS Direct Connect Resilienzempfehlung.

VPN mit Transit Gateway verbinden

Um Ihrem Transit Gateway eine VPN-Verbindung anzuhängen, müssen Sie das Kunden-Gateway angeben. Weitere Informationen zu den Anforderungen für ein Kunden-Gateway finden Sie unter Anforderungen für Ihr Kunden-Gateway im Amazon VPC Network Administrator Guide.

Sie müssten die BGP-ASN-Nummer, die statische öffentliche IP-Adresse und die Routing-Option (statisch oder dynamisch) angeben. Sobald diese Details bereitgestellt wurden, erstellt AMS den VPN-Anhang und ordnet den Anhang der lokalen Transit Gateway Gateway-Routingtabelle zu.

Weitere Informationen zu Transit Gateway-Anhängen finden Sie unter Transit Gateway VPN-Anlagen.

Direct Connect and/or VPN mit dem Konto verbinden VPCs

Sie können Ihr VPCs Gerät auch direkt mit Direct Connect oder VPN verbinden. Der Datenverkehr fließt direkt von Direct Connect oder VPN, ohne das Transit-Gateway zu passieren. VPCs

> **Note**
>
> Die Shared Services-VPC und das Anwendungskonto VPCs müssen mit einer Direct Connect- oder VPN-Verbindung verbunden sein, um eine private Konnektivität herzustellen.

AWS Direct Connect Einrichtung in AMS

Richten Sie eine AWS Direct Connect für die Kommunikation zwischen Ihrer AMS-verwalteten VPC und Ihrem internen Netzwerk ein.

> **Note**
>
> Informationen zur Verwendung von Direct Connect mit AWS Diensten finden Sie unter Erste Schritte an einem AWS Direct Connect Standort.

Gehen Sie wie folgt vor, um eine Direct Connect-Verbindung einzurichten:

1. Bei Amazon Web Services registrieren (AWS)
2. Reichen Sie eine AWS Direct Connect Verbindungsanfrage ein.
3. Schließe den Cross Connect ab.
4. (Optional) Konfigurieren Sie redundante Verbindungen mit AWS Direct Connect.
5. Von AMS ausgeführt: Erstellen Sie eine virtuelle Schnittstelle.
6. Durchgeführt von AMS: Router-Konfiguration herunterladen.
7. Überprüfen Sie Ihre virtuelle Schnittstelle.

VPN-Einrichtung

Die grundlegenden Schritte, die AMS bei der Einrichtung eines VPN für die Kommunikation zwischen Ihrer von AMS verwalteten VPC und Ihrem internen Netzwerk befolgt.

> **Note**
>
> Allgemeine Informationen zur Verwendung eines VPN mit AWS Diensten finden Sie unter Was ist AWS Site-to-Site VPN und Ihr Kunden-Gateway (Ihre VPN-Appliance).

Wir folgen den AWS Abschnitten Erste Schritte und Testen der Site-to-Site VPN-Verbindung im VPN-Benutzerhandbuch, um die folgenden Schritte durchzuführen:

1. Erstellen Sie in Ihrer AWS VPC ein Kunden-Gateway.
2. Erstellen Sie in Ihrer AWS VPC ein Virtual Private Gateway.
3. Aktivieren Sie in Ihrer AWS VPC Route Propagation in Ihrer Routentabelle.
4. Aktualisieren Sie in Ihrer AWS VPC Ihre Sicherheitsgruppe, um eingehenden SSH-, RDP- und ICMP-Zugriff zu aktivieren.
5. Stellen Sie in Ihrem internen Netzwerk eine VPN-Verbindung her und konfigurieren Sie das Kunden-Gateway.
6. Testen Sie die VPN-Konnektivität zwischen der VPC und Ihrem internen Netzwerk.

Zugangsverwaltung einrichten

Die Nutzung eines von AWS Managed Services (AMS) verwalteten Netzwerks bedeutet, AMS Zugriff auf die Verwaltung Ihrer Cloud-Infrastruktur zu gewähren. Sie müssen eine Methode zur sicheren Verbindung zwischen Ihrem privaten Netzwerk und AMS konfigurieren. Das beginnt mit einigen Entscheidungen:

- AMS API/CLI - und Konsolenzugriff: Sie sollten die AMS-CLI installieren (Anweisungen finden Sie in diesem Dokument). Sie verwenden die AMS Change Management API, um Änderungsanfragen an AMS zu stellen, und die AMS SKMS API, um mehr über Ihre vom AMS verwalteten Ressourcen zu erfahren. Mithilfe der Active Directory Federation Services (AD FS) können Sie auf die AMS-Konsole zugreifen.
- Benutzerzugriff: Zwischen AD auf der AMS-Seite (über Directory Services) und dem Verzeichnis, das Sie zur Benutzerverwaltung verwenden, muss eine Konnektivität hergestellt werden.

- Instanzzugriff: Der Zugriff auf Instanzebene erfolgt über eine unidirektionale Vertrauenskonfiguration. Directory Services vertraut den Anmeldeinformationen in Ihrem CORP AD, sodass Stacks innerhalb der AMS-Seite die Anmeldung mit CORP-Anmeldeinformationen ermöglichen.

> **Note**
>
> Ihr Active Directory (AD), für das AMS die Vertrauensstellung einrichtet, muss das Verzeichnis sein, das die Konten von Benutzern enthält, die von Ihnen autorisiert wurden, um Zugriff auf Ihre AWS-Ressourcen zu erhalten.

Richten Sie ein Active Directory-Vertrauen ein

Um eine Vertrauensstellung einzurichten, benötigt AMS auf Ihrem Domänencontroller Lokale Richtlinien -> Sicherheitsoptionen -> Netzwerkzugriff: Bei Named Pipes, auf die anonym zugegriffen werden kann, müssen die Pipes Netlogon und lsarpc aufgeführt sein. Diese Pipes sind standardmäßig aufgeführt, werden aber manchmal aus Sicherheitsgründen entfernt. Sobald die Vertrauensstellung hergestellt ist, können sie wieder aus der Liste entfernt werden.

Conditional Forwarder konfigurieren

1. Verwenden Sie im AD DNS Manager -> Create a New Conditional Forwarder unter DNS-Domain: Verwenden Sie den Domainnamen, den AMS Ihnen zur Verfügung gestellt hat, z. B. a523434123.amazonaws.com (ändern Sie dies in den Domainnamen, den Sie im Onboarding-Fragebogen ausgewählt haben).
2. Unter IP-Adressen der Masterserver: Fügen Sie die vom AMS bereitgestellten IP-Adressen hinzu. Stellen Sie sicher, dass kein Verbindungsproblem vorliegt, indem Sie beide Adressen überprüfen.
3. Wählen Sie Diese bedingte Weiterleitung in Active Directory speichern und replizieren Sie wie folgt: Alle DNS-Server in dieser Domäne und drücken Sie OK.

AD-Trust konfigurieren

Folgen Sie diesem Microsoft AD-Artikel Erstellen Sie mithilfe der in diesem Abschnitt beschriebenen Einstellungen und Optionen eine unidirektionale, eingehende Gesamtvertrauensstellung für eine Seite der Vertrauensstellung.

1. Öffnen Sie das Dialogfeld Start -> Verwaltung -> Active Directory-Domänen und Vertrauensstellungen. Klicken Sie mit der rechten Maustaste auf den Domänenknoten der Domäne, für die Sie eine Vertrauensstellung einrichten möchten, und klicken Sie dann auf Eigenschaften -> Vertrauensstellungen -> Neue Vertrauensstellung, um den Assistenten für neue Vertrauensstellungen zu öffnen. Geben Sie den Domainnamen ein, den Sie von AMS für den Vertrauensnamen erhalten haben, und klicken Sie auf Weiter.
2. Wählen Sie unter Vertrauenstyp die entsprechende Vertrauensstufe aus (z. B. Forest Trust). Drücken Sie auf Weiter.
3. Wählen Sie unter Vertrauensrichtung die Option Einseitig: eingehend aus. Wählen Sie Weiter aus.
4. Wählen Sie unter Vertrauensseiten die Option Nur diese Domain aus. Wählen Sie Weiter aus.
5. Geben Sie unter Vertrauenspasswort ein Passwort Ihrer Wahl ein. Wählen Sie Weiter aus.
6. Drücken Sie für Trust Selections Completed und Trust Creation Complete einfach auf Weiter.
7. Wählen Sie unter Eingehendes Vertrauen bestätigen die Option Nein, eingehende Vertrauensstellung nicht bestätigen aus. Wählen Sie Weiter aus.
8. Wählen Sie unter Der Assistent für neue Vertrauensstellungen abgeschlossen die Option Fertig stellen und dann OK aus, um den Vorgang zu schließen.
9. Geben Sie das Vertrauenspasswort ein (kontaktieren Sie uns aus Sicherheitsgründen über die Telefonnummer Ihres CSDM). AMS schließt die Trust-Konfiguration ab.

Active Directory-Standorte und -Dienste

Um die Anmeldelatenz zu reduzieren, fügen Sie den VPC-CIDR-Bereich zu Ihren Active Directory-Standorten und -Diensten hinzu (Start -> Verwaltung -> Active Directory-Standorte und -Dienste). Fügen Sie den VPC-CIDR-Bereich zu einem Active Directory-Standort hinzu, der Domain-Controller enthält, die AWS am nächsten sind.

Geben Sie Ihrem CSDM den AD-Site-Namen der Site an, die Sie für AMS reserviert haben. AMS benennt die Standard-Site auf der AMS-Seite von AD so um, dass sie dem angegebenen Namen entspricht.

Routing von Active Directory-Namenssuffixes

Nachdem das unidirektionale Forest Trust eingerichtet wurde, führen Sie die folgenden Schritte aus, um das Suffix-Routing zu überprüfen:

1. Klicken Sie unter Start > Alle Programme > Verwaltung auf Active Directory-Domänen und Vertrauensstellungen.

   Die Konsole „Active Directory-Domänen und Vertrauensstellungen“ wird geöffnet.
2. Klicken Sie mit der rechten Maustaste auf Ihre Unternehmensdomäne und dann auf Eigenschaften

   Das Eigenschaftendialogfeld für diese Domain wird geöffnet.
3. Klicken Sie auf die Registerkarte Vertrauensstellungen.

   Die Seite Trusts wird geöffnet.
4. Klicken Sie auf den Amazon-Domainnamen und dann auf Eigenschaften.

   Die Eigenschaftenseite für den Amazon Domain Trust wird geöffnet.
5. Klicken Sie auf Name Suffix Routing und dann auf Aktualisieren.

   Stellen Sie sicher, dass keine Konflikte vorliegen, um sicherzustellen, dass die Service Principal Names (SPNs) über die Vertrauensstellung gelöst werden können.

Verbinden Sie Ihr Active Directory mit den AMS IAM-Rollen

Der Zweck der Verbindung Ihres Verzeichnisses mit den AMS IAM-Rollen besteht darin, Unternehmensbenutzern die Möglichkeit zu geben, ihre Unternehmensanmeldedaten für die Interaktion mit der AWS-Konsole und der AWS APIs und somit der AMS-Konsole und zu verwenden. APIs

Beispiel für einen Föderationsprozess

In diesem Beispiel werden Active Directory Federation Services (AD FS) verwendet. Es wird jedoch jede Technologie unterstützt, die AWS IAM Federation unterstützt. Weitere Informationen zum von AWS unterstützten IAM-Verbund finden Sie unter IAM-Partner und Identitätsanbieter und Verbund. Ihr CSDM hilft Ihnen bei diesem Prozess, der eine gemeinsame Anstrengung mit Ihrem AD-Team und AMS erfordert.

Ausführliche Informationen zur Integration von SAML für den API-Zugriff finden Sie in diesem AWS-Blog How to Implementation Federated API and CLI Access Using SAML 2.0 and AD FS.

Ein Beispiel für die Installation von AMS CLI und SAML finden Sie im Anhang: AD FS-Anspruchsregel und SAML-Einstellungen.

Konfiguration des Verbunds zur AMS-Konsole (MALZ)

Die in der folgenden Tabelle aufgeführten IAM-Rollen und der SAML-Identitätsanbieter (Trusted Entity) wurden als Teil der AMS-Infrastruktur bereitgestellt. Mit diesen Rollen können Sie die AMS-Kernkonten prüfen und einsehen.

Rolle	Berechtigungen
AWSManagedServicesReadOnlyRole	Ermöglicht es Ihnen, die AMS-Infrastruktur in den Kernkonten einzusehen.
AWSManagedServicesCaseRole	Ermöglicht es Ihnen, die Ressourcen in Ihrem neuen Anwendungskonto einzusehen und AMS-Vorfälle und Serviceanfragen einzureic hen.
AWSManagedServicesChangeManagementRo le	Ermöglicht es Ihnen, die AMS-Infrastruktur in den Kernkonten einzusehen, AWS-Support-Tickets einzureichen und einige anzufordern RFCs.

Die vollständige Liste der Rollen, die unter den verschiedenen Konten verfügbar sind, finden Sie unterIAM-Benutzerrolle in AMS .

Überprüfen Sie den Konsolenzugriff

Gehen Sie wie folgt vor, sobald Sie mit ADFS eingerichtet sind und über die AMS-URL verfügen, die Sie für die Authentifizierung verwenden möchten.

Mit einer Active Directory Federated Service (ADFS) -Konfiguration können Sie die folgenden Schritte ausführen:

1. Öffnen Sie ein Browserfenster und rufen Sie die Anmeldeseite auf, die Ihnen für Ihr Konto zur Verfügung gestellt wurde. Die IdpInitiatedSignOnADFS-Seite für Ihr Konto wird geöffnet.
2. Wählen Sie das Optionsfeld neben Auf einer der folgenden Websites anmelden aus. Die Auswahlliste für die Anmeldeseite wird aktiv.
3. Wählen Sie die Website signin.aws.amazon.com aus und klicken Sie auf Anmelden. Optionen für die Eingabe Ihrer Anmeldeinformationen werden geöffnet.

4. Geben Sie Ihre CORP-Anmeldeinformationen ein und klicken Sie auf Anmelden. Das AWS Management Console wird geöffnet.
5. Fügen Sie die URL der AMS-Konsole in die Adressleiste ein und drücken Sie die Eingabetaste. Die AMS-Konsole wird geöffnet.

API-Zugriff verifizieren

AMS verwendet die AWS-API mit einigen AMS-spezifischen Vorgängen, über die Sie in der AMS-API-Referenz nachlesen können.

AWS bietet mehrere SDKs , auf die Sie unter Tools für Amazon Web Services zugreifen können. Wenn Sie kein SDK verwenden möchten, können Sie direkte API-Aufrufe tätigen. Informationen zur Authentifizierung finden Sie unter Signieren von AWS-API-Anfragen. Wenn Sie kein SDK verwenden oder direkte HTTP-API-Anfragen stellen, können Sie AMS CLIs for Change Management (CM) und SKMS verwenden.

Installieren Sie das AMS CLIs

Die AWS-CLI ist eine Voraussetzung für die Verwendung von AMS CLIs (Change Management und SKMS).

1. Informationen zur Installation der AWS-CLI finden Sie unter Installation der AWS-Befehlszeilenschnittstelle und folgen Sie den entsprechenden Anweisungen. Beachten Sie, dass sich unten auf dieser Seite Anweisungen zur Verwendung verschiedener Installationsprogramme befinden: Linux, MS Windows, macOS, Virtual Environment, Bundled Installer (Linux, macOS oder Unix).
2. Führen Sie nach der Installation aws help aus, um die Installation zu überprüfen.
3. Sobald die AWS-CLI installiert ist, laden Sie zur Installation oder zum Upgrade der AMS-CLI die ZIP-Datei für AMS-Distributables herunter und entpacken Sie sie. Sie können über den Link Dokumentation im linken Navigationsbereich der AMS-Konsole auf die AMS-CLI-Distributionsdateien zugreifen oder Ihren Cloud Service Delivery Manager (CSDM) bitten, Ihnen die ZIP-Datei zu senden.
4. Öffnen Sie je nach Betriebssystem entweder das Verzeichnis Managed Cloud Distributables -> CLI -> Windows oder das Verzeichnis Managed Cloud Distributables -> CLI -> Linux/macOS und:
5. Führen Sie für Windows das entsprechende Installationsprogramm aus (diese Methode funktioniert nur auf Windows 32- oder 64-Bit-Systemen):

- 32 Bit: ManagedCloud API_x86.msi
- 64 Bit: ManagedCloud API_x64.msi

6. Führen Sie für Mac/Linux die Datei mit dem Namen MC_CLI.sh aus, indem Sie diesen Befehl ausführen: sh MC_CLI.sh. Beachten Sie, dass sich die Verzeichnisse amscm und amsskms und ihr Inhalt im selben Verzeichnis wie die Datei MC_CLI.sh befinden müssen.
7. Wenn Ihre Unternehmensanmeldedaten über den Verbund mit AWS (die AMS-Standardkonfiguration) verwendet werden, müssen Sie ein Tool zur Verwaltung von Anmeldeinformationen installieren, das auf Ihren Verbundservice zugreifen kann. Sie können beispielsweise diesen AWS-Sicherheitsblog How to Implementation Federated API and CLI Access Using SAML 2.0 and AD FS verwenden, um Hilfe bei der Konfiguration Ihrer Tools für die Verwaltung Ihrer Anmeldeinformationen zu erhalten.
8. Führen Sie nach der Installation die Befehle und Optionen aus `aws amscm help` und sehen Sie `aws amsskms help` sich diese an.

MALZ: Onboarding des Bewerbungskontos

Sie müssen über eine AWS Managed Services (AMS) -Umgebung mit mehreren Konten und Kernkonten verfügen, bevor Sie ein neues Anwendungskonto beantragen können. Hier sind die Schritte, die Sie nach der Einrichtung Ihrer Umgebung ausführen müssen.

Themen

- Beantragung eines neuen Anwendungskontos
- Einrichtung von Active Directory für den Verbundzugriff auf AMS IAM-Rollen
- Einrichtung des Netzwerks mit dem neuen Anwendungskonto
- Zusätzliches Konto VPCs im Anwendungskonto einrichten

Bei Fragen zum Onboarding wenden Sie sich an Ihren Cloud Service Delivery Manager (CSDM). Siehe auch Anwendungskonten: AMS-verwaltet, Dev-Modus, Kundenverwaltet. Allgemeine Informationen zu Modi finden Sie unter AMS-Modi. Servicemanagement in AWS Managed Services

Informationen zu den verschiedenen Modi von Anwendungskonten finden Sie unter Anwendungskonten: AMS-verwaltet, Dev-Modus, Kundenverwaltet. Allgemeine Informationen zu Modi finden Sie unter AMS-Modi.

Beantragung eines neuen Anwendungskontos

Sie müssen über eine AWS Managed Services (AMS) -Umgebung mit mehreren Konten und Kernkonten verfügen, bevor Sie ein neues Anwendungskonto beantragen können. Informationen zur Einrichtung einer Umgebung mit mehreren Konten und Kernkonten finden Sie unter. MALZ: Onboarding von Kernkonten

Sie können einen der folgenden Amazon VPC-Typen für die erste VPC im Anwendungskonto wählen:

- Privat: An diese VPC ist kein Internet-Gateway angeschlossen. Dies ist für private Anwendungen geeignet, die keinen Internetzugang to/from benötigen.
- Öffentlich: An diese VPC ist ein Internet-Gateway angeschlossen und es gibt öffentliche und private Subnetze. Dies ist für öffentliche Anwendungen geeignet, die Zugriff auf to/from das Internet benötigen.

Sie können ein neues Anwendungskonto beantragen, indem Sie einen RFC Deployment | Managed landing zone | Management Account | Create Application Account (with VPC) (ct-1zdasmc2ewzrs) einreichen und die folgenden Werte im RFC angeben:

- Kontoname: Ein benutzerdefinierter Name für das Konto. Beachten Sie, dass der Kontoname eine maximale Länge von 50 Zeichen hat.
- Konto-E-Mail: Die E-Mail-Adresse der Verteilerliste für das Konto. Diese E-Mail-ID wird für die Erstellung des AWS-Kontos verwendet.
- Support-Stufe: Die AWS-Supportstufe, Premium oder Plus.
- VPC-Name: Ein Name für die VPC.
- Anzahl der Availability Zones (AZs): 2 oder 3.
- VPC CIDR: Der CIDR-Block für die VPC.
- Routentyp: Dies kann entweder oder sein. `routable` `isolated` `Routable`bedeutet, dass die der Transit Gateway (TGW) -Anwendungsroutentabelle VPCs zugeordnete Anwendung eine Verbindung zu dieser VPC herstellen kann. `Isolated`bedeutet, dass die der TGW-Anwendungsroutentabelle VPCs zugeordnete Anwendung keine Verbindung zu dieser VPC herstellen kann. Der Standardwert ist `routable`.
- Transit Gateway Gateway-Anwendungsroutentabelle: Die Transit Gateway Gateway-Routentabelle, der das Anwendungskonto VPC zugeordnet werden muss. Wenn kein Wert angegeben wird, `defaultAppRouteDomain` wird der Standard verwendet, was bedeutet, dass dieses Konto mit allen anderen Konten in derselben Routentabelle kommunizieren kann.

- PublicSubnetAZ *<1-3>* CIDRCIDR für das öffentliche Subnetz in AZ 1: Das CIDR für das öffentliche Subnetz in Availability Zone 1.
- PrivateSubnet*<1-10>*AZ *<I-3>* CIDRCIDR für das öffentliche Subnetz in AZ 1: Das CIDR für das öffentliche Subnetz in Availability Zone 1.

Zu diesem Zeitpunkt stellt AMS ein neues Anwendungskonto in Ihrem AMS-Verwaltungskonto mit der angegebenen VPC-Konfiguration bereit.

Einrichtung von Active Directory für den Verbundzugriff auf AMS IAM-Rollen

Verbinden Sie Ihr Verzeichnis mit den AMS IAM-Rollen, damit Unternehmensbenutzer ihre Unternehmensanmeldedaten für die Interaktion mit der AWS-Konsole und AWS sowie der APIs AMS-Konsole und AMS verwenden können. APIs

Beispiel für einen Föderationsprozess

In diesem Beispiel werden Active Directory Federation Services (ADFS) verwendet. Es wird jedoch jede Technologie unterstützt, die AWS IAM Federation unterstützt. Weitere Informationen zum von AWS unterstützten IAM-Verbund finden Sie unter IAM-Partner und Identitätsanbieter und Verbund. Ihr CSDM hilft Ihnen bei diesem Prozess, der eine gemeinsame Anstrengung mit Ihrem AD-Team und AMS erfordert.

Ausführliche Informationen zur Integration von SAML für den API-Zugriff finden Sie in diesem AWS-Blog How to Implementation Federated API and CLI Access Using SAML 2.0 and AD FS.

Ein Beispiel für die Installation von AMS CLI und SAML finden Sie im Anhang: AD FS-Beanspruchungsregel und SAML-Einstellungen im AMS-Benutzerhandbuch.

Konfiguration des Verbunds zur AMS-Konsole

Die in der folgenden Tabelle aufgeführten IAM-Rollen und der SAML-Identitätsanbieter (Trusted Entity) werden in Ihrem neuen Anwendungskonto bereitgestellt. Mit diesen Rollen können Sie auf das neue Anwendungskonto und die neue Anwendungsdatei zugreifen RFCs, in S3-Buckets schreiben und andere Aktionen ausführen.

Rolle	Permissions (Berechtigungen)
AWSManagedServicesReadOnlyRole	Ermöglicht es Ihnen, die Ressourcen in Ihrem neuen Anwendungskonto einzusehen.

Rolle	Permissions (Berechtigungen)
AWSManagedServicesCaseRole	Ermöglicht es Ihnen, die Ressourcen in Ihrem neuen Anwendungskonto einzusehen und AWS-Support-Tickets einzureichen.
AWSManagedServicesChangeManagementRole	Ermöglicht es Ihnen, die AMS-Infrastruktur in den Anwendungskonten einzusehen, AWS-Support-Tickets zu RFCs archivieren, in S3-Buckets zu schreiben, Secrets Manager zu verwalten und reservierte Amazon Elastic Compute Cloud (Amazon EC2) -Instances zu verwalten.
AWSManagedServicesSecurityOpsRole	Ermöglicht es Ihnen, die AMS-Infrastruktur in den Anwendungskonten einzusehen, Secrets Manager zu verwalten, Web Application Firewall-Regeln zu verwalten, Zertifikate zu verwalten und AWS-Support-Tickets einzureichen.
AWSManagedServicesAdminRole	Ermöglicht es Ihnen, die AMS-Infrastruktur in den Anwendungskonten einzusehen, Marketplace-Abonnements zu verwalten, Secrets Manager zu verwalten, Web Application Firewall-Regeln zu verwalten, Zertifikate zu verwalten, reservierte EC2 Amazon-Instances zu erstellen RFCs, zu verwalten, in S3-Buckets zu schreiben, AWS-Support-Tickets einzureichen und AWS Artifacts-Verträge zu verwalten.

Einreichung der Föderationsanfrage an AMS

Wenn dies Ihr erstes Konto ist, arbeiten Sie mit Ihren CSDM (s) and/or Cloud Architect (s) zusammen, um die Metadaten-XML-Datei für Ihren Identitätsanbieter bereitzustellen.

Wenn Sie ein zusätzliches Konto oder einen Identitätsanbieter einrichten und Zugriff entweder auf das Verwaltungskonto oder das gewünschte Anwendungskonto haben, gehen Sie wie folgt vor.

1. Erstellen Sie eine Serviceanfrage von der AMS-Konsole aus.

   > **Note**
   >
   > - Wenn Sie einen Identitätsanbieter für ein Anwendungskonto erstellen, reichen Sie diese Anfrage entweder vom Anwendungskonto selbst oder vom Verwaltungskonto aus ein.
   > - Wenn Sie einen Identitätsanbieter für ein AMS-Hauptkonto erstellen, reichen Sie diese Anfrage vom Verwaltungskonto aus ein.
   > - Wenn Sie einen Identitätsanbieter für das Verwaltungskonto erstellen, reichen Sie diese Anfrage über das Verwaltungskonto ein oder wenden Sie sich an Ihren CSDM, um Unterstützung zu erhalten.

   Geben Sie in der Serviceanfrage die Details an, die zum Hinzufügen des Identitätsanbieters erforderlich sind:

   - AccountId des Kontos, in dem der neue Identitätsanbieter erstellt wird.
   - Der Name des gewünschten Identitätsanbieters, falls nicht angegeben, ist der Standardwert customer-saml. In der Regel muss dieser Name den Einstellungen entsprechen, die in Ihrem Federation Provider konfiguriert sind.
   - Geben Sie bei vorhandenen Konten an, ob der neue Identitätsanbieter an alle vorhandenen Konsolenrollen weitergegeben werden soll, oder geben Sie eine Liste der Rollen an, die dem neuen Identitätsanbieter vertrauen sollten.
   - Hängen Sie die von Ihrem Federation Agent exportierte Metadaten-XML-Datei als Dateianhang an die Serviceanfrage an.
2. Erstellen Sie mit demselben Konto, in dem Sie die Serviceanfrage erstellt haben, einen neuen RFC mit der CT-ID ct-1e1xtak34nx76 (Management | Other | Other | Create) mit den folgenden Informationen.

   - <Name>Titel: „Integrierter SAML-IDP für Konto < >“. AccountId
   - AccountId des Kontos, in dem der Identitätsanbieter erstellt wird.
   - Name des Identitätsanbieters.

- Für bestehende Konten: Ob der Identitätsanbieter auf alle vorhandenen Konsolenrollen übertragen werden soll, oder die Liste der Rollen, die dem neuen Identitätsanbieter vertrauen sollen.
- Fall-ID der in Schritt 1 erstellten Serviceanfrage, an die die XML-Metadatendatei angehängt ist.

Überprüfen Sie den Konsolenzugriff

Nachdem Sie AD FS eingerichtet haben und über die AMS-URL verfügen, die Sie für die Authentifizierung verwenden möchten, können Sie das folgende Verfahren ausführen.

Mit einer Active Directory Federated Service (AD FS) -Konfiguration können Sie die folgenden Schritte ausführen:

1. Öffnen Sie ein Browserfenster und rufen Sie die Anmeldeseite auf, die Ihnen für Ihr Konto zur Verfügung gestellt wurde. Die AD IdpInitiatedSignOn FS-Seite für Ihr Konto wird geöffnet.
2. Wählen Sie das Optionsfeld neben Auf einer der folgenden Websites anmelden aus. Die Liste der Anmeldeseiten wird aktiv.
3. Wählen Sie die Website signin.aws.amazon.com und dann Anmelden aus. Optionen für die Eingabe Ihrer Anmeldeinformationen werden geöffnet.
4. Geben Sie Ihre CORP-Anmeldeinformationen ein und wählen Sie Anmelden. Die AWS-Managementkonsole wird geöffnet.
5. Fügen Sie die URL der AMS-Konsole in die Adressleiste ein und drücken Sie die Eingabetaste. Die AMS-Konsole wird geöffnet.

API-Zugriff verifizieren

AMS verwendet die AWS-API mit einigen AMS-spezifischen Vorgängen, über die Sie in der AMS-API-Referenz nachlesen können.

AWS bietet mehrere SDKs , auf die Sie unter Tools für Amazon Web Services zugreifen können. Wenn Sie kein SDK verwenden möchten, können Sie direkte API-Aufrufe tätigen. Informationen zur Authentifizierung finden Sie unter Signieren von AWS-API-Anfragen. . Wenn Sie kein SDK verwenden oder direkte HTTP-API-Anfragen stellen, können Sie AMS CLIs für Change Management (CM) und SKMS verwenden.

Einrichtung des Netzwerks mit dem neuen Anwendungskonto

Die Einrichtung des Netzwerks für das Anwendungskonto umfasst die Konfiguration von Firewallregeln und möglicherweise die Einrichtung zusätzlicher Transit Gateway (TGW) - Routentabellen.

Deine Firewall einrichten

Um die in Ihrer AMS-Umgebung bereitgestellten Anwendungen verwenden zu können, müssen Sie einige Firewallregeln erstellen. Sie benötigen diese Regeln nicht, um auf Ihre Instances zuzugreifen. Sie können durch die Bastionen zu Ihren Instances springen.

Firewall-Regeln für den Anwendungszugriff

Sie müssen die folgenden Ports für den Datenverkehr durch Ihre Firewall öffnen:

- Von Ihrem lokalen Netzwerk bis hin zu Ihrer neuen Anwendungs-VPC, sowohl CIDRs in Eingangs- als auch in Ausgangsrichtung.
- Von Ihrer neuen Anwendungs-VPC CIDRs zu Ihrem lokalen Netzwerk, sowohl in der Eingangs- als auch in der Ausgangsrichtung (falls Ihre Cloud-Anwendungen Ihre lokalen Anwendungen erreichen müssen).

Port	Protocol (Protokoll)	Service	Von/Bis	Nach/Von
80	TCP	HTTP-Webzugriff	Netzwerk vor Ort	AMS-Anwendung VPC
443	TCP	HTTPS-Webzugriff	Netzwerk vor Ort	AMS-Anwendung VPC

Einrichtung zusätzlicher Routentabellen für Transit-Gateway-Anwendungen

Das Netzwerk von AWS Managed Services (AMS) ist flexibel und unterstützt eine Vielzahl von Netzwerkanwendungsfällen.

- Kommunikation zwischen Anwendungen VPCs im selben Konto.
- Kommunikation zwischen Anwendungen VPCs in verschiedenen Konten.

- Isolierung zwischen Anwendungen VPCs in verschiedenen Konten.
- Isolierung zwischen Anwendungen VPCs in denselben Konten.

Wenn Sie unique/special Netzwerkanforderungen haben, wenden Sie sich an Ihren AMS Cloud Architect, der einen Plan für die Erfüllung Ihrer Anforderungen durch die AMS-Netzwerkarchitektur ausarbeitet.

Basierend auf der Netzwerkentscheidung für das Anwendungskonto können Sie mehrere Transit Gateway (TGW) -Anwendungsroutentabellen erstellen VPCs, indem Sie einen RFC für Bereitstellung | Verwaltete landing zone | Netzwerkkonto | Transit-Gateway-Routentabelle erstellen (ct-3dscwaeyi6cup) einreichen.

Für den Änderungstyp müssen Sie `TransitGatewayRouteTableName` (einen aussagekräftigen Namen für die TGW-Routentabelle), und angeben. `TransitGatewayId` `TGWRouteTableType`

> **Note**
>
> Wenn createCustomRoute Domain für ausgewählt ist TGWRouteTableType, ist die erstellte Routentabelle leer. Sie müssen einen RFC mit dem Änderungstyp Bereitstellung | Verwaltete landing zone | Netzwerkkonto | Statische Route hinzufügen (ct-3r2ckznmt0a59) einreichen.

Zusätzliches Konto VPCs im Anwendungskonto einrichten

Sie können eine zusätzliche Anwendungskonto-VPC anfordern, indem Sie einen RFC Deployment | Managed landing zone | Application Account | Create VPC (ct-1j3503fres5a5) einreichen.

Dies funktioniert genauso wie die Konfiguration einer VPC für ein neues Anwendungskonto. Details hierzu finden Sie unter Beantragung eines neuen Anwendungskontos.

Anhang: Liste der Überlegungen zum Onboarding in der Multi-Account-Landezone (MALZ)

Es gibt eine Reihe wichtiger Überlegungen, die Sie bei der Planung Ihrer AMS-Landezone für mehrere Konten berücksichtigen müssen. Durch Ihre Auswahl erhält AMS die Informationen, die es benötigt, um zu bestimmen, welche Infrastrukturkomponenten Sie benötigen. Ihr Cloud Architect (CA) stellt Ihnen einen Fragebogen zur Verfügung, der Sie bei dieser Arbeit unterstützt.

Themen

- Konfiguration eines AMS-Landingzone-Kontos mit mehreren Konten
- Warnmeldungen zur Überwachung der AMS-Landezone mit mehreren Konten
- Netzwerkkonfiguration
- Active Directory-Konfiguration
- Trend Micro Endpoint Protection (EPS)
- Zugriff: Bastions, SSH und RDP
- Verbund

> **Note**
>
> Weitere Informationen zu Instance-Typen finden Sie unter EC2 Amazon-Instance-Typen.
> Weitere Informationen zu Datenbank-Instance-Typen finden Sie unter Amazon RDS-Instance-Typen.
> Wenn Sie Direct Connect benötigen, finden Sie im AMS Single-Account landing zone Onboarding Guide Informationen zum Erstellen einer Direct Connect-Verbindung.

Sie erhalten von Ihrem Cloud Service Delivery Manager (CSDM) einen Onboarding-Fragebogen mit Fragen zu den gewünschten Konfigurationseinstellungen für Ihr Konto. Arbeiten Sie mit Ihrem CSDM zusammen, um den Fragebogen auszufüllen, bevor Sie fortfahren.

Konfiguration eines AMS-Landingzone-Kontos mit mehreren Konten

- Neue Konto-ID

  Die AWS-Konto ID, die Sie für die AMS-Landingzone mit mehreren Konten erstellt haben. Sollte nicht Teil einer AWS Organisation sein.

- Serviceregion

  Die primäre Region, in der die AMS-Landezonenumgebung mit mehreren Konten bereitgestellt wird.

- Die E-Mails des Hauptkontos für Benachrichtigungen. (Diese sollten sich alle in derselben Domain befinden). Geben Sie jeweils eine E-Mail-Adresse an:
  - Shared Services-Konto

- Netzwerkkonto
- Konto protokollieren
- Sicherheitskonto

- Ihr Servicetyp, Premium oder Plus

  Dies bestimmt die Service Level Agreements (SLAs) zur Lösung von Problemen in Ihrer Umgebung

Warnmeldungen zur Überwachung der AMS-Landezone mit mehreren Konten

AMS bietet Ihnen die Möglichkeit, bei bestimmten Überwachungswarnungen direkt benachrichtigt zu werden (anstatt AMS-Servicemeldungen zu erhalten). Um sich dafür zu registrieren, stellen Sie sicher, dass Ihr Cloud Architect (CA) oder Cloud Service Delivery Manager (CSDM) die folgenden Informationen erhält:

E-Mail mit direkten Benachrichtigungen: Dies sind die E-Mail-Adressen, an die AMS bestimmte ressourcenbasierte Benachrichtigungen senden soll. Einzelheiten dazu, welche Benachrichtigungen direkt per E-Mail gesendet werden, finden Sie unter Warnmeldungen aus der Basisüberwachung in AMS im AMS-Benutzerhandbuch für Fortgeschrittene. Weitere Informationen zur AMS-Überwachung finden Sie unter Monitoring Management im AMS-Benutzerhandbuch für Single-Account-Landing Zone.

Netzwerkkonfiguration

- ASN-Nummer für Transit Gateway

  Dies ist die Autonomous System Number (ASN) für die AWS-Seite einer Border Gateway Protocol (BGP) -Sitzung. Sie muss eindeutig sein und darf nicht dieselbe sein, die für Ihre Direct Connect- oder VPN-Verbindung verwendet wurde. Der Bereich reicht von 64512 bis 65534 (einschließlich) für 16-Bit. ASNs

- Die VPC-CIDR-Bereiche Ihrer AMS-Landezoneninfrastruktur mit mehreren Konten.

  Diese CIDR-Bereiche dürfen sich nicht mit Ihrem lokalen Netzwerk überschneiden

  Sie können entweder einen /22-CIDR-Bereich angeben oder jeden VPC-CIDR einzeln bereitstellen. Beachten Sie, dass nur diese CIDR-Bereiche zulässig sind:

  - 10.0.0.0 - 10.255.255.255 (10/8 Präfix)

  - 172.16.0.0 - 172.31.255.255 (172.16/12 Präfix)
  - 192.168.0.0 - 192.168.255.255 (192.168/16 Präfix)

  Beachten Sie, dass der IP-Bereich 198.18.0.0/15 nicht verwendet werden darf (er ist vom AWS Directory Service reserviert).

  - Core Infrastructure VPC CIDR-Bereich (/22-Bereich empfohlen)
  - Netzwerk-VPC CIDR-Bereich (/24-Bereich empfohlen)
  - Shared Services VPC CIDR-Bereich (Bereich /23 empfohlen)
  - DMZ VPC CIDR-Bereich (Bereich /25 empfohlen)
- VPN ECMP (aktivieren oder deaktivieren)

  Bei VPN ECMP support (VPN-ECMP-Unterstützung) wählen Sie enable (Aktivieren) aus, wenn ECMP-Routing (Equal Cost Multipath) zwischen VPN-Verbindungen unterstützt werden soll. Wenn Verbindungen dasselbe ankündigen CIDRs, wird der Verkehr gleichmäßig auf sie verteilt.

Liste der Netzwerkzugriffskontrolle (NACL)

Eine Network Access Control List (NACL) ist eine optionale Sicherheitsebene für Ihre VPC, die als Firewall zur Steuerung des Datenverkehrs in und aus einem oder mehreren Subnetzen fungiert. Sie können ein Netzwerk ACLs mit Regeln einrichten, die Ihren Sicherheitsgruppen ähneln, um Ihrer VPC eine zusätzliche Sicherheitsebene hinzuzufügen. Weitere Informationen zu den Unterschieden zwischen Sicherheitsgruppen und Netzwerk ACLs finden Sie unter Vergleich von Sicherheitsgruppen und Netzwerk ACLs.

In der AMS-Landezone mit mehreren Konten NACLs ist der Einsatz von jedoch auf folgenden Umfang beschränkt, damit AMS die Infrastruktur effektiv verwalten und überwachen kann:

- NACLs werden in den Hauptkonten der landing zone mit mehreren Konten nicht unterstützt: Management, Networking, Shared-Services, Logging und Security.
- NACLs werden in Landingzone-Anwendungskonten mit mehreren Konten unterstützt, sofern sie nur als Ablehnungsliste verwendet werden. Darüber hinaus muss für sie die Option „Alle zulassen“ konfiguriert sein, um die Überwachung und Verwaltung von AMS sicherzustellen.

In großen Umgebungen mit mehreren Konten können Sie auch Funktionen wie zentralisierte Ausgangsfirewalls zur Steuerung des ausgehenden Datenverkehrs und/oder AWS Transit

Gateway Gateway-Routingtabellen in der AMS-Landezone für mehrere Konten nutzen, um den Netzwerkverkehr zwischen den einzelnen Konten zu trennen. VPCs

Active Directory-Konfiguration

Domänen-FQDN für AMS-verwaltetes Active Directory

Trend Micro Endpoint Protection (EPS)

- Instanzgrößen für Ihre EC2 Instances und Auto Scaling Scaling-Gruppen

  Trend Micro Endpoint Protection (EPS) ist die Hauptkomponente von AMS für die Betriebssystemsicherheit. Das System besteht aus Deep Security Manager (DSM) EC2 -Instanzen, EC2 Relay-Instances und einem Agenten, der auf der gesamten AMS-Datenebene und Ihren EC2 Instanzen präsent ist.

  - Relay-Instance-Typ (von AMS wird mindestens m5.large unterstützt)
  - Größe der DB-Instance (200 GB empfohlen)
  - RDS-Instance-Typ (nur db.m5.large oder db.m5.xlarge zulässig)
- DSM-Lizenztyp (Marketplace oder BYOL)

  Wenn Sie bereits über eine Lizenz verfügen, wählen Sie BYOL (Bring Your Own License). AMS wird sich mit Ihnen in Verbindung setzen, um die erforderlichen Informationen zur Lizenz zu erhalten.
- AWS Amazon-Ressourcenname (ARN) für IAM-Benutzer oder Rolle für das Trend Micro Deep Security-Abonnement (Rollen-ARN: arn:aws:iam: ::role/) *ACCOUNT_ID ROLE_NAME*

  Geben Sie uns eine IAM-Rolle, einen ARN oder einen IAM-Benutzer-ARN von einem Ihrer vorhandenen, AWS-Konten auf den Sie Zugriff haben. AMS erstellt eine IAM-Rolle in Ihrer AMS-Landingzone Shared Services-Konto mit mehreren Konten und fügt die Rolle oder den Benutzer hinzu, die als vertrauenswürdig einer IAM-Rolle in Shared Services zugewiesen wurden, sodass Sie die Rolle übernehmen können, um Trend Micro Deep Security in zu abonnieren. AWS Marketplace

Zugriff: Bastions, SSH und RDP

- SSH-Bastion-Einstellungen

AMS stellt SSH-Bastionen in Ihrem Shared Services-Konto bereit, um auf Hosts in der AMS-Umgebung zuzugreifen. Um als SSH-Benutzer auf das AMS-Netzwerk zuzugreifen, müssen Sie SSH Bastions als Einstiegspunkt verwenden. Der Netzwerkpfad stammt aus dem lokalen Netzwerk, führt DX/VPN zum Transit Gateway (TGW) und wird dann an die Shared Services-VPC weitergeleitet. Sobald Sie auf die Bastion zugreifen können, können Sie zu anderen Hosts in Ihrer AMS-Umgebung springen, vorausgesetzt, die richtige Zugriffsanfrage wurde genehmigt.

- Anzahl der gewünschten Instanzen (2 empfohlen)
- Maximale Anzahl Instanzen (4 empfohlen)
- Minimale Anzahl von Instanzen (2 empfohlen)
- Instanztyp (m5.large empfohlen)
- Ingress CIDRs: IP-Adressbereiche, von denen aus Benutzer in Ihrem Netzwerk auf SSH Bastions zugreifen (IP-Bereich 1, IP-Bereich 2, IP-Bereich 3 usw.)

- RDP Bastion-Einstellungen

  AMS stellt optional RDP-Bastionen in Ihrem Shared Services-Konto bereit, um auf Hosts in der AMS-Umgebung zuzugreifen. Um als RDP-Benutzer auf das AMS-Netzwerk zuzugreifen, müssen Sie RDP Bastions als Einstiegspunkt verwenden. Der Netzwerkpfad stammt aus dem lokalen Netzwerk, führt zum TGW und wird dann DX/VPN an Shared Services VPC weitergeleitet. Sobald Sie auf die Bastion zugreifen können, können Sie zu anderen Hosts in der AMS-Umgebung springen, vorausgesetzt, die richtige Zugriffsanfrage wurde genehmigt.

  - Instanztyp (t3.medium empfohlen)
  - Gewünschte Mindestanzahl an Sitzungen (2 empfohlen)
  - Gewünschte maximale Anzahl an Sitzungen (10 empfohlen)

- RDP-Bastion-Konfigurationstyp, Shared Standard oder Shared HA (Standard ist Shared Standard)

  SecureStandard = Ein Benutzer erhält eine Bastion und nur ein Benutzer kann sich mit der Bastion verbinden.

  SecureHA = Ein Benutzer erhält zwei Bastionen in zwei verschiedenen AZs, mit denen er sich verbinden kann, und nur ein Benutzer kann sich mit der Bastion verbinden.

  SharedStandard = Ein Benutzer erhält eine Bastion, mit der er sich verbinden kann, und zwei Benutzer können sich gleichzeitig mit derselben Bastion verbinden.

shareDHA = Ein Benutzer erhält zwei Bastionen in zwei verschiedenen AZs, mit denen er sich verbinden kann, und zwei Benutzer können sich gleichzeitig mit derselben Bastion verbinden.

Verbund

Name des Identitätsanbieters (IDP)

Standard-Einstellung: `customer-saml`

Onboarding der AMS Single-Account-Landingzone (SALZ)

Der Onboarding-Prozess von AMS SALZ

Um AMS-Konten mit Einzelkonto landing zone (SALZ) zu integrieren, müssen Sie die folgenden Schritte ausführen:

1. Erstellen Sie ein neues AWS-Konto, das AMS als Netzwerkkonto für das Hosten der Firewall konfiguriert. Erstellen Sie das neue Konto in Ihrer AWS-Organisation, falls Sie eines haben. AMS folgt dem Verfahren zur Erstellung eines normalen AMS-Kontos, sodass alle erforderlichen Informationen gesammelt werden müssen (z. B. CIDR, EPS-Lizenzen und Benutzer). Hinweis: Eine CIDR-Zuweisung von /24 ist gut.
2. Geben Sie an, ob Sie die Internet-Gateways (IGWs) aus den Konten für ausgehenden Datenverkehr entfernen möchten oder nicht.
3. Ermitteln Sie Ihre zugelassenen Domänen. AMS ermöglicht die Zielfilterung, indem es eine Liste zugelassener Domänen verwaltet. Die Liste kann später geändert werden.
4. Bestätigen Sie die Instance-Größe, die Sie verwenden möchten, auf der Grundlage Ihres erwarteten Durchsatzes. Standardmäßig wird die Instanz in einer m4.xlarge-Instance erstellt, bei der wir festgestellt haben, dass der Firewall-Durchsatz 350 Mbit/s beträgt. AMS kann die Größe auf eine C4.8xLarge-Instance erhöhen, bei der der erwartete Durchsatz 1,25 Gbit/s beträgt.
5. Richten Sie ein Netzwerk zwischen AMS und Ihrem privaten Netzwerk ein. Dazu müssen Sie folgende Aufgaben ausführen:
    a. Ordnen Sie IP-Speicherplatz zu
    b. Stellen Sie eine private Netzwerkkonnektivität zu AWS her
    c. Richten Sie Ihre Firewall ein
    d. Richten Sie die Zugriffsverwaltung ein
    e. Planen Sie Backups
6. Gewähren Sie AMS Zugriff auf das erstellte Konto.
7. Stellen Sie sicher, dass der AMS-Dienst ordnungsgemäß funktioniert.

AMS kann den Kontoausbau (Onboarding) Ihres Kontos innerhalb von 2 Wochen (10 Werktagen) ab dem Datum der ursprünglichen Anfrage durchführen. Jede Folgeaktivität kann mithilfe von AMS Planned Event Management (PEM) durchgeführt werden.

Note

- USA Ost (Virginia)
- USA West (Nordkalifornien)
- USA West (Oregon)
- USA Ost (Ohio)
- Kanada (Zentral)
- Südamerika (São Paulo)
- EU (Irland)
- EU (Frankfurt)
- EU (London)
- EU West (Paris)
- Asien-Pazifik (Mumbai)
- Asia Pacific (Seoul)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Tokio)

Neue Regionen werden häufig hinzugefügt. Die aktuelle Liste finden Sie unter AWS-Regionen und Availability Zones.

SALZ Netzwerkarchitektur

Das folgende Diagramm zeigt das VPC-Netzwerklayout von AWS Managed Services (AMS) für Einzelkonten (SALZ) und ist ein Beispiel für die Einrichtung mit hoher Verfügbarkeit.

AMS konfiguriert alle Netzwerkaspekte für Sie auf der Grundlage unserer Standardvorlagen und Ihrer ausgewählten Optionen, die Sie beim Onboarding ausgewählt haben. Ein standardmäßiges AWS-Netzwerkdesign wird auf Ihr AWS-Konto angewendet, und eine virtuelle private Cloud (VPC) wird für Sie erstellt und entweder über VPN oder Direct Connect mit AMS verbunden. Erfahren

Sie mehr über Direct Connect bei AWS Direct Connect. Zum Standard VPCs gehören die DMZ, Shared Services und ein Anwendungssubnetz. Während des Onboarding-Prozesses VPCs können zusätzliche Informationen angefordert und erstellt werden, die Ihren Anforderungen entsprechen (z. B. Kundenabteilungen, Partner). Nach dem Onboarding erhalten Sie ein Netzwerkdiagramm, ein Umgebungsdokument, in dem erklärt wird, wie Ihr Netzwerk eingerichtet wurde.

> **Note**
>
> Informationen zu den standardmäßigen Service-Limits und Einschränkungen für alle aktiven Services finden Sie in der Dokumentation zu AWS-Servicelimits.

Unser Netzwerkdesign basiert auf dem „Prinzip der geringsten Rechte“ von Amazon. Um dies zu erreichen, leiten wir den gesamten eingehenden und ausgehenden Datenverkehr über Gateways weiter, mit Ausnahme des Datenverkehrs, der von einem vertrauenswürdigen Netzwerk stammt. Das einzige vertrauenswürdige Netzwerk ist das, das zwischen Ihrer lokalen Umgebung und der VPC mithilfe and/or eines VPN und AWS Direct Connect (DX) konfiguriert wurde. Der Zugriff wird durch die Verwendung von Bastion-Instances gewährt, wodurch ein direkter Zugriff auf Produktionsressourcen verhindert wird. Alle Ihre Anwendungen und Ressourcen befinden sich in privaten Subnetzen, die über öffentliche Load Balancer erreichbar sind. Öffentlicher Ausgangsverkehr fließt über unsere Forward-Proxys zum Internet Gateway und dann zum Internet. Alternativ kann der Datenverkehr über Ihr VPN oder Direct Connect in Ihre lokale Umgebung fließen.

AMS landing zone Shared Services mit einem Konto

Shared Services-Subnetze enthalten AMS Directory Services, den Management-Host, der die Bereitstellung und allgemeine Aufgaben automatisiert, den Antivirus (TrendMicro) -Management-Server und interne Bastion-Hosts:

- AMS Directory Services = AD-Domänencontroller

  Erstellt ein Active Directory in AMS-Konten, erstellt die AMS-Domäne und verbindet verwaltete Stacks beim Start mit der Domäne.
- Management-Hosts = AMS Management Host (automatische Bereitstellung und allgemeine Aufgaben)

  Fungiert als API-Endpunkt AWS Directory Service, um AWS Directory Service Domänencontroller zu modifizieren und mit ihnen zu interagieren.

- Sicherheitsdienste: Antivirus (TrendMicro) -Managementserver = EPS DSM + EPS Relay

  Nutzt die Trend Micro™ Deep Security Software (DSM), arbeitet in einem Client-Server-Modell und verfügt über eine Back-End-Datenbank mit Deep Security Managern, -Agenten und Relays.
- Interne Bastion-Hosts = Bastionen der Kunden

  Spezialserver, die als primärer Zugriffspunkt für das Internet konzipiert sind und als Proxy für Ihre anderen EC2 Amazon-Instances fungieren.

SALZ: Neues AWS Konto für AMS erstellen

Die fünf Schritte zur Erstellung eines neuen AWS Kontos für AWS Managed Services (AMS) sind:

1. Erstelle eine AWS-Konto
2. Konsolidierte Abrechnung einrichten — neues Konto mit Zahlerkonto verknüpfen
3. Konfigurieren Sie Ihren AWS-Konto für AMS-Zugriff
4. Sichern Sie das neue Konto mit Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer in AMS
5. Abonnieren Sie AWS Marketplace für EPS

Bitte wenden Sie sich bei Fragen an Ihren Customer Service Delivery Manager (CSDM).

Erstelle eine AWS-Konto

Das AMS-Programm erfordert die Bereitstellung eines neuen Amazon Web Services (AWS) -Kontos. Eine schrittweise Anleitung finden Sie im folgenden Video: Wie erstelle und aktiviere ich ein neues Amazon Web Services Services-Konto? Die einfachen Schritte sind:

Melde dich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

Erstellen eines Benutzers mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Benutzerzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie IAM-Identity-Center-Verzeichnis im Benutzerhandbuch unter Benutzerzugriff mit der Standardeinstellung konfigurieren.AWS IAM Identity Center

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Access-Portal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

   Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center Benutzerhandbuch.
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center Benutzerhandbuch.

> **Note**
>
> Wenn Sie bereits ein Konto haben, können Sie auf der Seite mit den AWS Preisen auf Kostenloses Konto erstellen klicken. Stellen Sie sicher, dass Sie sich mindestens für den EC2 Service anmelden. Wenn Sie sich für einen Dienst anmelden, haben Sie Zugriff auf alle Dienste in AWS. Berechnet werden Ihnen aber nur die Services, die Sie nutzen.
> Wenn Sie beabsichtigen, Ihr neues Konto für Zwecke der konsolidierten Fakturierung mit einem Zahlerkonto zu verknüpfen, müssen Sie keine Informationen zur Zahlungsmethode eingeben, wenn Sie dazu aufgefordert werden. Sobald Sie den Bildschirm zur Eingabe

der Kreditkarteninformationen erreicht haben, gehen Sie stattdessen einfach zur Seite. Sie benötigen die mit dem Zahlerkonto verknüpfte E-Mail-Adresse, um eine Anfrage zu einem konsolidierten billing/linked Konto zu senden, die im nächsten Abschnitt detailliert beschrieben wird.

Important

Es ist wichtig, dass Sie sicherstellen, dass dem Konto eine E-Mail-Adresse und eine Telefonnummer zugeordnet sind, damit Sie Antworten auf potenzielle Sicherheitsvorfälle erhalten. Die Telefonnummer und E-Mail-Adresse für das Konto können nicht geändert werden, ohne das Kontopasswort zurückzusetzen, was für ein AMS-Root-Konto ein erhebliches Unterfangen ist. Um sicherzustellen, dass diese Werte stabil sind, ist es wichtig, Kontaktinformationen auszuwählen, die nicht mit Personen verknüpft sind, da diese sich ändern können. Wählen Sie einen E-Mail-Alias, der auf eine Gruppe verweisen kann. Gehen Sie bei der Auswahl einer Telefonnummer nach der gleichen bewährten Methode vor: Wählen Sie eine Nummer, die auf eine Gruppe oder auf eine Nummer verweisen kann, die dem Unternehmen gehört und nicht auf eine Einzelperson.

Konsolidierte Abrechnung einrichten — neues Konto mit Zahlerkonto verknüpfen

Wenn Sie möchten, dass Ihre neue, von AMS verwaltete AWS-Konto Rechnung als Zahlung für ein bestehendes AWS Organizations Verwaltungskonto zusammengefasst wird, müssen Sie eine konsolidierte Abrechnung einrichten und die Konten verknüpfen. Einzelheiten dazu finden Sie unter

- Konsolidierte Fakturierung AWS Organizations und Strategie für die AWS Abrechnung mehrerer Konten.
- Laden Sie einen ein AWS-Konto , Ihrer Organisation beizutreten

Note

Sie können diese Schritte ausführen, bevor Sie das Konto an AMS übergeben. Nach der Übergabe können die Schritte für den Beitritt zu Ihrer Organisation (siehe oben) im Rahmen des Change-Management-Prozesses durchgeführt werden. Wenden Sie sich an Ihren

Cloud Service Deliver Manager (CSDM) oder Cloud Architect (CA), wenn Sie Unterstützung benötigen.

Allgemeine Abrechnungsinformationen, einschließlich der Verwaltung der konsolidierten Fakturierung, finden Sie unter Was ist AWS Fakturierung. Allgemeine AWS Organizations Informationen darüber, wie Konten zusammenarbeiten können, finden Sie unter Was ist AWS Organizations. Eine ausführliche Anleitung zu AWS Organizations Verwaltungskonten finden Sie unter Das Verwaltungskonto, vertrauenswürdiger Zugriff und delegierte Administratoren

Konfigurieren Sie Ihren AWS-Konto für AMS-Zugriff

Nachdem Sie die oben genannten Schritte abgeschlossen haben, haben Sie Ihr neues Gerät erfolgreich gesichert AWS-Konto und sichergestellt, dass die damit verbundenen Kosten ordnungsgemäß in Rechnung gestellt werden. Der letzte Schritt des Prozesses besteht darin, AMS Zugriff auf das neue Konto für die anfängliche Stack-Konfiguration und die Erfüllung laufender Änderungs- und Bereitstellungsanfragen zu gewähren. Einzelheiten finden Sie unter AWS Kontenübergreifendes Delegieren des Zugriffs mithilfe von IAM-Rollen. Die grundlegenden Schritte werden in diesem Abschnitt beschrieben.

Zugriff auf die AWS Website aktivieren

Um Ihren IAM-Benutzern Zugriff auf die Rechnungsinformationen und Tools Ihres Kontos zu gewähren, müssen Sie die Funktion aktivieren.

Dazu gehen Sie wie folgt vor:

1. Melden Sie sich AWS Management Console mit Ihren Root-Kontoanmeldeinformationen an (die E-Mail-Adresse und das Passwort, mit denen Sie Ihr Konto erstellt haben AWS-Konto). Melden Sie sich nicht mit Ihrer IAM-Benutzer-Anmeldeinformationen an.

   Die AWS Management Console Startseite wird geöffnet.
2. Öffnen Sie in der oberen Navigationsleiste das Drop-down-Menü für Ihren Kontonamen und wählen Sie dann Mein Konto aus.

   Die Startseite für die Abrechnung wird geöffnet.
3. Scrollen Sie nach unten zum Bereich „IAM-Benutzerzugriff auf Rechnungsinformationen“ und klicken Sie auf der rechten Seite auf Bearbeiten. *The area does not appear unless you are logged in with root credentials*.

Der Bereich „IAM-Zugriff aktivieren“ wird geöffnet.

4. Aktivieren Sie das Kontrollkästchen und klicken Sie auf Aktualisieren.

   Sie können nun IAM-Richtlinien verwenden, um zu steuern, auf welche Seiten ein Benutzer zugreifen kann.

Weitere Informationen zu diesem Vorgang finden Sie unter Überblick über die Verwaltung von Zugriffsberechtigungen. AWS

Erstellen Sie eine IAM-Rolle mit Zugriff auf die Website AWS

AWS Identity and Access Management (IAM) ist ein Webdienst, mit dem Sie den Zugriff Ihrer Benutzer auf AWS Ressourcen sicher kontrollieren können. Sie verwenden IAM, um zu kontrollieren, wer Ihre AWS Ressourcen nutzen kann (Authentifizierung) und welche Ressourcen sie auf welche Weise verwenden können (Autorisierung).

1. Gehen Sie zur IAM Management Console und klicken Sie im linken Navigationsbereich auf Rollen.

   Die Seite zur Rollenverwaltung wird mit Informationen zu IAM-Rollen, der Option „Rolle erstellen“ und einer Liste vorhandener Rollen geöffnet.

2. Klicken Sie auf Rolle erstellen.

   Die Seite Rolle erstellen Wählen Sie den Typ der vertrauenswürdigen Entität aus wird geöffnet. Klicken Sie auf „Weiteres“ AWS-Konto und unten wird ein Einstellungsbereich geöffnet.

   Geben Sie die ID des vertrauenswürdigen AMS-Kontos ein, die Sie von AMS erhalten haben. Lassen Sie die Optionen Externe ID erforderlich und MFA erforderlich deaktiviert.

3. Klicken Sie auf Next: Permissions.

   Die Seite Rolle erstellen Zugriffsrichtlinien anhängen wird geöffnet. Sie enthält Optionen zum Erstellen einer neuen Richtlinie, zum Aktualisieren der Seite und zum Durchsuchen vorhandener Richtlinien. Eine Liste vorhandener Richtlinien wird bereitgestellt.

4. Wählen Sie die AdministratorAccessRichtlinie aus und klicken Sie dann auf Weiter: Überprüfen.

   Die Seite „Rolle erstellen — Überprüfung“ wird geöffnet.

5. Nennen Sie die neue Rolle aws_managedservices_onboarding_role und geben Sie „AMS Onboarding Role“ als Rollenbeschreibung ein. Überprüfen Sie die Einstellungen für die neue Rolle und klicken Sie, wenn Sie zufrieden sind, auf Rolle erstellen.

   Die Seite zur Rollenverwaltung wird geöffnet, auf der Ihre neue Rolle aufgeführt ist.

Abonnieren Sie AWS Marketplace für EPS

Aufgrund der jüngsten Änderungen an AMS Endpoint Security (EPS) müssen Sie TrendMicro Deep Security über die abonnieren AWS Marketplace und die Softwarebedingungen akzeptieren.

TrendMicro bietet zwei Lizenzmodelle an: Pro Protected Instance Hour und Bring Your Own License (BYOL).

- VON OL:
  1. Sie verwenden Ihre eigene Lizenz, die Sie über externe Kanäle erworben haben.
  2. Sie müssen AMS alle Lizenzschlüssel zur Verfügung stellen, um die EPS-Infrastruktur aufzubauen. Sie können einen Aktivierungscode angeben, der alle Module lizenziert, oder einzelne Aktivierungscodes, die eine bestimmte Gruppe von Modulen lizenzieren. AMS erstellt nur die Lizenzdateien, die den von Ihnen bereitgestellten Aktivierungscodes entsprechen. Da die Lizenzaktivierung während des Onboardings erfolgt, können Sie diese Informationen dann in Anwesenheit eines leitenden AMS-Technikers und des CSDM weitergeben.
  3. Darüber hinaus müssen Sie das BYOL TrendMicro Market Place AMI-Abonnement abonnieren. Weitere Informationen finden Sie unter Trend Micro Deep Security (BYOL).
- Pro Stunde geschützter Instance:
  1. Für dieses Abonnement benötigen Sie keine zuvor erworbene Trend Lizenz.
  2. Sie müssen jedoch das Marketplace-Abonnement abonnieren.
  3. Bei diesem Modell ist keine gemeinsame Nutzung der Lizenzschlüssel mit AMS erforderlich, da die Trend-Nutzung automatisch gemessen wird, einschließlich der Softwarelizenz und der EC2 Infrastrukturnutzung. Siehe Trend Micro Deep Security.

Gehen Sie wie folgt vor, um Trend Micro zu abonnieren:

1. Melden Sie sich bei Ihrem an AWS-Konto.
2. Rufen Sie die Produktseite von Trend Micro Deep Security (BYOL oder Per Protected Instance Hour) auf.
3. Klicken Sie im rechten Bereich auf Weiter zum Abonnieren.
4. Klicken Sie in der oberen rechten Ecke auf Nutzungsbedingungen akzeptieren.

IDS und IPS in Trend Micro Deep Security aktivieren

Sie können verlangen, dass AMS die nicht standardmäßigen Funktionen Trend Micro Intrusion Detection System (IDS) und Intrusion Protection Systems (IPS) für Ihr Konto aktiviert.

Senden Sie dazu eine Aktualisierungsanfrage (Verwaltung | Andere | Andere | Update) und fügen Sie eine Liste mit E-Mail-Adressen für den Empfang von IDS- und IPS-Benachrichtigungen bei. Diese Adressen werden zu einem SNS-Thema in Ihrem Konto hinzugefügt, das AMS für Sie erstellt.

> **Note**
>
> AMS kann keinen Trend Micro Service hinzufügen, der unsere Fähigkeit, andere AMS-Dienste anzubieten, beeinträchtigen könnte.

Nächster Schritt: Sichern Sie das neue Konto mit Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer in AMS

CentOS 7.6 abonnieren AWS Marketplace

AMS bietet jetzt das CentOS 7 (x86_64) — mit Updates HVM, das von CentOS.org verkauft wird — als AMS-AMI an. Um dieses AMI nutzen zu können, müssen Sie sich für die KOSTENLOSE Cent OS-Lizenz entscheiden und die Lizenz für alle Ihre AMS-Konten akzeptieren.

Um ein Abonnement abzuschließen, gehen Sie zu AWS Marketplaceund folgen Sie den Anweisungen zur Anmeldung.

Für die Nutzung dieses Produkts fallen keine Softwaregebühren an, Sie sind jedoch weiterhin für andere AWS Gebühren, einschließlich der Nutzung, verantwortlich. EC2 Wenn es sich um ein „Bring Your Own License“ -Produkt handelt, müssen Sie über eine gültige Softwarelizenz verfügen, um es verwenden zu können.

Informationen zu dieser Software finden Sie unter CentOS 7 (x86_64) - mit Updates HVM.

Sichern Sie das neue Konto mit Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer in AMS

Dieser Abschnitt wurde redigiert, da er sensible AMS-Sicherheitsinformationen enthält. Diese Informationen sind in der AMS-Konsolendokumentation verfügbar. Um auf AWS Artifact zuzugreifen, können Sie sich an Ihren CSDM wenden, um Anweisungen zu erhalten, oder gehen Sie zu Erste Schritte mit AWS Artifact.

SALZ: Netzwerk einrichten

Es gibt mehrere Prozesse, die abgeschlossen werden müssen, um das Netzwerk für AWS Managed Services (AMS) einzurichten:

1. Zuweisen von IP-Speicherplatz für Ihre AMS-Umgebung
2. Einrichtung einer privaten Netzwerkkonnektivität zu AWS
3. Richten Sie Ihre Firewall ein, um den AMS-Betrieb zu ermöglichen

Weisen Sie IP-Speicherplatz für Ihre AMS-Umgebung zu

AMS wurde unter Verwendung eines /16 CIDR-Blocks als empfohlene Netzwerkzuweisung entworfen und getestet. Es ist wichtig, dass das mit AMS verbundene vertrauenswürdige Netzwerk einen CIDR-Block verwendet, der sich nicht mit dem dem AMS zugewiesenen CIDR-Block überschneidet. Diese Adressen sind erforderlich, um Ihre Virtual Private Cloud (VPC) und Subnetze einzurichten. Weitere Informationen zu AWS VPCs finden Sie unter Amazon VPC Limits und Amazon FAQs VPC.

Ein /16 CIDR-Block mag zwar wie eine Menge IP-Adressen erscheinen, aber eine einmal erstellte VPC kann nicht erweitert werden. Diese Zuweisung stellt also sicher, dass Ihre von AMS verwaltete VPC über einen längeren Zeitraum funktionieren kann. Innerhalb des CIDR-Blocks müssen Sie IP-Adressbereiche für mindestens zwei private Subnetze und zwei öffentliche Subnetze zuweisen.

AWS akzeptiert Konnektivität zur AMS-Umgebung über die native AWS-Funktionalität für virtuelle private Netzwerke (VPN). Auf Ihrer Seite kann dies über AWS Direct Connect (DX), Hardware-VPN oder Software-VPN erreicht werden. Auf der AMS-Seite verwenden wir die Virtual Gateway-Funktionalität von VPCs.

Grundlegende Umgebungskomponenten

Network-to-AmazonVPC-Verbindungsoptionen für Benutzer	
Hardware-VPN	Stellt eine Hardware-VPN-Verbindung von Ihren Netzwerkgeräten in einem Remote-Netzwerk zu AMS-verwalteten Netzwerkgeräten her, die an Ihre VPC angeschlossen sind.
AWS Direct Connect (DX)	Stellt mithilfe von AWS Direct Connect eine private, logische (oder bei Verwendung mit einem VPN verschlüsselte) Verbindung von Ihrem Remote-Netzwerk zur Amazon VPC her.
Software-VPN	Stellt eine VPN-Verbindung von Ihren Geräten in einem Remote-Netzwerk zu einer benutzerverwalteten Software-VPN-Appliance her, die in einer Amazon VPC ausgeführt wird.

> **Note**
>
> AMS empfiehlt redundante private VPN-zu-DX-Verbindungen. Ihr Customer Service Delivery Manager (CSDM) hilft Ihnen bei der Einrichtung bei der Einrichtung Ihres Kontos.

Private Netzwerkkonnektivität zu AWS einrichten

Fügen Sie AMS zu Ihrem Unternehmens-Active Directory hinzu, um Konnektivität herzustellen. Möglicherweise möchten Sie administrative Aktionen oder Benutzerzugriff über eine private Netzwerkverbindung ausführen. AWS bietet sowohl VPN-Konnektivität als auch Standleitungen über AWS Direct Connect. In den folgenden Schritten wird erklärt, wie Sie mit AMS zusammenarbeiten, um eine (oder beide) Verbindungsmöglichkeiten herzustellen.

VPN-Einrichtung

In diesem Abschnitt werden die grundlegenden Schritte zur Einrichtung eines VPN für die Kommunikation zwischen Ihrer AMS-verwalteten VPC und Ihrem internen Netzwerk beschrieben.

> **Note**
>
> Allgemeine Informationen zur Verwendung eines VPN mit AWS-Services finden Sie unter Was ist Site-to-Site AWS-VPN und alles über Ihr Kunden-Gateway (Ihre VPN-Appliance).

Folgen Sie den Abschnitten Erste Schritte im AWS-VPN-Benutzerhandbuch und Testen der Site-to-Site VPN-Verbindung, um die folgenden Schritte auszuführen.

- Schritt 1: Erstellen Sie in Ihrer AWS-VPC ein Kunden-Gateway
- Schritt 2: Erstellen Sie in Ihrer AWS-VPC ein Virtual Private Gateway
- Schritt 3: Aktivieren Sie in Ihrer AWS-VPC Route Propagation in Ihrer Routing-Tabelle
- Schritt 4: Aktualisieren Sie in Ihrer AWS-VPC Ihre Sicherheitsgruppe, um eingehenden SSH-, RDP- und ICMP-Zugriff zu aktivieren
- Schritt 5: Stellen Sie in Ihrem internen Netzwerk eine VPN-Verbindung her und konfigurieren Sie das Kunden-Gateway
- Schritt 6: Testen Sie die VPN-Konnektivität zwischen der VPC und Ihrem internen Netzwerk

AWS Direct Connect Einrichtung

In diesem Abschnitt werden die grundlegenden Schritte zum Einrichten eines AWS Direct Connect (DX) für die Kommunikation zwischen Ihrer AMS-verwalteten VPC und Ihrem internen Netzwerk beschrieben.

> **Note**
>
> Informationen zur Verwendung eines DX mit AWS-Services finden Sie unter Erste Schritte an einem AWS Direct Connect Standort.

Um eine DX-Verbindung einzurichten, müssen Sie die folgenden Schritte ausführen:

1. Melden Sie sich für Amazon Web Services an
2. Verbindungsanfrage für AWS Direct Connect einreichen
3. Schließe den Cross Connect ab
4. (Optional) Konfiguration redundanter Verbindungen mit AWS Direct Connect

5. Durchgeführt von AMS: Erstellen Sie eine virtuelle Schnittstelle
6. Durchgeführt von AMS: Router-Konfiguration herunterladen
7. Überprüfen Sie Ihre virtuelle Schnittstelle

Richten Sie Ihre Firewall ein

Dieser Abschnitt wurde redigiert, da er sensible sicherheitsrelevante AMS-Informationen enthält. Diese Informationen sind in der AMS-Konsolendokumentation verfügbar. Um auf AWS Artifact zuzugreifen, können Sie sich an Ihren CSDM wenden, um Anweisungen zu erhalten, oder gehen Sie zu Erste Schritte mit AWS Artifact.

AMS Bastion-Optionen bei Anwendungsmigrationen/Onboarding

Um Ihnen die bestmögliche Erfahrung bei der Migration zu bieten, finden Sie im Folgenden die potenziellen Optionen, die AMS derzeit nutzen könnte:

- Option 1: Umgehen Sie Bastions nur für Migrationsmaßnahmen (Sie müssen dies aus Sicherheitsgründen als vorübergehende Maßnahme unterzeichnen).

  Hinweis: Es werden weiterhin Prüffunktionen zur Verfügung stehen, um sicherzustellen, dass AMS Einblick in jede Anfrage hat.
- Option 2: SSH-Tunneling mit einem Tool Ihrer Wahl, z. B. PuTTy, wie abgebildet.

  Die beschriebenen Umgebungskomponenten müssten für diese Option bereits vorhanden sein.

  AMS würde zusätzliche Hinweise und Anweisungen bereitstellen.

Schritte zum SSH-Tunneling mit Pu: TTy

In PuTTY würden Sie eine SSH-Sitzung mit der öffentlichen IP des Bastion-Hosts erstellen, den PEM-Schlüssel im AUTH-Abschnitt angeben und dann einen Tunnel erstellen. Der Quellport des Tunnels sollte ein ungenutzter lokaler Port sein (z. B. 5000) und die IP wäre die IP des Zielhosts (der Windows-Box, die Sie erreichen möchten) mit angehängtem RDP-Port (3389). Achten Sie darauf, Ihre Konfiguration zu speichern, da Sie dies nicht jedes Mal tun müssen möchten, wenn Sie sich in die Box einloggen. Connect zum Bastion-Host her und melden Sie sich an. Starten Sie dann eine RDP-Sitzung für localhost:5000 (oder welchen Port Sie auch wählen).

1. Stellen Sie den Hostnamen oder die öffentliche IP des Bastion-Hosts ein

2. Stellen Sie in SSH ->Auth die Datei mit dem privaten Schlüssel im PPK-Format ein

3. Fügen Sie unter SSH ->Tunnels den neuen weitergeleiteten Port hinzu. Der Quellport sollte der beliebige ungenutzte Port sein, und das Ziel sollte die IP des Zielservers hinter dem Bastion-Host sein, mit angehängtem RDP-Port.

4. Stellen Sie über PuTTY eine Connect zum Bastion-Host her und melden Sie sich an.

5. Starten Sie eine RDP-Sitzung mit localhost:5000, um den Zielserver zu erreichen.

SALZ: Zugangsmanagement einrichten

Die Nutzung eines von AWS Managed Services (AMS) verwalteten Netzwerks bedeutet, AMS Zugriff auf die Verwaltung Ihrer Cloud-Infrastruktur zu gewähren. Sie müssen eine Methode zur sicheren Verbindung zwischen Ihrem privaten Netzwerk und AMS konfigurieren. Dies beginnt mit einigen Entscheidungen über die Art des Zugriffs, den Sie bereitstellen möchten:

- Für AMS API/CLI - und Konsolenzugriff: Sie sollten die AMS-CLI installieren (Anweisungen finden Sie in diesem Dokument). Sie verwenden die AMS Change Management API, um Änderungsanfragen an AMS zu stellen, und die AMS SKMS API, um mehr über Ihre vom AMS verwalteten Ressourcen zu erfahren. Mithilfe der Active Directory Federation Services (AD FS) können Sie auf die AMS-Konsole zugreifen.

  > **Note**
  >
  > Wenn Sie Ihr eigenes ITSM einrichten, müssen Sie die AWS Support API (SAPI) für Serviceanfragen und Vorfallberichte verwenden. SAPI ist in der AWS Support API Reference dokumentiert.

- Für den Benutzerzugriff: Unabhängig davon, ob Sie Benutzer mit Windows Active Directory (AD) oder einer Linux/LDAP Lösung verwalten, muss eine Konnektivität zwischen AD auf der AMS-Seite (über Directory Services) und Ihrem Verzeichnis hergestellt werden.

- Zum Beispiel Zugriff: Der Zugriff auf Instanzebene erfolgt über eine unidirektionale Forest-Trust-Konfiguration. Directory Services vertraut den Anmeldeinformationen in ihrem CORP AD, sodass Stacks innerhalb der AMS-Seite die Anmeldung mit CORP-Anmeldeinformationen ermöglichen.

  Beachten Sie, dass Ihr Active Directory (AD), für das AMS den Trust einrichtet, das Verzeichnis sein muss, in dem die Konten von Benutzern gespeichert sind, die von Ihnen autorisiert wurden, Zugriff auf Ihre AWS-Ressourcen zu erhalten.

> **Important**
>
> Um einen Forest Trust einzurichten, benötigt AMS auf Ihrem Domain-Controller Lokale Richtlinien -> Sicherheitsoptionen -> Netzwerkzugriff: Bei Named Pipes, auf die anonym zugegriffen werden kann, müssen die Pipes Netlogon und lsarpc aufgeführt sein. Diese Pipes sind standardmäßig aufgeführt, werden aber manchmal aus Sicherheitsgründen entfernt. Sobald die Vertrauensstellung hergestellt ist, können sie wieder aus der Liste entfernt werden.

Richten Sie eine Active Directory-Vertrauensstellung (AD) ein

Bevor Sie mit der Einrichtung einer Active Directory-Vertrauensstellung (AD) für Ihr AWS Managed Services (AMS) -Konto beginnen, stellen Sie sicher, dass die entsprechenden Firewall-Ports geöffnet sind.

Die Vertrauensstellung durch das von AMS verwaltete Active Directory und Ihren Unternehmensverzeichnisdienst ermöglicht es Ihnen, Ihre vom Unternehmen verwalteten Anmeldeinformationen für den Zugriff auf AMS-verwaltete Instances zu verwenden, um Entwicklungs-, Test- oder Verwaltungsfunktionen durchzuführen.

Das Erstellen einer Vertrauensverbindung besteht aus zwei Teilen:

Konfigurieren Sie zunächst eine bedingte Weiterleitung, eine DNS-Konfiguration, damit DNS-Abfragen wissen, zu welchem DNS-Server sie gehen müssen.

Zweitens konfigurieren Sie eine Vertrauensstellung, ein Active Directory-Konstrukt (AD), das Benutzern in einer Domäne den Zugriff auf Ressourcen in einer anderen Domäne ermöglicht.

Konfigurieren Sie den bedingten Forwarder

Folgen Sie diesem Microsoft AD-Artikel Zuweisen einer bedingten Weiterleitung für einen Domainnamen und verwenden Sie diese Einstellungen und Auswahlmöglichkeiten:

1. Verwenden Sie im AD DNS Manager -> Create a New Conditional Forwarder unter DNS-Domain: Verwenden Sie den Domainnamen AMS, den Sie erhalten haben, z. B. `A523434123.amazonaws.com`
2. Unter IP-Adressen der Masterserver: Fügen Sie die vom AMS bereitgestellten IP-Adressen hinzu. Stellen Sie sicher, dass kein Verbindungsproblem vorliegt, indem Sie beide Adressen überprüfen.
3. Wählen Sie Diese bedingte Weiterleitung in Active Directory speichern und replizieren Sie wie folgt: Alle DNS-Server in dieser Domäne und drücken Sie OK.

Konfigurieren Sie das Vertrauen

Um die Vertrauensstellung für Ihr AWS Managed Services (AMS) -Konto zu konfigurieren, folgen Sie diesem MicroSoft AD-Artikel Erstellen Sie eine unidirektionale, eingehende Gesamtvertrauensstellung für eine Seite der Vertrauensstellung mithilfe der in diesem Abschnitt beschriebenen Einstellungen und Auswahlmöglichkeiten.

1. Öffnen Sie das Dialogfeld Start -> Verwaltung -> Active Directory-Domänen und Vertrauensstellungen. Klicken Sie mit der rechten Maustaste auf den Domänenknoten der Domäne, für die Sie eine Vertrauensstellung einrichten möchten, und klicken Sie dann auf Eigenschaften -> Vertrauensstellungen -> Neue Vertrauensstellung, um den Assistenten für neue Vertrauensstellungen zu öffnen. Geben Sie den Domainnamen ein, den Sie von AMS für den Vertrauensnamen erhalten haben, und klicken Sie auf Weiter.
2. Wählen Sie unter Vertrauenstyp die Option Forest Trust aus. Wählen Sie Weiter aus.
3. Wählen Sie unter Vertrauensrichtung die Option Einseitig: eingehend aus. Wählen Sie Weiter aus.
4. Wählen Sie unter Vertrauensseiten die Option Nur diese Domain aus. Wählen Sie Weiter aus.
5. Geben Sie unter Vertrauenspasswort ein Passwort Ihrer Wahl ein. Wählen Sie Weiter aus.
6. Für Trust Selections Completed und Trust Creation Complete klicken Sie einfach auf Weiter.
7. Wählen Sie unter Eingehendes Vertrauen bestätigen die Option Nein, eingehende Vertrauensstellung nicht bestätigen aus. Wählen Sie Weiter aus.
8. Wählen Sie unter Der Assistent für neue Vertrauensstellungen abgeschlossen die Option Fertig stellen und dann OK aus, um den Vorgang zu schließen.

9. Geben Sie das Vertrauenspasswort ein (kontaktieren Sie uns aus Sicherheitsgründen über die Telefonnummer Ihres CSDM). AMS schließt die Trust-Konfiguration ab.

Active Directory-Standorte und -Dienste

Um die Anmeldelatenz zu reduzieren, fügen Sie den VPC-CIDR-Bereich zu Ihren Active Directory-Standorten und -Diensten hinzu (Start -> Verwaltung -> Active Directory-Standorte und -Dienste). Fügen Sie den VPC-CIDR-Bereich zu einem Active Directory-Standort hinzu, der Domain-Controller enthält, die AWS am nächsten sind.

Routing von Active Directory-Namenssuffixes

Nachdem der unidirektionale Forest Trust eingerichtet wurde, führen Sie bitte die zusätzlichen Schritte aus.

1. Klicken Sie unter Start > Alle Programme > Verwaltungstools auf Active Directory-Domänen und -Vertrauensstellungen.

   Die Konsole „Active Directory-Domänen und Vertrauensstellungen“ wird geöffnet.
2. Klicken Sie mit der rechten Maustaste auf Ihre Unternehmensdomäne und dann auf Eigenschaften

   Das Eigenschaftendialogfeld für diese Domain wird geöffnet.
3. Klicken Sie auf die Registerkarte Vertrauensstellungen.

   Die Seite Trusts wird geöffnet.
4. Klicken Sie auf den Amazon-Domainnamen und dann auf Eigenschaften.

   Die Eigenschaftenseite für den Amazon Domain Trust wird geöffnet.
5. Klicken Sie auf Name Suffix Routing und dann auf Aktualisieren.

   Durch diese Schritte wird sichergestellt, dass die Service Principal Names (SPNs) über die Vertrauensstellung hinweg aufgelöst werden können.

Fehlersuche

Einige Dinge, die Sie ausprobieren sollten, wenn Sie auf Probleme stoßen:

- Für die vom AMS verwaltete ausgehende Active Directory-Sicherheitsgruppe muss die Verbindung über Ihren CIDR-Block (z. B. 10.27.0.0/16) zu Ihrem Domänencontroller zugelassen werden.
- Verfolgen Sie die Route in der AWS-Konsole von Domain-Controller zu Domain-Controller und überprüfen Sie dabei alle Sicherheitsgruppen.
- Stellen Sie sicher, dass Sie die vom AMS verwalteten Active Directory-Domänencontroller anpingen können, wenn das Internet Control Message Protocol (ICMP) zulässig ist.
- Stellen Sie sicher, dass Ihr Domain-Controller mit AWS Directory Services kommunizieren kann.
- Stellen Sie sicher, dass die bedingten Weiterleitungen das Problem lösen und validiert sind.
- Wenn Forest Trust im Assistenten für neue Vertrauensstellungen nicht angezeigt wird, funktionieren Ihre bedingten Weiterleitungen möglicherweise nicht richtig:
  - Verwenden Sie nslookup, um die Auflösung zu testen
  - Versuchen Sie, den Domänencontroller neu zu starten

Von AMS verwaltetes Active Directory

AMS bietet jetzt einen neuen Dienst namens Managed Active Directory (auch bekannt als Managed AD) an, der es AMS ermöglicht, sich um den Betrieb Ihrer Active Directory-Infrastruktur (AD) zu kümmern, während Sie gleichzeitig die Kontrolle über Ihre Active Directory-Verwaltung behalten.

Die AMS-Unterstützung für Managed AD ähnelt der AMS-Unterstützung für den Amazon Relational Database Service (Amazon RDS). In beiden Fällen AWS (einschließlich AMS) werden die Erstellung und Verwaltung der Infrastruktur, auf der der Service ausgeführt wird, unterstützt, während Sie gleichzeitig die Zugriffskontrolle und alle Verwaltungsfunktionen übernehmen. Dieses Modell bietet die folgenden Vorteile:

- Schränkt Sicherheitsrisiken ein: AWS AMS benötigt keine Administratorrechte für Ihre Domain.
- Direkte Integrationen: Sie können Ihr aktuelles Autorisierungsmodell verwenden und es in AD integrieren, ohne eine Schnittstelle zu AMS herstellen zu müssen.

Hinweise:

- Weder AMS noch Sie haben Zugriff auf Ihre Managed AD-Domänencontroller, sodass keine Software auf den Domain-Controllern installiert werden kann. Dies ist wichtig, da Lösungen von Drittanbietern, für die Software auf Domänencontrollern installiert werden muss, nicht zulässig sind.

  Access funktioniert wie folgt:

  - AWS Verzeichnisdienst-Team: Hat Zugriff auf Domänencontroller.
  - AMS: Hat Zugriff auf den Directory Service APIs , um bestimmte Aktionen auf der Domain auszuführen. Zu diesen Aktionen gehören das Erstellen von AD-Snapshots, das Ändern des AD-Schemas und andere Aktionen.
  - Sie: Sie haben Zugriff auf die Domain (AD), um Benutzer, Gruppen usw. zu erstellen.
- Wir empfehlen Ihnen, vor der Migration Ihres Unternehmens-AD einen Machbarkeitsnachweis für Managed AD durchzuführen, da nicht alle Funktionen einer herkömmlichen AD-Umgebung in einer Managed AD-Umgebung verfügbar sind.
- AMS wird Ihr AD-Management nicht verwalten oder Ihnen diesbezüglich weiterhelfen. AMS stellt beispielsweise keine Leitlinien zur Struktur der Organisationseinheit, zur Gruppenrichtlinienstruktur, zu Konventionen zur Benennung von AD-Benutzern usw. bereit.

Das funktioniert wie folgt:

1. AMS installiert eine neue AWS-Konto für Sie, getrennt von und zusätzlich zu Ihrem AMS-Konto, und stellt über Directory Service eine Active Directory (AD) -Umgebung AWS bereit (siehe auch Was ist AWS Directory Service?).

   Die folgenden Informationen müsste ein Systemintegrator von Ihnen einholen, damit AMS Managed AD integrieren kann:

   - Informationen zum Konto
     - Konto-ID des AWS-Konto , das für Ihr von AMS verwaltetes AD erstellt wurde: Nummer AWS-Konto
     - Region, in der Sie Ihr Managed AD einbinden möchten für: AWS-Region
   - Informationen zu verwaltetem Active Directory:
     - Microsoft AD Edition: Standard/Enterprise. AWS Microsoft AD (Standard Edition) umfasst 1 GB Verzeichnisobjektspeicher. Diese Kapazität kann bis zu 5.000 Benutzer oder 30.000 Verzeichnisobjekte, einschließlich Benutzer, Gruppen und Computer, unterstützen. AWS Microsoft AD (Enterprise Edition) umfasst 17 GB Verzeichnisobjektspeicher, der bis zu 100.000 Benutzer oder 500.000 Objekte unterstützen kann.

       Weitere Informationen finden Sie unter AWS Directory Service FAQs.
     - Domain-FQDN: Der FQDN für Ihre AMS Managed AD-Domain.
     - Domain-NetBIOS-Name: Der NetBIOS-Name für Ihre AMS Managed AD-Domäne.

- Kontonummern der AMS-Standardkonten, für die Sie eine Managed AD-Integration wünschen (AMS konfiguriert eine unidirektionale Vertrauensstellung vom AD des AMS-Standardkontos zum Managed AD)
- Sind Änderungen am Active Directory-Schema erforderlich und wenn ja, welche Änderungen?
- Standardmäßig werden zwei Domänencontroller bereitgestellt. Benötigen Sie mehr? Falls ja, wie viele benötigen Sie und aus welchem Grund?

- Netzwerke für verwaltete Active Directory-Informationen:
  - Managed AD VPC CIDR für Domänencontroller (ein CIDR in Ihrem privaten Subnetzbereich für die Managed AD-Domänencontroller):
    - Subnetz CIDR 1 für Domänencontroller: [Ihr CIDR, muss Teil von AMS Managed AD VPC CIDR sein]
    - Subnetz CIDR 2 für Domänencontroller: [Ihr CIDR, muss Teil von AMS Managed AD VPC CIDR sein]

    Beispiel:

    - Verwaltetes AD-VPC-CIDR: 192.168.0.0/16
    - CIDR 1 für Domänencontroller: 192.168.1.0/24
    - CIDR 2 für Domänencontroller: 192.168.2.0/24

    Um IP-Adresskonflikte zu vermeiden, stellen Sie sicher, dass das von Ihnen angegebene Managed AD VPC CIDR nicht mit einem anderen privaten Subnetz-CIDR in Konflikt steht, das Sie in Ihrem Unternehmensnetzwerk verwenden.
  - VPN-Technologie (optional): [Direct Connect/Direct Connect und VPN]
    - Die autonome BGP Systemnummer (ASN) Ihres Gateways: [Vom Kunden bereitgestellte ASN]
    - Die über das Internet routbare IP-Adresse für die externe Schnittstelle Ihres Gateways. Die Adresse muss statisch sein: [Vom Kunden bereitgestellte IP-Adresse]
    - Ob Ihre VPN-Verbindung statische Routen erfordert oder nicht: [ja/nein]

2. AMS stellt Ihnen das Administratorkonto-Passwort für die AD-Umgebung zur Verfügung und fordert Sie auf, das Passwort zurückzusetzen, sodass AMS-Techniker nicht mehr auf Ihre AD-Umgebung zugreifen können.
3. Um das Passwort für das Administratorkonto zurückzusetzen, stellen Sie mithilfe von Active Directory-Benutzern und -Computern (ADUC) eine Verbindung zu Ihrer Active Directory-Umgebung her. ADUC und andere Remote Server Administration Tools (RSAT) sollten auf

administrativen Hosts installiert und ausgeführt werden, die Sie in einer Infrastruktur ohne AMS bereitgestellt haben. Microsoft verfügt über bewährte Methoden zur Sicherung solcher administrativer Hosts. Informationen finden Sie unter Implementieren sicherer administrativer Hosts. Sie verwalten Ihre Active Directory-Umgebung mithilfe dieser administrativen Hosts.

4. Im täglichen Betrieb kümmert sich AMS um alles, was AWS-Konto bis zum AWS Directory Service reicht, z. B. die VPC-Konfiguration, AD-Backups, Erstellung und Löschung von AD-Vertrauensstellungen usw. Sie verwenden und verwalten Ihre AD-Umgebung, z. B. Benutzererstellung, Gruppenerstellung, Gruppenrichtlinienerstellung usw.

Die aktuelle RACI-Tabelle finden Sie im Abschnitt „Rollen und Verantwortlichkeiten“ in der Servicebeschreibung von See.

Verbinden Sie Ihr Active Directory mit den AMS-Rollen AWS Identity and Access Management

Der Zweck der Verbindung Ihres Verzeichnisses mit den AMS-IAM-Rollen besteht darin, Unternehmensbenutzern die Möglichkeit zu geben, ihre Unternehmensanmeldedaten für die Interaktion mit der AWS Management Console und der und und somit der AWS APIs AMS-Konsole und zu verwenden. APIs

Beispiel für einen Föderationsprozess

In diesem Beispiel werden Active Directory Federation Services (AD FS) verwendet. Es wird jedoch jede Technologie unterstützt, die AWS Identity and Access Management Federation unterstützt. Weitere Informationen zum AWS unterstützten IAM-Verbund finden Sie unter IAM-Partner und Identitätsanbieter und Verbund. Ihr CSDM hilft Ihnen bei diesem Prozess, der eine gemeinsame Anstrengung mit Ihrem AD-Team und AMS erfordert.

Ausführliche Informationen zur Integration von SAML für den API-Zugriff finden Sie in diesem AWS Blog How to Implementation Federated API and CLI Access Using SAML 2.0 and AD FS.

> **Note**
>
> Ein Beispiel für die Installation von AMS CLI und SAML finden Sie unterAnhang: ActiveDirectory Federation Services (ADFS) -Anspruchsregel und SAML-Einstellungen.

Konfiguration des Verbunds zur AMS-Konsole (SALZ)

Die in der folgenden Tabelle aufgeführten IAM-Rollen und der SAML-Identitätsanbieter (Trusted Entity) wurden im Rahmen der Kontoeinführung bereitgestellt. Mit diesen Rollen können Sie Serviceanfragen und Vorfallberichte einreichen und überwachen RFCs sowie Informationen zu Ihren und Ihren Stacks abrufen. VPCs

Rolle	Identität sanbieter	Berechtigungen
Kunde_ _Rolle ReadOnly	SAML	Für Standard-AMS-Konten. Ermöglicht das Einreichen von Änderungen RFCs an der von AMS verwalteten Infrastru ktur sowie das Erstellen von Servicean fragen und Vorfällen.
customer_managed_ad_user_role	SAML	Für von AMS verwaltete Active Directory -Konten. Ermöglicht Ihnen, sich bei der AMS-Konsole anzumelden, um Serviceanfragen und Vorfälle zu erstellen (nein RFCs).

Eine vollständige Liste der Rollen, die unter verschiedenen Konten verfügbar sind, finden Sie unterIAM-Benutzerrolle in AMS .

Ein Mitglied des Onboarding-Teams lädt die Metadatendatei von Ihrer Verbundlösung auf den vorkonfigurierten Identitätsanbieter hoch. Sie verwenden einen SAML-Identitätsanbieter, wenn Sie eine Vertrauensstellung zwischen einem SAML-kompatiblen IdP (Identitätsanbieter) wie Shibboleth oder Active Directory Federation Services herstellen möchten, sodass Benutzer in Ihrer Organisation auf AWS-Ressourcen zugreifen können. SAML-Identitätsanbieter in IAM werden als Principals in einer IAM-Vertrauensrichtlinie mit den oben genannten Rollen verwendet.

Während andere Verbundlösungen Integrationsanweisungen für AWS bereitstellen, verfügt AMS über separate Anweisungen. Mithilfe des folgenden Blogbeitrags Enabling Federation to AWS Using Windows Active Directory, AD FS, and SAML 2.0 sowie der unten aufgeführten Änderungen können Ihre Unternehmensbenutzer von einem einzigen Browser aus auf mehrere AWS-Konten zugreifen.

Nachdem Sie das Vertrauen der vertrauenden Partei gemäß dem Blogbeitrag eingerichtet haben, konfigurieren Sie die Anspruchsregeln wie folgt:

- NameId: Folgen Sie dem Blogbeitrag.
- RoleSessionName: Verwenden Sie die folgenden Werte:
  - Name der Anspruchsregel: RoleSessionName
  - Attributspeicher: Active Directory
  - LDAP-Attribut: SAM-Account-Name
  - Art des ausgehenden Anspruchs: Attribute/ https://aws.amazon.com/SAML/ RoleSessionName
- AD-Gruppen abrufen: Folgen Sie dem Blogbeitrag.
- Rollenanspruch: Folgen Sie dem Blogbeitrag, aber verwenden Sie für die benutzerdefinierte Regel Folgendes:

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^d]{12})-"]
 => issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
 RegExReplace(c.Value, "AWS-([^d]{12})-",
 "arn:aws:iam::$1:saml-provider/customer-readonly-saml,arn:aws:iam::$1:role/"));
```

Wenn Sie AD FS verwenden, müssen Sie Active Directory-Sicherheitsgruppen für jede Rolle in dem in der folgenden Tabelle angegebenen Format erstellen (customer_managed_ad_user_role gilt nur für AMS Managed AD-Konten):

Gruppe	Rolle
AWS- [AccountNo] -Kunden_ _Rolle ReadOnly	ReadOnlyKunde_ _Rolle
AWS- [AccountNo] -customer_managed_ ad_user_role	vom Kunden verwaltete_ad_user_role

Weitere Informationen finden Sie unter Konfiguration von SAML-Assertionen für die Authentifizierungsantwort.

> **Tip**
>
> Laden Sie das SAML-Tracer-Plugin für Ihren Browser herunter, um Hilfe bei der Fehlerbehebung zu erhalten.

Einreichung der Föderationsanfrage an AMS

Wenn dies Ihr erstes Konto ist, arbeiten Sie mit Ihren CSDM (s) and/or Cloud Architect (s) zusammen, um die Metadaten-XML-Datei für Ihren Identitätsanbieter bereitzustellen.

Wenn Sie ein zusätzliches Konto oder einen Identitätsanbieter einrichten und Zugriff entweder auf das Verwaltungskonto oder das gewünschte Anwendungskonto haben, gehen Sie wie folgt vor.

1. Erstellen Sie eine Serviceanfrage von der AMS-Konsole aus und geben Sie die Details an, die zum Hinzufügen des Identitätsanbieters erforderlich sind:
   - AccountId des Kontos, in dem der neue Identitätsanbieter erstellt wird.
   - Der Name des gewünschten Identitätsanbieters, falls nicht angegeben, ist der Standard customer-saml. In der Regel muss dieser mit den Einstellungen übereinstimmen, die in Ihrem Federation Provider konfiguriert sind.
   - Geben Sie bei vorhandenen Konten an, ob der neue Identitätsanbieter an alle vorhandenen Konsolenrollen weitergegeben werden soll, oder geben Sie eine Liste der Rollen an, die dem neuen Identitätsanbieter vertrauen sollten.
   - Hängen Sie die von Ihrem Federation Agent exportierte Metadaten-XML-Datei als Dateianhang an die Serviceanfrage an.
2. Erstellen Sie mit demselben Konto, in dem Sie die Serviceanfrage erstellt haben, einen neuen RFC mit der CT-ID ct-1e1xtak34nx76 (Management | Other | Other | Create) mit den folgenden Informationen.
   - <Name>Titel: „Integrierter SAML-IDP für Konto < >“. AccountId
   - AccountId des Kontos, in dem der Identitätsanbieter erstellt wird.
   - Name des Identitätsanbieters.
   - Für bestehende Konten: Ob der Identitätsanbieter auf alle vorhandenen Konsolenrollen übertragen werden soll, oder die Liste der Rollen, die dem neuen Identitätsanbieter vertrauen sollen.
   - Fall-ID der in Schritt 1 erstellten Serviceanfrage, an die die XML-Metadatendatei angehängt ist.

Überprüfen Sie den Konsolenzugriff

Gehen Sie wie folgt vor, sobald Sie mit ADFS eingerichtet sind und über die AMS-URL verfügen, die Sie für die Authentifizierung verwenden möchten.

Mit einer Active Directory Federated Service (ADFS) -Konfiguration können Sie die folgenden Schritte ausführen:

1. Öffnen Sie ein Browserfenster und rufen Sie die Anmeldeseite auf, die Ihnen für Ihr Konto zur Verfügung gestellt wurde. Die IdpInitiatedSignOnADFS-Seite für Ihr Konto wird geöffnet.
2. Wählen Sie das Optionsfeld neben Auf einer der folgenden Websites anmelden aus. Die Auswahlliste für die Anmeldeseite wird aktiv.
3. Wählen Sie die Website signin.aws.amazon.com aus und klicken Sie auf Anmelden. Optionen für die Eingabe Ihrer Anmeldeinformationen werden geöffnet.
4. Geben Sie Ihre CORP-Anmeldeinformationen ein und klicken Sie auf Anmelden. Das AWS Management Console wird geöffnet.
5. Fügen Sie die URL der AMS-Konsole in die Adressleiste ein und drücken Sie die Eingabetaste. Die AMS-Konsole wird geöffnet.

API-Zugriff verifizieren

AMS verwendet die AWS-API mit einigen AMS-spezifischen Vorgängen, über die Sie in der AMS-API-Referenz nachlesen können.

AWS bietet mehrere SDKs , auf die Sie unter Tools für Amazon Web Services zugreifen können. Wenn Sie kein SDK verwenden möchten, können Sie direkte API-Aufrufe tätigen. Informationen zur Authentifizierung finden Sie unter Signieren von AWS-API-Anfragen. Wenn Sie kein SDK verwenden oder direkte HTTP-API-Anfragen stellen, können Sie AMS CLIs for Change Management (CM) und SKMS verwenden.

Installieren Sie das AMS CLIs

Ein Beispiel für die Installation der AWS Managed Services (AMS) CLI zur Verwendung mit SAML finden Sie unterAnhang: ActiveDirectory Federation Services (ADFS) -Anspruchsregel und SAML-Einstellungen.

Wenn Sie temporären Zugriff benötigen, um die AWS Managed Services (AMS) zu erhalten und zu installieren SDKs, finden Sie weitere Informationen unter Temporärer Zugriff auf die AMS-Konsole.

> **Note**
>
> Für dieses Verfahren benötigen Sie Administratoranmeldedaten.

Die AWS-CLI ist eine Voraussetzung für die Nutzung der AWS Managed Services (AMS) CLIs (Change Management und SKMS).

1. Informationen zur Installation der AWS-CLI finden Sie unter Installation der AWS-Befehlszeilenschnittstelle und folgen Sie den entsprechenden Anweisungen. Beachten Sie, dass sich unten auf dieser Seite Anweisungen zur Verwendung verschiedener Installationsprogramme befinden: Linux, MS Windows, macOS, Virtual Environment, Bundled Installer (Linux, macOS oder Unix).

   Führen Sie nach der Installation den Befehl aus, `aws help` um die Installation zu überprüfen.
2. Sobald die AWS-CLI installiert ist, laden Sie zur Installation oder zum Upgrade der AMS CLI entweder die AMS CLI- oder die AMS SDK-Distributionsdatei herunter und entpacken Sie sie. Sie können über den Link Developer's Resources im linken Navigationsbereich der AMS-Konsole auf die AMS-CLI-Distributionsdateien zugreifen.
3. Die README-Datei enthält Anweisungen für jede Installation.

   Öffnen Sie entweder:

   - CLI zip: Stellt nur die AMS-CLI bereit.
   - SDK-Zip: Stellt das gesamte AMS APIs und die AMS-CLI bereit.

   Führen Sie für Windows das entsprechende Installationsprogramm aus (nur 32- oder 64-Bit-Systeme):

   - 32 Bit: ManagedCloudAPI_x86.msi
   - 64 Bit: ManagedCloudAPI_x64.msi

   Führen Sie für Mac/Linux die Datei mit dem Namen: AWSManagedServices_InstallCLI.sh aus, indem Sie diesen Befehl ausführen:. `sh AWSManagedServices_InstallCLI.sh` Beachten Sie, dass sich die Verzeichnisse amscm und amsskms und ihr Inhalt im selben Verzeichnis wie die .sh-Datei befinden müssen. AWSManagedServices_InstallCLI

4. Wenn Ihre Unternehmensanmeldedaten über den Verbund mit AWS (die AMS-Standardkonfiguration) verwendet werden, müssen Sie ein Tool zur Verwaltung von Anmeldeinformationen installieren, das auf Ihren Verbundservice zugreifen kann. Sie können beispielsweise diesen AWS-Sicherheitsblog How to Implementation Federated API and CLI Access Using SAML 2.0 and AD FS verwenden, um Hilfe bei der Konfiguration Ihrer Tools zur Verwaltung Ihrer Anmeldeinformationen zu erhalten.
5. Führen Sie nach der Installation die Befehle und Optionen aus `aws amscm help` und sehen Sie `aws amsskms help` sich diese an.

> **Note**
>
> Die AMS-CLI muss installiert sein, damit diese Befehle funktionieren. Um die AMS-API oder CLI zu installieren, rufen Sie die Seite Entwicklerressourcen der AMS-Konsole auf. Referenzmaterial zur AMS CM API oder AMS SKMS API finden Sie im Abschnitt AMS-Informationsressourcen im Benutzerhandbuch. Möglicherweise müssen Sie eine `--profile` Option für die Authentifizierung hinzufügen, `aws amsskms` *`ams-cli-command`* `--profile SAML` z. B. Möglicherweise müssen Sie die `--region` Option auch hinzufügen, da allen AMS-Befehlen beispielsweise us-east-1 ausgeht. `aws amscm` *`ams-cli-command`* `--region=us-east-1`

Planung von AMS-Backups auf VPC-Ebene

Die Backup-Planung von AWS Managed Services (AMS) in der VPC, der die Ziel-Instances zugewiesen sind, wird während der Kontoerstellung mit einem Standard-Tag im VPC-Erstellungsschema erstellt. Das Backup-System plant die Ausführung der Snapshots in Abhängigkeit von diesem VPC-Tag. Der Zeitplan kann geändert werden, indem eine Serviceanfrage erstellt wird. Weitere Informationen finden Sie unter VPC-Tag und Standardeinstellungen.

Informationen zu den Standardeinstellungen für Backups finden Sie unter Grundlegendes zu AMS-Standardwerten

SALZ: Standardeinstellungen

Ihr AWS Managed Services (AMS) -Netzwerk ist auf standardisierte Weise mit Standardeinstellungen für die meisten Services konfiguriert.

In diesem Abschnitt werden die Standardeinstellungen beschrieben, die AMS für Sicherheit, Zugriff, Überwachung, Protokollierung, Kontinuität sowie Patching und Verwaltung verwendet.

Ein Beispiel für Infrastrukturkosten finden Sie unter Grundkomponenten.

Firewallregeln finden Sie in Richten Sie Ihre Firewall ein

Endpunktsicherheit (EPS)

Zu den Ressourcen, die Sie in Ihrer AMS Advanced-Umgebung bereitstellen, gehört automatisch die Installation eines Endpoint Security (EPS) -Überwachungsclients. Dieser Prozess stellt sicher, dass die von AMS Advanced verwalteten Ressourcen rund um die Uhr überwacht und unterstützt werden. Darüber hinaus überwacht AMS Advanced alle Agentenaktivitäten, und es wird ein Vorfall ausgelöst, wenn ein Sicherheitsereignis erkannt wird.

> **Note**
>
> Sicherheitsvorfälle werden als Vorfälle behandelt. Weitere Informationen finden Sie unter Reaktion auf Vorfälle.

Endpoint Security bietet Anti-Malware-Schutz, insbesondere werden die folgenden Aktionen unterstützt:

- EC2 Instanzen werden bei EPS registriert
- EC2 Instanzen werden von EPS abgemeldet
- EC2 Instanzen Anti-Malware-Schutz in Echtzeit
- Vom EPS-Agenten initiierter Heartbeat
- EPS stellt die Datei unter Quarantäne wieder her
- EPS-Ereignisbenachrichtigung
- EPS-Berichterstattung

AMS Advanced verwendet Trend Micro für Endpoint Security (EPS). Dies sind die EPS-Standardeinstellungen. Weitere Informationen über Trend Micro finden Sie im Trend Micro Deep Security Help Center. Beachten Sie, dass Links, die nicht von Amazon stammen, sich ändern können, ohne uns darüber in Kenntnis zu setzen.

Die Standardeinstellungen für AMS Advanced Multi-Account landing zone (MALZ) werden in den folgenden Abschnitten beschrieben. Informationen zu den nicht standardmäßigen EPS-Einstellungen für AMS Multi-Accounts Landing Zone finden Sie unter AMS Advanced Multi-Account Landing Zone EPS-Standardeinstellungen.

> **Note**
>
> Sie können Ihr eigenes EPS mitbringen. Weitere Informationen finden Sie unter AMS Bring your own EPS.

Allgemeine EPS-Einstellungen

Allgemeine Netzwerkeinstellungen für Endpoint Security.

EPS-Standardeinstellungen

Einstellung	Standard
Firewall-Ports (Sicherheitsgruppe der Instanzen)	Bei EPS Deep Security Manager-Agenten (DSMs) muss Port 4120 für die Agent/Relay Kommunikation mit Manager und Port 4119 für die Manager-Konsole geöffnet sein. Bei EPS-Relays muss Port 4122 für die Kommunika tion zu Relay geöffnet sein. Manager/Agent Für die eingehende Kommunikation zwischen Kundeninstanzen sollten keine spezifisc hen Ports geöffnet sein, da die Agenten alle Anfragen initiieren.
Richtung der Kommunikation	Agent/Appliance wurde initiiert
Taktintervall	Zehn Minuten
Anzahl der verpassten Herzschläge vor einer Warnung	Zwei
Maximal zulässige Abweichung (Differenz) zwischen Serverzeiten	Unbegrenzt

Einstellung	Standard
Löst Offlinefehler für inaktive (registrierte, aber nicht online) virtuelle Maschinen aus	Nein
Standardrichtlinie	Basisrichtlinie (im Folgenden beschrieben)
Aktivierung mehrerer Computer mit demselben Hostnamen	Ist erlaubt
Es werden Warnmeldungen für ausstehende Updates ausgelöst	Nach sieben Tagen
Zeitplan aktualisieren	AMS strebt einen monatlichen Veröffent lichungszyklus für die Software-Updates für Trend Micro Deep Security Manager (DSM) / Deep Security Agent (DSA) an. AMS hält jedoch kein SLA für Updates ein. Updates werden während einer Bereitstellung flottenweit von AMS-Entwicklerteams durchgeführt. DSA/DSA-Updates werden in Trend Micro DSM Systemereignissen protokolliert, die AMS standardmäßig 13 Wochen lang lokal speichert . Die Herstellerdokumentation finden Sie im Trend Micro Deep Security Help Center unter Systemereignisse. Protokolle werden auch in die Protokollgruppe/aws/ams/eps/var/log/ DSM.log in Amazon CloudWatch exportiert.
Quelle aktualisieren	Trend Micro Update Server (https://ipv6-iaus .trendmicro.com/iau_server.dll/)
Löschen von Ereignis- oder Protokolldaten	Ereignisse und Protokolle werden nach sieben Tagen aus der DSM-Datenbank gelöscht.
Die Versionen der Agentensoftware werden gespeichert	Bis zu fünf

Einstellung	Standard
Die neuesten Regelaktualisierungen finden statt	Bis zu zehn
Speicherung von Protokollen	Standardmäßig werden Protokolldateien sicher in Amazon S3 gespeichert. Sie können sie jedoch auch in Amazon Glacier archivieren, um Audit- und Compliance-Anforderungen zu erfüllen.

Grundlegende Richtlinie

Standardeinstellungen der Basisrichtlinie für Endpoint Security.

EPS-Basisrichtlinie

Einstellung	Standard
Aktivierte Module	Anti-Malware
Deaktivierte Module	Web Reputation
	Firewall
	Schutz vor Eindringlingen
	Überwachung der Integrität
	Inspektion von Protokollen
	Kontrolle von Anwendungen

Anti-Malware

Anti-Malware-Einstellungen für Endpoint Security.

Standardeinstellungen für EPS-Anti-Malware

Einstellung	Standard	Hinweise
Echtzeit-Scan	Alles scannen Jeden Day/All Tag (24 Stunden)	Alle verdächtigen Viren unter Quarantäne stellen. Aktivierung IntelliTrap und spyware/grayware Schutz. Spyware und Grayware lösen Anti-Malware aus und führen dazu, dass das Objekt unter Quarantäne gestellt wird.
Manueller Scan	Alles scannen	Muss angefordert werden, dann folgt die Standardkonfiguration für den Echtzeitscan.
Geplanter Scan	Alles scannen	Jeweils am letzten Sonntag im Monat, 6 Uhr morgens, festgelegt.
Intelligenter Schutz	Disabled	N/A
Dateien in Quarantäne	Trend Micro Deep Security Manager (DSM)	Etwa 1 GB Festplatte ist für die Quarantäne reserviert.
Scan-Beschränkung	Trend Micro DSM	Dateien aller Größen scannen.
Erlaubte Spyware oder Grayware	Keine	N/A

Einstellung	Standard	Hinweise
Benachrichtigung über ein lokales Ereignis	Ja	N/A

Sicherheitsgruppen

In AWS VPCs agieren AWS-Sicherheitsgruppen als virtuelle Firewalls und kontrollieren den Datenverkehr für einen oder mehrere Stacks (eine Instanz oder eine Reihe von Instances). Wenn ein Stack gestartet wird, wird er einer oder mehreren Sicherheitsgruppen zugeordnet, die festlegen, welcher Datenverkehr ihn erreichen darf:

- Für Stacks in Ihren öffentlichen Subnetzen akzeptieren die Standardsicherheitsgruppen Traffic von HTTP (80) und HTTPS (443) von allen Standorten (dem Internet). Die Stacks akzeptieren auch internen SSH- und RDP-Verkehr aus Ihrem Unternehmensnetzwerk und AWS-Bastionen. Diese Stacks können dann über jeden beliebigen Port ins Internet gelangen. Sie können auch in Ihre privaten Subnetze und andere Stacks in Ihrem öffentlichen Subnetz gelangen.
- Stacks in Ihren privaten Subnetzen können zu jedem anderen Stack in Ihrem privaten Subnetz austreten, und Instances innerhalb eines Stacks können vollständig über jedes Protokoll miteinander kommunizieren.

> **Important**
>
> Die Standardsicherheitsgruppe für Stacks in privaten Subnetzen ermöglicht es allen Stacks in Ihrem privaten Subnetz, mit anderen Stacks in diesem privaten Subnetz zu kommunizieren. Wenn Sie die Kommunikation zwischen Stacks innerhalb eines privaten Subnetzes einschränken möchten, müssen Sie neue Sicherheitsgruppen erstellen, die die Einschränkung beschreiben. Wenn Sie beispielsweise die Kommunikation mit einem Datenbankserver einschränken möchten, sodass die Stacks in diesem privaten Subnetz nur von einem bestimmten Anwendungsserver über einen bestimmten Port kommunizieren können, fordern Sie eine spezielle Sicherheitsgruppe an. Wie das geht, wird in diesem Abschnitt beschrieben.

Standardsicherheitsgruppen

MALZ

In der folgenden Tabelle werden die Standardeinstellungen für eingehende Sicherheitsgruppen (SG) für Ihre Stacks beschrieben. Die SG trägt den Namen „SentinelDefaultSecurityGroupPrivateOnly-VPC-ID“, wobei *ID* es sich um eine VPC-ID in Ihrem AMS-Landingzone-Konto mit mehreren Konten handelt. Der gesamte Datenverkehr darf über diese Sicherheitsgruppe nach "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly" ausgehen (der gesamte lokale Verkehr innerhalb von Stack-Subnetzen ist zulässig).

Jeglicher Datenverkehr darf von einer zweiten Sicherheitsgruppe "" nach 0.0.0.0/0 ausgehen. SentinelDefaultSecurityGroupPrivateOnly

> **Tip**
>
> Wenn Sie eine Sicherheitsgruppe für einen AMS-Änderungstyp wie EC2 Create oder OpenSearch Create Domain auswählen, würden Sie eine der hier beschriebenen Standardsicherheitsgruppen oder eine von Ihnen erstellte Sicherheitsgruppe verwenden. Sie finden die Liste der Sicherheitsgruppen pro VPC entweder in der EC2 AWS-Konsole oder in der VPC-Konsole.

Es gibt zusätzliche Standardsicherheitsgruppen, die für interne AMS-Zwecke verwendet werden.

AMS-Standardsicherheitsgruppen (eingehender Verkehr)

Typ	Protocol (Protokoll)	Port-Bereich	Quelle
Gesamter Datenverkehr	Alle	Alle	SentinelDefaultSecurityGroupPrivateOnly (schränkt ausgehenden Datenverkehr auf Mitglieder derselben Sicherheitsgruppe ein)
Gesamter Datenverkehr	Alle	Alle	SentinelDefaultSecurityGroupPrivateOnlyEgressAll (schränkt ausgehenden Verkehr nicht ein)

Typ	Protocol (Protokoll)	Port-Bereich	Quelle
HTTP, HTTPS, SSH, RDP	TCP	80/443 (Quelle 0.0.0.0/0) SSH- und RDP-Zugriff ist von Bastionen aus erlaubt	SentinelDefaultSecurityGroupPublic (schränkt den ausgehenden Verkehr nicht ein)
MALZ-Bastionen:			
SSH	TCP	22	SharedServices VPC CIDR und DMZ VPC CIDR sowie vom Kunden bereitgestelltes On-Premise-System CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
SALZ-Bastionen:			
SSH	TCP	22	mc-initial-garden- SG LinuxBastion
SSH	TCP	22	mc-initial-garden- LinuxBastion DMZSG
RDP	TCP	3389	mc-initial-garden- SG WindowsBastion
RDP	TCP	3389	mc-initial-garden- WindowsBastion DMZSG

SALZ

In der folgenden Tabelle werden die Standardeinstellungen für eingehende Sicherheitsgruppen (Inbound Security Group, SG) für Ihre Stacks beschrieben. Die SG trägt den Namen "mc-initial-garden- SentinelDefaultSecurityGroupPrivateOnly -*ID*", wobei *ID* es sich um einen eindeutigen Bezeichner handelt. Der gesamte Datenverkehr darf über diese Sicherheitsgruppe nach "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly" ausgehen (der gesamte lokale Verkehr innerhalb von Stack-Subnetzen ist zulässig).

Der gesamte Datenverkehr darf von einer zweiten Sicherheitsgruppe "- -“ nach 0.0.0.0/0 ausgesendet werden. mc-initial-garden SentinelDefaultSecurityGroupPrivateOnlyEgressAll *ID*

> **Tip**
>
> Wenn Sie eine Sicherheitsgruppe für einen AMS-Änderungstyp wie EC2 Create oder OpenSearch Create Domain auswählen, würden Sie eine der hier beschriebenen Standardsicherheitsgruppen oder eine von Ihnen erstellte Sicherheitsgruppe verwenden. Sie finden die Liste der Sicherheitsgruppen pro VPC entweder in der EC2 AWS-Konsole oder in der VPC-Konsole.

Es gibt zusätzliche Standardsicherheitsgruppen, die für interne AMS-Zwecke verwendet werden.

AMS-Standardsicherheitsgruppen (eingehender Verkehr)

Typ	Protocol (Protokoll)	Port-Bereich	Quelle
Gesamter Datenverkehr	Alle	Alle	SentinelDefaultSecurityGroupPrivateOnly (schränkt ausgehenden Datenverkehr auf Mitglieder derselben Sicherheitsgruppe ein)
Gesamter Datenverkehr	Alle	Alle	SentinelDefaultSecurityGroupPrivateOnlyEgressAll (schränkt ausgehenden Verkehr nicht ein)
HTTP, HTTPS, SSH, RDP	TCP	80/443 (Quelle 0.0.0.0/0) SSH- und RDP-Zugriff ist von Bastionen aus erlaubt	SentinelDefaultSecurityGroupPublic (schränkt den ausgehenden Verkehr nicht ein)
MALZ-Bastionen:			

Typ	Protocol (Protokoll)	Port-Bereich	Quelle
SSH	TCP	22	SharedServices VPC CIDR und DMZ VPC CIDR sowie vom Kunden bereitgestelltes On-Premise-System CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
SALZ-Bastionen:			
SSH	TCP	22	mc-initial-garden- SG LinuxBastion
SSH	TCP	22	mc-initial-garden- LinuxBastion DMZSG
RDP	TCP	3389	mc-initial-garden- SG WindowsBastion
RDP	TCP	3389	mc-initial-garden- WindowsBastion DMZSG

Sicherheitsgruppen erstellen, ändern oder löschen

Sie können benutzerdefinierte Sicherheitsgruppen anfordern. In Fällen, in denen die Standardsicherheitsgruppen nicht den Anforderungen Ihrer Anwendungen oder Ihrer Organisation entsprechen, können Sie neue Sicherheitsgruppen ändern oder erstellen. Eine solche Anfrage würde als genehmigungspflichtig erachtet und vom AMS-Betriebsteam geprüft.

Um eine Sicherheitsgruppe außerhalb von Stacks zu erstellen und einen RFC mit dem `Deployment | Advanced stack components | Security group | Create (review required)` Änderungstyp (VPCsct-1oxx2g2d7hc90) einzureichen.

Verwenden Sie für Änderungen an Active Directory (AD) -Sicherheitsgruppen die folgenden Änderungstypen:

- Um einen Benutzer hinzuzufügen: Senden Sie einen RFC mit Management | Directory Service | Benutzer und Gruppen | Benutzer zur Gruppe hinzufügen [ct-24pi85mjtza8k]
- Um einen Benutzer zu entfernen: Senden Sie einen RFC mit Management | Directory Service | Benutzer und Gruppen | Benutzer aus Gruppe entfernen [ct-2019s9y3nfml4]

> **Note**
>
> Wenn Sie „Überprüfung erforderlich“ verwenden CTs, empfiehlt AMS, die ASAP-Scheduling-Option zu verwenden (wählen Sie ASAP in der Konsole, lassen Sie Start- und Endzeit leer in der API/CLI), da diese einen AMS-Operator CTs erfordern, der den RFC überprüft und möglicherweise mit Ihnen kommuniziert, bevor er genehmigt und ausgeführt werden kann. Wenn Sie diese einplanen, achten Sie darauf RFCs, dass Sie mindestens 24 Stunden einplanen. Wenn die Genehmigung nicht vor der geplanten Startzeit erfolgt, wird der RFC automatisch abgelehnt.

Suchen Sie nach Sicherheitsgruppen

Verwenden Sie die EC2 Konsole, um die Sicherheitsgruppen zu finden, die einem Stack oder einer Instance zugeordnet sind. Nachdem Sie den Stack oder die Instance gefunden haben, können Sie alle damit verbundenen Sicherheitsgruppen sehen.

Möglichkeiten, Sicherheitsgruppen in der Befehlszeile zu finden und die Ausgabe zu filtern, finden Sie unter `describe-security-groups`.

EC2 IAM-Instanzprofil

Ein Instanzprofil ist ein Container für eine IAM-Rolle, den Sie verwenden können, um Rolleninformationen an eine EC2 Instance zu übergeben, wenn die Instance gestartet wird.

MALZ

Es gibt zwei AMS-Standard-Instanzprofile, `customer-mc-ec2-instance-profile` und`customer-mc-ec2-instance-profile-s3`. Diese Instanzprofile bieten die in der folgenden Tabelle beschriebenen Berechtigungen.

Beschreibungen der Richtlinien

Profil	Richtlinien
`customer-mc-ec2-instance-profile`	`AmazonSSMManagedInstanceCore` : Ermöglicht Ec2-Instances die Verwendung des SSM-Agenten.

Profil	Richtlinien
	`AMSInstanceProfileLoggingPolicy` : Ermöglicht Ec2-Instances, Protokolle an S3 zu übertragen und. CloudWatch
	`AMSInstanceProfileManagementPolicy` : Ermöglicht Ec2-Instances das Ausführen von Startaktionen, z. B. den Beitritt zu Active Directory.
	`AMSInstanceProfileMonitoringPolicy` : Ermöglicht Ec2-Instances, Ergebnisse an die AMS-Überwachungsdienste zu melden.
	`AMSInstanceProfilePatchPolicy` : Ermöglicht Ec2-Instances den Empfang von Patches.
`customer-mc-ec2-instance-profile-s3`	`AMSInstanceProfileBYOEPSPolicy` : Ermöglicht Ec2-Instances die Verwendung von AMS Bring Your Own EPS.
	`AMSInstanceProfileLoggingPolicy` : Ermöglicht Ec2-Instances, Logs an S3 zu übertragen und. CloudWatch
	`AMSInstanceProfileManagementPolicy` : Ermöglicht Ec2-Instances das Ausführen von Startaktionen, z. B. den Beitritt zu Active Directory.
	`AMSInstanceProfileMonitoringPolicy` : Ermöglicht Ec2-Instances, Ergebnisse an die AMS-Überwachungsdienste zu melden.
	`AMSInstanceProfilePatchPolicy` : Ermöglicht Ec2-Instances den Empfang von Patches.
	`AMSInstanceProfileS3WritePolicy` : Ermöglicht den Zugriff von Ec2-Instances read/write auf Kunden-S3-Buckets.

SALZ

Es gibt ein AMS-Standard-Instanzprofil`customer-mc-ec2-instance-profile`, das Berechtigungen gemäß der IAM-Instanzrichtlinie gewährt. `customer_ec2_instance_profile_policy` Dieses Instanzprofil stellt die in der folgenden Tabelle beschriebenen Berechtigungen bereit. Das Profil gewährt den Anwendungen, die auf der Instanz ausgeführt werden, Berechtigungen, nicht den Benutzern, die sich bei der Instanz anmelden.

Richtlinien enthalten häufig mehrere Anweisungen, wobei jede Anweisung Berechtigungen für eine andere Gruppe von Ressourcen oder unter einer bestimmten Bedingung erteilt.

CW = CloudWatch. ARN = Amazon-Ressourcenname. * = Platzhalter (beliebig).

EC2 Standardberechtigungen für das Profil einer IAM-Instanz

CW =. CloudWatch ARN = Amazon-Ressourcenname. * = Platzhalter (beliebig).			
Richtlinienanweisung	Auswirkung	Aktionen	Beschreibung und Ressource (ARN)
Amazon Elastic Compute Cloud (Amazon EC2)			
EC2 Nachrichtenaktionen	Sobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf	AcknowledgeMessage, DeleteMessage, FailMessage, GetEndpoint, GetMessages, SendReply	Ermöglicht EC2 Systems Manager Manager-Messaging-Aktionen in Ihrem Konto.
Ec2 Beschreiben	Sobald Sie die Details auf dieser	* (Alle)	Ermöglicht der Konsole, die Konfigurationsdetails eines EC2 in Ihrem Konto anzuzeigen.

CW =. CloudWatch ARN = Amazon-Ressourcenname. * = Platzhalter (beliebig).			
Richtlinienanweisung	Auswirkung	Aktionen	Beschreibung und Ressource (ARN)
	Seite überprüf haben, klicken Sie auf		
Ich bin Get Role ID	Sobald Sie die Details auf dieser Seite überprüf haben, klicken Sie auf	GetRole	Ermöglicht EC2 das Abrufen Ihrer IAM-ID von `aws:iam::*:role/customer-*` und. `aws:iam::*:role/customer_*`
Instanz zum Hochladen von Protokollereignissen	Sobald Sie die Details auf dieser Seite überprüf haben, klicken Sie auf	Protokollgruppe erstellen	Ermöglicht das Erstellen von Protokollen in: `aws:logs:*:*:log-group:i-*`
		Log-Stream erstellen	Ermöglicht das Streamen von Protokollen nach: `aws:logs:*:*:log-group:i-*`

CW =. CloudWatch ARN = Amazon-Ressourcenname. * = Platzhalter (beliebig).			
Richtlinienanweisung	Auswirkung	Aktionen	Beschreibung und Ressource (ARN)
CW Für MMS	Sobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf	DescribeAlarms, PutMetricAlarm, PutMetricData	Ermöglicht das CloudWatch Abrufen von Alarmen in Ihrem Konto. Ermöglicht CW, einen Alarm zu erstellen oder zu aktualisieren und ihn der angegebenen Metrik zuzuordnen. Ermöglicht CW, metrische Datenpunkte in Ihrem Konto zu veröffentlichen.
Ec2-Tags	Sobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf	CreateTags, DescribeTags,	Ermöglicht das Hinzufügen, Überschreiben und Beschreiben von Tags für die angegebenen Instanzen in Ihrem Konto.
CW-Protokolle explizit ablehnen	Deny	DescribeLogStreams, FilterLogEvents, GetLogEvents	Verbietet das Auflisten, Filtern oder Abrufen der Protokollstreams für: `aws:logs:*:*:log-group:/mc/*`
Amazon EC2 Simple Systems Manager (SSM)			

CW =. CloudWatch ARN = Amazon-Ressourcenname. * = Platzhalter (beliebig).			
Richtlinienanweisung	Auswirkung	Aktionen	Beschreibung und Ressource (ARN)
SSM-Aktionen	Sobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf	DescribeAssociation, GetDocument, ListAssociations, UpdateAssociationStatus, UpdateInstanceInformation	Ermöglicht eine Vielzahl von SSM-Funktionen in Ihrem Konto.
SSM-Zugriff in S3	Sobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf	GetObject, PutObject, AbortMultipartUpload, ListMultipartUploadPorts, ListBucketMultipartUploads	Ermöglicht dem SSM auf dem, Objekte abzurufen und EC2 zu aktualisieren und den Upload eines mehrteiligen Objekts zu beenden und die Ports und Buckets aufzulisten, die für mehrteilige Uploads verfügbar sind. `aws:s3:::mc-*-internal-*/aws/ssm*`
Amazon EC2 Simple Storage Service (S3)			

CW =. CloudWatch ARN = Amazon-Ressourcenname. * = Platzhalter (beliebig).			
Richtlinienanweisung	Auswirkung	Aktionen	Beschreibung und Ressource (ARN)
Objekt in S3 abrufen	Sobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf	Get Auflisten	Ermöglicht EC2 Anwendungen, Objekte in S3-Buckets in Ihrem Konto abzurufen und aufzulisten.
Verschlüsselter S3-Zugriff auf das Kundenprotokoll	Sobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf	PutObject	Ermöglicht EC2 Anwendungen das Aktualisieren von Objekten in `aws:s3:::mc-*-logs-*/encrypted/app/*`

CW =. CloudWatch ARN = Amazon-Ressourcenname. * = Platzhalter (beliebig).			
Richtlinienanweisung	Auswirkung	Aktionen	Beschreibung und Ressource (ARN)
Patch-Daten-Put-Objekt S3	Sobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf	PutObject	Ermöglicht EC2 Anwendungen das Hochladen von Patching-Daten in Ihre S3-Buckets unter `aws:s3:::awsms-a*-patch-data-*`
Eigene Logs auf S3 hochladen	Sobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf	PutObject	Ermöglicht EC2 Anwendungen das Hochladen benutzerdefinierter Protokolle auf: `aws:s3:::mc-a*-logs-*/aws/instances/*/${aws:userid}/*`

CW =. CloudWatch ARN = Amazon-Ressourcenname. * = Platzhalter (beliebig).			
Richtlinienanweisung	Auswirkung	Aktionen	Beschreibung und Ressource (ARN)
MC-Namespace-S3-Protokolle explizit verweigern	Deny	GetObject* Eingeben*	Verbietet EC2 Anwendungen das Abrufen oder Platzieren von Objekten von oder nach: `aws:s3:::mc-*-logs-*/encrypted/mc*` , `aws:s3:::mc-*-logs-*/mc/*`, `aws:s3:::mc-a*-logs-*-audit/*`
S3-Löschen ausdrücklich verweigern	Deny	* (alle)	Verbietet EC2 Anwendungen, Aktionen an Objekten durchzuführen in: `aws:s3:::mc-a*-logs-*/*` , `aws:s3:::mc-a*-internal-*/*` ,
S3-CFN-Bucket explizit ablehnen	Deny	Delete*	Verbietet EC2 Anwendungen das Löschen von Objekten aus: `aws:s3:::cf-templates-*`
List-Bucket S3 explizit ablehnen	Deny	ListBucket	Verbietet das Auflisten verschlüsselter Objekte, Audit-Log-Objekte oder reservierter Objekte (MC) von: `aws:s3:::mc-*-logs-*`
AWS Secrets Manager bei Amazon EC2			

CW =. CloudWatch ARN = Amazon-Ressourcenname. * = Platzhalter (beliebig).			
Richtlinienanweisung	Auswirkung	Aktionen	Beschreibung und Ressource (ARN)
Zugang zu Trend Cloud One Secrets	Sobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf	GetSecretValue	Ermöglicht Amazon EC2 den Zugriff auf geheime Daten für die Trend Cloud One-Migration: `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-id*` , `arn:aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-activation-token*` , `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-id*` , `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-guid*`
AWS Key Management Service bei Amazon EC2			

CW =. CloudWatch ARN = Amazon-Ressourcenname. * = Platzhalter (beliebig).			
Richtlinienanweisung	Auswirkung	Aktionen	Beschreibung und Ressource (ARN)
Trend Cloud One Entschlüsselungsschlüssel	Sobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf	Decrypt	Erlauben EC2 Sie Amazon, den AWS KMS Schlüssel mit dem Aliasnamen/ams/eps/cloudone-migration zu entschlüsseln `arn:aws:kms:*:*:alias/ams/eps/cloudone-migration`

Wenn Sie mit den Amazon IAM-Richtlinien nicht vertraut sind, finden Sie wichtige Informationen unter Überblick über die IAM-Richtlinien.

> **Note**
>
> Richtlinien enthalten oft mehrere Aussagen, wobei jede Erklärung Berechtigungen für eine andere Gruppe von Ressourcen oder unter einer bestimmten Bedingung erteilt.

Standardwerte für überwachte Metriken

Die folgende Tabelle zeigt, was überwacht wird und welche Standardschwellenwerte für Warnmeldungen gelten. Sie können die Standardwerte mit einem Change Management Request for Change (RFC) ändern.

> **Note**
>
> CloudWatch hat am 1. November 2016 die erweiterte Aufbewahrung von Kennzahlen eingeführt. Weitere Informationen finden Sie unter CloudWatch Limits.

Warnmeldungen aus der Basisüberwachung

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
Bei Warnmeldungen mit Sternchen (*) bewertet AMS proaktiv die Auswirkungen und behebt sie, wenn möglich. Wenn eine Behebung nicht möglich ist, erstellt AMS einen Vorfall. Wenn die Automatisierung das Problem nicht behebt, informiert AMS Sie über den Vorfall und ein AMS-Techniker wird hinzugezogen. Darüber hinaus können diese Benachrichtigungen direkt an Ihre E-Mail-Adresse gesendet werden (sofern Sie sich für das Direct-Customer-Alerts SNS-Thema entschieden haben).			
Application Load Balancer (ALB) - Instanz	Nein	RejectedConnectionCount Summe > 0 für 1 Minute, 5 aufeinanderfolgende Male.	CloudWatch Alarm, wenn die Anzahl der Verbindungen, die abgelehnt wurden, weil der Load Balancer sein Maximum erreicht hat, angezeigt wird.
Ziel des Application Load Balancer (ALB)	Nein	TargetConnectionErrorCount Summe > 0 für 1 Minute, 5 aufeinanderfolgende Male.	CloudWatch Alarm, wenn die Anzahl der Verbindungen zwischen dem Load Balancer und den registrierten Instances nicht erfolgreich hergestellt wurde.
EC2 Amazon-Instanz — Windows	Nein	SecureChannelFailure > 0,0 für 10 der letzten 15 Datenpunkte.	CloudWatch Alarm auf Windows-Instanzen, um zu warnen, wenn Secure a Channel-Verbindung fehlgeschlagen ist.
Aurora-Instanz	Nein	CPUUtilization > 85% für 5 Minuten, 2 Mal hintereinander.	CloudWatch Alarm.
AWS Backup	Ja	DeleteRecoveryPoint Ein unerwarteter IAM-Rollenprinzipal oder ein IAM-Benutzerprinzipal	CloudWatch Ereignis. Wird ausgelöst, wenn ein Backup-Wiederherstellungspunkt gelöscht wird.

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
		hat einen AWS Backup Wiederherstellungspunkt gelöscht.	
AWS Outposts	Ja	AMSOutpostsInstanceFamilyCapacityAvailability InstanceFamilyCapacityAvailability = 80% für 5 Minuten, 12 Mal hintereinander.	CloudWatch Alarm bei Verfügbarkeit der AWS Outposts Ressource durch die Instance-Familie.
		AMSOutpostsInstanceTypeCapacityAvailability TypeCapacityAvailability = 80% für 5 Minuten, 12 aufeinanderfolgende Male.	CloudWatch Alarm bei Kapazitätsverfügbarkeit der AWS Outposts Ressource vom Instanztyp.
		AMSOutpostsConnectedStatusConnectedStatus < 1 für 5 Minuten, 1 Mal hintereinander.	CloudWatch Alarm bei AWS Outposts Service Link-Verbindung, weniger als 1 Zählung ist beeinträchtigt.
		AMSOutpostsCapacityExceptionCapacityExceptions 0 für 5 Minuten, 1 Mal hintereinander.	CloudWatch Alarm bei Fehlern mit unzureichender Kapazität, z. B. bei AWS Outposts Starts für eine Ressource .
EC2 Instanz - alles OSs	Nein	CPUUtilization* >= 95% für 5 Minuten, 6 aufeinanderfolgende Male.	CloudWatch Alarm. Eine hohe CPU-Auslastung ist ein Indikator für eine Änderung des Anwendungsstatus, z. B. Deadlocks, Endlosschleifen, böswillige Angriffe und andere Anomalien.

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
		StatusCheckFailed > 0 für 5 Minuten, dreimal hintereinander.	CloudWatch Alarm.
		Nutzung des Root-Volumes >= 95% für 5 Minuten, 6 aufeinanderfolgende Male.	
		Nutzung von Volumes ohne Root-Rechte > 85% für 5 Minuten, 2 Mal hintereinander. Standardmäßig deaktiviert; weitere Informationen finden Sie unter https://docs.aws.amazon.com/managedservices/latest/ctref/management-monitoring-cloudwatch-enable-non-root-volumes-monitoring.html#management-monitoring-cloudwatch-enable-non-root-volumes-monitoring-info.	
		Freier Speicher * MemoryFree < 5% für 5 Minuten, 6 Mal hintereinander.	
	Ja	EPS-Malware Auf der Instanz wurde Malware gefunden.	CloudWatch Ereignis.

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
EC2 Amazon-Instanz — Linux	Nein	Inode-Nutzung des Root-Volumes Durchschnittlich >= 95% für 5 Minuten, 6 aufeinanderfolgende Male.	CloudWatch Alarm. Gilt nur für Linux-Instances.
		Kostenlos tauschen * Speicheraustausch < 5% für 5 Minuten, 6 Mal hintereinander.	
ElastiCache Cluster	Nein	CurrConnections = 65000	Dieser Alarm informiert AMS über das maximale Verbindungslimit eines ElastiCache Hosts. CloudWatch Alarm. Wenn Sie diesen Schwellenwert aktualisieren möchten, wenden Sie sich an den AMS-Support.

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
ElastiCache Knoten	Nein	CPUUtilization Durchschnitt > vordefinierter Wert für 15 Minuten, 2 aufeinanderfolgende Male.	CloudWatch Alarm. Die Standardeinstellung ist 90. Bei Redis verwenden Sie je nach Instanztyp einen der folgenden Werte: • cache.t1.micro: 90% • cache.m1.small: 90% • cache.m1.medium: 90% • cache.m1.large: 45% • cache.m1.xlarge: 22,5% • cache.m2.xlarge: 45% • cache.m2.4xlarge: 11,25% • cache.c1.xlarge: 11,25% • cache.t2.micro: 90% • cache.t2.small: 90% • cache.t2.medium: 45% • cache.m3.medium: 90% • cache.m3.large: 45% • cache.m3.xlarge: 22,5% • cache.m3.2xgroß: 11,25% • cache.r3.large: 45% • cache.r3.xlarge: 22,5% • cache.r3.2xlarge: 11,25% • cache.r3.4xgroß: 5,62% • cache.r3.8xgroß: 2.8125%

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
ElastiCache Knoten — Memcached	Nein	SwapUsage maximal > 50.000.000 Byte für 5 Minuten, 5 aufeinanderfolgende Male.	CloudWatch Alarm. Gilt nur für Memcached.
OpenSearch Cluster	Nein	ClusterStatus.red Das Maximum ist >= 1 für 1 Minute, 1 Mal hintereinander. AMS ergreift proaktive Maßnahmen, um die betrieblichen Auswirkungen zu verringern, wenn diese Warnung ausgelöst wird.	CloudWatch Alarm. Mindestens ein primärer Shard und dessen Replikate sind keinem Knoten zugewiesen. Weitere Informationen finden Sie unter Status des roten Clusters.
OpenSearch Domäne	Nein	KMSKeyFehler >= 1 für 1 Minute, 1 Mal hintereinander.	CloudWatch Alarm. Der KMS-Verschlüsselungsschlüssel für die Verschlüsselung gespeicherter Daten in Ihrer Domäne ist deaktiviert. Reaktivieren Sie es, um den normalen Betrieb wiederherzustellen. Weitere Informationen finden Sie unter Verschlüsselung ruhender Daten für OpenSearch Service Service.
		ClusterStatus. gelb Das Maximum ist >= 1 für 1 Minute, 1 Mal hintereinander AMS ergreift proaktive Maßnahmen, um die betrieblichen Auswirkungen zu verringern, wenn diese Warnung ausgelöst wird.	Mindestens ein Replikat-Shard ist nicht einem Knoten zugewiesen. Weitere Informationen finden Sie unter Gelber Clusterstatus.

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
		FreeStorageSpace Der Mindestwert ist <= 20480 für 1 Minute, 1 Mal hintereinander AMS ergreift proaktive Maßnahmen, um die betrieblichen Auswirkungen zu verringern, wenn diese Warnung ausgelöst wird.	Ein Knoten in Ihrem Cluster hat nur noch 20 GiB freien Speicherplatz. Weitere Informationen finden Sie unter Mangel an verfügbarem Speicherplatz.
		ClusterIndexWritesBlocked >= 1 für 5 Minuten, 1 Mal hintereinander AMS ergreift proaktive Maßnahmen, um die betrieblichen Auswirkungen zu reduzieren, wenn diese Warnung ausgelöst wird.	Der Cluster blockiert Schreibanforderungen. Weitere Informationen finden Sie unter ClusterBlockException.
		Knoten Der Mindestwert ist < x für 1 Tag, 1 aufeinanderfolgende Zeit AMS ergreift proaktive Maßnahmen, um die betrieblichen Auswirkungen zu reduzieren, wenn diese Warnung ausgelöst wird.	x ist die Anzahl der Knoten in Ihrem Cluster. Dieser Alarm gibt an, dass mindestens ein Knoten in Ihrem Cluster für einen Tag nicht erreichbar war. Weitere Informationen finden Sie unter Fehlgeschlagene Clusterknoten.

Service	Sicherhe tswarnu	Name der Warnung und Auslösebe dingung	Hinweise
		CPUUtilization Der Durchschnitt liegt bei >= 80% für 15 Minuten, dreimal hintereinander AMS ergreift proaktive Maßnahmen , um die betrieblichen Auswirkungen zu verringern, wenn diese Warnung ausgelöst wird.	Eine 100-prozentige CPU-Auslastung ist üblich, aber dauerhaft hohe Durchschn ittswerte sind problematisch. Ziehen Sie die Verwendung von größeren Instance-Typen oder das Hinzufügen von Instances in Betracht.
		JVMMemoryDruck Der Höchstwert liegt bei > = 80% für 5 Minuten, dreimal hintereinander AMS ergreift proaktive Maßnahmen , um die betrieblichen Auswirkungen zu verringern, wenn diese Warnung ausgelöst wird.	Der Cluster könnte Fehler aufgrund von unzureichendem Speicherplatz erhalten, wenn die Nutzung zunimmt. Ziehen Sie eine vertikale Skalierun g in Betracht. Amazon ES verwendet die Hälfte des RAM einer Instance für den Java-Heap , bis zu einer Heap-Größe von 32 GiB. Sie können Instances bis zu 64 GiB RAM vertikal skalieren. Dann können Sie eine horizonta le Skalierung durchführen, indem Sie Instances hinzufügen.

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
		Meister CPUUtilization Der Durchschnitt liegt bei >= 50% für 15 Minuten, dreimal hintereinander AMS ergreift proaktive Maßnahmen, um die betrieblichen Auswirkungen zu verringern, wenn diese Warnung ausgelöst wird.	Erwägen Sie die Verwendung größerer Instance-Typen für Ihre dedizierten Master-Knoten. Aufgrund ihrer Rolle bei der Clusterstabilität und blue/green -bereitstellung sollten dedizierte Masterknoten eine geringere durchschnittliche CPU-Auslastung aufweisen als Datenknoten.
		Meistern JVMMemory Sie den Druck Der Höchstwert liegt bei >= 80% für 15 Minuten, 1 Mal hintereinander AMS ergreift proaktive Maßnahmen, um die betrieblichen Auswirkungen zu verringern, wenn diese Warnung ausgelöst wird.	Erwägen Sie die Verwendung größerer Instance-Typen für Ihre dedizierten Master-Knoten. Aufgrund ihrer Rolle bei der Clusterstabilität und blue/green -bereitstellung sollten dedizierte Masterknoten eine geringere durchschnittliche CPU-Auslastung aufweisen als Datenknoten.
OpenSearch Instanz	Nein	AutomatedSnapshotFailure Das Maximum ist >= 1 für 1 Minute, 1 Mal hintereinander.	CloudWatch Alarm. Ein automatisierter Snapshot ist fehlgeschlagen. Dieser Fehler ist häufig das Ergebnis eines roten Cluster-Integritätsstatus. Siehe Status des roten Clusters.
Elastic Load Balancing Balancing-Instanz	Nein	SurgeQueueLength > 100 für 1 Minute, 15 aufeinanderfolgende Male.	CloudWatch Alarm, wenn zu viele Anfragen noch weitergeleitet werden müssen.

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
		HTTPCode_ELB_5xx_Count Summe > 0 für 5 Minuten, 3 aufeinanderfolgende Male.	CloudWatch Alarm bei zu großer Anzahl von HTTP 5XX-Antwortcodes, die vom Load Balancer stammen.
		SpilloverCount > 1 für 1 Minute, 15 aufeinanderfolgende Male.	CloudWatch Alarm bei zu vielen Anfragen, die abgelehnt wurden, weil die Surge-Warteschlange voll ist.
GuardDuty Dienst	Ja	Nicht zutreffend; alle Ergebnisse (Bedrohungszwecke) werden überwacht. Jeder Befund entspricht einer Warnung. Änderungen der GuardDuty Ergebnisse. Zu solchen Änderungen gehören beispielsweise neu generierte Ergebnisse oder alle nachfolgenden Vorkommen dieser vorhandenen Ergebnisse.	Die Liste der unterstützten GuardDuty Befundtypen befindet sich unter GuardDuty Aktive Findingtypen.
Gesundheitswesen	Variiert	AWS Health Dashboard	Benachrichtigungen werden gesendet, wenn sich der Status von AWS Health Dashboard (AWS Health) -Ereignissen in Bezug auf die von AMS unterstützten Basisdienste ändert. Weitere Informationen finden Sie unter Unterstützte Dienste.

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
AWS Managed Microsoft AD	Nein	Active Directory-Status AWS Managed Microsoft AD Die Instanz sendet ein aktives Statusereignis.	Serviceereignis. Wird ausgegeben, wenn das Verzeichnis nach einem Ereignis normal funktioniert.
		Beeinträchtigter Verzeichnisstatus AWS Managed Microsoft AD Die Instanz sendet ein Ereignis mit dem Status eines beeinträchtigten Verzeichnisses.	Dienstereignis. Wird ausgegeben, wenn das Verzeichnis in einem heruntergestuften Zustand ausgeführt wird. Mindestens ein Problem wurde erkannt und vermutlich wird nicht bei allen Verzeichnisvorgängen die volle Leistungskapazität erreicht.
		Status des Verzeichnisses nicht funktionsfähig AWS Managed Microsoft AD Die Instanz sendet ein Statusereignis, das nicht funktioniert.	Dienstereignis. Wird ausgegeben, wenn das Verzeichnis nicht funktioniert. Alle Verzeichnisendpunkte haben Probleme gemeldet.
		Der Verzeichnisstatus wird gelöscht AWS Managed Microsoft AD Die Instanz sendet ein Ereignis zum Löschen des Verzeichnisstatus.	Dienstereignis. Wird ausgegeben, wenn das Verzeichnis gerade gelöscht wird.
		Verzeichnisstatus fehlgeschlagen AWS Managed Microsoft AD Die Instanz sendet ein fehlgeschlagenes Statusereignis.	Dienstereignis. Wird ausgegeben, wenn das Verzeichnis nicht erstellt werden konnte.

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
		RestoreFailed Status des Verzeichnisses AWS Managed Microsoft AD Die Instanz sendet ein Ereignis zum Status eines Verzeichnisses, bei dem die Wiederherstellung fehlgeschlagen ist.	Dienstereignis. Wird ausgegeben, wenn das Wiederherstellen des Verzeichnisses aus einem Snapshot fehlgeschlagen ist.
Amazon RDS-Instanz	Nein	Die Warnung „Niedriger Speicherplatz“ wird ausgelöst, wenn der zugewiesene Speicherplatz für die DB-Instance erschöpft ist.	RDS-EVENT-0007, Einzelheiten finden Sie unter Verwenden der Amazon RDS-Ereignisbenachrichtigung.
		DB-Instance schlägt fehl Die DB-Instance ist aufgrund einer inkompatiblen Konfiguration oder eines zugrunde liegenden Speicherproblems ausgefallen. Starten Sie a point-in-time-restore für die DB-Instance.	Serviceereignis. RDS-EVENT-0031, Amazon RDS-Ereigniskategorien und Ereignismeldungen.
		Es wurde kein Failover versucht Amazon RDS führt das angeforderte Failover nicht aus, da erst vor Kurzem ein Failover auf dieser DB-Instance erfolgt ist.	Serviceereignis. RDS-EVENT-0034, Amazon RDS-Ereigniskategorien und Ereignismeldungen.

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
		Ungültige Parameter der DB-Instance Beispielsweise konnte MySQL nicht gestartet werden, weil ein speicherbezogener Parameter für diese Instance-Klasse zu hoch gesetzt ist. Die Kundenaktion würde also darin bestehen, den Speicherparameter zu ändern und die DB-Instance neu zu starten.	Serviceereignis. RDS-EVENT-0035, Amazon RDS-Ereigniskategorien und Ereignismeldungen.
		Ungültige IDs Subnetz-DB-Instance Die DB-Instance befindet sich in einem inkompatiblen Netzwerk. Einige der angegebenen Subnetze IDs sind ungültig oder existieren nicht.	Dienstereignis. RDS-EVENT-0036, Amazon RDS-Ereigniskategorien und Ereignismeldungen.
		Fehler beim Lesen der Replikation der DB-Instance Bei der Read-Replikation ist ein Fehler aufgetreten. Weitere Informationen finden Sie in der Ereignismeldung. Informationen zur Behebung von Read Replica-Fehlern finden Sie unter Problembehandlung bei MySQL Read Replica-Problemen.	Serviceereignis. RDS-EVENT-0045, Amazon RDS-Ereigniskategorien und Ereignismeldungen.

Service	Sicherhe tswarnu	Name der Warnung und Auslösebe dingung	Hinweise
		Die Lesereplikation der DB-Instance wurde beendet Die Replikation auf der Read Replica wurde beendet.	Serviceereignis. RDS-EVENT -0057, Amazon RDS-Ereig niskategorien und Ereignism eldungen.
		Fehler beim Erstellen des Statspack-Benutzerkontos Fehler beim Erstellen des Statspack -Benutzerkontos PERFSTAT. Löschen Sie das Konto, bevor Sie die Statspack-Option hinzufügen.	Serviceereignis. RDS-EVENT -0058, Amazon RDS-Ereig niskategorien und Ereignism eldungen.
		Start der Wiederherstellung der DB-Instance Die SQL Server-DB-Instance stellt ihre Spiegelung wieder her. Die Leistung ist beeinträchtigt, bis die Spiegelung wiederhergestellt ist. Datenbank mit einem anderen Wiederherstellungsmodell als FULL gefunden. Das Wiederher stellungsmodell wurde wieder auf FULL umgestellt und die Wiederher stellung mit Spiegelung wurde gestartet. (<dbname>: <recovery model found>[,...]).	Serviceveranstaltung. RDS-EVENT-0066, Amazon RDS-Ereigniskategorien und Ereignismeldungen.
		Ein Failover für das DB-Cluster ist fehlgeschlagen.	RDS-EVENT-0069, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Mel dungen.

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
		S3-Bucket zur Wiederherstellung ungültiger Berechtigungen Die IAM-Rolle, die Sie zum Zugriff auf den Amazon S3-Bucket für die SQL Server-nativen Backups und Wiederherstellungen verwenden, ist falsch konfiguriert. Weitere Informationen finden Sie unter Einrichtung für systemeigenes Backup und Wiederherstellung.	Serviceereignis. RDS-EVENT-0081, Amazon RDS-Ereigniskategorien und Ereignismeldungen.
		Aurora konnte die Sicherungsdaten aus einem Amazon S3-Bucket nicht kopieren.	RDS-EVENT-0082, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
		Warnung bei niedrigem Speicherplatz, wenn die DB-Instance mehr als 90% des zugewiesenen Speichers verbraucht hat	RDS-EVENT-0089, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
		Benachrichtigungsdienst, wenn die Skalierung für den Aurora Serverless DB-Cluster fehlgeschlagen ist.	RDS-EVENT-0143, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
		Die DB-Instance hat den Status Ungültig. Es sind keine Aktionen erforderlich. Die Auto Scaling wird später erneut versucht.	RDS-EVENT-0219, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
		Die DB-Instance hat den Schwellenwert für den Speicher vollständig erreicht, und die Datenbank wurde heruntergefahren.	RDS-EVENT-0221, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
		Dieses Ereignis weist darauf hin, dass die automatische Skalierung des RDS-Instance-Speichers nicht skaliert werden kann. Es kann mehrere Gründe geben, warum die automatische Skalierung fehlgeschlagen ist.	RDS-EVENT-0223, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
		Das Auto Scaling von Speicher hat eine ausstehende Skalierungsspeicheraufgabe ausgelöst, die den maximalen Speicherschwellenwert erreichen würde.	RDS-EVENT-0224, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
		Der Speichertyp der DB-Instance ist der derzeit in der Availability Zone nicht verfügbar. Die Auto Scaling wird später erneut versucht.	RDS-EVENT-0237, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
		RDS konnte keine Kapazität für den Proxy bereitstellen, da in Ihren Subnetzen nicht genügend IP-Adressen verfügbar sind.	RDS-EVENT-0243, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.
		Der Speicherplatz für Ihr AWS-Konto hat das zulässige Speicherkontingent überschritten.	RDS-EVENT-0254, Einzelheiten finden Sie unter Amazon RDS-Event-Kategorien und Event-Meldungen.

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
		CPUUtilization Durchschnittliche CPU-Auslastung > 90% für 15 Minuten, 2 aufeinanderfolgende Male.	CloudWatch Alarm.
		DiskQueueDepth Die Summe ist > 75 für 1 Minute, 15 aufeinanderfolgende Male.	
		FreeStorageSpace Durchschnitt < 1.073.741.824 Byte für 5 Minuten, 2 aufeinanderfolgende Male.	
		SwapUsage Durchschnitt = 104.857.600 Byte für 5 Minuten, 2 aufeinanderfolgende Male.	
Amazon-Redshift-Cluster	Nein	RedshiftClusterStatus Der Zustand des Clusters, wenn er sich nicht im Wartungsmodus befindet, < 1 für 5 Minuten.	1 steht für einen fehlerfreien Cluster.

Service	Sicherheitswarnung	Name der Warnung und Auslösebedingung	Hinweise
Amazon Macie	Ja	Neu generierte Warnungen und Aktualisierungen vorhandener Warnungen. Macie stellt fest, dass sich die Ergebnisse geändert haben. Zu solchen Änderungen gehören beispielsweise neu generierte Ergebnisse oder alle nachfolgenden Vorkommen dieser vorhandenen Ergebnisse.	Amazon Macie Macie-Warnung. Eine Liste der unterstützten Macie-Warnungstypen finden Sie unter Analysieren von Amazon Macie Macie-Ergebnissen. Beachten Sie, dass Macie nicht für alle Konten aktiviert ist.

Standardeinstellungen für die Aufbewahrung und Rotation von Protokollen

In diesem Abschnitt werden die Standardeinstellungen für die AMS-Protokollverwaltung beschrieben. Weitere Informationen finden Sie unter Protokollverwaltung.

- Rotation = Protokollwechsel innerhalb der Instanzen
- Aufbewahrung = Zeitraum, in dem wir die Protokolle in Amazon CloudWatch Logs und Amazon Simple Storage Service (S3) aufbewahren

Die Protokolle werden nach Bedarf in CloudWatch Logs (Sie können dies konfigurieren) und in S3 aufbewahrt. Sie laufen nicht ab und werden nicht gelöscht und unterliegen der Lebensdauer des Dienstes. Detaillierte Informationen zur Haltbarkeit von S3 finden Sie unter Datenschutz in Amazon S3.

Sie können eine Änderung der Protokollspeicherung für alle Protokolle beantragen, mit Ausnahme von AWS CloudTrail Protokollen, die aus Prüfungs- und Sicherheitsgründen auf unbestimmte Zeit aufbewahrt werden.

Die Protokollrotation wird innerhalb der Instanzen konfiguriert. Standardmäßig rotieren Betriebssystem- und Sicherheitsprotokolle stündlich, wenn sie mehr als 100 MB erreichen. Dadurch wird sichergestellt, dass Sie in den Instanzen nicht zu wenig Speicherplatz haben.

Der Log-Agent innerhalb der Instances lädt das Protokoll online in CloudWatch Logs hoch. Von dort aus werden die Logs in S3 archiviert.

Die Protokolle werden in CloudWatch Logs und S3 im Rohformat gespeichert, in dem sie generiert wurden. Es findet keine Vorverarbeitung statt.

Standardwerte für das Kontinuitätsmanagement

In diesem Abschnitt werden die Standardeinstellungen für das AMS Continuity Management beschrieben. Weitere Informationen zu AMS-Backups finden Sie im AMS-Benutzerhandbuch im Kapitel Continuity Management.

Die Backup-Konfiguration erfolgt zum Zeitpunkt des Onboardings. Dies sind die standardmäßigen (empfohlenen) Backup-Einstellungen.

VPC-Tag und Standardeinstellungen

Die aktuellsten Informationen zum AMS-Backup finden Sie unter Continuity Management.

> **Important**
>
> Standardmäßig sind EC2 Stack-Backups deaktiviert (Backup = False). Sie können EC2 Instanz-Backups zum Zeitpunkt der Erstellung aktivieren, indem Sie ein Tag hinzufügen, `Key: Backup, Value: True` wenn Sie einen EC2 Stack über einen RFC anfordern (CT ct-14027q0sjyt1h). Wenn Sie das Tag hinzufügen möchten, nachdem die Instanz erstellt wurde, reichen Sie einen RFC mit dem CT Management | Advanced Stack Components | Instance Stack | Update CT ein (ct-38s4s4tm4ic4u). EC2

EC2 Instanz-Tag und Standardwerte

Das EC2 Stack-Backup-Tag gibt an, ob der Stack einen Snapshot der angehängten EBS-Volumes benötigt oder nicht.

Tag `Key: Backup`

Etikett `Value: True, False`

Standardmäßig ist der Wert, dass `False` das Backup-Tag nicht vorhanden ist und der Stack keine geplanten Backups hat.

Ändern Sie das Tag `Key: Backup` in, `Value: True` um Backups zu aktivieren, die dann nach dem mit dem VPC-Backup-Tag festgelegten Zeitplan durchgeführt werden.

> **Note**
>
> Die Groß- und Kleinschreibung des Tag-Werts (nur Wert) wird nicht berücksichtigt, sodass True/true alle Werte False/false akzeptabel sind.

Sicherung und Standardeinstellungen der RDS-Instanz

Die Standardwerte von Amazon Relational Database Service (RDS) sind in den Stack-Vorlagen definiert:

```
Backup: Yes

Backup Window: 22:00-23:00 (RDS local time zone)

Retention Period: 7 (7 snapshots stored)
```

Standardeinstellungen patchen

In diesem Abschnitt werden die AMS-Patching-Standardeinstellungen beschrieben. Weitere Informationen zum AMS-Patching finden Sie im AMS-Benutzerhandbuch im Kapitel Patch Management.

AMS-Releases werden AMIs monatlich gepatcht; alle neuen Stack-Anfragen sollten mit dem neuesten AMS-AMI konfiguriert werden.

> **Important**
>
> AMS Patch Orchestrator, tagbasiertes Patchen, verwendet die Funktionen von AWS Systems Manager (SSM), damit Sie Instances taggen oder mit einem AMS-Tag versehen können und diese Instances mithilfe einer Baseline und eines von Ihnen konfigurierten Fensters patchen lassen können. Weitere Informationen finden Sie unter Patch Orchestrator: ein tagbasiertes Patching-Modell.

Kontenbasiertes Patching nach AMS-Standard: Für jedes Konto mit Stacks, die direkt gepatcht werden, wird kurz nach dem „Patch Tuesday“ eine Benachrichtigung über bevorstehende

entsprechende Patches versendet. Die Benachrichtigung enthält eine Liste aller Stacks und der entsprechenden Patches sowie das vorgeschlagene Patch-Fenster. Für kritische Patches wird das Zeitfenster nicht länger als 10 Tage im Voraus und für Standard-Patches nicht mehr als 14 Tage im Voraus festgelegt. Wenn Sie nicht auf die Benachrichtigung antworten, erfolgt kein Patching. Wenn Sie bestimmte Patches ausschließen möchten, antworten Sie auf die Benachrichtigung oder reichen Sie eine Serviceanfrage ein. Wenn Sie mit Ihrer Zustimmung zum Patchen antworten, aber nicht ausdrücklich einen anderen Zeitplan anfordern, werden Patches wie in der Benachrichtigung beschrieben installiert, die Sie erhalten.

> **Note**
>
> Die Patch-Service-Benachrichtigung ist eine E-Mail, die an die Kontokontakte gesendet wird und einen Link zur AWS-Support-Konsole enthält. Sie können über die AWS-Supportkonsole oder über die AMS-Serviceanforderungsseite antworten, auf der die Benachrichtigung als Servicemeldung angezeigt wird.

Zum Zeitpunkt des AMS-Standard-Patching-Prozesses führt AMS Folgendes durch:

1. Sie erhalten vierzehn Tage vor dem geplanten Patch-Fenster eine Benachrichtigung über den Patch-Service. Die Benachrichtigung über den Patch-Service wird per E-Mail an die Kontakt-E-Mail-Adresse gesendet, die Sie für Ihr Konto hinterlegt haben.
2. Identifiziert alle erreichbaren EC2 Instanzen im Stack anhand der Liste der Stacks in der Patching-Benachrichtigung. In diesem Fall bedeutet „Erreichbar“ Instanzen, die sich im EC2 Status „Wird ausgeführt“ befinden und bei denen der EC2 Run Command-Agent voll funktionsfähig ist.
3. AMS führt das Patchen so durch, dass sichergestellt wird, dass eine ausreichende Anzahl von EC2 Instances gleichzeitig ausgeführt wird (anhand der `healthy-host-threshold` Einstellung konfiguriert), sodass der Stack fehlerfrei bleibt.
4. Nachdem der Patchvorgang für alle EC2 Instanzen abgeschlossen ist, aktualisiert AMS den RFC mit dem Patch-Status: Erfolgreich, Teilweise erfolgreich oder Fehlgeschlagen. Bei einem anderen Status als „Erfolgreich“ wird ein Ticket erstellt, über das ein Operator die Ergebnisse des Patches nachverfolgen und gegebenenfalls Korrekturmaßnahmen ergreifen kann.

Den AMS-Service validieren (SALZ)

Um zu überprüfen, ob der AWS Managed Services (AMS) -Service wie erwartet funktioniert, werden in diesem Kapitel einige Übungen beschrieben, die Sie durchführen können.

Finden Sie die AMS-Kontoeinstellungen

Kontoeinstellungen, die verwendet werden, um AMS zu erstellen RFCs, Zeitpläne festzulegen und festzulegen, wer Benachrichtigungen erhält.

Einige Einstellungen werden beim Onboarding erstellt und erfordern eine Serviceanfrage, um sie zu ändern. Sie sollten sich diese Kontodaten notieren, da Sie sie für die Kommunikation mit AMS verwenden werden:

- Anmeldeinformationen: Wenn Sie Ihren AMS-Benutzernamen oder Ihr AMS-Passwort abrufen müssen, wenden Sie sich an Ihren lokalen IT-Administrator. AMS verwendet das Active Directory Ihres Unternehmens.
- Cloud Service Delivery Manager (CSDM): Diese Person ist Ihr Ansprechpartner bei AMS und steht Ihnen für Servicefragen zur Verfügung. Sie erhalten die Kontaktinformationen dieser Person beim Onboarding und sollten sie allen Mitarbeitern Ihrer Organisation zur Verfügung stellen, die mit AMS interagieren. Sie können davon ausgehen, dass Sie von dieser Person monatliche Berichte über Ihren AMS-Service erhalten.
- Konsolenzugriff: Sie greifen über eine URL auf die AMS-Konsole zu, die speziell für Ihr Konto eingerichtet wurde. Sie können die URL von Ihrem CSDM abrufen.
- AMS-CLI: Sie können die AMS-CLI über die Entwicklerressourcenseite der AMS-Konsole oder über das Distributions-Paket, das Sie von Ihrem CSDM erhalten, abrufen. Nachdem Sie das Paket für die Distributionsdateien erhalten haben, folgen Sie den unter Installation oder Upgrade der AMS-CLI beschriebenen Schritte.
- Wartungsfenster: Ihr Wartungsfenster bestimmt, wann das Patchen für Ihre EC2 Instances erfolgt. Das AWS Managed Services Maintenance Window (oder Maintenance Window) führt Wartungsaktivitäten für AWS Managed Services (AMS) durch und findet jeden zweiten Donnerstag im Monat von 15:00 Uhr bis 16:00 Uhr pazifischer Zeit statt. AMS kann das Wartungsfenster 48 Stunden im Voraus ändern. Möglicherweise haben Sie beim Onboarding ein anderes Fenster gewählt. Notieren Sie sich das von Ihnen gewählte Wartungsfenster.
- Überwachung: AMS stellt standardmäßig eine Reihe von CloudWatch Metriken bereit, aber Sie können auch zusätzliche Metriken anfordern. Wenn Sie dies tun, zeichnen Sie diese auf.

- Logs: Standardmäßig werden Ihre Logs unter ams-a- *ACCOUNT_ID* -log-management- gespeichert. Dabei *REGION* handelt es sich um die Region*REGION*, in der das Protokoll generiert wurde.
- Schadensbegrenzung: Beim Onboarding zeichnet AMS die Abhilfemaßnahmen Ihrer Wahl auf, falls ein Malware-Angriff auf Ihre Ressourcen erkannt wird. Nehmen Sie beispielsweise Kontakt mit bestimmten Personen auf. Halten Sie diese Informationen für alle Personen in Ihrer Organisation verfügbar, die mit AMS interagieren.
- Region: Sie können sich die VPC-Detailseite in der AMS-Konsole ansehen. Sie können diesen Befehl auch ausführen, nachdem Sie die AMS SKMS-CLI installiert haben (dieser Befehl verwendet ein SAML-Profil, entfernen Sie es, wenn Ihre Authentifizierungsmethode anders ist):

```
aws --profile saml amsskms get-vpc --vpc-id VPC_ID
```

Important

Note

Die AMS-Endpunkte API/CLI (amscm und amsskms) befinden sich in der AWS-Region Nord-Virginia,. `us-east-1` Je nachdem, wie Ihre Authentifizierung eingerichtet ist und in welcher AWS-Region sich Ihr Konto und Ihre Ressourcen befinden, müssen Sie `--region us-east-1` bei der Ausgabe von Befehlen möglicherweise zusätzliche Informationen hinzufügen. Möglicherweise müssen Sie auch angeben`--profile saml`, ob dies Ihre Authentifizierungsmethode ist.

FQDNs In AMS suchen

Für die Zugriffsänderungstypen () von AWS Managed Services (AMSCTs) ist der vollqualifizierte Domainname oder FQDN Ihrer von AMS vertrauenswürdigen Domain in der Form von erforderlich. `C844273800838.amazonaws.com` Gehen Sie wie folgt vor, um Ihren AWS FQDN zu ermitteln:

- AWS-Konsole: Suchen Sie in der AWS Directory Service-Konsole in der Spalte Verzeichnisname nach.
- CLI: Verwenden Sie diese Befehle, während Sie in Ihrer Domain angemeldet sind:

  Windows (gibt Benutzer und FQDN zurück):

```
whoami /upn
```

oder (DC+DC+DC=FQDN)

```
whoami /fqdn
```

Linux:

```
hostname --fqdn
```

> **Note**
>
> Die AMS-Endpunkte API/CLI (amscm und amsskms) befinden sich in der AWS-Region Nord-Virginia,. `us-east-1` Je nachdem, wie Ihre Authentifizierung eingerichtet ist und in welcher AWS-Region sich Ihr Konto und Ihre Ressourcen befinden, müssen Sie `--region us-east-1` bei der Ausgabe von Befehlen möglicherweise zusätzliche Informationen hinzufügen. Möglicherweise müssen Sie auch angeben`--profile saml`, ob dies Ihre Authentifizierungsmethode ist.

Finden Sie Verfügbarkeitszonen (AZs) in AMS

Availability Zone: Alle Konten haben mindestens zwei Availability Zones. Um die Namen Ihrer Verfügbarkeitszonen genau zu ermitteln, müssen Sie zunächst die zugehörige Subnetz-ID kennen.

- AMS-Konsole: Klicken Sie im Navigationsbereich auf VPCsund klicken Sie dann gegebenenfalls auf die entsprechende VPC. Wählen Sie auf der VPCs Detailseite das entsprechende Subnetz in der Tabelle der Subnetze aus, um die Seite mit den Subnetzdetails mit dem Namen der zugehörigen Availability Zone zu öffnen.
- AMS SMS-API/CLI:

```
aws amsskms list-subnet-summaries --output table
```

```
aws amsskms get-subnet --subnet-id SUBNET_ID
```

> **Note**
>
> Die AMS-Endpunkte API/CLI (amscm und amsskms) befinden sich in der AWS-Region Nord-Virginia,. `us-east-1` Je nachdem, wie Ihre Authentifizierung eingerichtet ist und in welcher AWS-Region sich Ihr Konto und Ihre Ressourcen befinden, müssen Sie `--region us-east-1` bei der Ausgabe von Befehlen möglicherweise zusätzliche Informationen hinzufügen. Möglicherweise müssen Sie auch angeben`--profile saml`, ob dies Ihre Authentifizierungsmethode ist.

Suchen Sie nach SNS-Themen in AMS

Ihre SNS-Themen bestimmen, wer unter verschiedenen Umständen benachrichtigt wird. AMS bietet SNS-Themen für AMI-Benachrichtigungen (siehe AMS-AMI-Benachrichtigungen mit SNS), CloudWatch Alarme und EC2 Ressourcen (siehe Empfangen von Warnmeldungen, die von AMS generiert wurden) und mehr. Um mehr über Ihre bestehenden SNS-Themen zu erfahren:

- AWS-Konsole: Verwenden Sie die SNS-Konsole, um alle Themen, Anwendungen und Abonnements sowie eine grafische Darstellung der Nachrichten anzuzeigen. Außerdem können Sie Themen erstellen, löschen, abonnieren und veröffentlichen.
- API/CLI (wenn Sie bei Ihrem AMS-Konto angemeldet sind, ist die AWS-CLI erforderlich):

  Listen Sie Ihre SNS-Themen auf:

  ```
  aws sns list-topics
  ```

  Listen Sie Ihre SNS-Abonnements auf:

  ```
  aws sns list-subscriptions
  ```

> **Note**
>
> Die AMS-Endpunkte API/CLI (amscm und amsskms) befinden sich in der AWS-Region Nord-Virginia,. `us-east-1` Je nachdem, wie Ihre Authentifizierung eingerichtet ist und in welcher AWS-Region sich Ihr Konto und Ihre Ressourcen befinden, müssen Sie `--region us-east-1` bei der Ausgabe von Befehlen möglicherweise zusätzliche Informationen

hinzufügen. Möglicherweise müssen Sie auch angeben`--profile saml`, ob dies Ihre Authentifizierungsmethode ist.

Finden Sie die Backup-Einstellungen in AMS

Backups und Snapshots werden von AMS über den systemeigenen AWS BackupService verwaltet.

Die Konfiguration wird über AWS Backup Pläne verwaltet. Sie können mehrere AWS Backup Pläne haben, die markierte Ressourcen mit Backup-Zeitplänen und Aufbewahrungsrichtlinien verknüpfen. Um Ihre AWS Backup AMS-Kontoeinstellungen zu finden, verwenden Sie die https://console.aws.amazon.com/backup-Konsole oder die AWS CLI Command Reference für Backup-Befehle.

Weitere Informationen zu AMS und AWS Backup finden Sie unter Continuity Management.

Eine Instanz-ID oder IP-Adresse finden

Sie benötigen eine Instanz-IP-Adresse, um sich bei der Instanz anzumelden.

- Um Zugriff auf eine Instance anzufordern, sich bei einer Instance anzumelden oder ein AMI zu erstellen, benötigen Sie die Instance-ID. Für eine EC2 Instance (entweder eine eigenständige Instance oder ein Teil eines Stacks) oder eine Datenbank-Instance können Sie die ID auf verschiedene Arten finden:
  - Die AMS-Konsole für eine Instance in einem ASG-Stack: Suchen Sie auf der RFC-Detailseite nach dem RFC, der den Stack erstellt hat. Im Abschnitt Execution Output finden Sie die Stack-ID für den ASG-Stack. Sie können dann auf der Seite EC2 Console Auto Scaling Groups nach dieser Stack-ID suchen und Instances dafür finden. Wenn Sie die Instance gefunden haben, wählen Sie sie aus und unten auf der Seite öffnet sich ein Bereich mit Details, einschließlich der IP-Adresse.
  - Die AMS-Konsole für eine Standalone EC2 - oder Datenbank-Instance (DB): Suchen Sie auf der RFC-Detailseite nach dem RFC, der den EC2 Stack oder die DB-Instance erstellt hat. Im Abschnitt Execution Output finden Sie die Instance-ID und die IP-Adresse.
  - EC2 AWS-Konsole:
    1. Wählen Sie im Navigationsbereich Instances aus. Die Seite Instances wird geöffnet.
    2. Klicken Sie auf die Instance, für die Sie die ID benötigen. Die Seite mit den Instanzdetails wird geöffnet und zeigt die ID und die IP-Adresse an.

- AWS-Datenbankkonsole:
  1. Wählen Sie auf der Startseite DB-Instances aus. Die Seite Instances wird geöffnet.
  2. Filtern Sie nach der DB-Instance, für die Sie die ID benötigen. Die Seite mit den Instance-Details wird geöffnet und die ID wird angezeigt.
- AMS CLI/API.

> **Note**
>
> Die AMS-CLI muss installiert sein, damit diese Befehle funktionieren. Um die AMS-API oder CLI zu installieren, rufen Sie die Seite Entwicklerressourcen der AMS-Konsole auf. Referenzmaterial zur AMS CM API oder AMS SKMS API finden Sie im Abschnitt AMS-Informationsressourcen im Benutzerhandbuch. Möglicherweise müssen Sie eine `--profile` Option für die Authentifizierung hinzufügen, `aws amsskms` *`ams-cli-command`* `--profile SAML` zum Beispiel. Möglicherweise müssen Sie die `--region` Option auch hinzufügen, da allen AMS-Befehlen beispielsweise us-east-1 ausgeht. `aws amscm` *`ams-cli-command`* `--region=us-east-1`

> **Note**
>
> Die AMS-Endpunkte API/CLI (amscm und amsskms) befinden sich in der AWS-Region Nord-Virginia,. `us-east-1` Je nachdem, wie Ihre Authentifizierung eingerichtet ist und in welcher AWS-Region sich Ihr Konto und Ihre Ressourcen befinden, müssen Sie `--region us-east-1` bei der Ausgabe von Befehlen möglicherweise zusätzliche Informationen hinzufügen. Möglicherweise müssen Sie auch angeben`--profile saml`, ob dies Ihre Authentifizierungsmethode ist.

Führen Sie den folgenden Befehl aus, um die Ausgabedetails zur Stack-Ausführung abzurufen:

```
aws amsskms get-stack --stack-id STACK_ID
```

Die Ausgabe sieht in etwa so aus, InstanceId dass sie unten unter angezeigt wird `Outputs` (die angegebenen Werte sind Beispiele):

```
{
    "Stack": {
        "StackId": "stack-7fa52bd5eb8240123",
        "Status": {
            "Id": "CreateCompleted",
            "Name": "CreateCompleted"
        },
        "VpcId": "vpc-01234567890abcdef",
        "Description": "Amazon",
        "Parameters": [
            {
                "Value": "sg-01234567890abcdef,sg-01234567890abcdef",
                "Key": "SecurityGroups"
            },
            {
                "Value": "subnet-01234567890abcdef",
                "Key": "InstanceSubnetId"
            },
            {
                "Value": "t2.large",
                "Key": "InstanceType"
            },
            {
                "Value": "ami-01234567890abcdef",
                "Key": "InstanceAmiId"
            }
        ],
        "Tags": [],
        "Outputs": [
            {
                "Value": "i-0b22a22eec53b9321",
                "Key": "InstanceId"
            },
            {
                "Value": "10.0.5.000",
                "Key": "InstancePrivateIP"
            }
        ],
        "StackTemplateId": "stm-s6xvs000000000000",
        "CreatedTime": "1486584508416",
        "Name": "Amazon"
    }
```

```
}
```

DNS-freundliche Bastion-Namen

MALZ

Für die Multi-Account-Landingzone (MALZ) werden DNS-Einträge für die Bastionen im FQDN des von AMS verwalteten Active Directory erstellt. AMS ersetzt bei Bedarf Linux- und Windows-Bastionen. Wenn beispielsweise ein neues Bastion-AMI bereitgestellt werden muss, werden die Bastion-DNS-Einträge dynamisch aktualisiert, sodass sie auf neue, gültige Bastionen verweisen.

1. Verwenden Sie DNS-Einträge wie folgt, um auf SSH-Bastionen (Linux) zuzugreifen: `sshbastion(1-4).Your_Domain.com`

   Zum Beispiel, wo die Domain ist: `Your_Domain`

   - `sshbastion1.Your_Domain.com`
   - `sshbastion2.Your_Domain.com`
   - `sshbastion3.Your_Domain.com`
   - `sshbastion4.Your_Domain.com`

2. Verwenden Sie DNS-Einträge wie folgt, um auf RDP-Bastionen (Windows) zuzugreifen:. `rdp-Username.Your_Domain.com`

   Beispiel: Der Benutzername ist`alex`,, oder `test` demobob, und die Domäne lautet: `Your_Domain.com`

   - `rdp-alex.Your_Domain.com`
   - `rdp-test.Your_Domain.com`
   - `rdp-demo.Your_Domain.com`
   - `rdp-bob.Your_Domain.com`

SALZ

Die Single-Account-Landingzone (SALZ) ersetzt bei Bedarf die Linux- und Windows-Bastionen. Wenn beispielsweise ein neues Bastion-AMI bereitgestellt werden muss, werden die Bastion-DNS-Einträge dynamisch aktualisiert, sodass sie auf neue, gültige Bastionen verweisen.

1. Verwenden Sie DNS-Einträge wie folgt, um auf SSH-Bastionen (Linux) zuzugreifen: `sshbastion(1-4).A`*`AccountNumber`*`.amazonaws.com.`

   Wo `123456789012` ist zum Beispiel die Kontonummer:

   - `sshbastion1.A123456789012.amazonaws.com`
   - `sshbastion2.A123456789012.amazonaws.com`
   - `sshbastion3.A123456789012.amazonaws.com`
   - `sshbastion4.A123456789012.amazonaws.com`
2. Verwenden Sie DNS-Einträge wie folgt, um auf RDP-Bastionen (Windows) zuzugreifen:. `rdpbastion(1-4).A`*`ACCOUNT_NUMBER`*`.amazonaws.com`

   Wo `123456789012` ist zum Beispiel die Kontonummer:

   - `rdpbastion1.A123456789012.amazonaws.com`
   - `rdpbastion2.A123456789012.amazonaws.com`
   - `rdpbastion3.A123456789012.amazonaws.com`
   - `rdpbastion4.A123456789012.amazonaws.com`

Suchen nach Bastion-IP-Adressen

AMS-Kunden können SSH- und RDP-Bastionen, entweder die zuvor DNS-freundliche Bastion-Namen beschriebenen, oder Bastion-IP-Adressen verwenden.

So finden Sie Bastion-IP-Adressen, SSH und RDP, für Ihr Konto:

1. Nur für landing zone mit mehreren Konten: Melden Sie sich beim Shared Services-Konto an.
2. Öffnen Sie die EC2 Konsole und wählen Sie Running Instances.

   Die Seite „Instances“ wird geöffnet.
3. Geben Sie im Filterfeld oben entweder ssh-bastion oder rdp-bastion ein.

   Geben Sie im Filterfeld oben entweder customer-ssh oder customer-rdp ein.

   Die and/or SSH-RDP-Bastionen für Ihr Konto werden angezeigt.

   Beachten Sie, dass Sie zusätzlich zu Ihren SSH-Bastionen möglicherweise auch AMS-Perimeter-Netzwerkbastionen in der Liste sehen, die dafür nicht verfügbar sind.

4. Wählen Sie eine SSH- oder RDP-Bastion aus. Wenn Sie einen Windows-Computer verwenden und sich bei einer Linux-Instanz anmelden möchten, verwenden Sie eine SSH-Bastion. Wenn Sie sich bei einer Windows-Instanz anmelden möchten, verwenden Sie eine RDP-Bastion. Wenn Sie ein Linux-Betriebssystem verwenden und sich bei einer Windows-Instanz anmelden möchten, verwenden Sie eine SSH-Bastion über einen RDP-Tunnel (so können Sie auf den Windows-Desktop zugreifen). Um von einem Linux-Betriebssystem aus auf eine Linux-Instanz zuzugreifen, verwenden Sie eine SSH-Bastion.

EC2 Instanzen: Erstellen

Sie können die AMS-Konsole verwenden oder API/CLI ein Amazon EC2 und ein Amazon EC2 mit zusätzlichen Volumes erstellen.

Stapel erstellen

Eine EC2 Instanz mit der Konsole erstellen

Im Folgenden wird dieser Änderungstyp in der AMS-Konsole gezeigt.

So funktioniert es:

1. Navigieren Sie zur Seite „RFC erstellen“: Klicken Sie im linken Navigationsbereich der AMS-Konsole, um die RFCs Listenseite RFCszu öffnen, und klicken Sie dann auf RFC erstellen.
2. Wählen Sie in der Standardansicht „Änderungstypen durchsuchen“ einen beliebten Änderungstyp (CT) oder wählen Sie in der Ansicht „Nach Kategorie auswählen“ einen CT aus.
   - Nach Änderungstyp suchen: Sie können im Bereich Schnellerstellung auf ein beliebtes CT klicken, um sofort die Seite RFC ausführen zu öffnen. Beachten Sie, dass Sie mit Quick Create keine ältere CT-Version auswählen können.

     Verwenden Sie zum Sortieren CTs den Bereich Alle Änderungstypen in der Karten - oder Tabellenansicht. Wählen Sie in einer der Ansichten einen CT aus und klicken Sie dann auf RFC erstellen, um die Seite RFC ausführen zu öffnen. Falls zutreffend, wird neben der Schaltfläche „RFC erstellen“ die Option Mit älterer Version erstellen angezeigt.
   - Nach Kategorie auswählen: Wählen Sie eine Kategorie, eine Unterkategorie, einen Artikel und einen Vorgang aus. Daraufhin wird das Feld mit den CT-Details geöffnet. Dort können Sie gegebenenfalls die Option „Mit älterer Version erstellen“ auswählen. Klicken Sie auf RFC erstellen, um die Seite RFC ausführen zu öffnen.

3. Öffnen Sie auf der Seite RFC ausführen den Bereich CT-Name, um das Feld mit den CT-Details zu sehen. Ein Betreff ist erforderlich (dieser wird für Sie ausgefüllt, wenn Sie Ihr CT in der Ansicht „Änderungstypen durchsuchen“ auswählen). Öffnen Sie den Bereich Zusätzliche Konfiguration, um Informationen zum RFC hinzuzufügen.

   Verwenden Sie im Bereich Ausführungskonfiguration die verfügbaren Dropdownlisten oder geben Sie Werte für die erforderlichen Parameter ein. Um optionale Ausführungsparameter zu konfigurieren, öffnen Sie den Bereich Zusätzliche Konfiguration.
4. Wenn Sie fertig sind, klicken Sie auf Ausführen. Wenn keine Fehler vorliegen, wird die Seite mit dem RFC erfolgreich erstellt mit den übermittelten RFC-Details und der ersten Run-Ausgabe angezeigt.
5. Öffnen Sie den Bereich Run-Parameter, um die von Ihnen eingereichten Konfigurationen zu sehen. Aktualisieren Sie die Seite, um den RFC-Ausführungsstatus zu aktualisieren. Brechen Sie optional den RFC ab oder erstellen Sie eine Kopie davon mit den Optionen oben auf der Seite.

Eine EC2 Instanz mit der CLI erstellen

So funktioniert es:

1. Verwenden Sie entweder Inline Create (Sie geben einen `create-rfc` Befehl mit allen RFC- und Ausführungsparametern aus) oder Template Create (Sie erstellen zwei JSON-Dateien, eine für die RFC-Parameter und eine für die Ausführungsparameter) und geben Sie den `create-rfc` Befehl mit den beiden Dateien als Eingabe aus. Beide Methoden werden hier beschrieben.
2. Reichen Sie den `aws amscm submit-rfc --rfc-id` *ID* Befehl RFC: mit der zurückgegebenen RFC-ID ein.

   Überwachen Sie den RFC: -Befehl. `aws amscm get-rfc --rfc-id` *ID*

Verwenden Sie diesen Befehl, um die Version des Änderungstyps zu überprüfen:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Sie können alle `CreateRfc` Parameter mit jedem RFC verwenden, unabhängig davon, ob sie Teil des Schemas für den Änderungstyp sind oder nicht. Um beispielsweise

Benachrichtigungen zu erhalten, wenn sich der RFC-Status ändert, fügen Sie diese Zeile dem RFC-Parameter-Teil der Anfrage hinzu (nicht den Ausführungsparametern). `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` Eine Liste aller CreateRfc Parameter finden Sie in der AMS Change Management API-Referenz.

INLINE-ERSTELLUNG:

Geben Sie den Befehl create RFC mit den direkt angegebenen Ausführungsparametern aus (vermeiden Sie Anführungszeichen, wenn Sie die Ausführungsparameter inline angeben), und senden Sie dann die zurückgegebene RFC-ID. Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:

```
aws amscm create-rfc --change-type-id "ct-14027q0sjyt1h" --change-type-version "4.0"
 --title "EC2-Create-RFC" --execution-parameters "{\"Description\": \"Create a new
 EC2 Instance stack\",\"VpcId\": \"vpc-0a60eb65b4EXAMPLE\",\"Name\": \"My-EC2\",
\"TimeoutInMinutes\": 60,\"Parameters\": {\"InstanceAmiId\": \"ami-1234567890EXAMPLE\",
\"InstanceDetailedMonitoring\": false,\"InstanceEBSOptimized\": false,\"InstanceProfile
\": \"customer-mc-ec2-instance-profile\",\"InstanceRootVolumeIops\": 3000,
\"InstanceRootVolumeType\": \"gp3\",\"InstanceType\": \"t2.large\",\"InstanceUserData
\": \"\",\"InstanceSubnetId\": \"subnet-0bb1c79de3EXAMPLE\",\"EnforceIMDSV2\":
 \"false\"}}"
```

VORLAGE ERSTELLEN:

1. Gibt die Ausführungsparameter für diesen Änderungstyp in eine JSON-Datei aus. In diesem Beispiel wird sie Create EC2 Params.json genannt:

   ```
   aws amscm get-change-type-version --change-type-id "ct-14027q0sjyt1h" --query
    "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2Params.json
   ```

2. Ändern und speichern Sie die Datei Create EC2 Params. Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:

   ```
   {
     "Description": "Create a new EC2 Instance stack",
     "VpcId": "vpc-0a60eb65b4EXAMPLE",
     "Name": "My-EC2",
     "TimeoutInMinutes": 60,
   ```

```
  "Parameters": {
    "InstanceAmiId": "ami-1234567890EXAMPLE",
    "InstanceDetailedMonitoring": false,
    "InstanceEBSOptimized": false,
    "InstanceProfile": "customer-mc-ec2-instance-profile",
    "InstanceRootVolumeIops": 3000,
    "InstanceRootVolumeType": "gp3",
    "InstanceType": "t2.large",
    "InstanceUserData": "",
    "InstanceSubnetId": "subnet-0bb1c79de3EXAMPLE",
    "EnforceIMDSV2": "false"
  }
}
```

3. Geben Sie die RFC-Vorlage in eine Datei in Ihrem aktuellen Ordner aus. In diesem Beispiel wird sie Create EC2 RFC.json genannt:

```
aws amscm create-rfc --generate-cli-skeleton > CreateEC2Rfc.json
```

4. Ändern und speichern Sie die Datei Create EC2 Rfc.json. Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:.

```
{
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-14027q0sjyt1h",
"Title":                "EC2-Create-RFC"
}
```

5. Erstellen Sie den RFC, indem Sie die Datei Create EC2 Rfc und die Datei Create EC2 Params angeben:

```
aws amscm create-rfc --cli-input-json file://CreateEC2Rfc.json  --execution-
parameters file://CreateEC2Params.json
```

Sie erhalten die ID des neuen RFC in der Antwort und können sie verwenden, um den RFC zu senden und zu überwachen. Bis Sie ihn abschicken, verbleibt der RFC im Bearbeitungszustand und startet nicht.

Tipps

Sicherheitsgruppen

Ab Version 3.0 dieses Änderungstyps fügt AMS die standardmäßigen AMS-Sicherheitsgruppen nicht an, wenn Sie Ihre eigenen Sicherheitsgruppen angeben. Wenn Sie in der Anfrage keine eigenen Sicherheitsgruppen angeben, hängt AMS die AMS-Standardsicherheitsgruppen an. In früheren Versionen hat AMS die Standardsicherheitsgruppen angehängt, unabhängig davon, ob Sie Ihre eigenen Sicherheitsgruppen angegeben haben oder nicht.
Wenn Sie benutzerdefinierte Sicherheitsgruppen angeben, müssen Sie derzeit auch die IDs AMS-Standardsicherheitsgruppen für Ihr Konto angeben, `mc-initial-garden-SG-name` und`mc-initial-garden-SG-name`.

Instance-Typen

AMS empfiehlt die Typen t2.micro/t3.micro und t2.nano/t3.nano nicht. Dies sind kleinere Instance-Typen, die die Leistung Ihrer Anwendung und Ihrer AMS-Tools beeinträchtigen können. EC2 Instanzen benötigen neben der Anwendungslast auch genügend Kapazität, um AMS-Tools wie EPS, SSM und Cloudwatch zu unterstützen. Weitere Informationen finden Sie unter Den richtigen EC2 Instance-Typ für Ihre Anwendung auswählen.

Informationen zum Erstellen eines EC2 Stacks mit zusätzlichen Volumes finden Sie unter EC2 Stapel | Erstellen (mit zusätzlichen Volumes).

Sie können bis zu 50 Tags hinzufügen, müssen dazu jedoch die Ansicht Zusätzliche Konfiguration aktivieren.

Falls erforderlich, finden Sie weitere Informationen unter EC2 Instanzstapelerstellung fehlgeschlagen.

Stack erstellen (mit zusätzlichen Volumes)

Eine EC2 Instance und zusätzliche Volumes mit der Konsole erstellen

Im Folgenden wird dieser Änderungstyp in der AMS-Konsole dargestellt.

So funktioniert es:

1. Navigieren Sie zur Seite „RFC erstellen“: Klicken Sie im linken Navigationsbereich der AMS-Konsole, um die RFCs Listenseite RFCszu öffnen, und klicken Sie dann auf RFC erstellen.
2. Wählen Sie in der Standardansicht „Änderungstypen durchsuchen“ einen beliebten Änderungstyp (CT) oder wählen Sie in der Ansicht „Nach Kategorie auswählen“ einen CT aus.
   - Nach Änderungstyp suchen: Sie können im Bereich Schnellerstellung auf ein beliebtes CT klicken, um sofort die Seite RFC ausführen zu öffnen. Beachten Sie, dass Sie mit Quick Create keine ältere CT-Version auswählen können.

     Verwenden Sie zum Sortieren CTs den Bereich Alle Änderungstypen in der Karten - oder Tabellenansicht. Wählen Sie in einer der Ansichten einen CT aus und klicken Sie dann auf RFC erstellen, um die Seite RFC ausführen zu öffnen. Falls zutreffend, wird neben der Schaltfläche „RFC erstellen“ die Option Mit älterer Version erstellen angezeigt.
   - Nach Kategorie auswählen: Wählen Sie eine Kategorie, eine Unterkategorie, einen Artikel und einen Vorgang aus. Daraufhin wird das Feld mit den CT-Details geöffnet. Dort können Sie gegebenenfalls die Option „Mit älterer Version erstellen“ auswählen. Klicken Sie auf RFC erstellen, um die Seite RFC ausführen zu öffnen.
3. Öffnen Sie auf der Seite RFC ausführen den Bereich CT-Name, um das Feld mit den CT-Details zu sehen. Ein Betreff ist erforderlich (dieser wird für Sie ausgefüllt, wenn Sie Ihr CT in der Ansicht „Änderungstypen durchsuchen“ auswählen). Öffnen Sie den Bereich Zusätzliche Konfiguration, um Informationen zum RFC hinzuzufügen.

   Verwenden Sie im Bereich Ausführungskonfiguration die verfügbaren Dropdownlisten oder geben Sie Werte für die erforderlichen Parameter ein. Um optionale Ausführungsparameter zu konfigurieren, öffnen Sie den Bereich Zusätzliche Konfiguration.
4. Wenn Sie fertig sind, klicken Sie auf Ausführen. Wenn keine Fehler vorliegen, wird die Seite mit dem RFC erfolgreich erstellt mit den übermittelten RFC-Details und der ersten Run-Ausgabe angezeigt.
5. Öffnen Sie den Bereich Run-Parameter, um die von Ihnen eingereichten Konfigurationen zu sehen. Aktualisieren Sie die Seite, um den RFC-Ausführungsstatus zu aktualisieren. Brechen Sie optional den RFC ab oder erstellen Sie eine Kopie davon mit den Optionen oben auf der Seite.

Eine EC2 Instanz und zusätzliche Volumes mit der CLI erstellen

So funktioniert es:

1. Verwenden Sie entweder Inline Create (Sie geben einen `create-rfc` Befehl mit allen RFC- und Ausführungsparametern aus) oder Template Create (Sie erstellen zwei JSON-Dateien, eine für die RFC-Parameter und eine für die Ausführungsparameter) und geben Sie den `create-rfc` Befehl mit den beiden Dateien als Eingabe aus. Beide Methoden werden hier beschrieben.
2. Reichen Sie den `aws amscm submit-rfc --rfc-id` *ID* Befehl RFC: mit der zurückgegebenen RFC-ID ein.

   Überwachen Sie den RFC: -Befehl. `aws amscm get-rfc --rfc-id` *ID*

Verwenden Sie diesen Befehl, um die Version des Änderungstyps zu überprüfen:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Sie können alle `CreateRfc` Parameter mit jedem RFC verwenden, unabhängig davon, ob sie Teil des Schemas für den Änderungstyp sind oder nicht. Um beispielsweise Benachrichtigungen zu erhalten, wenn sich der RFC-Status ändert, fügen Sie diese Zeile dem RFC-Parameter-Teil der Anfrage hinzu (nicht den Ausführungsparametern). `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` Eine Liste aller CreateRfc Parameter finden Sie in der AMS Change Management API-Referenz.

INLINE-ERSTELLUNG:

Geben Sie den Befehl create RFC mit den direkt angegebenen Ausführungsparametern aus (vermeiden Sie Anführungszeichen, wenn Sie die Ausführungsparameter inline angeben), und senden Sie dann die zurückgegebene RFC-ID (das Beispiel zeigt nur die erforderlichen Parameter). Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:

```
aws amscm create-rfc --change-type-id "ct-1aqsjf86w6vxg" --change-type-version "4.0"
 --title "EC2-Create-A-V-QC" --execution-parameters "{\"Description\":\"My EC2 stack
 with addl vol\",\"VpcId\":\"VPC_ID\",\"Name\":\"My Stack\",\"StackTemplateId\":
\"stm-nn8v8ffhcal611bmo\",\"TimeoutInMinutes\":60,\"Parameters\":{\"InstanceAmiId\":
\"AMI_ID\",\"InstanceSubnetId\":\"SUBNET_ID\"}}
```

VORLAGE ERSTELLEN:

1. Geben Sie die Ausführungsparameter für diesen Änderungstyp in eine JSON-Datei mit dem Namen Create EC2 AVParams .json aus.

```
aws amscm get-change-type-version --change-type-id "ct-1aqsjf86w6vxg" --query
 "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2AVParams.json
```

2. Ändern und speichern Sie die EC2 AVParams Create-Datei (das Beispiel zeigt die meisten Parameter). Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:

```
{
"Description":      "EC2-Create-1-Addl-Volumes",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-nn8v8ffhcal611bmo",
"Name":             "My-EC2-1-Addl-Volume",
"TimeoutInMinutes": 60,
"Parameters":   {
    "InstanceAmiId":    "AMI_ID",
    "InstanceSecurityGroupIds": "SECURITY_GROUP_ID",
    "InstanceCoreCount": 1,
    "InstanceThreadsPerCore": 2,
    "InstanceDetailedMonitoring": "true",
    "InstanceEBSOptimized": "false",
    "InstanceProfile": "customer-mc-ec2-instance-profile",
    "InstanceRootVolumeIops": 100,
    "InstanceRootVolumeName": "/dev/xvda",
    "InstanceRootVolumeSize": 50,
    "InstanceRootVolumeType": "io1",
    "RootVolumeKmsKeyId": "default",
    "InstancePrivateStaticIp": "10.27.0.100",
    "InstanceSecondaryPrivateIpAddressCount": 0,
    "InstanceTerminationProtection": "false",
    "InstanceType": "t3.large",
    "CreditSpecification": "unlimited",
    "InstanceUserData": "echo $",
    "Volume1Encrypted": "true",
    "Volume1Iops":      "IOPS"
    "Volume1KmsKeyId":  "KMS_MASTER_KEY_ID",
    "Volume1Name":      "xvdh"
    "Volume1Size":      "2 GiB",
    "Volume1Snapshot":  "SNAPSHOT_ID",
    "Volume1Type":      "iol",
```

```
    "InstanceSubnetId": "SUBNET_ID"
    }
}
```

3. Geben Sie die RFC-Vorlage in eine Datei in Ihrem aktuellen Ordner aus. In diesem Beispiel wird sie Create EC2 AVRfc .json genannt:

```
aws amscm create-rfc --generate-cli-skeleton > CreateEC2AVRfc.json
```

4. Ändern und speichern Sie die Datei Create EC2 AVRfc .json. Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:

```
{
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-1aqsjf86w6vxg",
"Title":                "EC2-Create-1-Addl-Volume-RFC"
}
```

5. Erstellen Sie den RFC und geben Sie dabei die EC2 AVRfc Create-Datei und die EC2 AVParams Create-Datei an:

```
aws amscm create-rfc --cli-input-json file://CreateEC2AVRfc.json  --execution-
parameters file://CreateEC2AVParams.json
```

Sie erhalten die ID des neuen RFC in der Antwort und können sie verwenden, um den RFC zu senden und zu überwachen. Bis Sie ihn abschicken, verbleibt der RFC im Bearbeitungszustand und startet nicht.

Tipps

> **Important**
>
> Es gibt eine neue Version dieses Änderungstyps, v 4.0, die eine andere Version verwendet StackTemplateId (stm-nn8v8ffhcal611bmo). Dies ist wichtig, wenn Sie den RFC mit diesem Änderungstyp über die Befehlszeile einreichen. Die neue Version führt zwei neue Parameter (RootVolumeKmsKeyIdund CreditSpecification) ein und ändert die Standardeinstellung für einen vorhandenen Parameter (InstanceType).

Instance-Typen

- Wenn Sie die Anzahl der Kerne oder Threads angeben möchten, müssen Sie Werte für beide angeben. Verwenden Sie die Parameter `InstanceCoreCount` und`InstanceThreadsPerCore`. Gültige Kombinationen von Kernen und Threads finden Sie unter CPU-Kerne und Threads pro CPU-Kern pro Instanztyp.
- AMS empfiehlt die Instance-Typen t2.micro/t3.micro oder t2.nano/t3.nano nicht. Diese sind zu klein, um zusätzlich zur Arbeitslast Ihres Unternehmens AMS-Tools wie EPS, SSM und Cloudwatch zu unterstützen. Weitere Informationen finden Sie unter Den richtigen EC2 Instance-Typ für Ihre Anwendung auswählen.
- In Version 4.0 wurde der Standardtyp von t2.large auf t3.large angehoben. T3-Instances werden standardmäßig mit „unbegrenzten Credits“ gestartet. Es kommt nicht zu einer CPU-Drosselung, selbst wenn die Instance alle CPU-Guthaben verbraucht. Sie können stattdessen T2-Instances wählen und die Option „Unbegrenzt“ verwenden. CreditSpecification
- Weitere Informationen zu Amazon EC2, einschließlich Größenempfehlungen, finden Sie in der Amazon Elastic Compute Cloud-Dokumentation.

Informationen zum Aktualisieren Ihres EC2 Stacks mit zusätzlichen Volumes, nachdem diese erstellt wurden, finden Sie unter EC2 Instance-Stack: Aktualisierung (mit zusätzlichen Volumes)

Zugriff, anfordern

Administratorzugriff beantragen

Administratorzugriff über die Konsole anfordern

Im Folgenden wird dieser Änderungstyp in der AMS-Konsole dargestellt.

So funktioniert es:

1. Navigieren Sie zur Seite RFC erstellen: Klicken Sie im linken Navigationsbereich der AMS-Konsole, um die RFCs Listenseite RFCszu öffnen, und klicken Sie dann auf RFC erstellen.
2. Wählen Sie in der Standardansicht „Änderungstypen durchsuchen“ einen beliebten Änderungstyp (CT) oder wählen Sie in der Ansicht „Nach Kategorie auswählen“ einen CT aus.

- Nach Änderungstyp suchen: Sie können im Bereich Schnellerstellung auf ein beliebtes CT klicken, um sofort die Seite RFC ausführen zu öffnen. Beachten Sie, dass Sie mit Quick Create keine ältere CT-Version auswählen können.

  Verwenden Sie zum Sortieren CTs den Bereich Alle Änderungstypen in der Karten - oder Tabellenansicht. Wählen Sie in einer der Ansichten einen CT aus und klicken Sie dann auf RFC erstellen, um die Seite RFC ausführen zu öffnen. Falls zutreffend, wird neben der Schaltfläche „RFC erstellen“ die Option Mit älterer Version erstellen angezeigt.
- Nach Kategorie auswählen: Wählen Sie eine Kategorie, eine Unterkategorie, einen Artikel und einen Vorgang aus. Daraufhin wird das Feld mit den CT-Details geöffnet. Dort können Sie gegebenenfalls die Option „Mit älterer Version erstellen“ auswählen. Klicken Sie auf RFC erstellen, um die Seite RFC ausführen zu öffnen.

3. Öffnen Sie auf der Seite RFC ausführen den Bereich CT-Name, um das Feld mit den CT-Details zu sehen. Ein Betreff ist erforderlich (dieser wird für Sie ausgefüllt, wenn Sie Ihr CT in der Ansicht „Änderungstypen durchsuchen“ auswählen). Öffnen Sie den Bereich Zusätzliche Konfiguration, um Informationen zum RFC hinzuzufügen.

   Verwenden Sie im Bereich Ausführungskonfiguration die verfügbaren Dropdownlisten oder geben Sie Werte für die erforderlichen Parameter ein. Um optionale Ausführungsparameter zu konfigurieren, öffnen Sie den Bereich Zusätzliche Konfiguration.
4. Wenn Sie fertig sind, klicken Sie auf Ausführen. Wenn keine Fehler vorliegen, wird die Seite mit dem RFC erfolgreich erstellt mit den übermittelten RFC-Details und der ersten Run-Ausgabe angezeigt.
5. Öffnen Sie den Bereich Run-Parameter, um die von Ihnen eingereichten Konfigurationen zu sehen. Aktualisieren Sie die Seite, um den RFC-Ausführungsstatus zu aktualisieren. Brechen Sie optional den RFC ab oder erstellen Sie eine Kopie davon mit den Optionen oben auf der Seite.

Administratorzugriff mit der CLI anfordern

So funktioniert es:

1. Verwenden Sie entweder Inline Create (Sie geben einen `create-rfc` Befehl mit allen RFC- und Ausführungsparametern aus) oder Template Create (Sie erstellen zwei JSON-Dateien, eine für die RFC-Parameter und eine für die Ausführungsparameter) und geben Sie den `create-rfc` Befehl mit den beiden Dateien als Eingabe aus. Beide Methoden werden hier beschrieben.

2. Reichen Sie den `aws amscm submit-rfc --rfc-id ID` Befehl RFC: mit der zurückgegebenen RFC-ID ein.

   Überwachen Sie den RFC: -Befehl. `aws amscm get-rfc --rfc-id ID`

Verwenden Sie diesen Befehl, um die Version des Änderungstyps zu überprüfen:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Sie können alle `CreateRfc` Parameter mit jedem RFC verwenden, unabhängig davon, ob sie Teil des Schemas für den Änderungstyp sind oder nicht. Um beispielsweise Benachrichtigungen zu erhalten, wenn sich der RFC-Status ändert, fügen Sie diese Zeile dem RFC-Parameter-Teil der Anfrage hinzu (nicht den Ausführungsparametern). `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` Eine Liste aller CreateRfc Parameter finden Sie in der AMS Change Management API-Referenz.

INLINE-ERSTELLUNG:

Geben Sie den Befehl create RFC mit den direkt angegebenen Ausführungsparametern aus (vermeiden Sie Anführungszeichen, wenn Sie die Ausführungsparameter inline angeben), und senden Sie dann die zurückgegebene RFC-ID. Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:

```
aws --profile saml amscm create-rfc --change-type-id "ct-1dmlg9g1l91h6" --change-type-
version "3.0" --title "Stack-Admin-Access-QC" --execution-parameters "{\"DomainFQDN
\":\"TEST.com\",\"StackIds\":[\"stack-01234567890abcdef\"],\"TimeRequestedInHours\":1,
\"Usernames\":[\"TEST\"],\"VpcId\":\"VPC_ID\"}"
```

VORLAGE ERSTELLEN:

1. Gibt das JSON-Schema der Ausführungsparameter für diesen Änderungstyp in eine Datei aus. In diesem Beispiel wird sie „ GrantAdminAccessParams.json“ genannt:

```
aws amscm get-change-type-version --change-type-id "ct-1dmlg9g1l91h6"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 GrantAdminAccessParams.json
```

Ändern und speichern Sie die GrantAdminAccessParams Datei. Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:

```
{
"DomainFQDN":           "mycorpdomain.acme.com",
"StackIds":             [STACK_ID, STACK_ID],
"TimeRequestedInHours": 12,
"Username":             ["USERNAME", "USERNAME"],
"VpcId":                "VPC_ID"
}
```

Beachten Sie, dass die `TimeRequestedInHours` Option standardmäßig auf eine Stunde eingestellt ist. Sie können bis zu zwölf Stunden anfordern.

2. Geben Sie die RFC-Vorlage in eine Datei in Ihrem aktuellen Ordner aus. In diesem Beispiel wird sie „ GrantAdminAccessRfc.json“ genannt:

```
aws amscm create-rfc --generate-cli-skeleton > GrantAdminAccessRfc.json
```

3. Ändern und speichern Sie die GrantAdminAccessRfc JSON-Datei. Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:

```
{
"ChangeTypeId":         "ct-1dmlg9g1l91h6",
"ChangeTypeVersion":    "3.0",
"Title":                "Request-Admin-Access-to-EC2-RFC"
}
```

4. Erstellen Sie den RFC und geben Sie die GrantAdminAccessRfc Datei und die GrantAdminAcessParams Datei an:

```
aws amscm create-rfc --cli-input-json file://GrantAdminAccessRfc.json --execution-
parameters file://GrantAdminAccessParams.json
```

Sie erhalten die ID des neuen RFC in der Antwort und können sie verwenden, um den RFC zu senden und zu überwachen. Bis Sie ihn abschicken, verbleibt der RFC im Bearbeitungszustand und startet nicht.

Um sich über eine Bastion bei der Instanz anzumelden, folgen Sie dem nächsten Verfahren, Beispiele für den Instanzzugriff.

Tipps

> **Note**
>
> Sie können eine Aktualisierung Ihrer Zugriffsanfrage einreichen, bevor sie abläuft. Weitere Informationen finden Sie unter Stack Admin Access | Update.
> Um sich bei einer Instance anzumelden, die Teil einer ASG ist, beantragen Sie Zugriff auf den ASG-Stack, der Ihnen Zugriff auf alle zugehörigen Instances gewährt.

Ein Beispiel für die Zugriffsanforderung finden Sie unter ReadOnly ReadOnly Zugriff: Anfordern.

ReadOnly Zugriff beantragen

ReadOnly Zugriff über die Konsole anfordern

Im Folgenden wird dieser Änderungstyp in der AMS-Konsole dargestellt.

So funktioniert es:

1. Navigieren Sie zur Seite RFC erstellen: Klicken Sie im linken Navigationsbereich der AMS-Konsole, um die RFCs Listenseite RFCszu öffnen, und klicken Sie dann auf RFC erstellen.
2. Wählen Sie in der Standardansicht „Änderungstypen durchsuchen“ einen beliebten Änderungstyp (CT) oder wählen Sie in der Ansicht „Nach Kategorie auswählen“ einen CT aus.
   - Nach Änderungstyp suchen: Sie können im Bereich Schnellerstellung auf ein beliebtes CT klicken, um sofort die Seite RFC ausführen zu öffnen. Beachten Sie, dass Sie mit Quick Create keine ältere CT-Version auswählen können.

     Verwenden Sie zum Sortieren CTs den Bereich Alle Änderungstypen in der Karten - oder Tabellenansicht. Wählen Sie in einer der Ansichten einen CT aus und klicken Sie dann auf RFC

erstellen, um die Seite RFC ausführen zu öffnen. Falls zutreffend, wird neben der Schaltfläche „RFC erstellen“ die Option Mit älterer Version erstellen angezeigt.

- Nach Kategorie auswählen: Wählen Sie eine Kategorie, eine Unterkategorie, einen Artikel und einen Vorgang aus. Daraufhin wird das Feld mit den CT-Details geöffnet. Dort können Sie gegebenenfalls die Option „Mit älterer Version erstellen“ auswählen. Klicken Sie auf RFC erstellen, um die Seite RFC ausführen zu öffnen.

3. Öffnen Sie auf der Seite RFC ausführen den Bereich CT-Name, um das Feld mit den CT-Details zu sehen. Ein Betreff ist erforderlich (dieser wird für Sie ausgefüllt, wenn Sie Ihr CT in der Ansicht „Änderungstypen durchsuchen“ auswählen). Öffnen Sie den Bereich Zusätzliche Konfiguration, um Informationen zum RFC hinzuzufügen.

   Verwenden Sie im Bereich Ausführungskonfiguration die verfügbaren Dropdownlisten oder geben Sie Werte für die erforderlichen Parameter ein. Um optionale Ausführungsparameter zu konfigurieren, öffnen Sie den Bereich Zusätzliche Konfiguration.

4. Wenn Sie fertig sind, klicken Sie auf Ausführen. Wenn keine Fehler vorliegen, wird die Seite mit dem RFC erfolgreich erstellt mit den übermittelten RFC-Details und der ersten Run-Ausgabe angezeigt.

5. Öffnen Sie den Bereich Run-Parameter, um die von Ihnen eingereichten Konfigurationen zu sehen. Aktualisieren Sie die Seite, um den RFC-Ausführungsstatus zu aktualisieren. Brechen Sie optional den RFC ab oder erstellen Sie eine Kopie davon mit den Optionen oben auf der Seite.

ReadOnly Zugriff mit der CLI anfordern

So funktioniert es:

1. Verwenden Sie entweder Inline Create (Sie geben einen `create-rfc` Befehl mit allen RFC- und Ausführungsparametern aus) oder Template Create (Sie erstellen zwei JSON-Dateien, eine für die RFC-Parameter und eine für die Ausführungsparameter) und geben Sie den `create-rfc` Befehl mit den beiden Dateien als Eingabe aus. Beide Methoden werden hier beschrieben.

2. Reichen Sie den `aws amscm submit-rfc --rfc-id` *`ID`* Befehl RFC: mit der zurückgegebenen RFC-ID ein.

   Überwachen Sie den RFC: -Befehl. `aws amscm get-rfc --rfc-id` *`ID`*

Verwenden Sie diesen Befehl, um die Version des Änderungstyps zu überprüfen:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Sie können alle `CreateRfc` Parameter mit jedem RFC verwenden, unabhängig davon, ob sie Teil des Schemas für den Änderungstyp sind oder nicht. Um beispielsweise Benachrichtigungen zu erhalten, wenn sich der RFC-Status ändert, fügen Sie diese Zeile dem RFC-Parameter-Teil der Anfrage hinzu (nicht den Ausführungsparametern). `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` Eine Liste aller CreateRfc Parameter finden Sie in der AMS Change Management API-Referenz.

INLINE-ERSTELLUNG:

Geben Sie den Befehl create RFC mit den direkt angegebenen Ausführungsparametern aus (vermeiden Sie Anführungszeichen, wenn Sie die Ausführungsparameter inline angeben), und senden Sie dann die zurückgegebene RFC-ID. Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:

```
aws --profile saml amscm create-rfc --change-type-id "ct-199h35t7uz6jl" --change-type-
version "3.0" --title "Stack-RO-Access-QC" --execution-parameters "{\"DomainFQDN\":
\"TEST.com\",\"StackIds\":[\"stack-01234567890abcdef\"],\"TimeRequestedInHours\":1,
\"Usernames\":[\"TEST\"],\"VpcId\":\"VPC_ID\"}"
```

VORLAGE ERSTELLEN:

1. Gibt das JSON-Schema der Ausführungsparameter für diesen Änderungstyp in eine Datei aus. In diesem Beispiel wird sie „ GrantReadOnlyAccessParams.json“ genannt:

   ```
   aws amscm get-change-type-version --change-type-id "ct-199h35t7uz6jl"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    GrantReadOnlyAccessParams.json
   ```

   Ändern und speichern Sie die GrantReadOnlyAccessParams Datei. Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:

   ```
   {
   ```

```
"DomainFQDN":           "mycorpdomain.acme.com",
"StackIds":             [STACK_ID, STACK_ID],
"TimeRequestedInHours": 12,
"Usernames":             ["USERNAME", "USERNAME"],
"VpcId":                "VPC_ID"
}
```

Beachten Sie, dass die `TimeRequestedInHours` Option standardmäßig auf eine Stunde eingestellt ist. Sie können bis zu zwölf Stunden anfordern.

2. Geben Sie die RFC-Vorlage in eine Datei in Ihrem aktuellen Ordner aus. In diesem Beispiel wird sie „ GrantReadOnlyAccessRfc.json“ genannt:

```
aws amscm create-rfc --generate-cli-skeleton > GrantReadOnlyAccessRfc.json
```

3. Ändern und speichern Sie die GrantReadOnlyAccessRfc JSON-Datei. Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:

```
{
"ChangeTypeId":         "ct-199h35t7uz6jl",
"ChangeTypeVersion":    "3.0",
"Title":                "Request-ReadOnly-Access-to-EC2-RFC"
}
```

4. Erstellen Sie den RFC und geben Sie die GrantReadOnlyAccessRfc Datei und die GrantReadOnlyAcessParams Datei an:

```
aws amscm create-rfc --cli-input-json file://GrantReadOnlyAccessRfc.json --
execution-parameters file://GrantReadOnlyAccessParams.json
```

Sie erhalten die ID des neuen RFC in der Antwort und können sie verwenden, um den RFC zu senden und zu überwachen. Bis Sie ihn abschicken, verbleibt der RFC im Bearbeitungszustand und startet nicht.

Um sich über eine Bastion bei der Instanz anzumelden, folgen Sie dem nächsten Verfahren, Beispiele für den Instanzzugriff.

Tipps

> **Note**
>
> Sie können eine Aktualisierung Ihrer Zugriffsanfrage einreichen, bevor sie abläuft. Einzelheiten finden Sie unter Stack Read-Only Access | Update.
> Um sich bei einer Instance anzumelden, die Teil einer EC2 Auto Scaling Scaling-Gruppe (ASG) ist, fordern Sie Zugriff auf den ASG-Stack an, der Ihnen Zugriff auf alle zugehörigen Instances gewährt.

Eine exemplarische Vorgehensweise zur Beantragung von Administratorzugriff finden Sie unter Administratorzugriff: beantragen.

Andere | Andere RFC, erstellen (CLI)

Dieses Beispiel zeigt, wie mithilfe von Management | Other | Other | Create CT (ct-1e1xtak34nx76) eine Änderung an keiner der verfügbaren CTs Adressen angefordert werden kann.

Verwenden Sie dieses CT, wenn Sie keinen gewünschten Änderungstyp finden können. Wenn Sie sich jedoch nicht sicher sind, ob Sie Parameter in einem vorhandenen CT angeben sollen, ist es besser, eine Serviceanfrage zu stellen, um Hilfe zu erhalten. Informationen zum Einreichen von Serviceanfragen finden Sie unter Beispiele für Serviceanfragen.

Diese Art von RFC ist genehmigungspflichtig, d. h., sie erfordert eine AMS-Genehmigung, bevor sie implementiert werden kann. Nach dem Absenden des RFC wird sich ein AMS-Mitarbeiter mit Ihnen in Verbindung setzen, um den Stack zu besprechen, den Sie bereitstellen möchten.

> **Note**
>
> Wenn Sie „Überprüfung erforderlich“ verwenden CTs, empfiehlt AMS, die ASAP-Scheduling-Option zu verwenden (wählen Sie ASAP in der Konsole, lassen Sie Start- und Endzeit leer in der API/CLI), da diese einen AMS-Operator CTs erfordern, der den RFC überprüft und möglicherweise mit Ihnen kommuniziert, bevor er genehmigt und ausgeführt werden kann. Wenn Sie diese einplanen, achten Sie darauf RFCs, dass Sie mindestens 24 Stunden einplanen. Wenn die Genehmigung nicht vor der geplanten Startzeit erfolgt, wird der RFC automatisch abgelehnt.

ERFORDERLICHE DATEN:

- `Comment`: Wofür der RFC ist.
- `ChangeTypeId`und`ChangeTypeVersion`: Verwenden Sie Other | Create (`ct-1e1xtak34nx76`), um neue Ressourcen anzufordern, verwenden Sie Other | Update (`ct-0xdawir96cy7k`), um bestehende Ressourcen zu ändern; beide sind `esv1`.

OPTIONALE DATEN`Priority`: Zulässige Werte sind `High`, `Medium`, oder`Low`.

INLINE-ERSTELLUNG:

- Geben Sie den Befehl create RFC mit den direkt angegebenen Ausführungsparametern aus (vermeiden Sie Anführungszeichen, wenn Sie die Ausführungsparameter inline angeben). Das Beispiel verwendet Other | Create.

```
aws amscm create-rfc --change-type-id "ct-1e1xtak34nx76" --change-type-version "1.0"
 --title "TITLE" --execution-parameters "{\"Comment\": \"What you want created\"}"
```

- Übermitteln Sie den RFC mit der RFC-ID, die bei der RFC-Erstellung zurückgegeben wurde. Bis zur Übermittlung verbleibt der RFC in seinem `Editing` Status und es wird nicht darauf reagiert.

```
aws amscm submit-rfc --rfc-id RFC_ID
```

- Überwachen Sie den RFC-Status und sehen Sie sich die Ausführungsausgabe an:

```
aws amscm get-rfc --rfc-id RFC_ID
```

VORLAGE ERSTELLEN:

1. Erstellen und speichern Sie eine JSON-Datei für die Ausführungsparameter. Beispiel nennt sie OtherParams .json und enthält den optionalen `Priority` Parameter:

```
{
"Comment":          "What you want created",
"Priority":         "Medium"
}
```

2. Erstellen und speichern Sie eine JSON-Datei für die RFC-Parameter; das Beispiel nennt sie OtherRfc .json.

```
{
"ChangeTypeId":          "ct-1e1xtak34nx76",
"ChangeTypeVersion":     "1.0",
"Title":                 "TITLE"
}
```

3. Erstellen Sie den RFC, indem Sie die OtherRfc Datei und die Datei angeben: OtherParams

```
aws amscm create-rfc --cli-input-json file://OtherRfc.json  --execution-parameters
 file://OtherParams.json
```

Sie erhalten den RfcId des neuen RFC in der Antwort. Beispiel:

```
{
"RfcId": "RFC-ID"
}
```

4. Reichen Sie den RFC ein:

```
aws amscm submit-rfc --rfc-id RFC-ID
```

Wenn keine Fehler gemeldet wurden, war der Vorgang erfolgreich.

5. Gehen Sie wie folgt vor, um den Status der Anfrage zu überwachen und die Ausführungsausgabe anzuzeigen:

```
aws amscm get-rfc --rfc-id RFC-ID
```

Beliebiger Stapel: Löschen, Neustarten, Starten, Stoppen

Sie können die AMS-Konsole oder API/CLI zum Löschen, Neustarten, Starten oder Stoppen eines AMS-Stacks verwenden.

Stapel löschen

Einen Stack mit der Konsole löschen

Screenshot dieses Änderungstyps in der AMS-Konsole:

So funktioniert es:

1. Navigieren Sie zur Seite RFC erstellen: Klicken Sie im linken Navigationsbereich der AMS-Konsole, um die RFCs Listenseite RFCszu öffnen, und klicken Sie dann auf RFC erstellen.
2. Wählen Sie in der Standardansicht „Änderungstypen durchsuchen“ einen beliebten Änderungstyp (CT) oder wählen Sie in der Ansicht „Nach Kategorie auswählen“ einen CT aus.
   - Nach Änderungstyp suchen: Sie können im Bereich Schnellerstellung auf ein beliebtes CT klicken, um sofort die Seite RFC ausführen zu öffnen. Beachten Sie, dass Sie mit Quick Create keine ältere CT-Version auswählen können.

     Verwenden Sie zum Sortieren CTs den Bereich Alle Änderungstypen in der Karten - oder Tabellenansicht. Wählen Sie in einer der Ansichten einen CT aus und klicken Sie dann auf RFC erstellen, um die Seite RFC ausführen zu öffnen. Falls zutreffend, wird neben der Schaltfläche „RFC erstellen“ die Option Mit älterer Version erstellen angezeigt.
   - Nach Kategorie auswählen: Wählen Sie eine Kategorie, eine Unterkategorie, einen Artikel und einen Vorgang aus. Daraufhin wird das Feld mit den CT-Details geöffnet. Dort können Sie gegebenenfalls die Option „Mit älterer Version erstellen“ auswählen. Klicken Sie auf RFC erstellen, um die Seite RFC ausführen zu öffnen.
3. Öffnen Sie auf der Seite RFC ausführen den Bereich CT-Name, um das Feld mit den CT-Details zu sehen. Ein Betreff ist erforderlich (dieser wird für Sie ausgefüllt, wenn Sie Ihr CT in der Ansicht „Änderungstypen durchsuchen“ auswählen). Öffnen Sie den Bereich Zusätzliche Konfiguration, um Informationen zum RFC hinzuzufügen.

   Verwenden Sie im Bereich Ausführungskonfiguration die verfügbaren Dropdownlisten oder geben Sie Werte für die erforderlichen Parameter ein. Um optionale Ausführungsparameter zu konfigurieren, öffnen Sie den Bereich Zusätzliche Konfiguration.
4. Wenn Sie fertig sind, klicken Sie auf Ausführen. Wenn keine Fehler vorliegen, wird die Seite mit dem RFC erfolgreich erstellt mit den übermittelten RFC-Details und der ersten Run-Ausgabe angezeigt.
5. Öffnen Sie den Bereich Run-Parameter, um die von Ihnen eingereichten Konfigurationen zu sehen. Aktualisieren Sie die Seite, um den RFC-Ausführungsstatus zu aktualisieren. Optional können Sie den RFC abbrechen oder eine Kopie davon mit den Optionen oben auf der Seite erstellen.

Löschen eines Stacks mit der CLI

So funktioniert es:

1. Verwenden Sie entweder Inline Create (Sie geben einen `create-rfc` Befehl mit allen RFC- und Ausführungsparametern aus) oder Template Create (Sie erstellen zwei JSON-Dateien, eine für die RFC-Parameter und eine für die Ausführungsparameter) und geben Sie den `create-rfc` Befehl mit den beiden Dateien als Eingabe aus. Beide Methoden werden hier beschrieben.
2. Reichen Sie den `aws amscm submit-rfc --rfc-id` *ID* Befehl RFC: mit der zurückgegebenen RFC-ID ein.

   Überwachen Sie den RFC: -Befehl. `aws amscm get-rfc --rfc-id` *ID*

Verwenden Sie diesen Befehl, um die Version des Änderungstyps zu überprüfen:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Sie können alle `CreateRfc` Parameter mit jedem RFC verwenden, unabhängig davon, ob sie Teil des Schemas für den Änderungstyp sind oder nicht. Um beispielsweise Benachrichtigungen zu erhalten, wenn sich der RFC-Status ändert, fügen Sie diese Zeile dem RFC-Parameter-Teil der Anfrage hinzu (nicht den Ausführungsparametern). `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` Eine Liste aller CreateRfc Parameter finden Sie in der AMS Change Management API-Referenz.

INLINE-ERSTELLUNG:

Geben Sie den Befehl create RFC mit den direkt angegebenen Ausführungsparametern aus (vermeiden Sie Anführungszeichen, wenn Sie die Ausführungsparameter inline angeben), und senden Sie dann die zurückgegebene RFC-ID. Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:

```
aws amscm create-rfc --change-type-id "ct-0q0bic0ywqk6c" --change-type-version "1.0" --
title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

VORLAGE ERSTELLEN:

1. Geben Sie die RFC-Vorlage in eine Datei in Ihrem aktuellen Ordner aus. Dieses Beispiel nennt sie DeleteStackRfc .json:

   ```
   aws amscm create-rfc --generate-cli-skeleton > DeleteStackRfc.json
   ```

2. Ändern und speichern Sie die DeleteStackRfc JSON-Datei.

   Die internen Anführungszeichen in der ExecutionParameters JSON-Erweiterung müssen mit einem umgekehrten Schrägstrich (\) maskiert werden. Beispiel ohne Start- und Endzeit:

   ```
   {
   "ChangeTypeVersion":    "1.0",
   "ChangeTypeId":         "ct-0q0bic0ywqk6c",
   "Title":                "Delete-My-Stack-RFC"
   "ExecutionParameters":  "{
           \"StackId\":\"STACK_ID\"}"
   }
   ```

3. Erstellen Sie den RFC:

   ```
   aws amscm create-rfc --cli-input-json file://DeleteStackRfc.json
   ```

   In der Antwort erhalten Sie die ID des neuen RFC und können damit den RFC einreichen und überwachen. Bis Sie ihn abschicken, verbleibt der RFC im Bearbeitungszustand und startet nicht.

Tipps

> **Note**
>
> Wenn ein S3-Bucket gelöscht wird, muss er zuerst von Objekten geleert werden.

> **Important**
>
> Das Löschen von Stacks kann unerwünschte und unerwartete Folgen haben. Wichtige Vorbehalte finden Sie im Abschnitt RFCs RFC-Fehlerbehebung für Delete Stack.

Den Stack neu starten

Einen Stack mit der Konsole neu starten

Screenshot dieses Änderungstyps in der AMS-Konsole:

So funktioniert es:

1. Navigieren Sie zur Seite RFC erstellen: Klicken Sie im linken Navigationsbereich der AMS-Konsole, um die RFCs Listenseite RFCszu öffnen, und klicken Sie dann auf RFC erstellen.
2. Wählen Sie in der Standardansicht „Änderungstypen durchsuchen“ einen beliebten Änderungstyp (CT) oder wählen Sie in der Ansicht „Nach Kategorie auswählen“ einen CT aus.
   - Nach Änderungstyp suchen: Sie können im Bereich Schnellerstellung auf ein beliebtes CT klicken, um sofort die Seite RFC ausführen zu öffnen. Beachten Sie, dass Sie mit Quick Create keine ältere CT-Version auswählen können.

     Verwenden Sie zum Sortieren CTs den Bereich Alle Änderungstypen in der Karten - oder Tabellenansicht. Wählen Sie in einer der Ansichten einen CT aus und klicken Sie dann auf RFC erstellen, um die Seite RFC ausführen zu öffnen. Falls zutreffend, wird neben der Schaltfläche „RFC erstellen“ die Option Mit älterer Version erstellen angezeigt.
   - Nach Kategorie auswählen: Wählen Sie eine Kategorie, eine Unterkategorie, einen Artikel und einen Vorgang aus. Daraufhin wird das Feld mit den CT-Details geöffnet. Dort können Sie gegebenenfalls die Option „Mit älterer Version erstellen“ auswählen. Klicken Sie auf RFC erstellen, um die Seite RFC ausführen zu öffnen.
3. Öffnen Sie auf der Seite RFC ausführen den Bereich CT-Name, um das Feld mit den CT-Details zu sehen. Ein Betreff ist erforderlich (dieser wird für Sie ausgefüllt, wenn Sie Ihr CT in der Ansicht „Änderungstypen durchsuchen“ auswählen). Öffnen Sie den Bereich Zusätzliche Konfiguration, um Informationen zum RFC hinzuzufügen.

   Verwenden Sie im Bereich Ausführungskonfiguration die verfügbaren Dropdownlisten oder geben Sie Werte für die erforderlichen Parameter ein. Um optionale Ausführungsparameter zu konfigurieren, öffnen Sie den Bereich Zusätzliche Konfiguration.
4. Wenn Sie fertig sind, klicken Sie auf Ausführen. Wenn keine Fehler vorliegen, wird die Seite mit dem RFC erfolgreich erstellt mit den übermittelten RFC-Details und der ersten Run-Ausgabe angezeigt.
5. Öffnen Sie den Bereich Run-Parameter, um die von Ihnen eingereichten Konfigurationen zu sehen. Aktualisieren Sie die Seite, um den RFC-Ausführungsstatus zu aktualisieren. Optional

können Sie den RFC abbrechen oder eine Kopie davon mit den Optionen oben auf der Seite erstellen.

Einen Stack mit der CLI neu starten

So funktioniert es:

1. Verwenden Sie entweder Inline Create (Sie geben einen `create-rfc` Befehl mit allen RFC- und Ausführungsparametern aus) oder Template Create (Sie erstellen zwei JSON-Dateien, eine für die RFC-Parameter und eine für die Ausführungsparameter) und geben Sie den `create-rfc` Befehl mit den beiden Dateien als Eingabe aus. Beide Methoden werden hier beschrieben.
2. Reichen Sie den `aws amscm submit-rfc --rfc-id` *`ID`* Befehl RFC: mit der zurückgegebenen RFC-ID ein.

   Überwachen Sie den RFC: -Befehl. `aws amscm get-rfc --rfc-id` *`ID`*

Verwenden Sie diesen Befehl, um die Version des Änderungstyps zu überprüfen:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Sie können alle `CreateRfc` Parameter mit jedem RFC verwenden, unabhängig davon, ob sie Teil des Schemas für den Änderungstyp sind oder nicht. Um beispielsweise Benachrichtigungen zu erhalten, wenn sich der RFC-Status ändert, fügen Sie diese Zeile dem RFC-Parameter-Teil der Anfrage hinzu (nicht den Ausführungsparametern). `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` Eine Liste aller CreateRfc Parameter finden Sie in der AMS Change Management API-Referenz.

INLINE-ERSTELLUNG:

Geben Sie den Befehl create RFC mit den direkt angegebenen Ausführungsparametern aus (vermeiden Sie Anführungszeichen, wenn Sie die Ausführungsparameter inline angeben), und senden Sie dann die zurückgegebene RFC-ID. Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:

```
aws amscm create-rfc --change-type-id "ct-02u0hoaa9grat" --change-type-version "1.0" --
title "Reboot My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

VORLAGE ERSTELLEN:

1. Geben Sie die RFC-Vorlage in eine Datei in Ihrem aktuellen Ordner aus. In diesem Beispiel wird sie „ RebootStackRfc.json“ genannt. Beachten Sie, dass es nur einen Ausführungsparameter zum Stoppen (Neustarten oder Starten) einer Instanz gibt, der Ausführungsparameter in der JSON-Schemadatei selbst enthalten sein kann und es nicht erforderlich ist, eine separate JSON-Datei mit Ausführungsparametern zu erstellen.

   ```
   aws amscm create-rfc --generate-cli-skeleton > StopInstanceRfc.json
   ```

2. Ändern und speichern Sie die RebootStackRfc JSON-Datei.

   Die internen Anführungszeichen in der `ExecutionParameters` JSON-Erweiterung müssen mit einem umgekehrten Schrägstrich (\) maskiert werden. Beispiel:

   ```
   {
   "ChangeTypeId":          "ct-02u0hoaa9grat",
   "Title":                 "Reboot-My-EC2-RFC",
   "TimeoutInMinutes":      60,
   "ExecutionParameters":   "{
           \"StackId\":\"STACK_ID\"
       }"
   }
   ```

3. Erstellen Sie den RFC:

   ```
   aws amscm create-rfc --cli-input-json file://RebootStackRfc.json
   ```

   In der Antwort erhalten Sie die ID des neuen RFC und können damit den RFC einreichen und überwachen. Bis Sie ihn abschicken, verbleibt der RFC im Bearbeitungszustand und startet nicht.

Tipps

Informationen zu Application Load Balancers finden Sie unter Application Load Balancers.

Starten Sie den Stack

Einen Stack mit der Konsole starten

Screenshot dieses Änderungstyps in der AMS-Konsole:

So funktioniert es:

1. Navigieren Sie zur Seite RFC erstellen: Klicken Sie im linken Navigationsbereich der AMS-Konsole, um die RFCs Listenseite RFCszu öffnen, und klicken Sie dann auf RFC erstellen.
2. Wählen Sie in der Standardansicht „Änderungstypen durchsuchen“ einen beliebten Änderungstyp (CT) oder wählen Sie in der Ansicht „Nach Kategorie auswählen“ einen CT aus.
   - Nach Änderungstyp suchen: Sie können im Bereich Schnellerstellung auf ein beliebtes CT klicken, um sofort die Seite RFC ausführen zu öffnen. Beachten Sie, dass Sie mit Quick Create keine ältere CT-Version auswählen können.

     Verwenden Sie zum Sortieren CTs den Bereich Alle Änderungstypen in der Karten - oder Tabellenansicht. Wählen Sie in einer der Ansichten einen CT aus und klicken Sie dann auf RFC erstellen, um die Seite RFC ausführen zu öffnen. Falls zutreffend, wird neben der Schaltfläche „RFC erstellen“ die Option Mit älterer Version erstellen angezeigt.
   - Nach Kategorie auswählen: Wählen Sie eine Kategorie, eine Unterkategorie, einen Artikel und einen Vorgang aus. Daraufhin wird das Feld mit den CT-Details geöffnet. Dort können Sie gegebenenfalls die Option „Mit älterer Version erstellen“ auswählen. Klicken Sie auf RFC erstellen, um die Seite RFC ausführen zu öffnen.
3. Öffnen Sie auf der Seite RFC ausführen den Bereich CT-Name, um das Feld mit den CT-Details zu sehen. Ein Betreff ist erforderlich (dieser wird für Sie ausgefüllt, wenn Sie Ihr CT in der Ansicht „Änderungstypen durchsuchen“ auswählen). Öffnen Sie den Bereich Zusätzliche Konfiguration, um Informationen zum RFC hinzuzufügen.

   Verwenden Sie im Bereich Ausführungskonfiguration die verfügbaren Dropdownlisten oder geben Sie Werte für die erforderlichen Parameter ein. Um optionale Ausführungsparameter zu konfigurieren, öffnen Sie den Bereich Zusätzliche Konfiguration.
4. Wenn Sie fertig sind, klicken Sie auf Ausführen. Wenn keine Fehler vorliegen, wird die Seite mit dem RFC erfolgreich erstellt mit den übermittelten RFC-Details und der ersten Run-Ausgabe angezeigt.
5. Öffnen Sie den Bereich Run-Parameter, um die von Ihnen eingereichten Konfigurationen zu sehen. Aktualisieren Sie die Seite, um den RFC-Ausführungsstatus zu aktualisieren. Optional

können Sie den RFC abbrechen oder eine Kopie davon mit den Optionen oben auf der Seite erstellen.

Einen Stack mit der CLI starten

So funktioniert es:

1. Verwenden Sie entweder Inline Create (Sie geben einen `create-rfc` Befehl mit allen RFC- und Ausführungsparametern aus) oder Template Create (Sie erstellen zwei JSON-Dateien, eine für die RFC-Parameter und eine für die Ausführungsparameter) und geben Sie den `create-rfc` Befehl mit den beiden Dateien als Eingabe aus. Beide Methoden werden hier beschrieben.
2. Reichen Sie den `aws amscm submit-rfc --rfc-id` *`ID`* Befehl RFC: mit der zurückgegebenen RFC-ID ein.

   Überwachen Sie den RFC: -Befehl. `aws amscm get-rfc --rfc-id` *`ID`*

Verwenden Sie diesen Befehl, um die Version des Änderungstyps zu überprüfen:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Sie können alle `CreateRfc` Parameter mit jedem RFC verwenden, unabhängig davon, ob sie Teil des Schemas für den Änderungstyp sind oder nicht. Um beispielsweise Benachrichtigungen zu erhalten, wenn sich der RFC-Status ändert, fügen Sie diese Zeile dem RFC-Parameter-Teil der Anfrage hinzu (nicht den Ausführungsparametern). `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` Eine Liste aller CreateRfc Parameter finden Sie in der AMS Change Management API-Referenz.

INLINE-ERSTELLUNG:

Geben Sie den Befehl create RFC mit den direkt angegebenen Ausführungsparametern aus (vermeiden Sie Anführungszeichen, wenn Sie die Ausführungsparameter inline angeben), und senden Sie dann die zurückgegebene RFC-ID. Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:

```
aws amscm create-rfc --change-type-id "ct-1h5xgl9cr4bzy" --change-type-version "1.0" --
title "Start My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

VORLAGE ERSTELLEN:

1. Geben Sie die RFC-Vorlage in eine Datei in Ihrem aktuellen Ordner aus. In diesem Beispiel wird sie „ StartInstanceRfc.json“ genannt. Beachten Sie, dass es nur einen Ausführungsparameter zum Starten eines Stacks gibt, der Ausführungsparameter in der JSON-Schema-Datei selbst enthalten sein kann und es nicht erforderlich ist, eine separate JSON-Datei mit Ausführungsparametern zu erstellen.

   ```
   aws amscm create-rfc --generate-cli-skeleton > StartStackRfc.json
   ```

2. Ändern und speichern Sie die StartStackRfc JSON-Datei. Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:

   ```
   {
   "ChangeTypeId":         "ct-1h5xgl9cr4bzy",
   "Title":                "Start-My-EC2-RFC",
   "TimeoutInMinutes":     60,
   "ExecutionParameters":  "{
           \"StackId\":\"STACK_ID\"
       }"
   }
   ```

3. Erstellen Sie den RFC:

   ```
   aws amscm create-rfc --cli-input-json file://StartStackRfc.json
   ```

   In der Antwort erhalten Sie die ID des neuen RFC und können damit den RFC einreichen und überwachen. Bis Sie ihn abschicken, verbleibt der RFC im Bearbeitungszustand und startet nicht.

Tipps

Informationen zu Application Load Balancers finden Sie unter Application Load Balancers.

Stapel beenden

Stoppen eines Stacks mit der Konsole

Screenshot dieses Änderungstyps in der AMS-Konsole:

So funktioniert es:

1. Navigieren Sie zur Seite RFC erstellen: Klicken Sie im linken Navigationsbereich der AMS-Konsole, um die RFCs Listenseite RFCszu öffnen, und klicken Sie dann auf RFC erstellen.
2. Wählen Sie in der Standardansicht „Änderungstypen durchsuchen“ einen beliebten Änderungstyp (CT) oder wählen Sie in der Ansicht „Nach Kategorie auswählen“ einen CT aus.
   - Nach Änderungstyp suchen: Sie können im Bereich Schnellerstellung auf ein beliebtes CT klicken, um sofort die Seite RFC ausführen zu öffnen. Beachten Sie, dass Sie mit Quick Create keine ältere CT-Version auswählen können.

     Verwenden Sie zum Sortieren CTs den Bereich Alle Änderungstypen in der Karten - oder Tabellenansicht. Wählen Sie in einer der Ansichten einen CT aus und klicken Sie dann auf RFC erstellen, um die Seite RFC ausführen zu öffnen. Falls zutreffend, wird neben der Schaltfläche „RFC erstellen“ die Option Mit älterer Version erstellen angezeigt.
   - Nach Kategorie auswählen: Wählen Sie eine Kategorie, eine Unterkategorie, einen Artikel und einen Vorgang aus. Daraufhin wird das Feld mit den CT-Details geöffnet. Dort können Sie gegebenenfalls die Option „Mit älterer Version erstellen“ auswählen. Klicken Sie auf RFC erstellen, um die Seite RFC ausführen zu öffnen.
3. Öffnen Sie auf der Seite RFC ausführen den Bereich CT-Name, um das Feld mit den CT-Details zu sehen. Ein Betreff ist erforderlich (dieser wird für Sie ausgefüllt, wenn Sie Ihr CT in der Ansicht „Änderungstypen durchsuchen“ auswählen). Öffnen Sie den Bereich Zusätzliche Konfiguration, um Informationen zum RFC hinzuzufügen.

   Verwenden Sie im Bereich Ausführungskonfiguration die verfügbaren Dropdownlisten oder geben Sie Werte für die erforderlichen Parameter ein. Um optionale Ausführungsparameter zu konfigurieren, öffnen Sie den Bereich Zusätzliche Konfiguration.
4. Wenn Sie fertig sind, klicken Sie auf Ausführen. Wenn keine Fehler vorliegen, wird die Seite mit dem RFC erfolgreich erstellt mit den übermittelten RFC-Details und der ersten Run-Ausgabe angezeigt.
5. Öffnen Sie den Bereich Run-Parameter, um die von Ihnen eingereichten Konfigurationen zu sehen. Aktualisieren Sie die Seite, um den RFC-Ausführungsstatus zu aktualisieren. Optional

können Sie den RFC abbrechen oder eine Kopie davon mit den Optionen oben auf der Seite erstellen.

Stoppen eines Stacks mit der CLI

So funktioniert es:

1. Verwenden Sie entweder Inline Create (Sie geben einen `create-rfc` Befehl mit allen RFC- und Ausführungsparametern aus) oder Template Create (Sie erstellen zwei JSON-Dateien, eine für die RFC-Parameter und eine für die Ausführungsparameter) und geben Sie den `create-rfc` Befehl mit den beiden Dateien als Eingabe aus. Beide Methoden werden hier beschrieben.
2. Reichen Sie den `aws amscm submit-rfc --rfc-id` *`ID`* Befehl RFC: mit der zurückgegebenen RFC-ID ein.

   Überwachen Sie den RFC: -Befehl. `aws amscm get-rfc --rfc-id` *`ID`*

Verwenden Sie diesen Befehl, um die Version des Änderungstyps zu überprüfen:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Sie können alle `CreateRfc` Parameter mit jedem RFC verwenden, unabhängig davon, ob sie Teil des Schemas für den Änderungstyp sind oder nicht. Um beispielsweise Benachrichtigungen zu erhalten, wenn sich der RFC-Status ändert, fügen Sie diese Zeile dem RFC-Parameter-Teil der Anfrage hinzu (nicht den Ausführungsparametern). `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` Eine Liste aller CreateRfc Parameter finden Sie in der AMS Change Management API-Referenz.

INLINE-ERSTELLUNG:

Geben Sie den Befehl create RFC mit den direkt angegebenen Ausführungsparametern aus (vermeiden Sie Anführungszeichen, wenn Sie die Ausführungsparameter inline angeben), und senden Sie dann die zurückgegebene RFC-ID. Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:

```
aws amscm create-rfc --change-type-id "ct-3dgbnh6gpst4d" --change-type-version "1.0" --
title "Stop My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

VORLAGE ERSTELLEN:

1. Geben Sie die RFC-Vorlage in eine Datei in Ihrem aktuellen Ordner aus. In diesem Beispiel wird sie „ StopStackRfc.json“ genannt. Beachten Sie, dass es nur einen Ausführungsparameter zum Stoppen (Neustarten oder Starten) einer Instanz gibt, der Ausführungsparameter in der JSON-Schemadatei selbst enthalten sein kann und es nicht erforderlich ist, eine separate JSON-Datei mit Ausführungsparametern zu erstellen.

   ```
   aws amscm create-rfc --generate-cli-skeleton > StopStackRfc.json
   ```

2. Ändern und speichern Sie die StopStackRfc JSON-Datei. Sie können den Inhalt beispielsweise durch etwas Ähnliches ersetzen:

   ```
   {
   "ChangeTypeId":          "ct-3dgbnh6gpst4d",
   "Title":                 "Stop-My-EC2-RFC",
   "TimeoutInMinutes":      60,
   "ExecutionParameters":   "{
           \"StackId\":\"STACK_ID\"
       }"
   }
   ```

3. Erstellen Sie den RFC:

   ```
   aws amscm create-rfc --cli-input-json file://StopInstanceRfc.json
   ```

   In der Antwort erhalten Sie die ID des neuen RFC und können damit den RFC einreichen und überwachen. Bis Sie ihn abschicken, verbleibt der RFC im Bearbeitungszustand und startet nicht.

Tipps

Gestoppte Instanzen bleiben gestoppt, es sei denn, Sie haben Neustarts mit dem AMS Resource Scheduler geplant.

Falls erforderlich, finden Sie weitere Informationen unter Stoppen des EC2 Instance-Stacks scheitern.

Beispiele aufrufen

Diese Beispiele zeigen, wie Sie sich über eine Bastion bei einer Instance anmelden, nachdem Ihnen der Zugriff über einen RFC gewährt wurde. Einzelheiten zur Gewährung von Zugriff finden Sie unter Zugriffsanfragen.

> **Note**
>
> Eine EC2 Instance, die über eine Auto Scaling Scaling-Gruppe erstellt wurde, hat eine IP-Adresse, die hin und her wechselt, und Sie müssen Ihre EC2 Konsole verwenden, um diese IP-Adresse zu finden.

Erforderliche Daten:

- DNS-freundlicher Name oder IP-Adresse von Bastion: Verwenden Sie einen DNS-freundlichen Namen, wie unter beschrieben, DNS-freundliche Bastion-Namen oder suchen Sie nach Bastion-IP-Adressen, wie unter beschrieben. Suchen nach Bastion-IP-Adressen
- Benutzername (zum Beispiel username@customerdomain.com) und Passwort: Zugangsdaten für das Konto.
- Stack-IP-Adresse: Finden Sie diese, indem Sie auf der Stack-Seite der AMS-Konsole nach dem Stack suchen, bei dem Sie sich anmelden möchten, und dann in der EC2 Konsole für Ihr Konto nach dieser Stack-ID filtern. Für eine einzelne EC2 Instance können Sie auch den AMS SKMS-Befehl verwenden. Die AMS SKMS-API-Referenz finden Sie auf der Registerkarte Berichte in der AWS Artifact Console. Sie finden die Stack-ID und dann die AMS SKMS-API-Referenz finden Sie auf der Registerkarte Berichte in der AWS Artifact Console. Dort finden Sie die Stack-IP-Adresse.

Greifen Sie auf die Bastion-IP-Adresse zu, entweder SSH oder RDP, je nach Bedarf, und melden Sie sich mit einem der folgenden Verfahren an.

Linux-Computer zu Linux-Instanz

Verwenden Sie SSH, um eine Verbindung zur SSH-Bastion und dann zur Linux-Instanz herzustellen.

MALZ

Weitere Informationen zu den Friendly Bastion Names finden Sie unter DNS-Bastionen.

Um eine Verbindung zur Linux-Instance herzustellen, müssen Sie zunächst eine Verbindung zu einer SSH-Bastion herstellen.

1. Öffnen Sie ein Shell-Fenster und geben Sie ein:

```
ssh Domain_FQDN\\Username@SSH_bastion_name
    or SSH_bastion_IP
```

Das würde so aussehen, wenn Ihr Domain_FQDN „corp.domain.com“ lautet, Ihre Kontonummer „123456789123" lautet, Ihre Domain „amazonaws.com“ lautet, Sie Bastion „4" wählen und Ihr Benutzername" „lautet: JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion4.A123456789123.amazonaws.com
```

2. Melden Sie sich mit den Active Directory-Anmeldeinformationen Ihres Unternehmens an.
3. Wenn Sie eine Bash-Eingabeaufforderung erhalten, melden Sie sich per SSH bei der Instanz an und geben Sie dann Folgendes ein:

```
ssh Domain_FQDN\\Username@Instance_IP
```

Sie können auch das Login-Flag (-l) verwenden:

```
ssh -l Domain_FQDN\\Username@Instance_IP
```

SALZ

Weitere Informationen zu den freundlichen Bastionsnamen finden Sie unter DNS-Bastionen.

Um eine Verbindung zur Linux-Instance herzustellen, müssen Sie zunächst eine Verbindung zu einer SSH-Bastion herstellen.

1. Öffnen Sie ein Shell-Fenster und geben Sie ein:

```
ssh DOMAIN_FQDN\\USERNAME@SSH_BASTION_name
    or SSH_BASTION_IP
```

Das würde so aussehen, wenn Ihre Kontonummer 123456789123 lautet, Sie Bastion 4 wählen und Ihr Benutzername lautet: JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion1.A123456789123.amazonaws.com
```

2. Melden Sie sich mit den Active Directory-Anmeldeinformationen Ihres Unternehmens an.
3. Wenn Sie eine Bash-Eingabeaufforderung erhalten, melden Sie sich per SSH bei der Instanz an und geben Sie dann Folgendes ein:

   ```
   ssh DOMAIN_FQDN\\USERNAME@INSTANCE_IP
   ```

   Sie können auch das Login-Flag (-l) verwenden:

   ```
   ssh -l DOMAIN_FQDN\\USERNAME@INSTANCE_IP
   ```

Linux-Computer zur Windows-Instanz

Verwenden Sie einen SSH-Tunnel und einen RDP-Client, um von Ihrem Linux-Computer aus eine Verbindung zu einer Windows-Instanz herzustellen.

MALZ

Für dieses Verfahren ist ein Remote Desktop Connection-Client für Linux erforderlich. Das Beispiel verwendet Microsoft Remote Desktop (ein Open-Source-UNIX-Client für die Verbindung mit Windows Remote Desktop Services). Rdesktop ist eine Alternative.

> **Note**
>
> Die Art und Weise, wie Sie sich bei Windows-Instanzen anmelden, kann sich je nach verwendetem Remote-Desktop-Client ändern.

Zuerst richten Sie einen SSH-Tunnel ein und melden sich dann an.

Weitere Informationen zu den Namen der freundlichen Bastion finden Sie unter. DNS-freundliche Bastion-Namen

Bevor Sie beginnen:

- Fordern Sie Zugriff auf die Instance an, zu der Sie eine Verbindung herstellen möchten. Weitere Informationen finden Sie unter Zugriffsanforderungen.

- Wählen Sie einen benutzerfreundlichen DNS-SSH-Bastionsnamen, zu dem Sie eine Verbindung herstellen möchten. Beispiel:

  ```
  sshbastion(1-4).Your_Domain
  ```

  Das würde so aussehen, wenn Ihr Domain_FQDN „corp.domain.com“ lautet, Ihre AMS-verwaltete Your_Domain „amazonaws.com“ lautet, Sie Bastion „4" wählen und Ihr Benutzername" „lautet: JoeSmith

  ```
  ssh corp.domain.com\\JoeSmith sshbastion4.amazonaws.com
  ```

- Suchen Sie die IP-Adresse der Instance, zu der Sie eine Verbindung herstellen möchten. Weitere Informationen finden Sie unter Instance-ID oder IP-Adresse suchen.

1. Richten Sie RDP über einen SSH-Tunnel von einem Linux-Desktop zu einer Windows-Instanz ein. Um den `ssh` Befehl mit den richtigen Werten auszugeben, gibt es mehrere Möglichkeiten, vorzugehen:

   - Stellen Sie in der Linux-Shell die Variablen ein und geben Sie dann den SSH-Verbindungsbefehl ein:

     ```
     BASTION="sshbastion(1-4).Your_Domain""
     WINDOWS="Windows_Instance_Private_IP"
     AD="AD_Account_Number"
     USER="AD_Username"
     ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
     ```

     Beispiel, wenn die folgenden Werte verwendet werden:

     ```
     BASTION="sshbastion4.A123456789123.amazonaws.com"

     WINDOWS="172.16.3.254"

     AD="ACORP_example"

     USER="john.doe"
     ```

   - Fügen Sie die Variablenwerte direkt zum `ssh` Befehl hinzu.

In beiden Fällen würde die gerenderte Anfrage wie folgt aussehen (unter der Annahme desselben Satzes von Variablenwerten):

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\\john.doe@myamsadomain.com
```

2. Entweder: Öffnen Sie Ihren Remote Desktop Client, geben Sie die Loopback-Adresse und den Port 127.0.0. 1:3389 ein und öffnen Sie dann die Verbindung.

   Oder melden Sie sich über eine neue Linux-Desktop-Shell bei der Windows-Instanz an. Wenn Sie verwenden RDesktop, sieht der Befehl wie folgt aus:

   ```
   rdesktop 127.0.0.1:3389
   ```

   Ein Remote-Desktop-Fenster für die Windows-Instanz wird auf Ihrem Linux-Desktop angezeigt.

   > **Tip**
   >
   > Wenn die Remote-Desktop-Sitzung nicht gestartet werden kann, überprüfen Sie in Schritt 1, ob die Netzwerkkonnektivität zur Windows-Instanz von der SSH-Bastion auf Port 3389 von der Shell aus zulässig ist (ersetzen Sie `private_ip_address_of_windows_instance` sie entsprechend):
   >
   > ```
   > nc private_ip_address_of_windows_instance 3389 -v –z
   > ```
   >
   > Erfolgreich:
   >
   > ```
   > nc 172.16.0.83 3389 -v -z
   >        Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
   >        netstat -anvp | grep 3389
   >        tcp    0     0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
   > ```

SALZ

Dieses Verfahren für eine landing zone mit einem Konto erfordert einen Remote Desktop Connection-Client für Linux. Das Beispiel verwendet Microsoft Remote Desktop (ein Open-

Source-UNIX-Client für die Verbindung mit Windows Remote Desktop Services). Rdesktop ist eine Alternative.

> **Note**
>
> Die Art und Weise, wie Sie sich bei Windows-Instanzen anmelden, kann sich je nach verwendetem Remote-Desktop-Client ändern.

Zuerst richten Sie einen SSH-Tunnel ein und melden sich dann an.

Weitere Informationen zu den Namen der freundlichen Bastion finden Sie unter. DNS-freundliche Bastion-Namen

Bevor Sie beginnen:

- Fordern Sie Zugriff auf die Instance an, zu der Sie eine Verbindung herstellen möchten. Weitere Informationen finden Sie unter Zugriffsanforderungen.
- Wählen Sie einen benutzerfreundlichen DNS-SSH-Bastionsnamen, zu dem Sie eine Verbindung herstellen möchten. Beispiel:

  ```
  sshbastion(1-4).AAMSAccountNumber.amazonaws.com
  ```

  Das würde so aussehen, wenn deine Kontonummer 123456789123 lautet und du Bastion 4 wählst:

  ```
  sshbastion4.A123456789123.amazonaws.com
  ```

- Suchen Sie die IP-Adresse der Instance, zu der Sie eine Verbindung herstellen möchten. Weitere Informationen finden Sie unter Instanz-ID oder IP-Adresse finden.

1. Richten Sie RDP über einen SSH-Tunnel von einem Linux-Desktop zu einer Windows-Instanz ein. Um den `ssh` Befehl mit den richtigen Werten auszugeben, gibt es mehrere Möglichkeiten, vorzugehen:

   - Stellen Sie in der Linux-Shell die Variablen ein und geben Sie dann den SSH-Verbindungsbefehl ein:

     ```
     BASTION="sshbastion(1-4).AAMSAccountNumber.amazonaws.com"
     ```

```
WINDOWS="WINDOWS_INSTANCE_PRIVATE_IP"
AD="AD_ACCOUNT_NUMBER"
USER="AD_USERNAME"
ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
```

Beispiel, wenn die folgenden Werte verwendet werden:

```
BASTION="sshbastion4.A123456789123.amazonaws.com"

WINDOWS="172.16.3.254"

AD="ACORP_example"

USER="john.doe"
```

- Fügen Sie die Variablenwerte direkt zum `ssh` Befehl hinzu.

In beiden Fällen würde die gerenderte Anfrage wie folgt aussehen (unter der Annahme desselben Satzes von Variablenwerten):

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\
\john.doe@sshbastion4.A123456789123.amazonaws.com
```

2. Entweder: Öffnen Sie Ihren Remote Desktop Client, geben Sie die Loopback-Adresse und den Port 127.0.0. 1:3389 ein und öffnen Sie dann die Verbindung.

   Oder melden Sie sich über eine neue Linux-Desktop-Shell bei der Windows-Instanz an. Wenn Sie verwenden RDesktop, sieht der Befehl wie folgt aus:

   ```
   rdesktop 127.0.0.1:3389
   ```

   Ein Remote-Desktop-Fenster für die Windows-Instanz wird auf Ihrem Linux-Desktop angezeigt.

   > **Tip**
   >
   > Wenn die Remote-Desktop-Sitzung nicht gestartet werden kann, überprüfen Sie in Schritt 1, ob die Netzwerkkonnektivität zur Windows-Instanz von der SSH-Bastion auf Port 3389 von der Shell aus zulässig ist (ersetzen Sie `private_ip_address_of_windows_instance` sie entsprechend):

```
nc private_ip_address_of_windows_instance 3389 -v -z
```

Erfolgreich:

```
nc 172.16.0.83 3389 -v -z
        Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
        netstat -anvp | grep 3389
        tcp    0     0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
```

Windows-Computer zur Windows-Instanz

Verwenden Sie den Windows Remote Desktop Connection-Client, um von Ihrem Windows-Computer aus eine Verbindung zu einer Windows-Instanz herzustellen.

MALZ

Weitere Informationen zu den Namen der freundlichen Bastion finden Sie unterDNS-freundliche Bastion-Namen.

1. Öffnen Sie das Programm Remote Desktop Connection, ein Windows-Standardprogramm, und geben Sie den freundlichen DNS-Namen der Windows-Bastion in das Feld Hostname ein.

2. Wählen Sie Connect aus. Die Remotedesktopverbindung versucht, eine RDP-Verbindung zur Bastion herzustellen.

   Bei Erfolg wird ein Dialogfeld mit den Anmeldeinformationen geöffnet. Um Zugriff zu erhalten, verwenden Sie Ihre Active Directory-Anmeldeinformationen Ihres Unternehmens, wie Sie es für die Windows-Instanz tun würden.

3. Öffnen Sie das Remote Desktop Connection-Programm auf der Bastion und geben Sie die IP-Adresse der Windows-Instanz ein, zu der Sie eine Verbindung herstellen möchten (z. B. 10.0.0.100), und wählen Sie dann Connect. Ihre Active Directory-Anmeldeinformationen für Ihr Unternehmen sind erneut erforderlich, bevor Sie eine Verbindung mit der Windows-Instanz herstellen.

SALZ

Weitere Informationen zu den Friendly Bastion-Namen finden Sie unterDNS-freundliche Bastion-Namen.

1. Öffnen Sie das Programm Remote Desktop Connection, ein Windows-Standardprogramm, und geben Sie den freundlichen DNS-Namen der Windows-Bastion in das Feld Hostname ein. Das würde beispielsweise so aussehen`rdpbastion(1-4).AAMSAccountNumber.amazonaws.com`, wenn Ihre Kontonummer 123456789123 lautet und Sie Bastion 4 wählen,. `rdpbastion4.A123456789123.amazonaws.com`

2. Wählen Sie Connect aus. Die Remotedesktopverbindung versucht, eine RDP-Verbindung zur Bastion herzustellen.

   Bei Erfolg wird ein Dialogfeld mit den Anmeldeinformationen geöffnet. Um Zugriff zu erhalten, verwenden Sie Ihre Active Directory-Anmeldeinformationen Ihres Unternehmens, wie Sie es für die Windows-Instanz tun würden.

3. Öffnen Sie das Remote Desktop Connection-Programm auf der Bastion und geben Sie die IP-Adresse der Windows-Instanz ein, zu der Sie eine Verbindung herstellen möchten (z. B. 10.0.0.100), und wählen Sie dann Connect. Ihre Active Directory-Anmeldeinformationen für Ihr Unternehmen sind erneut erforderlich, bevor Sie eine Verbindung mit der Windows-Instanz herstellen.

Windows-Computer zur Linux-Instanz

Gehen Sie wie folgt vor, um von einer Windows-Umgebung aus per RDP zu einer SSH-Bastion zu gelangen.

MALZ

Bevor Sie beginnen:

- Fordern Sie Zugriff auf die Instanz an, zu der Sie eine Verbindung herstellen möchten. Weitere Informationen finden Sie unter Zugriffsanforderungen.

- Wählen Sie einen benutzerfreundlichen DNS-SSH-Bastionsnamen, zu dem Sie eine Verbindung herstellen möchten. Beispiel:

  ```
  sshbastion(1-4).YOUR_DOMAIN
  ```

  Das würde so aussehen, wenn YOUR_DOMAIN „myamsaddomain.com“ lautet und Sie Bastion 4 wählen:

  ```
  sshbastion4.myamsaddomain.com
  ```

- Suchen Sie die IP-Adresse der Instance, zu der Sie eine Verbindung herstellen möchten. Weitere Informationen finden Sie unter Instanz-ID oder IP-Adresse suchen.

Um von Ihrem Windows-Computer aus eine Verbindung zur Linux-Instance herzustellen, müssen Sie zunächst eine Verbindung zu einer SSH-Bastion herstellen.

Verwenden Sie den nativen Windows OpenSSH-Client oder installieren Sie PuTTY auf Ihrem lokalen Computer. Weitere Informationen zu OpenSSH finden Sie unter OpenSSH in Windows.

1. Verwenden Sie das native Windows oder öffnen Sie PuTTY und geben Sie den SSH-Bastion-Hostnamen oder die IP-Adresse der SSH-Bastion ein. Zum Beispiel 10.65.2.214 (22 ist der Port, der für SSH verwendet wird; er wird standardmäßig festgelegt).
2. OpenSSH oder PuTTY versucht, eine SSH-Verbindung zur Bastion herzustellen und ein Shell-Fenster zu öffnen.
3. Verwenden Sie Ihre Active Directory-Anmeldeinformationen Ihres Unternehmens wie bei den RDP-Hosts, um Zugriff zu erhalten.
4. Wenn Sie eine Bash-Eingabeaufforderung erhalten, greifen Sie per SSH auf die Instanz zu. Geben Sie ein:

   ```
   ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
   ```

SALZ

Bevor Sie beginnen:

- Fordern Sie Zugriff auf die Instance an, zu der Sie eine Verbindung herstellen möchten. Weitere Informationen finden Sie unter Zugriffsanforderungen.

- Wählen Sie einen benutzerfreundlichen DNS-SSH-Bastionsnamen, zu dem Sie eine Verbindung herstellen möchten. Beispiel:

  ```
  sshbastion(1-4).AAMSAccountNumber.amazonaws.com
  ```

  Das würde so aussehen, wenn deine Kontonummer 123456789123 lautet und du Bastion 4 wählst:

  ```
  sshbastion4.A123456789123.amazonaws.com
  ```

- Suchen Sie die IP-Adresse der Instance, zu der Sie eine Verbindung herstellen möchten. Weitere Informationen finden Sie unter Instanz-ID oder IP-Adresse finden.

Um von Ihrem Windows-Computer aus eine Verbindung zur Linux-Instance herzustellen, müssen Sie zunächst eine Verbindung zu einer SSH-Bastion herstellen.

Verwenden Sie den nativen Windows OpenSSH-Client oder installieren Sie PuTTY auf Ihrem lokalen Computer. Weitere Informationen zu OpenSSH finden Sie unter OpenSSH in Windows.

1. Verwenden Sie das native Windows oder öffnen Sie PuTTY und geben Sie den SSH-Bastion-Hostnamen oder die IP-Adresse der SSH-Bastion ein. Zum Beispiel 10.65.2.214 (22 ist der Port, der für SSH verwendet wird; er wird standardmäßig festgelegt).
2. OpenSSH oder PuTTY versucht, eine SSH-Verbindung zur Bastion herzustellen und ein Shell-Fenster zu öffnen.
3. Verwenden Sie Ihre Active Directory-Anmeldeinformationen Ihres Unternehmens wie bei den RDP-Hosts, um Zugriff zu erhalten.
4. Wenn Sie eine Bash-Eingabeaufforderung erhalten, greifen Sie per SSH auf die Instanz zu. Geben Sie ein:

   ```
   ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
   ```

Einen Vorfall melden

Verwenden Sie die AMS-Konsole, um einen Vorfall zu melden. Es ist wichtig, für jedes neue Problem oder jede neue Frage einen neuen Vorfall zu erstellen. Bei der Eröffnung von Fällen, die sich auf alte

Anfragen beziehen, ist es hilfreich, die entsprechende Fallnummer anzugeben, damit wir auf frühere Korrespondenz zurückgreifen können.

> **Note**
>
> Wenn die Fallkorrespondenz vom ursprünglichen Problem abweicht, bittet Sie ein AMS-Mitarbeiter möglicherweise, einen neuen Vorfall zu melden.

Gehen Sie wie folgt vor, um einen Vorfall über die AMS-Konsole zu melden:

1. Wählen Sie in der linken Navigationsleiste Incidents

   Die Liste der Vorfälle wird geöffnet:

   Wenn Ihre Vorfallliste leer ist, setzt die Option Filter löschen den Filter auf den Status Beliebig zurück.

   Wenn Sie wissen, dass Sie Telefon oder Chat verwenden möchten, klicken Sie im Support Center auf Incident erstellen, um die Seite Incident Create in der Support Center-Konsole zu öffnen, die automatisch mit dem AMS-Servicetyp gefüllt wird.

   > **Important**
   >
   > - Telefonanrufe, die mit initiiert wurden, Support werden aufgezeichnet, um die Reaktionszeit zu verbessern. Wenn der Anruf unterbrochen wird, müssen Sie über das Support Center zurückrufen. Es gibt keine Möglichkeit, AWS Sie zurückzurufen.
   > - Der Telefon- und Chat-Support ist darauf ausgelegt, bei Supportfällen, Vorfällen und Serviceanfragen zu helfen, nicht bei RFC- oder Sicherheitsproblemen.
   > - Verwenden Sie bei RFC-Problemen die Korrespondenzoption auf der entsprechenden RFC-Detailseite, um einen AMS-Techniker zu kontaktieren.
   > - Erstellen Sie bei Sicherheitsproblemen eine Support-Anfrage mit hoher Priorität (P1 oder P2). Die Live-Chat-Funktion ist nicht für Sicherheitsereignisse vorgesehen.

2. Wenn Sie nach einem vorhandenen Vorfall suchen möchten, wählen Sie in der Drop-down-Liste einen Vorfallstatusfilter aus.

	• Alle Vorfälle, die noch nicht gelöst sind. • Ein neuer Vorfall, der noch nicht zugewiesen wurde. • Ein Vorfall, der zugewiesen wurde. • Ein Vorfall, den Sie erneut aufgegriffen haben. • Ein zugewiesener, komplizierter Vorfall. • Vorfälle, für die vor dem nächsten Schritt Ihr Feedback erforderlich ist. • Vorfälle, zu denen Sie kürzlich Informati onen übermittelt haben. • Ein Vorfall, der abgeschlossen ist. • Alle Vorfälle auf dem Konto.

3. Wählen Sie Erstellen aus.

   Die Seite „Vorfall erstellen“ wird geöffnet:

4. Wählen Sie eine Priorität aus:

   - Niedrig: Nicht kritische Funktionen Ihres Unternehmensdienstes oder Ihrer Anwendung im Zusammenhang mit AWS/AMS-Ressourcen sind betroffen.
   - Mittel: Ein Unternehmensdienst oder eine Anwendung, die sich auf AWS/AMS-Ressourcen bezieht, ist mäßig beeinträchtigt und funktioniert in einem eingeschränkten Zustand.
   - Hoch: Ihr Unternehmen ist erheblich beeinträchtigt. Kritische Funktionen Ihrer Anwendung im Zusammenhang mit AWS/AMS-Ressourcen sind nicht verfügbar. Reserviert für die kritischsten Ausfälle, die Produktionssysteme betreffen.

5. Wählen Sie eine Kategorie aus.

> **Note**
>
> Wenn Sie die Incident-Funktionalität testen möchten, fügen Sie Ihrem Incident-Titel das Kennzeichen „Keine Aktion“ (AMSTestNoOpsActionRequired) hinzu.

6. Geben Sie Informationen ein für:

   - Betreff: Ein aussagekräftiger Titel für den Vorfallbericht.
   - CC-E-Mails: Eine Liste mit E-Mail-Adressen für Personen, die Sie über den Bericht und die Lösung des Vorfalls informieren möchten.
   - Einzelheiten: Eine umfassende Beschreibung des Vorfalls, der betroffenen Systeme und des erwarteten Ergebnisses der Lösung. Beantworten Sie die voreingestellten Fragen oder löschen Sie sie und geben Sie alle relevanten Informationen ein.

   Um einen Anhang hinzuzufügen, wählen Sie Anlage hinzufügen, suchen Sie nach der gewünschten Anlage und klicken Sie auf Öffnen. Um den Anhang zu löschen, klicken Sie auf das Symbol Löschen:

7. Wählen Sie Absenden aus.

   Es öffnet sich eine Detailseite mit Informationen zu dem Vorfall — wie Typ, Betreff, Erstellt, ID und Status — sowie ein Korrespondenzbereich, der die Beschreibung der von Ihnen erstellten Anfrage enthält.

   Klicken Sie auf Antworten, um einen Korrespondenzbereich zu öffnen und zusätzliche Informationen oder Statusaktualisierungen bereitzustellen.

   Klicken Sie auf Fall schließen, wenn der Vorfall gelöst wurde.

   Klicken Sie auf Mehr laden, wenn mehr Korrespondenz vorhanden ist, als auf eine Seite passt.

   Vergessen Sie nicht, die Kommunikation zu bewerten!

   Ihr Vorfall wird auf der Seite mit der Liste der Vorfälle angezeigt.

Eine Serviceanfrage erstellen

So erstellen Sie eine Serviceanfrage mit der AWS Managed Services (AMS) -Konsole:

1. Wählen Sie in der linken Navigationsleiste Serviceanfragen aus.

   Die Liste der Serviceanfragen wird geöffnet.

   Wenn Ihre Liste mit Serviceanfragen leer ist, setzt die Option Filter löschen den Filter auf den Status Beliebig zurück.

   Wenn Sie wissen, dass Sie Telefon oder Chat verwenden möchten, klicken Sie im Support Center auf Serviceanfrage erstellen, um die Seite Serviceanfrage erstellen in der Support Center-Konsole zu öffnen, die automatisch mit dem AMS-Servicetyp gefüllt wird.

   > **Note**
   >
   > Telefonanrufe, die mit dem Support Center eingeleitet wurden, werden aufgezeichnet, um die Reaktion zu verbessern. Wenn der Anruf unterbrochen wird, müssen Sie über das Support Center zurückrufen. Es gibt keine Möglichkeit, AWS Sie zurückzurufen.

   > **Important**
   >
   > Der Telefon- und Chat-Support ist darauf ausgelegt, Ihnen bei Supportfällen, Vorfällen und Serviceanfragen zu helfen. Verwenden Sie bei RFC-Problemen die Korrespondenzoption auf der entsprechenden RFC-Detailseite, um einen AMS-Techniker zu kontaktieren.

2. Wenn Sie nach einer vorhandenen Serviceanfrage suchen möchten, wählen Sie in der Dropdownliste einen Statusfilter für Serviceanfragen aus.

   - Alle Serviceanfragen, die noch nicht gelöst wurden.
   - Eine neue Serviceanfrage, die noch nicht zugewiesen wurde.

	• Eine Serviceanfrage, die zugewiesen wurde. • Eine Serviceanfrage, die Sie erneut geöffnet haben. • Eine zugewiesene, komplizierte Servicean frage. • Serviceanfragen, für die Ihr Feedback vor dem nächsten Schritt erforderlich ist. • Serviceanfragen, für die Sie kürzlich Informationen eingereicht haben. • Eine Serviceanfrage, die abgeschlossen wurde. • Alle Serviceanfragen im Konto.

3. Wählen Sie Erstellen aus.

   Die Seite Serviceanfrage erstellen wird geöffnet.

4. Wählen Sie eine Kategorie aus.

   > **Note**
   >
   > Wenn Sie die Funktionalität für Serviceanfragen testen möchten, fügen Sie dem Titel Ihrer Serviceanfrage das Kennzeichen „Keine Aktion“ hinzu`AMSTestNoOpsActionRequired`.

5. Geben Sie Informationen ein für:

   - Betreff: Dadurch wird ein Link zu den Details der Serviceanfrage auf der Listenseite erstellt.
   - CC-E-Mails: Diese E-Mails erhalten zusätzlich zu Ihren Standard-E-Mail-Kontakten Korrespondenz.
   - Einzelheiten: Geben Sie hier so viele Informationen wie möglich an.

   Um eine Anlage hinzuzufügen, wählen Sie Anlage hinzufügen, suchen Sie nach der gewünschten Anlage und klicken Sie auf

Öffnen. Um den Anhang zu löschen, klicken Sie auf das Symbol
Löschen:

6. Wählen Sie Absenden aus.

   Es öffnet sich eine Detailseite mit Informationen zur Serviceanfrage — wie Typ, Betreff, Erstellt, ID und Status — sowie ein Korrespondenzbereich, der die Beschreibung der von Ihnen erstellten Anfrage enthält.

   Darüber hinaus wird Ihre Serviceanfrage auf der Listenseite mit der Serviceanfrage angezeigt. Verwenden Sie diese Option, wenn Sie eine Warnung erhalten, aber noch nichts von AMS gehört haben.

   Klicken Sie auf Antworten, um einen Korrespondenzbereich zu öffnen und zusätzliche Informationen oder Statusmeldungen bereitzustellen.

   Klicken Sie auf „Fall lösen“, wenn die Serviceanfrage gelöst wurde.

   Klicken Sie auf Mehr laden, um weitere Korrespondenzen anzuzeigen, die nicht auf die erste Seite passen.

   Vergessen Sie nicht, die Kommunikation zu bewerten!

Verwenden Sie für abrechnungsbezogene Anfragen die Kategorie Andere in der AMS-Konsole, die `ChangeTypeId ct-1e1xtak34nx76` in der AMS CM-API oder die `IssueType=AMS` in der AWS-Support-API.

Schritte nach dem Onboarding

Jetzt, wo Sie ein AMS-Konto eingerichtet haben, sollten Sie mehr AMS-Dokumentation lesen. Sehen Sie sich diese Dokumente an:

- Die Tutorials zur Verwendung des HA Two-Tier Stack CT zur Erstellung eines voll funktionsfähigen WordPress Stacks bieten als Nächstes ein umfassendes AMS-Erlebnis.
- AMS-Benutzerhandbuch: Das AMS-Benutzerhandbuch beschreibt die AMS-Funktionalität, listet wichtige Begriffe, Abläufe und Schnittstellen auf und bietet einen Überblick über eine typische AMS-Architektur für verwaltete Infrastrukturen. Darüber hinaus werden Details zur Zugriffsverwaltung und AMS-Standardeinstellungen angegeben. Außerdem finden Sie

detaillierte Beschreibungen zur Verwendung des AMS-Change-Management-Systems sowie mehrere exemplarische Vorgehensweisen. Zusätzliche Managementkonzepte werden ebenfalls beschrieben.

- AMS-API-Referenz: Diese API-Referenz enthält Beschreibungen aller API-Aufrufe, einschließlich Anfragen, Antworten und Beispielen.
- AMS-Anwendungsleitfaden: Der AMS-Anwendungsleitfaden beschreibt verschiedene Optionen und Methoden für die Bereitstellung und Wartung Ihrer Anwendungen in AMS.

Tutorials

In den folgenden Tutorials werden die Schritte zum Erstellen eines zweistufigen Stacks mit dem High Availability (Advanced) CT (ct-06mjngx5flwto) mithilfe der CLI und der Konsole beschrieben. Es wird ein Tutorial für die Bereitstellung einer Linux Auto Scaling Scaling-Gruppe (ASG) und für die Bereitstellung einer Windows ASG gegeben.

Beschreibungen aller CT-Optionen, einschließlich, ChangeTypeId finden Sie in der AMS Change Type Reference.

CLI-Tutorial: Zweistufiger Stack mit hoher Verfügbarkeit (Linux/RHEL)

In diesem Abschnitt wird beschrieben, wie Sie mithilfe der AMS-CLI einen zweistufigen Hochverfügbarkeits-Stack (HA) in einer AMS-Umgebung bereitstellen.

> **Note**
>
> Diese exemplarische Vorgehensweise für die Bereitstellung wurde in AMZN Linux- und RHEL-Umgebungen getestet.

Zusammenfassung der Aufgaben und der erforderlichen Aufgaben: RFCs

1. Infrastruktur erstellen (zweistufiger HA-Stack)
2. Erstellen Sie einen S3-Bucket für Anwendungen CodeDeploy
3. Erstellen Sie das WordPress Anwendungspaket und laden Sie es in den S3-Bucket hoch
4. Stellen Sie die Anwendung bereit mit CodeDeploy
5. Greifen Sie auf die WordPress Site zu und melden Sie sich an, um die Bereitstellung zu validieren

Bevor Sie beginnen

Deployment | Advanced Stack Components | High Availability Two Tier Stack Advanced | Create CT erstellt eine Auto Scaling Scaling-Gruppe, einen Load Balancer, eine Datenbank sowie einen CodeDeploy Anwendungsnamen und eine Bereitstellungsgruppe (mit demselben Namen, den Sie der Anwendung geben). Weitere Informationen finden CodeDeploy Sie unter Was ist CodeDeploy?

In dieser exemplarischen Vorgehensweise wird ein High Availability Two-Tier Stack (Advanced) -RFC verwendet, der beinhaltet UserData und auch beschreibt, wie ein WordPress Paket erstellt wird, das CodeDeploy bereitgestellt werden kann.

Im Beispiel werden Instanzmetadaten wie Instanz-ID, Region usw. aus einer laufenden Instanz abgerufen, indem der unter http://169.254.169.254/latest/meta-data/ verfügbare Instanz-Metadatendienst abgefragt wird. `UserData` EC2 Diese Zeile im Benutzerdatenskript:`REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`, ruft den Namen der Verfügbarkeitszone aus dem Metadatendienst in die $REGION-Variable für unsere unterstützten Regionen ab und vervollständigt damit die URL für den S3-Bucket, in den der Agent heruntergeladen wird. CodeDeploy Die 169.254.169.254 IP ist nur innerhalb der VPC routingfähig (alle können den Service abfragen). VPCs Informationen zum Service finden Sie unter Instanz-Metadaten und Benutzerdaten. Beachten Sie auch, dass Skripte, UserData die als eingegeben wurden, als „root“ -Benutzer ausgeführt werden und den Befehl „sudo“ nicht verwenden müssen.

In dieser exemplarischen Vorgehensweise werden die folgenden Parameter auf dem Standardwert belassen (siehe Abbildung):

- Auto Scaling Scaling-Gruppe:`Cooldown=300, DesiredCapacity=2, EBSOptimized=false, HealthCheckGracePeriod=600, IAMInstanceProfile=customer-mc-ec2-instance-profile, InstanceDetailedMonitoring=true, InstanceRootVolumeIops=0, InstanceRootVolumeType=standard, InstanceType=m3.medium, MaxInstances=2, MinInstances=2, ScaleDownPolicyCooldown=300, ScaleDownPolicyEvaluationPeriods=4, ScaleDownPolicyPeriod=60, ScaleDownPolicyScalingAdjustment=-1, ScaleDownPolicyStatistic=Average, ScaleDownPolicyThreshold=35, ScaleMetricName=CPUUtilization, ScaleUpPolicyCooldown=60, ScaleUpPolicyEvaluationPeriods=2, ScaleUpPolicyPeriod=60, ScaleUpPolicyScalingAdjustment=2, ScaleUpPolicyStatistic=Average, ScaleUpPolicyThreshold=75`.

- Load Balancer:`HealthCheckInterval=30, HealthCheckTimeout=5`.
- Datenbank:`BackupRetentionPeriod=7, Backups=true, InstanceType=db.m3.medium, IOPS=0, MultiAZ=true, PreferredBackupWindow=22:00-23:00, PreferredMaintenanceWindow=wed:03:32-wed:04:02, StorageEncrypted=false, StorageEncryptionKey="", StorageType=gp2`.
- Anwendung:`DeploymentConfigName=CodeDeployDefault.OneAtATime`.
- S3-Eimer:`AccessControl=Private`.

ZUSÄTZLICHE EINSTELLUNGEN:

`RequestedStartTime`und `RequestedEndTime` wenn Sie Ihren RFC planen möchten: Sie können Time.is verwenden, um die richtige UTC-Zeit zu ermitteln. Die bereitgestellten Beispiele müssen entsprechend angepasst werden. Ein RFC kann nicht fortgesetzt werden, wenn die Startzeit abgelaufen ist. Alternativ können Sie diese Werte auch weglassen, um einen ASAP-RFC zu erstellen, der ausgeführt wird, sobald die Genehmigungen bestanden wurden.

> **Note**
>
> Es gibt viele Parameter, die Sie möglicherweise anders als in der Abbildung festlegen möchten. Die im Beispiel gezeigten Werte für diese Parameter wurden getestet, sind aber möglicherweise nicht für Sie geeignet.

Erstellen Sie die Infrastruktur

Wenn Sie die folgenden Daten sammeln, bevor Sie beginnen, kann die Bereitstellung schneller vonstattengehen.

DIE ERFORDERLICHEN DATEN SIND GESTAPELT:

- AutoScalingGroup:
  - `UserData`: Dieser Wert wird in diesem Tutorial bereitgestellt. Er enthält Befehle zum Einrichten der Ressource für den Agenten CodeDeploy und zum Starten des CodeDeploy Agenten.
  - `AMI-ID`: Dieser Wert bestimmt, welche Art von EC2 Instances Ihre Auto Scaling Scaling-Gruppe (ASG) hochfahren wird. Stellen Sie sicher, dass Sie in Ihrem Konto ein AMI auswählen, das mit „Kunde-“ beginnt und das von Ihnen gewünschte Betriebssystem hat. Finden Sie AMI

IDs mit der Referenz zur AMS SKMS API auf der Registerkarte Berichte in der AWS Artifact Console. Operation (CLI: list-amis) oder auf der Seite AMS-Konsole -> Details. VPCs VPCs Diese exemplarische Vorgehensweise ist für die ASGs Konfiguration zur Verwendung eines Linux-AMI AMI.

- Datenbank:
  - Diese Parameter, `DBEngineEngineVersion`, und `LicenseModel` sollten entsprechend Ihrer Situation eingestellt werden, obwohl die im Beispiel gezeigten Werte getestet wurden.
  - Diese Parameter, `RDSSubnetIds` `DBNameMasterUsername`, und `MasterUserPassword` sind bei der Bereitstellung des Anwendungspakets erforderlich. Verwenden Sie für RDSSubnet IDs zwei private Subnetze.
- LoadBalancer:
  - Diese Parameter, `DBEngineEngineVersion`, und `LicenseModel` sollten entsprechend Ihrer Situation eingestellt werden, obwohl die im Beispiel gezeigten Werte getestet wurden.
  - `ELBSubnetIds`: Verwenden Sie zwei öffentliche Subnetze.
- Anwendung: Der `ApplicationName` Wert legt den CodeDeploy Anwendungsnamen und den Namen der CodeDeploy Bereitstellungsgruppe fest. Sie verwenden ihn, um Ihre Anwendung bereitzustellen. Es muss für das Konto eindeutig sein. Um in Ihrem Konto nach CodeDeploy Namen zu suchen, schauen Sie in der CodeDeploy Konsole nach. Im Beispiel wird "WordPress" verwendet, aber wenn Sie diesen Wert verwenden, stellen Sie sicher, dass er nicht bereits verwendet wird.

Bei diesem Verfahren werden der zweistufige Hochverfügbarkeits-Stack (Advanced) CT (ct-06mjngx5flwto) und der Create S3-Speicher-CT (ct-1a68ck03fn98r) verwendet. Gehen Sie von Ihrem authentifizierten Konto aus in der Befehlszeile wie folgt vor.

1. Starten Sie den Infrastruktur-Stack.

   a. Geben Sie das JSON-Schema der Ausführungsparameter für den HA Two-Tier-Stack-CT in eine Datei in Ihrem aktuellen Ordner namens CreateStackParams .json aus.

   ```
   aws amscm get-change-type-version --change-type-id "ct-06mjngx5flwto"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    CreateStackParams.json
   ```

   b. Ändern Sie das Schema. Ersetzen Sie das nach *`variables`* Bedarf. Verwenden Sie beispielsweise das gewünschte Betriebssystem für die EC2 Instanzen, die die ASG erstellen

wird. Notieren Sie das, `ApplicationName` wie Sie es später für die Bereitstellung der Anwendung verwenden werden. Beachten Sie, dass Sie bis zu 50 Tags hinzufügen können.

```
{
"Description":      "HA two tier stack for WordPress",
"Name":             "WordPressStack",
"TimeoutInMinutes":  360,
"Tags": [
        {
            "Key": "ApplicationName",
            "Value": "WordPress"
        }
    ],
"AutoScalingGroup": {
            "AmiId":    "AMI-ID",
            "UserData": "#!/bin/bash \n
            REGION=$(curl 169.254.169.254/latest/meta-data/placement/
availability-zone/ | sed 's/[a-z]$//') \n
            yum -y install ruby httpd \n
            chkconfig httpd on \n
            service httpd start \n
            touch /var/www/html/status \n
            cd /tmp \n
            curl -O https://aws-codedeploy-$REGION.s3.amazonaws.com/latest/
install \n
            chmod +x ./install \n
            ./install auto \n
            chkconfig codedeploy-agent on \n
            service codedeploy-agent start"
    },
    "LoadBalancer": {
        "Public":               true,
        "HealthCheckTarget":    "HTTP:80/status"
    },
    "Database":     {
        "DBEngine":             "MySQL",
        "DBName":               "wordpress",
        "EngineVersion":        "8.0.16 ",
        "LicenseModel":         "general-public-license",
        "MasterUsername":       "admin",
        "MasterUserPassword":   "p4ssw0rd"
    },
    "Application":  {
```

```
    "ApplicationName":  "WordPress"
        }
}
```

c. Geben Sie die CreateRfc JSON-Vorlage in eine Datei in Ihrem aktuellen Ordner namens CreateStackRfc .json aus:

```
aws amscm create-rfc --generate-cli-skeleton > CreateStackRfc.json
```

d. Ändern Sie die RFC-Vorlage wie folgt und speichern Sie sie. Sie können den Inhalt löschen und ersetzen. Beachten Sie, dass `RequestedStartTime` sie jetzt optional `RequestedEndTime` sind. Wenn Sie sie ausschließen, wird ein ASAP-RFC erstellt, der ausgeführt wird, sobald er genehmigt wurde (was normalerweise automatisch geschieht). Um einen geplanten RFC einzureichen, fügen Sie diese Werte hinzu.

```
{
"ChangeTypeVersion":    "3.0",
"ChangeTypeId":         "ct-06mjngx5flwto",
"Title":                "HA-Stack-For-WP-RFC"
}
```

e. Erstellen Sie den RFC, indem Sie die CreateStackRfc JSON-Datei und die Ausführungsparameterdatei mit den CreateStackParams JSON-Dateien angeben:

```
aws amscm create-rfc --cli-input-json file://CreateStackRfc.json --execution-
parameters file://CreateStackParams.json
```

Sie erhalten die RFC-ID in der Antwort. Speichern Sie die ID für nachfolgende Schritte.

f. Reichen Sie den RFC ein:

```
aws amscm submit-rfc --rfc-id  RFC_ID
```

Wenn der RFC erfolgreich ist, erhalten Sie keine Ausgabe.

g. Führen Sie folgenden Befehl aus, um den RFC-Status zu überprüfen

```
aws amscm get-rfc --rfc-id RFC_ID
```

Notieren Sie sich die RFC-ID.

2. Starten Sie einen S3-Bucket

   Wenn Sie die folgenden Daten sammeln, bevor Sie beginnen, kann die Bereitstellung schneller vonstattengehen.

   ERFORDERLICHER DATEN-S3-BUCKET:

   - `VPC-ID`: Dieser Wert bestimmt, wo sich Ihr S3-Bucket befinden wird. Verwenden Sie dieselbe VPC-ID, die Sie zuvor verwendet haben.
   - `BucketName`: Dieser Wert legt den Namen des S3-Buckets fest. Sie verwenden ihn, um Ihr Anwendungspaket hochzuladen. Er muss in der gesamten Region des Kontos eindeutig sein und darf keine Großbuchstaben enthalten. Die Angabe Ihrer Konto-ID als Teil von BucketName ist keine Voraussetzung, erleichtert jedoch die spätere Identifizierung des Buckets. Um zu sehen, welche S3-Bucket-Namen in dem Konto vorhanden sind, rufen Sie die Amazon S3 S3-Konsole für Ihr Konto auf.

   a. Geben Sie das JSON-Schema der Ausführungsparameter für den S3-Speicher Create CT in eine JSON-Datei mit dem Namen CreateS3 StoreParams .json aus.

   ```
   aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    CreateS3StoreParams.json
   ```

   b. Ändern Sie das Schema wie folgt. Sie können den Inhalt löschen und ersetzen. Ersetze es *`VPC_ID`* entsprechend. Die Werte im Beispiel wurden getestet, sind aber möglicherweise nicht für Sie geeignet.

   > **Tip**
   >
   > Die `BucketName` müssen in der gesamten Region des Kontos eindeutig sein und dürfen keine Großbuchstaben enthalten. Die Angabe Ihrer Konto-ID als Teil von BucketName ist keine Voraussetzung, erleichtert jedoch die spätere Identifizierung des Buckets. Um zu sehen, welche S3-Bucket-Namen in dem Konto vorhanden sind, rufen Sie die Amazon S3 S3-Konsole für Ihr Konto auf.

   ```
   {
   "Description":      "S3BucketForWordPressBundle",
   ```

```
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-s2b72beb000000000",
"Name":             "S3BucketForWP",
"TimeoutInMinutes":  60,
"Parameters":   {
    "AccessControl":    "Private",
    "BucketName":       "ACCOUNT_ID-BUCKET_NAME"
    }
}
```

c. Geben Sie die JSON-Vorlage für CreateRfc in eine Datei in Ihrem aktuellen Ordner mit dem Namen CreateS3 StoreRfc .json aus:

```
aws amscm create-rfc --generate-cli-skeleton > CreateS3StoreRfc.json
```

d. Ändern und speichern Sie die Datei CreateS3 StoreRfc .json. Sie können den Inhalt löschen und ersetzen. Beachten Sie, dass `RequestedStartTime` sie jetzt optional `RequestedEndTime` sind. Wenn Sie sie ausschließen, wird ein ASAP-RFC erstellt, der ausgeführt wird, sobald er genehmigt wurde (was normalerweise automatisch geschieht). Um einen geplanten RFC einzureichen, fügen Sie diese Werte hinzu.

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-1a68ck03fn98r",
"Title":                "S3-Stack-For-WP-RFC"
}
```

e. Erstellen Sie den RFC, indem Sie die Datei CreateS3 StoreRfc .json und die Ausführungsparameterdatei StoreParams CreateS3 .json angeben:

```
aws amscm create-rfc --cli-input-json file://CreateS3StoreRfc.json  --
execution-parameters file://CreateS3StoreParams.json
```

Sie erhalten den Wert des neuen RFC in RfcId der Antwort. Speichern Sie die ID für nachfolgende Schritte.

f. Reichen Sie den RFC ein:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

Wenn der RFC erfolgreich ist, erhalten Sie keine Ausgabe.

g. Führen Sie folgenden Befehl aus, um den RFC-Status zu überprüfen

```
aws amscm get-rfc --rfc-id RFC_ID
```

Anwendung erstellen, hochladen und bereitstellen

Erstellen Sie zunächst ein WordPress Anwendungspaket und verwenden Sie dann das, CodeDeploy CTs um die Anwendung zu erstellen und bereitzustellen.

1. Laden Sie die Dateien herunter WordPress, extrahieren Sie sie und erstellen Sie eine. Verzeichnis /scripts.

   Linux-Befehl:

   ```
   wget https://github.com/WordPress/WordPress/archive/master.zip
   ```

   Windows: `https://github.com/WordPress/WordPress/archive/master.zip` In ein Browserfenster einfügen und die Zip-Datei herunterladen.

   Erstellen Sie ein temporäres Verzeichnis, in dem das Paket zusammengestellt werden soll.

   Linux:

   ```
   mkdir /tmp/WordPress
   ```

   Windows: Erstellen Sie ein "WordPress" Verzeichnis. Sie werden den Verzeichnispfad später verwenden.

2. Extrahieren Sie die WordPress Quelle in das Verzeichnis WordPress "" und erstellen Sie ein. Verzeichnis /scripts.

   Linux:

   ```
   unzip master.zip -d /tmp/WordPress_Temp
   cp -paf /tmp/WordPress_Temp/WordPress-master/* /tmp/WordPress
   rm -rf /tmp/WordPress_Temp
   rm -f master
   cd /tmp/WordPress
   mkdir scripts
   ```

Windows: Gehen Sie in das Verzeichnis "WordPress", das Sie erstellt haben, und erstellen Sie dort ein Verzeichnis „scripts“.

Wenn Sie sich in einer Windows-Umgebung befinden, stellen Sie sicher, dass Sie den Unterbrechungstyp für die Skriptdateien auf Unix (LF) setzen. In Notepad ++ ist dies eine Option unten rechts im Fenster.

3. Erstellen Sie die Datei CodeDeploy appspec.yml im WordPress Verzeichnis (wenn Sie das Beispiel kopieren, überprüfen Sie den Einzug, jedes Leerzeichen zählt). WICHTIG: Stellen Sie sicher, dass der Quellpfad für das Kopieren der WordPress Dateien (in diesem Fall in Ihrem WordPress Verzeichnis) an das erwartete Ziel (/) korrekt ist. var/www/html/WordPress Im Beispiel befindet sich die Datei appspec.yml im Verzeichnis mit den WordPress Dateien, sodass nur „/“ benötigt wird. Auch wenn Sie ein RHEL-AMI für Ihre Auto Scaling Scaling-Gruppe verwendet haben, sollten Sie die Zeile „os: linux“ unverändert lassen. Beispiel für eine appspec.yml-Datei:

```
version: 0.0
os: linux
files:
  - source: /
    destination: /var/www/html/WordPress
hooks:
  BeforeInstall:
    - location: scripts/install_dependencies.sh
      timeout: 300
      runas: root
  AfterInstall:
    - location: scripts/config_wordpress.sh
      timeout: 300
      runas: root
  ApplicationStart:
    - location: scripts/start_server.sh
      timeout: 300
      runas: root
  ApplicationStop:
    - location: scripts/stop_server.sh
      timeout: 300
      runas: root
```

4. Erstellen Sie Bash-Dateiskripts in der. WordPress Verzeichnis /scripts.

Erstellen Sie zunächst `config_wordpress.sh` mit dem folgenden Inhalt (wenn Sie möchten, können Sie die Datei wp-config.php direkt bearbeiten).

> **Note**
>
> *DBName*Ersetzen Sie durch den Wert, der im HA Stack-RFC angegeben ist (z. B.`wordpress`).
> *DB_MasterUsername*Ersetzen Sie durch den `MasterUsername` Wert, der im HA Stack-RFC angegeben ist (z. B.`admin`).
> *DB_MasterUserPassword*Ersetzen Sie durch den `MasterUserPassword` Wert, der im HA Stack-RFC angegeben ist (z. B.`p4ssw0rd`).
> *DB_ENDPOINT*Ersetzen Sie es in den Ausführungsausgaben des HA Stack-RFC durch den DNS-Namen des Endpunkts (z. B.`srt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com`). Sie finden dies mit der GetRfcOperation (CLI: get-rfc --rfc-id RFC_ID) oder auf der RFC-Detailseite der AMS-Konsole für den HA Stack-RFC, den Sie zuvor eingereicht haben.

```
#!/bin/bash
chmod -R 755 /var/www/html/WordPress
cp /var/www/html/WordPress/wp-config-sample.php /var/www/html/WordPress/wp-
config.php
cd /var/www/html/WordPress
sed -i "s/database_name_here/DBName/g" wp-config.php
sed -i "s/username_here/DB_MasterUsername/g" wp-config.php
sed -i "s/password_here/DB_MasterUserPassword/g" wp-config.php
sed -i "s/localhost/DB_ENDPOINT/g" wp-config.php
```

5. Erstellen Sie im selben Verzeichnis mit dem folgenden Inhalt: `install_dependencies.sh`

```
#!/bin/bash
yum install -y php
yum install -y php-mysql
yum install -y mysql
service httpd restart
```

> **Note**
>
> HTTPS wird beim Start als Teil der Benutzerdaten installiert, damit Integritätsprüfungen von Anfang an funktionieren.

6. Erstellen Sie im selben Verzeichnis `start_server.sh` mit dem folgenden Inhalt:

   - Verwenden Sie für Amazon Linux-Instances Folgendes:

   ```
   #!/bin/bash
   service httpd start
   ```

   - Verwenden Sie für RHEL-Instances Folgendes (die zusätzlichen Befehle sind Richtlinien, die es SELINUX ermöglichen, sie zu akzeptieren): WordPress

   ```
   #!/bin/bash
   setsebool -P  httpd_can_network_connect_db 1
   setsebool -P  httpd_can_network_connect 1
   chcon -t httpd_sys_rw_content_t /var/www/html/WordPress/wp-content -R
   restorecon -Rv /var/www/html
   service httpd start
   ```

7. Erstellen Sie im selben Verzeichnis `stop_server.sh` mit dem folgenden Inhalt:

   ```
   #!/bin/bash
   service httpd stop
   ```

8. Erstellen Sie das Zip-Bundle.

   Linux:

   ```
   $ cd /tmp/WordPress
   $ zip -r wordpress.zip .
   ```

   Windows: Gehen Sie in Ihr "WordPress" -Verzeichnis, wählen Sie alle Dateien aus und erstellen Sie eine ZIP-Datei. Achten Sie darauf, sie wordpress.zip zu nennen.

1. Laden Sie das Anwendungspaket in den S3-Bucket hoch.

Das Bundle muss vorhanden sein, um den Stack weiter bereitstellen zu können.

Sie haben automatisch Zugriff auf jede S3-Bucket-Instanz, die Sie erstellen. Sie können über Ihre Bastions oder über die S3-Konsole darauf zugreifen und das WordPress Paket mit hochladen drag-and-drop oder die ZIP-Datei durchsuchen und auswählen.

Sie können auch den folgenden Befehl in einem Shell-Fenster verwenden. Vergewissern Sie sich, dass Sie den richtigen Pfad zur ZIP-Datei haben:

```
aws s3 cp wordpress.zip s3://BUCKET_NAME/
```

2. Stellen Sie das WordPress Anwendungspaket bereit.

   Wenn Sie die folgenden Daten sammeln, bevor Sie beginnen, kann die Bereitstellung schneller vonstattengehen.

   ERFORDERLICHE DATEN:

   - `VPC-ID`: Dieser Wert bestimmt, wo sich Ihr S3-Bucket befinden wird. Verwenden Sie dieselbe VPC-ID, die Sie zuvor verwendet haben.
   - `CodeDeployApplicationNameundCodeDeployApplicationName`: Der `ApplicationName` Wert, den Sie im HA 2-Tier Stack-RFC verwendet haben, legt den und den CodeDeployApplicationName fest. CodeDeployDeploymentGroupName Das Beispiel verwendet "WordPress", aber Sie haben möglicherweise einen anderen Wert verwendet.
   - `S3Location`: Verwenden Sie für den `S3BucketBucketName`, den Sie zuvor erstellt haben. Die `S3BundleType` und `S3Key` stammen aus dem Paket, das Sie in Ihren S3-Shop gestellt haben.

   a. Geben Sie das JSON-Schema der Ausführungsparameter für die CodeDeploy Anwendung Deploy CT in eine JSON-Datei mit dem Namen Deploy CDApp Params.json aus.

      ```
      aws amscm get-change-type-version --change-type-id "ct-2edc3sd1sqmrb"
       --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
       DeployCDAppParams.json
      ```

   b. Ändern Sie das Schema wie folgt und speichern Sie es unter. Sie können den Inhalt löschen und ersetzen.

```
{
"Description":                          "DeployWPCDApp",
"VpcId":                                "VPC_ID",
"Name":                                 "WordPressCDAppDeploy",
"TimeoutInMinutes":                     60,
"Parameters":   {
    "CodeDeployApplicationName":                "WordPress",
    "CodeDeployDeploymentGroupName":            "WordPress",
    "CodeDeployIgnoreApplicationStopFailures":   false,
    "CodeDeployRevision": {
      "RevisionType": "S3",
      "S3Location": {
        "S3Bucket":     "BUCKET_NAME",
        "S3BundleType": "zip",
        "S3Key":        "wordpress.zip" }
        }
    }
}
```

c. Geben Sie die JSON-Vorlage für CreateRfc in eine Datei in Ihrem aktuellen Ordner mit dem Namen Deploy CDApp rfc.json aus:

```
aws amscm create-rfc --generate-cli-skeleton > DeployCDAppRfc.json
```

d. Ändern und speichern Sie die Datei Deploy CDApp RFC.json. Sie können den Inhalt löschen und ersetzen. Beachten Sie, dass `RequestedStartTime` sie jetzt optional `RequestedEndTime` sind. Wenn Sie sie ausschließen, wird ein ASAP-RFC erstellt, der ausgeführt wird, sobald er genehmigt wurde (was normalerweise automatisch geschieht). Um einen geplanten RFC einzureichen, fügen Sie diese Werte hinzu.

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-2edc3sd1sqmrb",
"Title":                "CD-Deploy-For-WP-RFC"
}
```

e. Erstellen Sie den RFC, indem Sie die Datei Deploy CDApp Rfc und die Ausführungsparameterdatei Deploy CDApp Params angeben:

```
aws amscm create-rfc --cli-input-json file://DeployCDAppRfc.json  --execution-
parameters file://DeployCDAppParams.json
```

Sie erhalten den Wert RfcId des neuen RFC in der Antwort. Speichern Sie die ID für nachfolgende Schritte.

f. Reichen Sie den RFC ein:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

Wenn der RFC erfolgreich ist, erhalten Sie keine Ausgabe.

g. Führen Sie folgenden Befehl aus, um den RFC-Status zu überprüfen

```
aws amscm get-rfc --rfc-id RFC_ID
```

Validieren Sie die Anwendungsbereitstellung

Navigieren Sie zum Endpunkt (ELB CName) des zuvor erstellten Load Balancers mit dem bereitgestellten Pfad:/. WordPress WordPress Beispiel:

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

Machen Sie die Anwendungsbereitstellung rückgängig

Sobald Sie mit dem Tutorial fertig sind, sollten Sie die Bereitstellung beenden, damit Ihnen die Ressourcen nicht in Rechnung gestellt werden.

Im Folgenden wird ein generischer Vorgang zum Löschen von Stacks beschrieben. Sie sollten ihn zweimal einreichen, einmal für den HA 2-Tier-Stack und einmal für den S3-Bucket-Stack. Als letzten Schritt reichen Sie eine Serviceanfrage ein, dass alle Snapshots für den S3-Bucket (einschließlich der S3-Bucket-Stack-ID in der Serviceanfrage) gelöscht werden. Sie werden nach 10 Tagen automatisch gelöscht, aber wenn Sie sie vorzeitig löschen, sparen Sie ein wenig Kosten.

Diese exemplarische Vorgehensweise bietet ein Beispiel für die Verwendung der AMS-Konsole zum Löschen eines S3-Stacks. Dieses Verfahren gilt für das Löschen eines beliebigen Stacks mithilfe der AMS-Konsole.

> **Note**
>
> Wenn Sie einen S3-Bucket löschen, müssen Sie ihn zuerst von Objekten leeren.

ERFORDERLICHE DATEN:

- `StackId`: Der zu verwendende Stapel. Sie finden ihn auf der Seite AMS Console Stacks, die Sie über einen Link im linken Navigationsbereich aufrufen können. Führen Sie mithilfe der AMS SKMS API/CLI den Vorgang For the AMS SKMS API reference, see the Reports in der AWS Artifact Console. (in der CLI) aus. `list-stack-summaries`
- Die Änderungstyp-ID für diese exemplarische Vorgehensweise lautet `ct-0q0bic0ywqk6c` „1.0“. Führen Sie den folgenden Befehl aus, um die neueste Version herauszufinden:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=ct-0q0bic0ywqk6c
```

INLINE-ERSTELLUNG:

- Geben Sie den Befehl create RFC mit den direkt angegebenen Ausführungsparametern aus (vermeiden Sie Anführungszeichen, wenn Sie die Ausführungsparameter inline angeben). E

```
aws amscm create-rfc --change-type-id "ct-0q0bic0ywqk6c" --change-type-version "1.0"
 --title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

- Senden Sie den RFC mit der RFC-ID, die bei der RFC-Erstellung zurückgegeben wurde. Bis zur Übermittlung verbleibt der RFC im `Editing` Status und es wird nicht darauf reagiert.

```
aws amscm submit-rfc --rfc-id RFC_ID
```

- Überwachen Sie den RFC-Status und sehen Sie sich die Ausführungsausgabe an:

```
aws amscm get-rfc --rfc-id RFC_ID
```

VORLAGE ERSTELLEN:

1. Gibt die RFC-Vorlage in eine Datei in Ihrem aktuellen Ordner aus. Beispiel nennt sie DeleteStackRfc .json:

```
aws amscm create-rfc --generate-cli-skeleton > DeleteStackRfc.json
```

2. Ändern und speichern Sie die DeleteStackRfc JSON-Datei. Da das Löschen eines Stacks nur einen Ausführungsparameter hat, können sich die Ausführungsparameter in der DeleteStackRfc JSON-Datei selbst befinden (es ist nicht erforderlich, eine separate JSON-Datei mit Ausführungsparametern zu erstellen).

   Die internen Anführungszeichen in der ExecutionParameters JSON-Erweiterung müssen mit einem Backslash (\) maskiert werden. Beispiel ohne Start- und Endzeit:

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-0q0bic0ywqk6c",
"Title":                "Delete-My-Stack-RFC"
"ExecutionParameters":  "{
        \"StackId\":\"STACK_ID\"}"
}
```

3. Erstellen Sie den RFC:

```
aws amscm create-rfc --cli-input-json file://DeleteStackRfc.json
```

   In der Antwort erhalten Sie den RfcId des neuen RFC. Beispiel:

```
{
"RfcId": "daaa1867-ffc5-1473-192a-842f6b326102"
}
```

   Speichern Sie die ID für nachfolgende Schritte.

4. Reichen Sie den RFC ein:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

   Wenn der RFC erfolgreich ist, erhalten Sie keine Bestätigung in der Befehlszeile.

5. Um den Status der Anfrage zu überwachen und die Ausführungsausgabe anzuzeigen:

```
aws amscm get-rfc --rfc-id RFC_ID --query "Rfc.
{Status:Status.Name,Exec:ExecutionOutput}" --output table
```

Konsolen-Tutorial: Zweistufiger Stack mit hoher Verfügbarkeit (Linux/RHEL)

In diesem Abschnitt wird beschrieben, wie Sie mithilfe der AMS-Konsole eine WordPress Hochverfügbarkeits-Site (HA) in einer AMS-Umgebung bereitstellen.

> **Note**
>
> Diese exemplarische Vorgehensweise für die Bereitstellung wurde in AMZN Linux- und RHEL-Umgebungen getestet.

Zusammenfassung der Aufgaben und der erforderlichen Aufgaben: RFCs

1. Infrastruktur erstellen (zweistufiger HA-Stack)
2. Erstellen Sie einen S3-Bucket für Anwendungen CodeDeploy
3. Erstellen Sie das WordPress Anwendungspaket und laden Sie es in den S3-Bucket hoch
4. Stellen Sie die Anwendung bereit mit CodeDeploy
5. Greifen Sie auf die WordPress Site zu und melden Sie sich an, um die Bereitstellung zu validieren
6. Reißen Sie die Bereitstellung ab

Beschreibungen aller CT-Optionen, einschließlich ChangeTypeId, finden Sie in der AMS Change Type Reference.

Bevor Sie beginnen

Deployment | Advanced Stack Components | High Availability Two Tier Stack | Create CT erstellt eine Auto Scaling Scaling-Gruppe, einen Load Balancer, eine Datenbank sowie einen CodeDeploy Anwendungsnamen und eine Bereitstellungsgruppe (mit demselben Namen, den Sie der Anwendung geben). Weitere Informationen finden CodeDeploy Sie unter Was ist CodeDeploy?

In dieser exemplarischen Vorgehensweise wird ein Two-Tier-Stack-RFC für hohe Verfügbarkeit verwendet, in dem auch beschrieben wird, wie ein WordPress Paket erstellt wird, das CodeDeploy bereitgestellt werden kann. `UserData`

Die im Beispiel `UserData` gezeigte Methode ruft Instanz-Metadaten wie Instanz-ID, Region usw. aus einer laufenden Instanz ab, indem der Instanz-Metadatendienst abgefragt wird, der unter EC2 http://169.254.169.254/latest/meta-data/ verfügbar ist. Diese Zeile im Benutzerdatenskript:`REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`, ruft den Namen der Verfügbarkeitszone aus dem Metadatendienst in die $REGION-Variable für unsere unterstützten Regionen ab und vervollständigt damit die URL für den S3-Bucket, in den der Agent heruntergeladen wird. CodeDeploy Die 169.254.169.254 IP ist nur innerhalb der VPC routingfähig (alle können den Service abfragen). VPCs Informationen zum Service finden Sie unter Instanz-Metadaten und Benutzerdaten. Beachten Sie auch, dass Skripte, UserData die als eingegeben wurden, als „root“ -Benutzer ausgeführt werden und den Befehl „sudo“ nicht verwenden müssen.

In dieser exemplarischen Vorgehensweise werden die folgenden Parameter auf dem Standardwert belassen (siehe Abbildung):

- Auto Scaling Scaling-Gruppe:`Cooldown=300, DesiredCapacity=2, EBSOptimized=false, HealthCheckGracePeriod=600, IAMInstanceProfile=customer-mc-ec2-instance-profile, InstanceDetailedMonitoring=true, InstanceRootVolumeIops=0, InstanceRootVolumeType=standard, InstanceType=m3.medium, MaxInstances=2, MinInstances=2, ScaleDownPolicyCooldown=300, ScaleDownPolicyEvaluationPeriods=4, ScaleDownPolicyPeriod=60, ScaleDownPolicyScalingAdjustment=-1, ScaleDownPolicyStatistic=Average, ScaleDownPolicyThreshold=35, ScaleMetricName=CPUUtilization, ScaleUpPolicyCooldown=60, ScaleUpPolicyEvaluationPeriods=2, ScaleUpPolicyPeriod=60, ScaleUpPolicyScalingAdjustment=2, ScaleUpPolicyStatistic=Average, ScaleUpPolicyThreshold=75`.
- Load Balancer:`HealthCheckInterval=30, HealthCheckTimeout=5`.
- Datenbank:`BackupRetentionPeriod=7, Backups=true, InstanceType=db.m3.medium, IOPS=0, MultiAZ=true, PreferredBackupWindow=22:00-23:00, PreferredMaintenanceWindow=wed:03:32-wed:04:02, StorageEncrypted=false, StorageEncryptionKey="", StorageType=gp2`.
- Anwendung:`DeploymentConfigName=CodeDeployDefault.OneAtATime`.

Variable Parameter:

Die Konsole bietet eine ASAP-Option für die Startzeit, und in dieser exemplarischen Vorgehensweise wird empfohlen, diese zu verwenden. ASAP veranlasst, dass der RFC ausgeführt wird, sobald die Genehmigungen bestanden wurden.

> **Note**
>
> Es gibt viele Parameter, die Sie möglicherweise anders als in der Abbildung festlegen möchten. Die im Beispiel gezeigten Werte für diese Parameter wurden getestet, sind aber möglicherweise nicht für Sie geeignet. In den Beispielen werden nur die erforderlichen Werte angezeigt. Die *`replaceable`* Schriftwerte sollten geändert werden, da sie für Ihr Konto spezifisch sind.

Erstellen Sie die Infrastruktur

Bei diesem Verfahren wird der zweistufige Hochverfügbarkeits-Stack-CT verwendet, gefolgt vom Create S3-Speicher-CT.

Wenn Sie die folgenden Daten sammeln, bevor Sie beginnen, kann die Bereitstellung schneller vonstattengehen.

DIE ERFORDERLICHEN DATEN SIND GESTAPELT:

- AutoScalingGroup:
  - UserData: Dieser Wert wird in diesem Tutorial bereitgestellt. Er enthält Befehle zum Einrichten der Ressource für den Agenten CodeDeploy und zum Starten des CodeDeploy Agenten.
  - AMI-ID: Dieser Wert bestimmt das Betriebssystem der EC2 Instances, die Ihre Auto Scaling Scaling-Gruppe (ASG) hochfahren wird. Wählen Sie in Ihrem Konto ein AMI aus, das mit „Kunde-“ beginnt und das von Ihnen gewünschte Betriebssystem hat. Suchen Sie AMI IDs in der AMS-Konsole VPCs -> VPCs Detailseite. Diese exemplarische Vorgehensweise bezieht sich auf die ASGs Konfiguration für die Verwendung eines Amazon Linux- oder RHEL-AMI.
- Datenbank:
  - Diese Parameter DBEngine, EngineVersion, und LicenseModelsollten entsprechend Ihrer Situation eingestellt werden, obwohl die im Beispiel gezeigten Werte getestet wurden. Das Tutorial verwendet jeweils diese Werte:*`MySQL`*,*`8.0.16`*,*`general-public-license`*.
  - Diese Parameter, DBNameMasterUserPassword, und MasterUsernamesind für die Bereitstellung des Anwendungspakets erforderlich. Das Tutorial verwendet jeweils

diese Werte:*wordpressDB*,*p4ssw0rd*,*admin*. Beachten DBName Sie, dass dieser nur alphanumerische Zeichen enthalten darf.

- Wenn Sie das MasterUsernamefür die RDS-Datenbank eingeben, wird es im Klartext angezeigt. Melden Sie sich daher so schnell wie möglich bei der Datenbank an und ändern Sie das Passwort, um Ihre Sicherheit zu gewährleisten.
- Verwenden Sie für RDSSubnetIDs zwei private Subnetze. Geben Sie sie nacheinander ein und drücken Sie jeweils die Eingabetaste. Suchen Sie das Subnetz IDs mit der Referenz For the AMS SKMS API auf der Registerkarte Berichte in der AWS Artifact Console. Operation (CLI: list-subnet-summaries) oder auf der Seite AMS-Konsole VPCs -> VPC-Details.

- LoadBalancer:
  - Setzen Sie diesen Parameter Public auf true, da das Tutorial öffentliche ELB-Subnetze verwendet.
  - ELBSubnetIds: Verwenden Sie zwei öffentliche Subnetze. Geben Sie sie nacheinander ein und drücken Sie jeweils die Eingabetaste. Suchen Sie das Subnetz IDs mit der Referenz For the AMS SKMS API auf der Registerkarte Berichte in der AWS Artifact Console. Operation (CLI: list-subnet-summaries) oder auf der Seite AMS-Konsole VPCs -> VPC-Details.
- Anwendung: Der ApplicationNameWert legt den Anwendungsnamen und den Namen der CodeDeploy Bereitstellungsgruppe fest. CodeDeploy Sie verwenden ihn, um Ihre Anwendung bereitzustellen. Es muss für das Konto eindeutig sein. In der CodeDeploy Konsole können Sie in Ihrem Konto nach CodeDeploy Namen suchen. Das Beispiel verwendet, *WordPress* aber wenn Sie diesen Wert verwenden, stellen Sie sicher, dass er nicht bereits verwendet wird.

1. Starten Sie den Hochverfügbarkeits-Stack.

   a. Wählen Sie auf der Seite RFC erstellen aus der Liste die Kategorie Deployment, die Unterkategorie Standard-Stacks, die Elemente High Availability Two-Tier-Stack und Operation Create aus.

   b. WICHTIG: Wählen Sie „Erweitert“ und legen Sie die Werte wie abgebildet fest.

      Sie müssen nur Werte für Optionen mit Sternchen (*) eingeben. Die getesteten Werte werden im Beispiel gezeigt. Sie können die nicht erforderlichen leeren Optionen leer lassen.

   c. Für den Abschnitt mit der RFC-Beschreibung:

      ```
      Subject: WP-HA-2-Tier-RFC
      ```

d. Legen Sie für den Abschnitt Ressourceninformationen die Parameter für AutoScalingGroup, Datenbank LoadBalancer, Anwendung und Tags fest.

Der Tag-Schlüssel "AppName" dient außerdem dazu, dass Sie in der EC2 Konsole einfach nach den ASG-Instanzen suchen können. Sie können diesen Tag-Schlüssel „Name“ oder einen beliebigen anderen Schlüsselnamen nennen. Beachten Sie, dass Sie bis zu 50 Tags hinzufügen können.

```
UserData:
    #!/bin/bash
    REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/
 | sed 's/[a-z]$//')
    yum -y install ruby httpd
    chkconfig httpd on
    service httpd start
    touch /var/www/html/status
    cd /tmp
    curl -O https://aws-codedeploy-$REGION.s3.amazonaws.com/latest/install
    chmod +x ./install
    ./install auto
    chkconfig codedeploy-agent on
    service codedeploy-agent start
AmiId:               AMI-ID
Description:         WP-HA-2-Tier-Stack

Database:
    LicenseModel:    general-public-license (USE RADIO BUTTON)
    EngineVersion:   8.0.16
    DBEngine:        MySQL
    RDSSubnetIds:    PRIVATE_AZ1 PRIVATE_AZ2 (ENTER ONE AT A TIME PRESSING
 "ENTER" AFTER EACH)
    MasterUserPassword:  p4ssw0rd
    MasterUsername:      admin
    DBName:              wordpressDB

LoadBalancer:
    Public:              true (USE RADIO BUTTON)
    ELBSubnetIds:        PUBLIC_AZ1 PUBLIC_AZ2

Application:
    ApplicationName:     WordPress
```

```
Tags:
    Name:                   WP-Rhel-Stack
```

e. Wenn Sie fertig sind, klicken Sie auf Senden.

2. Melden Sie sich bei der Datenbank an, die Sie erstellt haben, und ändern Sie das Passwort.
3. Starten Sie einen S3-Bucket-Stack.

   Wenn Sie die folgenden Daten sammeln, bevor Sie beginnen, kann die Bereitstellung schneller vonstattengehen.

   ERFORDERLICHER DATEN-S3-BUCKET:

   - VPC-ID: Dieser Wert bestimmt, wo sich Ihr S3-Bucket befinden wird. Suchen Sie VPC IDs mit der Referenz For the AMS SKMS API auf der Registerkarte Berichte in der AWS Artifact Console. Operation (CLI: list-vpc-summaries) oder auf der AMS-Konsolenseite. VPCs
   - BucketName: Dieser Wert legt den Namen des S3-Buckets fest. Sie verwenden ihn, um Ihr Anwendungspaket hochzuladen. Er muss in der gesamten Region des Kontos eindeutig sein und darf keine Großbuchstaben enthalten. Die Angabe Ihrer Konto-ID als Teil von BucketName ist keine Voraussetzung, erleichtert jedoch die spätere Identifizierung des Buckets. Um zu sehen, welche S3-Bucket-Namen in dem Konto vorhanden sind, rufen Sie die Amazon S3 S3-Konsole für Ihr Konto auf.

   a. Wählen Sie auf der Seite Create RFC die Kategorie Deployment, die Unterkategorie Advanced Stack Components, den Artikel S3 storage und Operation Create aus der RFC CT-Auswahlliste aus.

   b. Behalten Sie die Standardoption Basic bei und legen Sie die Werte wie gezeigt fest.

```
Subject:                S3-Bucket-WP-HA-RFC
Description:            S3BucketForWordPressBundles
BucketName:             ACCOUNT_ID-BUCKET_NAME
AccessControl:          Private
VpcId:                  VPC_ID
Name:                   S3-Bucket-WP-HA-Stack
TimeoutInMinutes:       60
```

   c. Wenn Sie fertig sind, klicken Sie auf Senden. Der mit diesem Änderungstyp bereitgestellte Bucket ermöglicht vollen read/write Zugriff auf das gesamte Konto.

Anwendung erstellen, hochladen und bereitstellen

Erstellen Sie zunächst ein WordPress Anwendungspaket und verwenden Sie dann das, CodeDeploy CTs um die Anwendung zu erstellen und bereitzustellen.

1. Laden Sie die Dateien herunter WordPress, extrahieren Sie sie und erstellen Sie eine. Verzeichnis /scripts.

   Linux-Befehl:

   ```
   wget https://github.com/WordPress/WordPress/archive/master.zip
   ```

   Windows: `https://github.com/WordPress/WordPress/archive/master.zip` In ein Browserfenster einfügen und die Zip-Datei herunterladen.

   Erstellen Sie ein temporäres Verzeichnis, in dem das Paket zusammengestellt werden soll.

   Linux:

   ```
   mkdir /tmp/WordPress
   ```

   Windows: Erstellen Sie ein "WordPress" Verzeichnis. Sie werden den Verzeichnispfad später verwenden.

2. Extrahieren Sie die WordPress Quelle in das Verzeichnis WordPress "" und erstellen Sie ein. Verzeichnis /scripts.

   Linux:

   ```
   unzip master.zip -d /tmp/WordPress_Temp
   cp -paf /tmp/WordPress_Temp/WordPress-master/* /tmp/WordPress
   rm -rf /tmp/WordPress_Temp
   rm -f master
   cd /tmp/WordPress
   mkdir scripts
   ```

   Windows: Gehen Sie in das Verzeichnis "WordPress", das Sie erstellt haben, und erstellen Sie dort ein Verzeichnis „scripts“.

Wenn Sie sich in einer Windows-Umgebung befinden, stellen Sie sicher, dass Sie den Unterbrechungstyp für die Skriptdateien auf Unix (LF) setzen. In Notepad ++ ist dies eine Option unten rechts im Fenster.

3. Erstellen Sie die Datei CodeDeploy appspec.yml im WordPress Verzeichnis (wenn Sie das Beispiel kopieren, überprüfen Sie den Einzug, jedes Leerzeichen zählt). WICHTIG: Stellen Sie sicher, dass der Quellpfad für das Kopieren der WordPress Dateien (in diesem Fall in Ihrem WordPress Verzeichnis) an das erwartete Ziel (/) korrekt ist. var/www/html/WordPress Im Beispiel befindet sich die Datei appspec.yml im Verzeichnis mit den WordPress Dateien, sodass nur „/“ benötigt wird. Auch wenn Sie ein RHEL-AMI für Ihre Auto Scaling Scaling-Gruppe verwendet haben, sollten Sie die Zeile „os: linux“ unverändert lassen. Beispiel für eine appspec.yml-Datei:

```
version: 0.0
os: linux
files:
  - source: /
    destination: /var/www/html/WordPress
hooks:
  BeforeInstall:
    - location: scripts/install_dependencies.sh
      timeout: 300
      runas: root
  AfterInstall:
    - location: scripts/config_wordpress.sh
      timeout: 300
      runas: root
  ApplicationStart:
    - location: scripts/start_server.sh
      timeout: 300
      runas: root
  ApplicationStop:
    - location: scripts/stop_server.sh
      timeout: 300
      runas: root
```

4. Erstellen Sie Bash-Dateiskripts in der. WordPress Verzeichnis /scripts.

   Erstellen Sie zunächst `config_wordpress.sh` mit dem folgenden Inhalt (wenn Sie möchten, können Sie die Datei wp-config.php direkt bearbeiten).

> **Note**
>
> *DBName*Ersetzen Sie durch den Wert, der im HA Stack-RFC angegeben ist (z. B.`wordpress`).
> *DB_MasterUsername*Ersetzen Sie durch den `MasterUsername` Wert, der im HA Stack-RFC angegeben ist (z. B.`admin`).
> *DB_MasterUserPassword*Ersetzen Sie durch den `MasterUserPassword` Wert, der im HA Stack-RFC angegeben ist (z. B.`p4ssw0rd`).
> *DB_ENDPOINT*Ersetzen Sie es in den Ausführungsausgaben des HA Stack-RFC durch den DNS-Namen des Endpunkts (z. B.`srt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com`). Sie finden dies mit der GetRfcOperation (CLI: get-rfc --rfc-id RFC_ID) oder auf der RFC-Detailseite der AMS-Konsole für den HA Stack-RFC, den Sie zuvor eingereicht haben.

```
#!/bin/bash
chmod -R 755 /var/www/html/WordPress
cp /var/www/html/WordPress/wp-config-sample.php /var/www/html/WordPress/wp-
config.php
cd /var/www/html/WordPress
sed -i "s/database_name_here/DBName/g" wp-config.php
sed -i "s/username_here/DB_MasterUsername/g" wp-config.php
sed -i "s/password_here/DB_MasterUserPassword/g" wp-config.php
sed -i "s/localhost/DB_ENDPOINT/g" wp-config.php
```

5. Erstellen Sie im selben Verzeichnis mit dem folgenden Inhalt: `install_dependencies.sh`

```
#!/bin/bash
yum install -y php
yum install -y php-mysql
yum install -y mysql
service httpd restart
```

> **Note**
>
> HTTPS wird beim Start als Teil der Benutzerdaten installiert, damit Integritätsprüfungen von Anfang an funktionieren.

6. Erstellen Sie im selben Verzeichnis `start_server.sh` mit dem folgenden Inhalt:

   - Verwenden Sie für Amazon Linux-Instances Folgendes:

     ```
     #!/bin/bash
     service httpd start
     ```

   - Verwenden Sie für RHEL-Instances Folgendes (die zusätzlichen Befehle sind Richtlinien, die es SELINUX ermöglichen, sie zu akzeptieren): WordPress

     ```
     #!/bin/bash
     setsebool -P  httpd_can_network_connect_db 1
     setsebool -P  httpd_can_network_connect 1
     chcon -t httpd_sys_rw_content_t /var/www/html/WordPress/wp-content -R
     restorecon -Rv /var/www/html
     service httpd start
     ```

7. Erstellen Sie im selben Verzeichnis `stop_server.sh` mit dem folgenden Inhalt:

   ```
   #!/bin/bash
   service httpd stop
   ```

8. Erstellen Sie das Zip-Bundle.

   Linux:

   ```
   $ cd /tmp/WordPress
   $ zip -r wordpress.zip .
   ```

   Windows: Gehen Sie in Ihr "WordPress" -Verzeichnis, wählen Sie alle Dateien aus und erstellen Sie eine ZIP-Datei. Achten Sie darauf, sie wordpress.zip zu nennen.

1. Laden Sie das Anwendungspaket in den S3-Bucket hoch

   Das Paket muss vorhanden sein, um den Stack weiter bereitstellen zu können.

   Sie haben automatisch Zugriff auf jede S3-Bucket-Instanz, die Sie erstellen. Sie können über Ihre Bastions (siehe Zugreifen auf Instances) oder über die S3-Konsole darauf zugreifen und das CodeDeploy Paket mit drag-and-drop der Datei hochladen oder indem Sie die Datei aufrufen und auswählen.

Sie können auch den folgenden Befehl in einem Shell-Fenster verwenden. Vergewissern Sie sich, dass Sie den richtigen Pfad zur ZIP-Datei haben:

```
aws s3 cp wordpress/wordpress.zip s3://BUCKET_NAME/
```

2. Stellen Sie das WordPress CodeDeploy Anwendungspaket bereit

   ERFORDERLICHER DATENCODE/ANWENDUNGSBEREITSTELLUNG BEREITSTELLEN:

   - CodeDeployApplicationName: Der Name, den Sie der CodeDeploy Anwendung gegeben haben.
   - CodeDeployGroupName: Da sowohl die CodeDeploy Anwendung als auch die Gruppe anhand des Namens erstellt wurden, den Sie der CodeDeploy Anwendung im HA-Stack-RFC gegeben haben, ist dies derselbe Name wie der CodeDeployApplicationName.
   - S3Bucket: Der Name, den Sie dem S3-Bucket gegeben haben.
   - S3 BundleType und S3Key: Diese sind Teil des von Ihnen bereitgestellten WordPress Anwendungspakets.
   - VpcId: Die entsprechende VPC.

   a. Wählen Sie auf der Seite RFC erstellen die Kategorie Deployment, die Unterkategorie Applications, Item CodeDeploy Application und Operation Deploy aus der RFC CT-Auswahlliste aus.

   b. Behalten Sie die Standardoption Basic bei und legen Sie die Werte wie gezeigt fest.

   > **Note**
   >
   > Verweisen Sie auf die CodeDeploy Anwendung, die CodeDeploy Bereitstellungsgruppe, den S3-Bucket und das Paket, die zuvor erstellt wurden.

```
Subject:                          WP-CD-Deploy-RFC
Description:                      DeployWordPress
S3Bucket:                         BUCKET_NAME
S3Key:                            wordpress.zip
S3BundleType:                     zip
CodeDeployApplicationName:        WordPress
CodeDeployDeploymentGroupName:    WordPress
```

```
CodeDeployIgnoreApplicationStopFailures:  false
RevisionType:                             S3



VpcId:                                    VPC_ID
Name:                                     WP-CD-Deploy-Op
TimeoutInMinutes:                         60
```

c. Wenn Sie fertig sind, klicken Sie auf Senden.

Validieren Sie die Anwendungsbereitstellung

Navigieren Sie zum Endpunkt (LoadBalancerCName) des zuvor erstellten Load Balancers mit dem bereitgestellten Pfad:/. WordPress WordPress Beispiel:

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

Sie sollten eine Seite wie diese sehen:

Zerreißen Sie die Hochverfügbarkeitsbereitstellung

Um die Bereitstellung rückgängig zu machen, reichen Sie den Delete Stack CT für den HA Two-Tier Stack und den S3-Bucket ein und Sie können beantragen, dass RDS-Snapshots gelöscht werden (sie werden nach zehn Tagen automatisch gelöscht, kosten aber dort einen geringen Betrag). Stellen Sie den Stack IDs für den HA-Stack und den S3-Bucket zusammen und folgen Sie dann diesen Schritten. Siehe Stapel | Löschen.

Anhang: SALZ-Onboarding-Fragebogen

Themen

- Zusammenfassung der Bereitstellung
- Überlegungen zur Umgebungsarchitektur
- Benachrichtigungen zur Überwachung der Landezone mit einem Konto
- Wartungsfenster
- Nächste Schritte

Dies sind einige der Informationen, über die Sie nachdenken müssen, bevor Sie ein Konto einrichten.

Zusammenfassung der Bereitstellung

Eine Beschreibung der Bereitstellung. Beispiel:

- Dieses Konto ist für eine Line-of-Business Anwendungsbereitstellung (im Gegensatz zur Bereitstellung einer Produktanwendung) vorgesehen.
- Die Bereitstellung umfasst einen automatisch skalierten ARP (authentifizierter Reverse-Proxy) innerhalb des öffentlichen Subnetzes oder des DMZ-Subnetzes des Kontos.
- Web- und Anwendungsserver werden im privaten Subnetz des Kontos bereitgestellt.
- Eine RDS-Instance (Amazon Relational Database Service) wird ebenfalls im privaten Subnetz des Kontos bereitgestellt.
- Die Server (ARP, Web, Anwendung, Datenbank, Load Balancer usw.) sind in verschiedene Sicherheitsgruppen unterteilt.
- Für das Konto ist ein HA-Design (Hochverfügbarkeit) erforderlich, das auf mehrere Availability Zones (AZs) verteilt ist, d. h. „Multi-AZ“.

Überlegungen zur Umgebungsarchitektur

Berücksichtigen Sie bei der Entscheidung, wie Sie Ihre Umgebung und Architektur konfigurieren möchten, die folgenden Kriterien.

- Stellt Ihr virtuelles Rechenzentrum wieder eine Verbindung zu Ihrem Unternehmensnetzwerk her?
  - Haben Sie einen bestehenden AWS DirectConnect Service oder benötigen Sie einen neuen DirectConnect Service?
  - Haben Sie eine bestehende VPN-Verbindung oder benötigen Sie einen neuen VPN-Dienst?
- Was ist der verfügbare CIDR-Blockbereich interner Adressen, den Sie zuweisen könnten? (/16 empfohlen, darf sich nicht mit den Bereichen von Unternehmensnetzwerken überschneiden)
- Benötigt Ihr virtuelles Rechenzentrum Internetzugang?
- Welche Region (en) beabsichtigen Sie zu nutzen? (Sydney/N. Virginia/Dublin)
- Benötigen Sie ein Shared Services-Subnetz, um Anwendungen zu hosten, die Konnektivität zu allen anderen Subnetzen haben?
- In welchen Unternehmensbereichen möchten Sie als separate Subnetze gehostet werden? Für jeden:

  - Welche Konnektivität zu anderen Subnetzen benötigen Sie?
  - Benötigt das Subnetz Internetzugang?
  - Gibt es Einschränkungen bei der Anwendungsbereitstellung in diesem Subnetz?
  - Gibt es spezielle Netzwerkanforderungen für dieses Subnetz?
- Möchten Sie separate and/or Entwicklungstestumgebungen? (Wird ein Duplikat für gemeinsame Dienste enthalten, sodass Sie jederzeit darauf zugreifen können)
- Was sind Ihre Anforderungen an Snapshot-Backups?
- Haben Sie einen bestehenden Wartungsprozess oder ein oder mehrere Patchfenster, die Sie beibehalten möchten?
- Was sind Ihre Anforderungen an die Domainregistrierung?
- Haben Sie Single-Sign-On-Anforderungen? (z. B. AD, LDAP)
- Was sind Ihre erwarteten Gesamtbetriebssystem- und Kapazitätsanforderungen?

Benachrichtigungen zur Überwachung der Landezone mit einem Konto

AMS bietet Ihnen die Möglichkeit, sich bei bestimmten Überwachungswarnungen direkt benachrichtigen zu lassen (anstatt AMS-Servicebenachrichtigungen zu erhalten). Um sich dafür zu registrieren, stellen Sie sicher, dass Ihr Cloud Architect (CA) oder Cloud Service Delivery Manager (CSDM) die folgenden Informationen erhält:

E-Mail mit direkten Benachrichtigungen: Dies sind die E-Mail-Adressen, an die AMS bestimmte ressourcenbasierte Benachrichtigungen senden soll. Einzelheiten dazu, welche Benachrichtigungen direkt per E-Mail gesendet werden, finden Sie unter Alerts from Baseline Monitoring in AMS im AMS-Benutzerhandbuch für Single-Account-Landing Zone. Weitere Informationen zur AMS-Überwachung finden Sie unter Monitoring Management im AMS-Benutzerhandbuch für Single-Account Landing Zone.

Wartungsfenster

Sie sollten ein Wartungsfenster einrichten, das unterschiedliche Anwendungsanforderungen sowie unterschiedliche AWS-Regionen Belastungsperioden berücksichtigt. Ihr Wartungsfenster ist der Zeitpunkt, an dem AMS das Patching durchführt. Hier sind einige Richtlinien:

- Um die Auswirkungen auf die Benutzer zu begrenzen, sollten Sie Ihr Wartungsfenster entsprechend dem Ort planen AWS-Region , an dem Ihre Umgebungen bereitgestellt werden.

- Planen Sie ein Fenster außerhalb der regulären Geschäftszeiten und zu dem Zeitpunkt ein, zu dem der geringste Verkehr auf den Produktionsservern zu erwarten ist.
- In der Regel erfordern Infrastruktur-Stacks monatliche Updates.
- Planen Sie ein Wartungsfenster von mindestens 300 Minuten ein. Das Patchen von Betriebssystemen dauert 60 bis 90 Minuten, das Patchen von Infrastruktur-Stacks 180 bis 300 Minuten.

Nächste Schritte

Das AMS-Onboarding-Team unterstützt Sie bei jedem Schritt der Eingliederung Ihres Kontos bei AMS. Dies sind die Onboarding-Anforderungen:

- Stellen Sie eine neue AWS-Konto zur Verwendung für AMS bereit und geben Sie eine AWS-Konto ID an.
- Melden Sie sich für das gewünschte Support-Level an.
- Erstellen Sie eine kontoübergreifende IAM-Rolle, um dem AMS-Bereitstellungskonto Zugriff zu gewähren, und geben Sie AMS den Rollennamen.
- Fügen Sie das Konto 753102745277 als vertrauenswürdige Entität hinzu.

Anhang: ActiveDirectory Federation Services (ADFS) - Anspruchsregel und SAML-Einstellungen

Ausführliche step-by-step Anweisungen zur Installation und Konfiguration von AD FS finden Sie unter Enabling Federation to AWS Using Windows Active Directory, ADFS, and SAML 2.0.

Konfigurationen von ADFS-Anspruchsregeln

Wenn Sie bereits über eine ADFS-Implementierung verfügen, konfigurieren Sie Folgendes:

- Vertrauen der Parteien
- Regeln für Ansprüche

Die Schritte zur Vertrauens- und Anspruchsregeln der vertrauenden Partei werden vom Blog Enabling Federation bis AWS Using Windows Active Directory, AD FS und SAML 2.0 durchgeführt

- Regeln für Ansprüche:
  - Nameid: Konfiguration pro Blogbeitrag
  - RoleSessionName: Konfigurieren Sie wie folgt
    - Name der Regel beanspruchen: **`RoleSessionName`**
    - Attributspeicher: **`Active Directory`**
    - LDAP-Attribut: **`SAM-Account-Name`**
    - Art des ausgehenden Anspruchs: **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`**
    - AD-Gruppen abrufen: Konfiguration pro Blogbeitrag
    - Rollenanspruch: Konfigurieren Sie wie folgt

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^d]{12})-"]
```

```
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
 RegExReplace(c.Value, "AWS-([^d]{12})-", "arn:aws:iam::$1:saml-provider/
customer-readonly-saml,arn:aws:iam::$1:role/"));
```

Web-Konsole

Sie können auf die AWS-Webkonsole zugreifen, indem Sie den Link unten verwenden und ihn *[ADFS-FQDN]* durch den FQDN Ihrer ADFS-Implementierung ersetzen.

https:///*[ADFS-FQDN]*.aspx adfs/ls/IdpInitiatedSignOn

Ihre IT-Abteilung kann den oben genannten Link über eine Gruppenrichtlinie für die Benutzerpopulation bereitstellen.

API- und CLI-Zugriff mit SAML

So konfigurieren Sie den API- und CLI-Zugriff mit SAML.

Die Python-Pakete stammen aus den folgenden Blogbeiträgen:

- NTLM: So implementieren Sie föderierten API- und CLI-Zugriff mit SAML 2.0 und AD FS
- Formulare: So implementieren Sie eine allgemeine Lösung für den API/CLI Verbundzugriff mithilfe von SAML 2.0
- PowerShell: So richten Sie den föderierten API-Zugriff auf AWS mithilfe von Windows ein PowerShell

Skript-Konfiguration

1. Ändern Sie mit Notepad++ die Standardregion in die richtige Region
2. Deaktivieren Sie mit Notepad++ die SSL-Überprüfung für Test- und Entwicklungsumgebungen
3. Konfigurieren Sie mit Notepad++ idpentryurl

```
https://[ADFS-FDQN]/adfs/ls/IdpInitiatedSignOn.aspx?
loginToRp=urn:amazon:webservices
```

Windows-Konfiguration

Die folgenden Anweisungen gelten für die Python-Pakete. Die generierten Anmeldeinformationen sind 1 Stunde gültig.

1. Downloaden und installieren Sie Python (2.7.11)

2. Laden Sie die AWS-CLI-Tools herunter und installieren Sie sie
3. Installieren Sie die AMS-CLI:

   a. Laden Sie die ZIP-Datei für AMS-Distributionsdateien herunter, die Sie von Ihrem Cloud Service Delivery Manager (CSDM) erhalten haben, und entpacken Sie sie.

      Es werden mehrere Verzeichnisse und Dateien zur Verfügung gestellt.

   b. Öffnen Sie je nach Betriebssystem entweder das Verzeichnis Managed Cloud Distributables -> CLI -> Windows oder das Verzeichnis Managed Cloud Distributables -> CLI -> Linux/ macOS und:

      Führen Sie für Windows das entsprechende Installationsprogramm aus (diese Methode funktioniert nur auf Windows 32- oder 64-Bit-Systemen):

      - 32 Bit: ManagedCloud API_x86.msi
      - 64 Bit: ManagedCloud API_x64.msi

      Führen Sie für Mac/Linux die Datei mit dem Namen MC_CLI.sh aus. Sie können dies tun, indem Sie diesen Befehl ausführen:. `sh MC_CLI.sh` Beachten Sie, dass sich die Verzeichnisse amscm und amsskms sowie ihr Inhalt im selben Verzeichnis wie die Datei MC_CLI.sh befinden müssen.

   c. Wenn Ihre Unternehmensanmeldedaten über den Verbund mit AWS (die AMS-Standardkonfiguration) verwendet werden, müssen Sie ein Tool zur Verwaltung von Anmeldeinformationen installieren, das auf Ihren Verbundservice zugreifen kann. Sie können beispielsweise diesen AWS-Sicherheitsblog How to Implementation Federated API and CLI Access Using SAML 2.0 and AD FS verwenden, um Hilfe bei der Konfiguration Ihrer Tools zur Verwaltung Ihrer Anmeldeinformationen zu erhalten.

   d. Führen Sie nach der Installation die Befehle und Optionen aus `aws amscm help` und sehen Sie `aws amsskms help` sich diese an.

4. Laden Sie das erforderliche SAML-Skript herunter

   Laden Sie es auf c:\aws\scripts herunter

5. Laden Sie PIP herunter

   Laden Sie es auf c:\aws\downloads herunter

6. Verwenden PowerShell und installieren Sie PIP

<pythondir>. \ python.exe c:\aws\downloads\get -pip.py

7. Verwenden PowerShell und installieren Sie das Boto-Modul

   <pythondir\ scripts>Verwenden, installieren Sie das Boto-Modul ----sep----pip install boto

8. Verwenden Sie das Modul PowerShell Anfragen und installieren Sie es

   <pythondir\ scripts>Verwenden des Moduls für Anfragen installieren ----sep----pip install requests

9. Verwenden PowerShell und installieren Sie das Sicherheitsmodul Anfragen

   <pythondir\ scripts>Verwenden des Sicherheitsmoduls install requests ----sep----pip install requests [security]

10. Verwenden PowerShell und installieren Sie das BeautifulSoup-Modul

    <pythondir\ scripts>Verwenden Sie das Modul beautifulsoup ----sep----pip install beautifulsoup4

11. Erstellen Sie mit Hilfe PowerShell eines Ordners namens .aws im Benutzerprofil (%userprofile% \ .aws)

    mkdir .aws

12. Erstellen Sie mit PowerShell, eine Datei mit Anmeldeinformationen im Ordner „.aws“

    Anmeldeinformationen für ein neues Objekt — Typ Datei —Force

    Die Anmeldeinformationsdatei darf keine Dateierweiterung haben

    Der Dateiname muss ausschließlich in Kleinbuchstaben geschrieben sein und die Anmeldeinformationen enthalten

13. Öffnen Sie die Anmeldeinformationsdatei mit Notepad und fügen Sie die folgenden Daten ein, wobei Sie die richtige Region angeben

    ```
    [default]
    output = json
    region = us-east-1
    aws_access_key_id =
    aws_secret_access_key =
    ```

14. Verwenden PowerShell des SAML-Skripts und der Anmeldung

    <pythondir>. \ python.exe c:\aws\scripts\samlapi.py

Benutzername: [BENUTZERNAME] @upn

Wählen Sie die Rolle, die Sie übernehmen möchten

Linux-Konfiguration

Die generierten Anmeldeinformationen sind 1 Stunde gültig.

1. Übertragen Sie das SAML-Skript mit WinSCP
2. Übertragen Sie das Root-CA-Zertifikat mit WinSCP (ignorieren Sie es für Test und Entwicklung)
3. Fügen Sie die ROOT-CA zu den vertrauenswürdigen Root-Zertifikaten hinzu (ignorieren Sie sie für Test und Entwicklung)

   $ openssl x509 -inform der -in [certname] .cer -out certificate.pem (für Test und Entwicklung ignorieren)

   Fügt den Inhalt von certificate.pem am Ende der Datei/-bundle.crt hinzu (bei Test-Entwicklung ignorieren) etc/ssl/certs/ca
4. Erstellen Sie den Ordner.aws unter home/ec2-user 5

   ```
   [default]
   output = json
   region = us-east-1
   aws_access_key_id =
   aws_secret_access_key =
   ```
5. Übertragen Sie die Anmeldeinformationsdatei mithilfe von WinSCP in den Ordner.aws
6. Installieren Sie das Boto-Modul

   $ sudo pip installiere Boto
7. Installieren Sie das Modul Anfragen

   $ sudo pip Installationsanfragen
8. Installieren Sie das BeautifulSoup-Modul

   $ sudo pip installiere beautifulsoup4
9. Kopieren Sie das Skript nach home/ec2-user

Stellen Sie die erforderlichen Berechtigungen ein

Führen Sie das Skript aus: samlapi.py

Dokumentverlauf

In der folgenden Tabelle werden die wichtigen Änderungen an der Dokumentation seit der letzten Version von AMS beschrieben.

- API-Version: 2019-05-21
- Letzte Aktualisierung der Dokumentation: 23. September 2025

Änderungen	Beschreibung	Datum
Aktualisierter Änderungstyp für die automatische Skalierung von Endpunkten in SageMaker KI im Abschnitt Häufig gestellte Fragen zu AWS Managed Services	Verwenden Sie AMS SSP, um Amazon SageMaker AI in Ihrem AMS-Konto bereitzustellen. Senden Sie einen RFC mit Management | Erweiterte Stack-Komponenten | Identity and Access Management (IAM) | Entität oder Richtlinie aktualisieren (Überprüfung erforderlich), Änderungstyp (ct-27tuth19k52b4), um Autoscaling-Berechtigungen vorübergehend oder dauerhaft zu erhöhen, da Autoscaling einen permissiven Zugriff auf den Service erfordert. CloudWatch	25. September 2025
Präzise Referenzen zum Änderungstyp	Sicherheitsgruppen erstellen, ändern oder löschen. Um einen Benutzer hinzuzufügen: Senden Sie einen RFC mit Management | Directory Service | Benutzer und Gruppen | Benutzer zur Gruppe hinzufügen [ct-24pi85mjtza8k] und Um einen Benutzer zu entfernen: Senden Sie einen RFC mit Management | Directory Service | Benutzer und Gruppen | Benutzer aus Gruppe entfernen [ct-2019s9y3nfml4]	08. August 2025

Änderungen	Beschreibung	Datum
Der Link zum Inhaltsverzeichnis wurde entfernt	Der Link zum AWS Inhaltsverzeichnis-Glossar wurde entfernt.	08. August 2025
Link für Anleitungen zur Verschreibung hinzugefügt	Konsolidierte Abrechnung einrichten — neues Konto mit Zahlerkonto verknüpfen.	08. Mai 2025
Aktualisierte Anweisungen zur Aktivierung des IAM-Zugriffs auf AWS Management Console	Die Anweisungen zur Aktivierung des IAM-Zugriffs auf den wurden klargestellt. AWS Management Console	Aktivieren Sie den IAM-Zugriff auf die Konsole AWS
Die Anzahl der zulässigen virtuellen Transitschnittstellen auf dedizierten Direct Connect-Verbindungen wurde aktualisiert	Dedizierte Direct Connect-Verbindungen haben jetzt ein Limit von 4 virtuellen Transitschnittstellen pro Verbindung	Direct Connect mit Transit Gateway verbinden
Verbessern Sie den Wortlaut.	Es wurde angegeben, dass „nur als Ablehnungsliste verwendet“ auch „Alle zulassen“ enthalten muss, um die Überwachung und Verwaltung von AMS sicherzustellen.	Netzwerkkonfiguration
Zusätzliche Informationen zur Verwendung der AMS-CLI.	„Hinweis hinzugefügt, dass die `--region` Option möglicherweise für einige CLI-Befehle benötigt wird“	Installieren Sie das AMS CLIs
Aktualisiert: Die Kapitelüberschriften wurden aus Gründen der Konsistenz und Lesbarkeit überarbeitet. Einige Unterbereiche wurden in passendere Abschnitte verschoben	„Modi für das Änderungsmanagement“ ist die neue Überschrift für „Änderungsmanagement“	Verwaltungsmodi ändern

Änderungen	Beschreibung	Datum
Aktualisierter Inhalt	Der AMS-Modus, der früher als „Change Management-Modus“ oder „Standard-CM-Modus“ bekannt war, ist jetzt als „RFC-Modus“ bekannt. Der Bereich Modi wurde erweitert.	RFC-Modus.
Aktualisierter Inhalt	Der AMS-Modus, der früher als „Change Management-Modus“ oder „Standard-CM-Modus“ bekannt war, ist jetzt als „RFC-Modu s“ bekannt. Der Abschnitt mit den Modi wurde gekürzt und Links zu den Abschnitten des AMS Advanced User Guide zu Modi hinzugefügt.	AMS-Modi.
MALZ: Das Diagramm der Netzwerkarchitektur wurde aktualisiert	Architektur von Netzwerkkontenm	16. Juni 2022
Die Themenliste wurde unter die ersten Absätze verschobe n	Einführung in das Onboarding von AWS Managed Services	16. Juni 2022
Aktualisierter Inhalt, inklusive Sprachinitiative	„Verwaltungskonto“ nicht „Hauptkonto“.	IAM-Benut zerrolle in AMS , Abschnitt „Beispiele für Richtlinien“
Aktualisierter Inhalt, Namen der Tools-Kontorollen	Der Rollenname wurde CustomerMigrationA ccessRole auf aktualisiert AWSManage dServicesMigrationRole.	AWS Service zur Anwendung smigration (AWS MGN)
SALZ: Standardwerte für das Kontinuitätsmanagement	Link aktualisiert und veraltete Informationen entfernt von VPC-Tag und Standardeinstellun gen	28. Februar 2022

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.